NETKOM 4.0

Netcompetence For A Digitized Working World 4.0

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

Fagskolen i Viken

Dette prosjektet har mottatt finansiering fra Den europeiske union sitt Erasmus+ program under registreringsnummer 2020-1-DE02-KA202-007393. Dette dokumentet reflekterer kun forfatterens synspunkt, og Kommisjonen er ikke ansvarlig for eventuell bruk som kan gjøres av informasjonen den inneholder.

Dette prosjektet har mottatt finansiering fra Den europeiske union sitt Erasmus+ program under registreringsnummer 2020-1-DE02-KA202-007393. Dette dokumentet reflekterer kun forfatterens synspunkt, og Kommisjonen er ikke ansvarlig for eventuell bruk som kan gjøres av informasjonen den inneholder.

Intellectual Outcome O5

Produksjonsplanlegging og produksjonskontroll i komplekse og autentiske Industry 4.0 miljøer

Dette dokumentet inneholder et resultat fra NetKOM_4.0_v2-prosjektet.

Det ble opprettet av Fagskolen i Viken, Norge.

Bidragsytere: Tommy Hvidsten (redaktør), Endre Jamtveit, Hjörtur D. Jonsson, Rasmus Trovåg, Helene Mallasvik, Andreas S. Hernandez og Emil Moholth.

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

Kurs / Læreplan - Pilotkurs / moduler

Dette prosjektet har mottatt finansiering fra Den europeiske union sitt Erasmus+ program under registreringsnummer 2020-1-DE02-KA202-007393. Dette dokumentet reflekterer kun forfatterens synspunkt, og Kommisjonen er ikke ansvarlig for eventuell bruk som kan gjøres av informasjonen den inneholder.

Generell informasjon om NetKom_4.0_v.2 prosjektet

Prosjekttittel:	Network competence for a digitalised working world 4.0 v.2
Forkortelse:	NetKom_4.0_v.2
Referansenummer:	2020-1-DE02-KA202-007393
Start:	01.11.2020
Slutt:	31.08.2023
Partnere:	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
Koordinator:	European University Flensburg

Content

1. En introduksjon til Industri 4.0

By Tommy Hvidsten

Industri 1.0

For å illustrere den industrielle utviklingen frem til Industri 4.0, vil vi begynne med utviklingen av Kongsbergs sølvgruver, grunnen til at byen ble til. Vi vil også kort se på livet til Tinius Olsen, en innovatør og industriell entreprenør som grunnla Tinius Olsen Testing Machine-selskapet. Han ble født i Kongsberg i 1845 og bidro med midler til etableringen av teknisk utdanning i Kongsberg gjennom sitt testamente. Til slutt førte hans initiativ til etableringen av Fagskolen Tinius Olsen, som var en viktig del da Viken fagskole ble etablert gjennom en sammenslåing med andre skoler i 2020.

Figur 1: Tinius Olsens barndomshjem i Kongsberg, hvor han ble født i 1845..

Vårt startpunkt er Tinius Olsens barndomshjem, og det er grunner til det:

- Tinius Olsen har vært knyttet til teknisk utdanning i Kongsberg de siste 70 årene.
- Han dro til USA etter å ha fullført sin tekniske utdannelse og startet en fabrikk for materialetesting.
- På slutten av livet kom han tilbake til Kongsberg og donerte penger til en teknisk skole.
- Dette er grunnen til etableringen av en teknisk høyskole i Kongsberg. Vikens forgjenger, Fagskolen Tinius Olsen, ble oppkalt etter ham.
- Den andre grunnen er at Tinius' far var en våpenmaker ved Kongsberg Våpenfabrikk (KV, Kongsberg Arms Factory).
- Han utførte sitt arbeid hjemme.
- Han arbeidet i bakgården og lagde kolber for forgjengerne til Krag-Jørgensen-riflen som en oppgave fra KV. Tinius pleide å hjelpe ham da han var ung gutt.

Denne måten å utføre industrielt arbeid hjemme på er forløperen til Industri 1.0. På engelsk kalles det en "cottage industry," på norsk kalles det "forlagssystemet." Hvis du tenker på forlagsbransjen, vil du forstå hvorfor. De fleste bøker ble skrevet hjemme, men et selskap publiserte dem og solgte produktene som ble laget hjemme. Dette er et eksempel på hvordan industrien fungerte rett før og etter den første industrielle revolusjonen. I Kongsberg var de flere år bak. Å drive sitt eget håndverk hjemmefra var en måte å tjene på livets opphold på den tiden.

Figur 1: Detaljer fra de gamle mekaniske verkstedene ved Kongsbergs sølvgruver:

Nå flytter vi scenen til de gamle mekaniske verkstedene ved sølvgruvene i Kongsberg. Dette er et fantastisk sted å studere Industri 1.0, eller den første industrielle revolusjonen. Den ble symbolisert av maskinen kalt Spinning Jenny. Den ble utviklet i England, og den gjorde det mulig å spinne flere tråder samtidig. Denne maskinen ble et eksempel på masseproduksjon, eller produksjon som var mekanisert.

De laget maskiner for å utføre arbeid som tidligere ble gjort manuelt av mennesker. Dette skjedde på begynnelsen av 1700-tallet. Sølvgruvene var i drift, men jeg er ikke sikker på om det så slik ut der. Det var ikke bare Spinning Jenny som førte til vekst i industrien. Andre oppfinnelser bidro også til denne veksten.

Det var også endringer i samfunnet. Innføringen av jernbaner og dampmaskinen var viktige faktorer i denne utviklingen. I dette verkstedet ble kraften distribuert til maskinene ved hjelp av store aksler. Den ble deretter transportert ned til maskinene via flate remmer. Maskinene kunne kobles sammen ved å stramme remmene. Alt ble mest sannsynlig drevet av vannkraft.

Like over verkstedet er det en gruvegang. Gruvegangen drenerer vannet ut av gruveområdet. Vannet ble ført rundt dette bygget, og det var mest sannsynlig et vannhjul på den nedre siden av det. Kraften fra vannhjulet ble ført inn via en reim som drev alle maskinene. Dette er et eksempel på tidlig industrialisering.

Dette betydde også at fabrikker ble bygget. I stedet for å jobbe hjemme, samlet folk seg i fabrikker, og oppgavene ble delt mellom dem. Arbeid på denne måten var mer effektivt. Å være "på jobb" ble det nye begrepet for organisering av arbeid. Fabrikker ble ofte plassert ved siden av en vannvei. Hvis du går langs Akerselva i Oslo, kan du se at det tidligere var mange industrielle selskaper som brukte elva som strømforsyning.

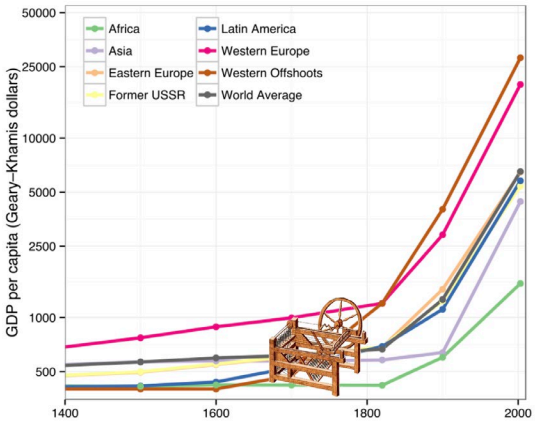
Den første dampmaskinen som fungerte skikkelig, kom ikke før den første industrielle revolusjonen hadde vært i gang i noen år. Da trengte vi ikke lenger å stole på vannveier, og fabrikker kunne plasseres hvor som helst. I England brukte de kull for å drive den; i Norge brukte vi både kull og tre. Dampmaskinene ble brukt til å produsere kraft som ble brukt i fabrikkene.

I verkstedet har vi også et snev av Industri 2.0. Dette verkstedet var i drift frem til sølvgruvene ble stengt rundt 1950. Nå er det elektriske motorer. Dette fenomenet oppstod tidlig på 1900-tallet og var en del av den andre industrielle revolusjonen. Dette verkstedet har blitt oppgradert fra Industri 1.0 til Industri 2.0 når det gjelder energi. Dette er et godt eksempel på hvordan bedrifter og industrien så ut tidlig i industrialiseringen.

Nå skal vi se på industriell utvikling i sammenheng. Kurven i figuren nedenfor viser hvordan inntekten per innbygger i den vestlige verden har utviklet seg fra år 1400 og frem til i dag. Kurven bøyer bratt seg når vi kommer inn i 1700- og 1800-tallet. Det er det vi kaller den første industrielle revolusjonen.

Det som har blitt symbolet på den første industrielle revolusjonen, var en maskin kalt Spinning Jenny. Den gjorde det mulig å spinne flere tråder samtidig. Det var den første maskinen som begynte å industrialisere og automatisere håndverk. Arbeid som tidligere ble utført hjemme og på gårder, kunne nå gjøres med en maskin.

Men det var ikke bare denne maskinen som utløste den første industrielle revolusjonen. Dampmaskinen kom, og vi var ikke lenger avhengige av vann som strømforsyning. En fabrikk kunne nå



plasseres hvor som helst.

Figur 2: Bruttonasjonalprodukt (BNP) per innbygger gjennom århundrene. "Spinning Jenny" er plassert der den industrielle revolusjonen begynte.

Fabrikker var også et nytt fenomen som fremmet den første industrielle revolusjonen.

Figur 3: Dampmaskinen ga fart til den industrielle revolusjonen. (Bilde av Ivan Tsaregorodtsev på Unsplash)

Dette bildet viser en dampmaskin. Den ble satt i drift mot slutten av den 1700s. James Watt oppfant en regulator som gjorde at dampmaskinen kunne arbeide med

konstant hastighet uavhengig av belastningen på den. Dette var en stor oppfinnelse på den tiden. Dette førte til økt produktivitet. Omsetningen i kroner eller dollar per innbygger økte dramatisk. Dette ble en industriell revolusjon.

Begrepet mekanisering brukes også om denne epoken. Fysikken som Newton samlet og utviklet på 1600-tallet, ble brukt i industrien. Mekanikk ble brukt til å produsere varer som igjen skapte arbeidsplasser. Når folk fikk arbeidsplasser, tjente de penger til å foreta kjøp. Denne selvforsterkende effekten førte til at markedet vokste, og antall arbeidsplasser og økonomien økte raskt. Kurven viser denne fortsatte veksten. Vi kan se flere bruddpunkter der veksten øker enda mer.

Vi har snakket om industrialisering og utvikling, men i dag kan vi også snakke om den andre industrielle revolusjonen og den tredje industrielle revolusjonen. Industri 4.0 er den fjerde.

Hvorvidt det vil være en revolusjon eller ikke, vet vi ikke sikkert. Digitaliseringen vil øke veksten enda mer i industrien.

Industri 2.0

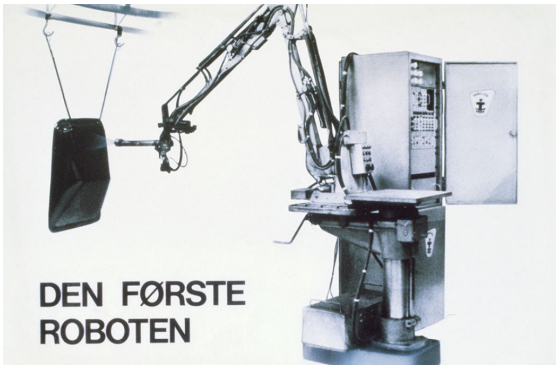
Den andre industrielle revolusjonen var resultatet av flere faktorer. Organisatoriske endringer var en viktig faktor. En mann ved navn Taylor oppdaget at når du laster korn inn i en togvogn, ville det være bedre hvis én person bar sekken til toget, en annen løftet sekken ombord på toget, og en tredje plasserte sekken. Da ville toget bli lastet raskere enn om bare én person bar sekken hele veien.

Arbeidet hadde blitt delt. Dette økte produktiviteten. Alt dette ledet til Henry Fords produksjonslinje. Han var den første som systematiserte dette i industrien og startet masseproduksjon. I dette tilfellet gjaldt det biler. Denne produksjonsformen har blitt kopiert og er fortsatt i bruk i dag.

Når du produserer noe på en produksjonslinje, er arbeidet delt slik at én person bare gjør én liten ting. Etter at personen er ferdig, beveger produktet seg videre, og noen andre gjør neste del. Dette førte til fortsatt vekst, og produktiviteten økte. Det mest åpenbare eksempelet på dette kommer fra andre verdenskrig da den amerikanske industrien økte, og masseproduksjonen av krigsutstyr startet. Produktiviteten de klarte å oppnå var enorm. Det var også fordi arbeiderne var sterkt motivert for å bidra til produksjonen, og det var organisert slik at man kunne komme inn og være produktiv uten å ha mange ferdigheter innenfor et bestemt felt. Det er en viktig del av dette. Dette var den andre industrielle revolusjonen.

Industri3.0

Vi hadde også en tredje industriell revolusjon på 1960- og 1970-tallet. Dette



ble forårsaket av innføringen av datakontroll i industrien.

Figur 4: Norges første industrielle robot utviklet av Trallfa på Bryne. (Bilde med tillatelse fra Trallfa)

Som et eksempel, dette er den første industrielle roboten. Den på bildet ble utviklet på Bryne, Jæren, av selskapet Trallfa. En maler kunne kontrollere roboten ved å utføre bevegelsene som kreves for å

male et produkt. Deretter kopierte roboten disse bevegelsene.

Vi kan se mer av dette i USA og bilindustrien. De begynte å bruke datateknologi tidlig. Utfordringen for dem oppstod når de måtte bytte fra én bilmodell til en annen. Henry Ford, under den første industrielle revolusjonen, sa at du kan få hvilken som helst bil du vil, så lenge det er en Model T og den er svart. Det var ingen andre modeller, men markedet ønsket å ha et bredere utvalg av biler. De måtte endre produksjonen for å introdusere nye bilmodeller. Kontrollene på de gamle produksjonslinjene var elektromekaniske. De var hovedsakelig reléer som fungerte som automasjons-systemer for produksjonslinjene.

Når datamaskiner kom, kunne de reprogrammeres ganske enkelt. I stedet for å bygge nye automatiseringsbokser for produksjonslinjen for å produsere en ny modell, kunne de reprogrammeres. Dette var da de første PLC-ene (programmerbare logiske kontrollere) kom på 1960-tallet. Dette var starten eller en av elementene i det vi kaller den tredje industrielle revolusjonen.

Numerisk styrte maskiner, som maskinverktøy, ble utviklet rundt 1950. De hadde vært tilgjengelige en stund. Industriell ingeniørvitenskap var ganske vanlig.

Toyota brukte amerikanske prinsipper, og produksjonen deres var i henhold til lean-prinsippene. Dette økte også produktiviteten. Og selvfølgelig de første PLC-ene og robotene. Dataassistert konstruksjon og produksjon ble introdusert i den tredje industrielle revolusjonen.

Vi skal ta en liten digresjon ... en av de første tredimensjonale CAD-verktøyene, et verktøy for å tegne maskinkomponenter, ble utviklet i Kongsberg av Kongsberg Våpenfabrikk. Det eksisterte ikke lenge, men det var en start. De var ikke store nok til å bryte gjennom og ta over AutoCAD og de andre store verktøyene som kom samtidig.

Industri 4.0

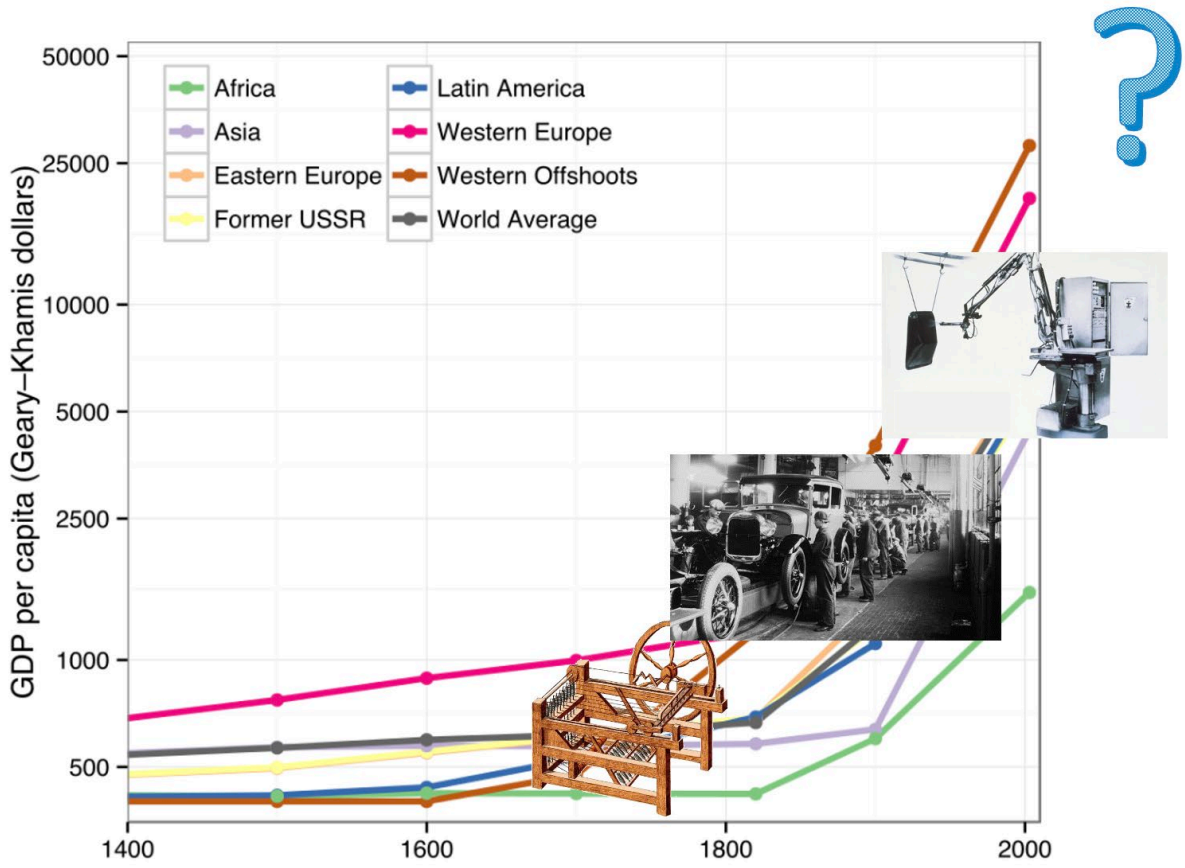
Vi tror at siden datanettverk nå er en stor del av industrien og gjør produksjonsutstyr i stand til å kommunisere med hverandre, og det er mulig å bruke dataintegrering i produksjon, kan dette føre til vekst i produktivitet som ligner resultatene av de tidligere industrielle revolusjonene.

Dette er ideen bak det forestilte Industri 4.0. Datanettverk og -kommunikasjon driver dette. Det er mange måter dette kan brukes på. Nye applikasjoner dukker opp omtrent hver annen dag. Datakommunikasjon er grunnlaget for det vi tror vil være den fjerde revolusjonen.

Med maskiner som samarbeider, og ikke bare i én fabrikk. Maskiner i én fabrikk kan kommunisere med maskiner i en annen fabrikk.

Det vil være mye mer autonomi i produksjonssystemene. Og fleksibilitet også. Det vil være lettere å tilpasse seg det kunden trenger.

Vi diskuterte tidligere Ford's Model T og fargen svart. I dag er det mulig å velge ganske mye mellom alternativene når du



Figur 5: En oversikt over de industrielle revolusjonene viser mekanisering i den første, masseproduksjon i den andre, og automatisering i den tredje. Digitalisering er den drivende kraften i den fjerde industrielle revolusjonen.

bestiller en bil. Du vil få enda flere valg i fremtiden enn det du har nå.

Digitalisering er et bredt begrep som også inkluderer elementer fra den tredje revolusjonen.

Vi håndterer kommunikasjon og behandlingen av et stort antall datasett. Dette er den fjerde revolusjonen. I denne kurset vil vi diskutere noen av disse teknologiene og bruken av teknologi i industrien.

Noen eksempler på effekten vi ser i dag fra Industri 4.0:

Kvalitetskontroll utført av big data. Du har mye data samlet inn av sensorer i produksjonen. De kan analyseres, kanskje automatisk, og avdekke kvalitetsfeil og produktfeil.

Robotassistert produksjon... Vi har hatt roboter i lang tid. Det som er nytt, er at Roboter til en større grad kan samarbeide med mennesker og arbeide sammen med mennesker på en måte som er trygg og sikker, men som øker menneskers produktivitet. Det er nytt. På Teknologiparken i Kongsberg kaller de det "robotisk assistanse."

Autonome kjøretøy i logistikksystemer. Flere autonome transportløsninger. Det er ikke bare Google og Tesla som jobber med disse tingene. Du kan også finne det i produksjon. Vi skal se hvordan det fungerer og kan brukes.

Simulering er viktig. Vi har kraftigere simuleringsverktøy. Før man bygger en fabrikk, kan vi simulere den i detalj og finne hvor vanskelighetene vil oppstå. Hvordan kan vi bygge fabrikken for å gjøre

produksjonen mest effektiv og fleksibel? Du har en datamodell som er en kopi av det som blir produsert. Den simulerer også slitasje i produksjonen. Dette er hvordan du kan finne feil eller mulige feil før de oppstår. En modell kan testes mer robust enn du ville kunne teste en fabrikk for å provosere feil på et tidligere stadium.

Smarte forsyningsnettverk. På grunn av nettverksteknologi kan maskiner på en måte kommunisere med leverandører. Du kan også ha automatiserte markedssteder. Hvis du trenger råvarer et sted i produksjonen, kan produksjonscellen gå inn på markedet og kjøpe råvarer blant godkjente leverandører med riktig pris og leveringsbetingelser uten at mennesker er involvert.

Prediktivt vedlikehold der du kan forutse feil. Industri 4.0 gjør det mulig. Stor data og datakommunikasjon, sammenstillinger. Overvåking og analyse. Analyse av data sammenstilling. Da kan du forutse feilen før den skjer, og du kan planlegge vedlikeholdsarbeid bedre.

Du kan planlegge slik at produksjonen holdes i gang så kontinuerlig som mulig. Et eksempel på en maskin som tilbyr en tjeneste er når en leverandør, i stedet for å selge et maskinverktøy, selger en produksjonstjeneste. Plasserer maskinen i dine lokaler og er ansvarlig for drift og vedlikehold. Som produsent kjøper du en tjeneste. Du betaler hver måned for tjenesten, og det er opp til leverandøren å sørge for at den fungerer.

Noen ganger kan det være lønnsomt å eie en dyr maskin som du ikke trenger etterpå. Dette kan redusere behovet for midler når du prøver å bygge opp et selskap.

Selvorganiserende produksjon. Maskiner kan automatisk koordinere med hverandre. Dette optimaliserer driften, slik at kostnadene er lavere og volumene er høyere. Det er en av tingene vi ser.

Additiv produksjon er en ny måte å produsere på. 3D-utskrift er et typisk eksempel. Du legger til materialer i stedet for å fjerne dem. Når du former ting, fjerner du materiale. I en 3D-skriver er det motsatt. Du legger til materiale der det er nødvendig. Vi ser det ofte i prototyper, men stadig flere produksjonsmaskiner er bygd på denne måten. Vi har eksempler i Norge på 3D-utskrift i titan. Flere selskaper jobber med det.

Et siste eksempel er utvidet virkelighet (AR). Det kan gi mennesker en ny måte å oppfatte informasjon på som kan hjelpe i noen situasjoner. For eksempel vedlikehold. Du kan ta på deg 3D-briller og mens du utfører vedlikeholdsarbeid, kan du se informasjonen du trenger. Du kan se hvor delene er plassert. Du kan også få informasjon om hvordan de fungerer og deres tilstand. I stedet for å løpe rundt med brukerhåndbøker eller måtte lese en hel haug med dem, kan du få informasjonen du trenger når du trenger den.

Et annet eksempel kan være monteringsprosesser der store ting skal monteres. AR-teknologien kan vise deg hvor modulene hører hjemme og hvordan de skal monteres. Det er mange bruksområder. Vi har bare sett begynnelsen.

Her er et siste eksempel som er litt morsomt. En av konsekvensene av Industri 4.0 er at forbrukeren har mer makt. Vi kan bestemme hvordan vi vil ha ting. NIKE joggesko kan bestilles online. Du kan designe dine egne joggesko, bestemme

farger og design. Dekorasjon, hvilken type såler og hvilken type merking.

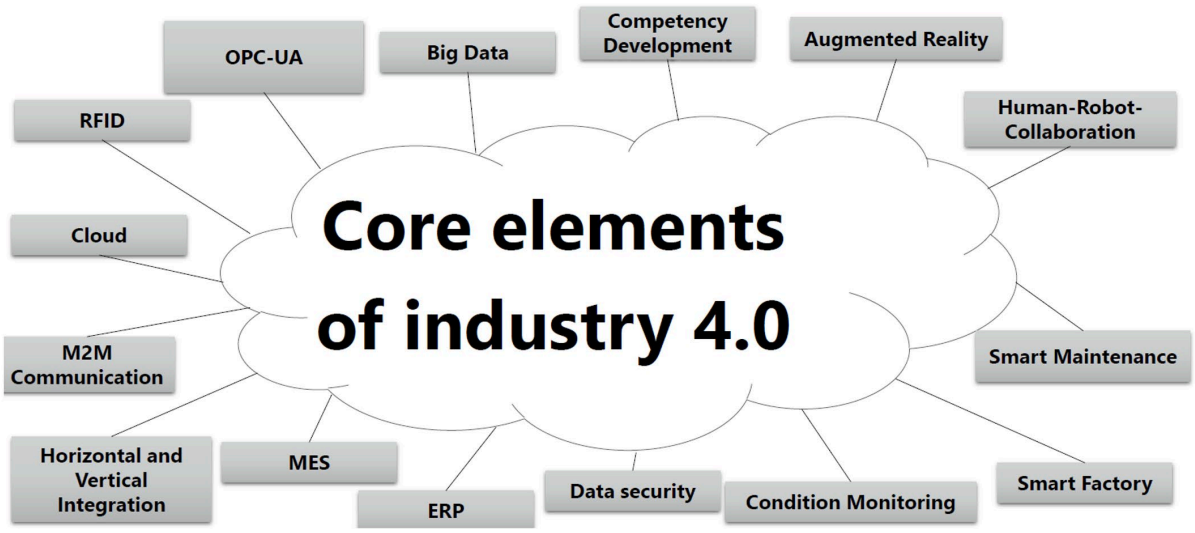
Vi har bestilt sko med teksten "Tinius ID lab" på siden og "FTO" på hælen. Du betaler samme beløp som om du hadde kjøpt dem i en butikk. Det er en viss leveringstid, omtrent en måned på denne. Du kan kjøpe joggesko med ditt eget navn på dem.

Dette er Industri 4.0 plassert i en historisk sammenheng. Vi vil se om vi kan vise enda flere aspekter senere og utløse noen ideer om hvordan dette kan brukes.

Figur 6: NIKE Joggesko med merket "Fagskolen Tinius Olsen" (Vikens forgjenger).

2. Teknologiske pådrivere for Industri 4.0

By Tommy Hvidsten



Figur 7: Mange teknologier som samarbeider driver Industri 4.0 (grafikk med tillatelse fra FESTO).

La oss nå studere de teknologiske pådriverne bak Industri 4.0. Mange teknologier samarbeider, noe som til sammen utgjør det vi kaller Industri 4.0.

Skyen gir en oversikt over relevante teknologier. Vi utdyper noen av disse overskriftene. I andre deler av kurset vil vi undersøke mange av disse teknologiene nærmere. Men Industri 4.0 handler også om organisatoriske endringer, ulike tilnærminger til oppgaver som bidrar til effekten. Ofte forårsaker teknologi disse organisatoriske endringene.

RFID

Den første, RFID, betraktes ofte som en av de viktigste teknologiene i begynnelsen av Industri 4.0. RFID står for radiofrekvensidentifikasjon. Det er en metode for å merke gjenstander, slik at du kan lokalisere dem. Men disse RFID-brikkene kan også lagre data. Et typisk eksempel er å feste RFID-brikker til klær i butikker, og en alarm vil lyde når brikkene passerer gjennom døren.

De kan også inneholde prisinformasjon og erstatte strekkoder. Inngangskort kan ha RFID-brikker, eller bankerens kort. Kontaktløs betaling er en RFID-funksjon. En brikke i kortet kommuniserer med dataleseren.

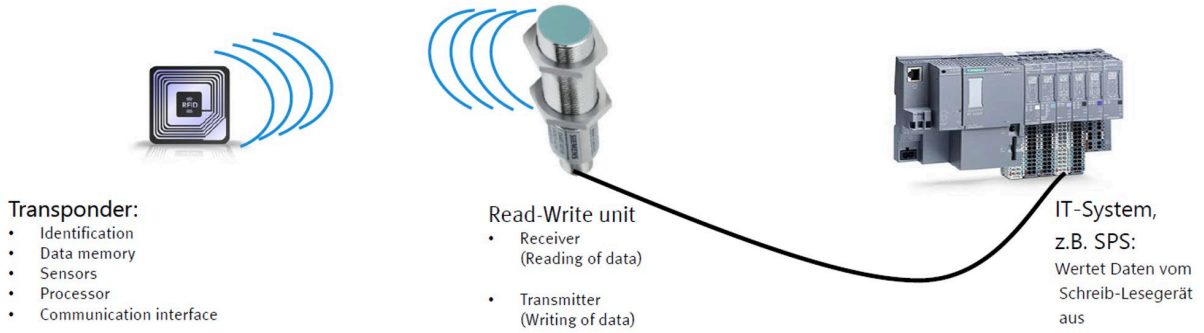
Figur 8: Dette er en RFID-brikke, og mønsteret rundt den er antennen (grafikk med tillatelse fra FESTO).

kan den kommunisere med datamaskinen i den andre enden, som PLCen som vises her.

Big data

Big data er en viktig term i Industri 4.0. Big data betyr egentlig store, ustrukturerte mengder data som samles inn fra overalt, som i produksjon. Alle data fra sensorer samles i en database. Etterpå, eller i sanntid, kan du analysere disse dataene for å få informasjon. Hvis dataene gjentar seg, for eksempel fra en temperatursensor, kan det indikere at noe skjer. Vi kommer tilbake til det når vi diskuterer vedlikehold.

Men å analysere store mengder data bidrar til Industri 4.0. Du kan plassere smarte algoritmer oppå dette, AI-algoritmer, som er dataprogrammer som analyserer

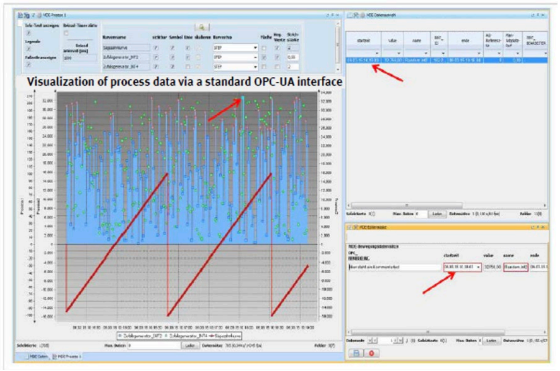


Figur 9: Typisk RFID-oppsett for industriell anvendelse (grafikk med tillatelse fra FESTO).

RFID-brikker blir stadig billigere. Så å feste en RFID-brikke til en gjenstand koster ikke mye. Det unike er at du kan skrive data til brikken, som den vil RFID er en av de viktige teknologiene bak Industri 4.0.

Etiketten kan være et klistremerke på et produkt. Eller du kan bake den inn i et produkt, som i et bankkort. Antennen som kommuniserer med etiketten er tilkoblet en datamaskin, og utvekslingen av data er trådløs. Det som virkelig gjør det geniale er at de enkleste RFID-brikkene ikke trenger noen strøm i seg selv. De får den nødvendige strømmen from magnetisk feltet i kortleseren til antennen. Dermed

dataene.



Figur 10: Visualisering av prosessdata (Programvare fra selskapet GTT mbH Hanover, grafikk med tillatelse fra FESTO).

Og de lærer hvordan de kan gjenkjenne mønstre og vil i økende grad kunne forutsi

ting basert på endringer i dataene. Det er big data, et felt som blir stadig viktigere.

Facebook, Google osv. samler data om alle mennesker, så mye som de kan. Og angående så mange aspekter av livene våre som mulig. Fordi de ønsker å forutsi vår atferd. På den måten vet de når jeg skal på ferie, og deretter vil de vise annonser for reisemål. Og så videre. Det er også big data. Store mengder data, litt ustrukturerte, som kan analyseres av maskiner. Kritiske aspekter ved big data er at de også kan samle unødvendig informasjon. Så du vil få mye unødvendige data som stjeler kapasitet. Og datasikkerhet er selvfølgelig et problem.

Datasikkerhet

Figur 11: Datasikkerhet har økt i betydning på grunn av Industri 4.0 (Foto av FLY:D på Unsplash).

Et typisk eksempel er smittesporingsappen for koronavirus. Den ble stoppet, da regjeringen hevdet at den samlet inn for mye personlig data. Så datasikkerhet er et problem som gjelder big data.

Industri 4.0 handler om data-kommunikasjon og utveksling av data. Når alle elementer i alle prosesser er basert på data og utveksler data, blir du sårbar. Det finnes mange eksempler. Norsk Hydro ble hacket, og det førte til at alle deres fabrikker over hele verden ble satt ut av drift. Å kunne beskytte dataene dine er avgjørende, og å kunne stole på at dataene dine ikke har blitt manipulert. Du trenger tilgang, men andre mennesker bør ikke ha det. Det handler ikke bare om datamaskiner og servere på kontorer, men også om PLCer som styrer prosesser for maskiner. De er like sårbare. Personer med dårlige hensikter kan bryte seg inn og ødelegge produksjonen din. Dette er et ekstremt antall PLC-er som finnes i Norge. Flere hundre tusen. De fleste moderne PLC-er kan beskyttes med passord, men få utnytter den muligheten. Det er viktig å tenke på disse tingene når du opererer et system som inneholder datakontrollere som en PLC.

Samarbeid mellom mennesker og roboter.

Samarbeid mellom mennesker og roboter er også en av driverne bak Industri 4.0. Mennesker og roboter kan samarbeide, hver gjør det de er best på. Robotene kan håndtere store belastninger repetitivt. Mennesker kan tilby presisjon, vi kan tilpasse og tenke. Derfor kan vi dra nytte av det beste med industrielle roboter og mennesker.

Disse samarbeidende robotene, eller "koboter", er trygge for mennesker. Hvis du berører dem, har de sensorer som

oppdager deg og stopper hvis de treffer

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

noen med en vis mengde kraft. Industrielle roboter er vanligvis tungt sikret. Koboter er derimot sikret av innebygde sensorer.

Augmented Reality

Utvidet virkelighet, AR, er en teknologi som sannsynligvis vil ha en betydelig innvirkning på industrien over tid. Mange prosjekter er basert på denne teknologien. AR handler om en forbedring av virkeligheten. Som det er i dag, bruker du briller der du har tilgjengelig informasjon i dem. Så du blander dine egne visuelle opplevelser med et datagenerert bilde. I en monterings-prosess kan det vise deg hvor ting skal plasseres, og under vedlikeholdsoppgaver kan du få hjelp direkte mens du arbeider. Det kan også være nyttig hvis du jobber med konstruksjon, ved å organisere AR er en begrenset term; det handler om å legge datagrafikk oppå virkelige bilder.

Figur 12: AR-briller for bruk i industrielle omgivelser (foto med tillatelse fra FESTO).

VR kan brukes til simuleringer, for eksempel av fabrikkbygninger. En kombinasjon av alle disse teknologiene kalles MR, eller blandet virkelighet.
AR er en del av Industri 4.0, som vi vil diskutere i denne kursen i forbindelse med vedlikehold. Dette er et felt som utvikler seg raskt, og det vil påvirke fremtiden vår.

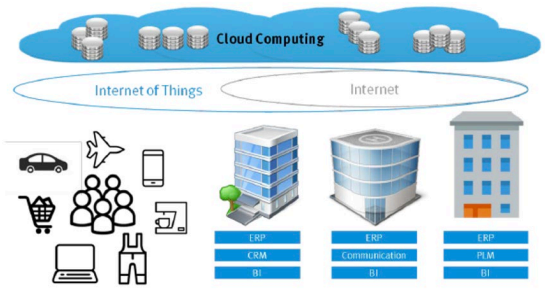
Vi snakker også om Operator 4.0. Tiden der operatørjobber kombinert med AR kan være mer effektive, kan gi deg nye ansvarsområder. Du kan forbedre arbeidet ditt som industrioperatør med denne teknologien implementert.

The cloud

"Cloud" er en samlebetegnelse, som betyr at du får datatjenester online. I stedet for å kjøpe maskiner, kan du leie maskiner som er koblet til internett et sted. De kan være plassert i store datasentre i Norge eller i andre land. Du kan også kjøpe lagring for store mengder data, som vi snakket om i "Big data". Et datasenter "i skyen" kan være akkurat det du trenger. Du kan også kjøpe tjenester fra dataskyene. Hvis du starter en bedrift og trenger et oppsett for kontorarbeid, kan du kjøpe rimelige bærbare datamaskiner og kjøpe programvaretjenester og støtte online. Deretter betaler du for bruken, og du trenger ikke å investere i programvare eller bygge en organisasjon. Så skyen bidrar til å gjøre Industri 4.0 mulig. Det finnes ulike skytjenester.

"Infrastruktur som en tjeneste", som jeg nettopp nevnte. At du kan leie datatjenester over internett.

"Plattform som en tjeneste" er å leie virtuelle datamaskiner, datamaskiner du får tilgang til nesten som om de står under skrivebordet. De er plassert et annet sted, men du kan installere programvare og konfigurere det som om det er på din egen datamaskin. like. Med "programvare som en tjeneste" kan du for eksempel leie Office365 i skyen og bruke det lokalt.

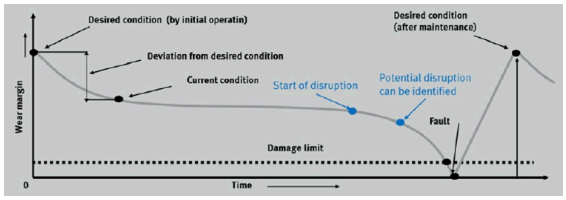


Figur 13: Skyen - levering av IT-infrastruktur og IT-tjenester fra internett (grafikk med tillatelse fra FESTO).

Skytjenester er ofte private, men noen ganger offentlige. Organisasjoner kan også ha sin egen sky. Datatjenestevirksomheten er tett knyttet til skyen, og den vokser. Store datasentre med datamaskiner som trenger strøm og kjøling. Risikoen med skytjenester er at du blir avhengig av at de fungerer. Hvis du leier tjenestene dine fra ett bestemt datasenter som kan oppleve strømbrudd, er du i alvorlige problemer. Men tjenesteleverandøren kan selge deg redundans, overflødighet i tjenestene deres, kanskje to sentre gjør samme jobben. Hvis noe skulle gå galt på ett senter, kunne det andre ta over. Disse tjenestene er ganske pålitelige, men også sårbare. I tillegg gir du andre organisasjoner tilgang til dataene dine, noe som kan true sikkerheten din, siden andre personer har tilgang til dataene dine. På den annen side er disse leverandørene avhengige av tillit, så dette er sjelden et problem, men det kan skje.

Tilstandsovervåking

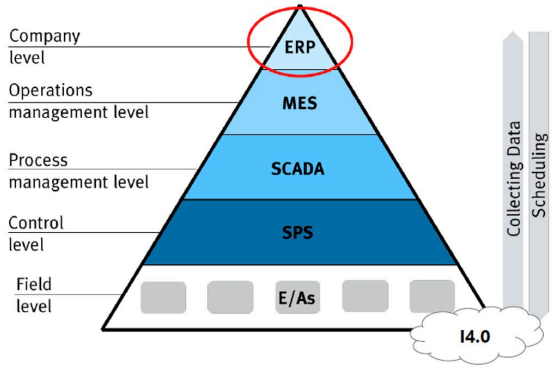
Tilstandsovervåking er prosessen med å overvåke tilstanden til ulike deler av din prosess. Samle data og bygge opp store datamengder. Dette kan innebære måling av temperaturer på ulike stadier, vibrasjoner, registrering av hvor lang tid forskjellige maskiner bruker, eller analyse av væsker for ulike maskinverktøy for å sjekke tilstanden til smøremidler og kjølevæsker. Alt er målbart, og data kan lagres. Så tilstandsovervåking er en viktig del av vedlikehold, det vi kaller "smart vedlikehold", moderne vedlikeholds-metoder.



Figur 14: Tilstandsovervåking - permanent eller periodisk måling av fysiske variabler (grafikk med tillatelse fra FESTO).

ERP

ERP står for Enterprise Resource Planning. Mange har erfaring med systemer som SAP. SAP er verdens største leverandør av ERP-systemer. Disse systemene kan håndtere de fleste prosessene i bedriften din. De tar seg av lagerplanlegging, der ERP-systemer startet. Ressurs-administrasjon, mennesker, penger, lager og så videre. Finans, regnskap, innkjøp, logistikk, personell og mye mer. SAP har moduler for det meste du trenger å gjøre i bedriften din.



Figur 15: ERP tar over oppgaven med å planlegge, kontrollere og koordinere alle ressursene i et selskap (grafikk med tillatelse fra FESTO).

Firkanter trekker opp en bedrifts systemer. Den nederste laget viser systemene som er koblet til maskineri, som PLS. Deretter har du kontrollene, som kontrollpaneler i systemet. Deretter har du SCADA-systemet, som kontrollerer andre, mindre systemer. Deretter har du MES-systemene, Manufacturing Execution Systems, som tar seg av planlegging og gjennomføring av produksjonen. Dette er koblet til ERP-systemet, som kontrollerer alt fra toppen.

Ofte tar ERP-systemet seg av datalagring og kontrollerer databasene nederst i systemet. ERP, MES og lavere nivåer, ned til PLS, er avgjørende deler av industrien 4.0 teknologiene. Her blir produksjons-prosesser og ressurser planlagt i detalj. I ERP utføres den grove planleggingen, i MES er det detaljert planlegging. MES snakker direkte med PLS og systemene som styrer maskinene. MES-systemet samler også data under produksjonsprosessene. Gjennom MES-systemet kan du planlegge og kontrollere produksjonsressurser. Og få driftsparametere som hjelper deg med å planlegge vedlikehold, for eksempel.

Smart vedlikehold

Det er ikke en offisiell term, men ideen bak det er å koble sammen ulike vedlikeholds-strategier og måter å utføre vedlikehold på, og det er basert på store datamengder, som nevnt tidligere. Samt overvåking. Med disse strategiene kan du sette opp et vedlikeholdssystem som er koblet til alle prosessene og maskinene i systemet ditt.

Som lærling var en av mine oppgaver å sjekke fabrikkens store elektriske motorer. Hver fredag tok jeg med meg en stor skrutrekker og lyttet til lagerne. Jeg plasserte skrutrekkeren på lagerhuset og lyttet etter tegn til slitasje. Og sjekket om lyden hadde endret seg siden uken før.

I dag utføres denne jobben av et dataovervåkingssystem. Data samles inn, lagres i en database og behandles som store data. Her kan du se hvordan vibrasjonene i lagrene vil utvikle seg. Lenge før lageret slites ut, kan du planlegge en utskifting. Tidligere, hvis du ikke brukte skrutrekkermetoden, ville du si at lagrene var utslitt etter et visst antall timer. Deretter byttet du dem, uavhengig av om det var nødvendig eller ikke. Dette er en mye brukt vedlikeholdsstrategi, for eksempel i luftfartsindustrien, der reglene er svært strenge. Alle flydeler har et visst antall driftstimer før de må byttes ut, uavhengig av om de er slitt eller ikke. Driftsforholdene for et fly kan variere mye, inkludert mellom flytyper.

Smart vedlikehold utføres når det er nødvendig. Du mottar advarsler, slik at vedlikeholdet kan planlegges, noe som er viktig i luftfartsindustrien. Du bør utføre vedlikeholdet lenge før flyet krasjer. Men du kan spare mye ved å utføre vedlikehold når det er nødvendig, i stedet for å bruke tidsintervaller som veiledning.

Den amerikanske luftfartsindustrien hevder de har fått tusenvis av flytimer med smart vedlikehold. Så de kan fly i stedet for å stå på bakken, og utnytte flyene mye mer.

Smart Factory

Selv om begrepet "Smart Factory" ikke har en nøyaktig oversettelse til norsk, kan det beskrives som en intelligent fabrikk. Dette er en kombinasjon av alle disse elementene, der alle ressursene til selskapet er koblet sammen via maskin-til-maskin kommunikasjon (M2M), altså kommunikasjon mellom maskiner. Dette resulterer i et kyberfysisk system, hvor produksjonen kan organisere seg selv. Mange beslutninger som tidligere ble tatt av mennesker, kan nå tas av dette systemet fordi systemet har informasjon om hva som skjer, hvor mye råvarer som er tilgjengelig, og hva som skjer i neste produksjons-prosess. Dette gjør det mulig å optimalisere produksjonen, redusere kostnader og behovet for arbeidskraft.

Mulighetene som skapes av dette, er at du kan tilby mer komplekse produkter og øke antallet varianter av produktet ditt. Men i dag har produkter en kortere levetid fordi utviklingen skjer raskere. Hvis du ønsker å gjøre dette, må produksjonen digitaliseres, og du må ha en smart fabrikk.

Figur 16: SMART fabrikk (grafikk med tillatelse fra FESTO).

Maskin-til-maskin kommunikasjon

En utfordring med å etablere en smart fabrikk kan være at utstyret har en lang levetid, og utstyret er ikke i stand til å kommunisere med andre systemer. Du trenger også en god kommunikasjons-standard og komplekse datasystemer. M2M, maskin-til-maskin kommunikasjon, betyr at maskiner kan snakke med hverandre på "datamål" som de kan utveksle informasjon via et nettverk. Dette krever en felles standard, et felles språk for kommunikasjon via en delt datastandard. Dette er en av faktorene som har gjort Industry 4.0 mulig.

At maskiner kan kommunisere seg imellom, og med maskiner utenfor systemet også, som ERP-systemer.

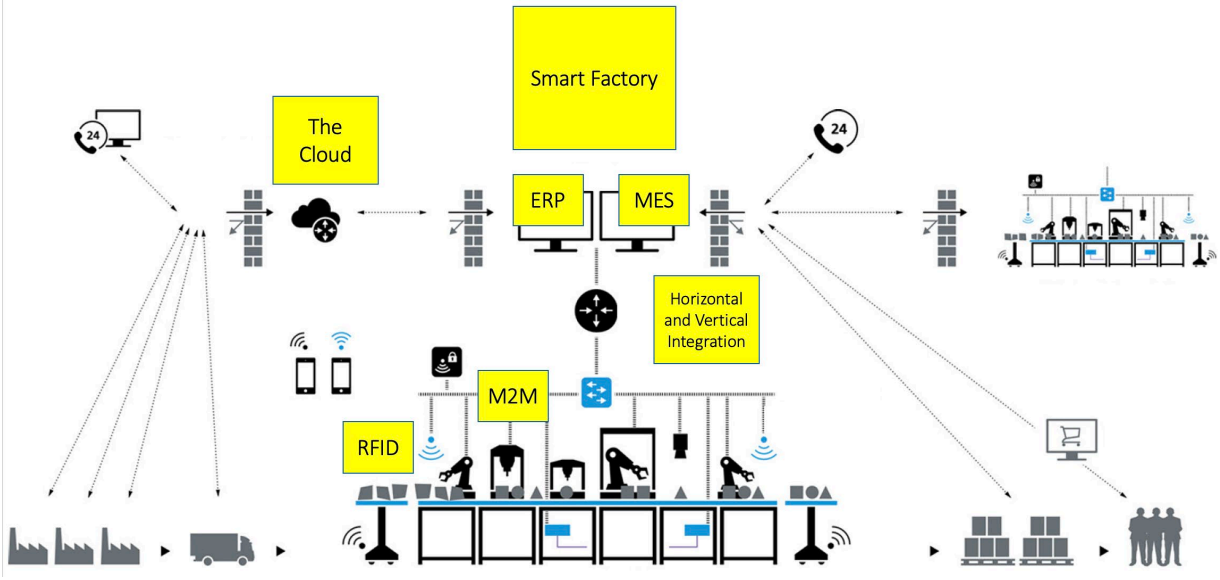
Horisontal og vertical integrasjon

Vi snakker også om horisontal og vertikal integrasjon. Dette betyr at systemer på samme nivå er koblet sammen, sammen med systemer over og under. "Samme nivå" betyr at maskiner i en stor prosess kan kommunisere. Det kan også kommunisere opp til ERP-systemer og ned til leverandørsystemene

OPC UA

OPC UA er en viktig kommunikasjons-standard i Industry 4.0. Det er et felles språk for datamaskinkommunikasjon og lar datamaskiner snakke med kontrollere i fabrikken, som PLC-er. På denne måten kan MES-systemer snakke med PLC-er, som igjen kan snakke med hverandre, og så videre. Maskinene kan kommunisere med hverandre gjennom denne Open Platform Communication Unified Architecture (OPC UA). Dette er en åpen standard. Ingen selskap eier den, noe som gir friheten til å koble utstyr fra forskjellige selskaper sammen. Tidligere kunne man etablere produksjon med muligheter for Industry 4.0, men man ville sannsynligvis være bundet til en leverandør med sin egen kommunikasjonsstandard. OPC UA har åpnet opp for dette, og det er en standard som støttes av de fleste leverandører. Slik kan utstyr fra forskjellige produsenter kommunisere med hverandre.

SMART factory overview



Figur 17: Oversikt over SMART-fabrikken (grafikk med tillatelse fra FESTO).

Dette er en oversikt over et selskap og systemene de bruker. Til venstre ser vi fabrikkens leverandører. Klientene er på høyre side. Over ser vi forskjellige systemer som kommuniserer. Og i midten ser vi produksjonen. Dette smarte fabrikk-systemet snakker med hverandre, skyen er til stede, samler data og tilbyr tjenester for fabrikken. ERP systemet på toppen hjelper deg med å planlegge alt, alle forretnings-prosessene. Den kommuniserer også med MES-systemet, som snakker med produksjonen og administrerer kommunikasjonen mellom ERP og produksjon. På produksjonsnivå snakker maskinene med hverandre, M2M. RFID brukes også, der produksjons-systemene kan kommunisere med produkter. Dette gir i praksis horisontal og vertikal integrasjon.

3. Tingenes internett

By Tommy Hvidsten

La oss studere hva som kanskje er det viktigste fenomenet bak Industri 4.0. Tingenes internett må være til stede for å oppnå Industri 4.0 og effektene innenfor den.

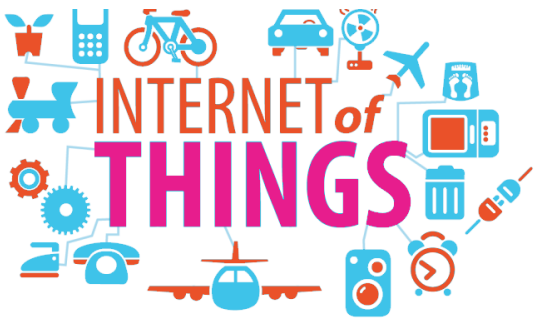
Først og fremst er det en klok mann ved navn Robert Metcalfe. Han er mannen bak Ethernet-standarden. Han kom opp med ideen først og valgte navnet Ethernet. Ethernet er en viktig basis for all internettrafikk rundt om i verden. Den er ryggraden for all datakommunikasjon. Metcalfes lov handler ikke om Ethernet, men om at effekten eller verdien av et telekommunikasjonsnettverk er proporsjonal med kvadratet av antall tilkoblede brukere i systemet, antall brukere multiplisert med seg selv.

> *"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)

Vi kan illustrere det slik: Hvis det bare finnes én telefon i verden, har den ingen verdi. Du har bare én telefon. Det er ingen verdi der før du har to av dem og kan snakke med noen. Da har du en tjeneste, og det er en verdi knyttet til den. Hvis det er en tredje telefon, øker verdien enda mer. Da er det to av dem du kan koble til, og så videre. Og når han sier at det er kvadrert, betyr det at når antallet øker, vil verdien øke enda raskere.

Internett er et typisk eksempel. Uten brukere ville verdien av Internett ikke vært særlig mye. Noen maskiner kunne samhandle og kunne koble seg til datanettverk via Ethernet og begynte å kommunisere med hverandre. Da var det grunnlag for innovasjon, utvikling og nye tjenester. Og på en måte skape nye bedrifter, nye måter å drive dem på. Det er Metcalfes lov. Den sier mye om verdien av et kommunikasjonsnettverk.

Internett of Things (IoT) er et nettverk av fysiske objekter eller ting som inneholder elektronisk teknologi, programvare, sensorer og en nettverkstilkobling. Dette gjør at tingene kan samle inn og utveksle data. Det er svært få ting tilgjengelig i dag som ikke er online. Vaskemaskiner vil snart være online, kjøleskapet ditt er online, bilen din. En "ting" i denne sammenhengen er et fysisk objekt med en unik identitet. Det må være mulig å kommunisere med det. Dette tillater Internett-protokollsystemet å fungere når hver datamaskin har sin egen IP-adresse. Det er mulig å kommunisere med hverandre og vite hvor ting kommer og går.



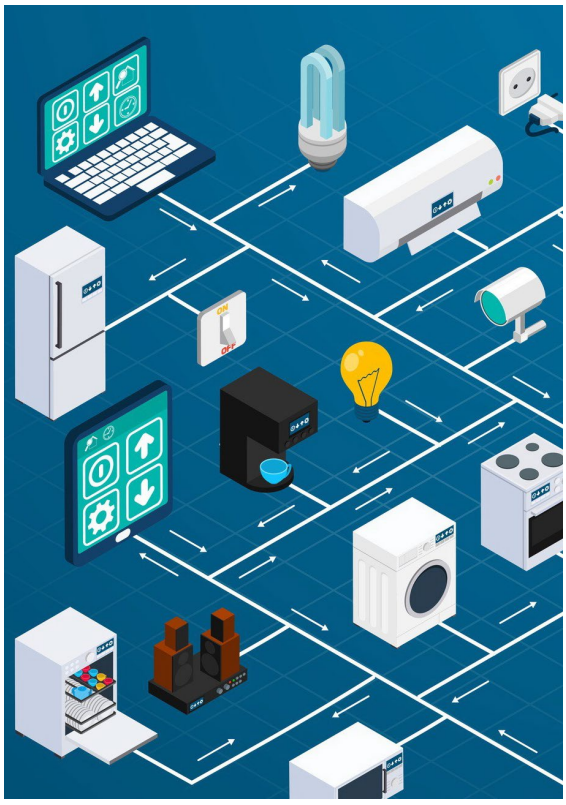
«The Internet of Things» implies that things such as the thermostat, sneakers and cars becomes smart. They get sensors and net connectivity, and can automatically collect, interpret and share information about when you wake up, how effectively you train, and how aggressively you drive.»

Teknologiradet.no

IoT betyr at objekter som termostater og biler har blitt smarte. De har sensorer og kan samle, tolke og dele informasjon om når du står opp og hvordan du kjører bilen din. Denne beskrivelsen er fra Norsk Teknologiråd. Man kan spørre seg hvor smarte ting kan bli når de er koblet til Internett og en datamaskin. I noen sammenhenger er det virkelig verdifullt å få dem online. Nesten hva som helst kan bli smart ved å legge til sensorer som måler temperatur, bevegelse, fuktighet eller hva som helst, og dataprosessorer som kan beregne og administrere den innsamlede dataen. Lagringsenheter som gjør det mulig å lagre data og beregninger slik at de kan brukes senere.

En Internett-tilkobling som gjør det mulig å overføre data til og fra "tingen". Og det er batterier som får dem til å fungere. De trenger strøm. Batteriene blir mindre, og levetiden deres blir lengre. Alt dette, hva gjør de? De samler inn data. Ting med sensorer samler data overalt. I hjemmet ditt, i bilen. På fabrikken, på kontoret. Når du er ute og jogger med en klokke som kan lagre hjertefrekvensen din, for eksempel. Eller hvor du er, posisjonen din, ved hjelp av GPS. Den kommuniserer, sender data om tilstanden og hendelser via et nettverk til en mottaker. Enten til en plattform på Din smartklokke kommuniserer med din mobiltelefon og overfører treningsdataen eller helsedataen din. Gjennom din mobiltelefon kan de lagres i skyen, og dataene kan brukes senere. På denne måten kan du følge din egen trenings- eller helseprogresjon. De analyserer data ved å trekke ut rådata og lage informasjon basert på det. Informasjonen kan visualiseres i en rapport med grafer eller fine pie-diagrammer. De kan også filtrere data for å fjerne det du ikke trenger å vite. Objekter kan handle, de kan utføre handlinger basert på den innsamlede informasjonen, og også ved å kommunisere med andre. En slik handling kan være å sende en tekstmelding eller e-post, eller kommunisere med andre maskiner eller systemer.

Et eksempel kan være "Varm opp hytta di ved hjelp av telefonen din." Systemet er gammelt. Imidlertid har du i dag en app. Før du forlater, gir du beskjed til appen om at du ønsker at hytta skal varmes opp. Det er IoT, Internet of Things, som gjør dette



mulig. Det er en IoT-enhet i hytta som slår på oppvarmingen for å varme den opp.

Andre eksempler inkluderer dørlåser. Jeg har en hjemme. De er tilkoblet nettet og kan kommunisere med et alarmsenter eller med deg. Det er et implantat i hjertet ditt som kan sørge for at det fungerer godt. Hvis du har en hjertesykdom, kan du få en enhet kirurgisk plassert i hjertet ditt som overvåker hjerteslaget ditt. Du kan også ha en defibrillator som overvåker hjertet ditt. Hvis noe skjer, hvis hjertet slutter å slå, starter den automatisk igjen. Dette kan ofte redde liv. I tillegg kan data trekkes ut fra enheten som er plassert inne i deg, og leger kan analysere helsedataene dine og handle om nødvendig.

Biler med innebygde sensorer blir stadig vanligere. Det er ingen begrensning for data som kan samles inn fra en bil. Jeg kjører en Nissan Leaf med et SIM-kort. Den kommuniserer med en stasjon og forteller den hva jeg gjør. Den kan også gjøre ting for meg tilbake. Jeg tror det er en begrenset mengde informasjon som kommer fra bilen min, men en Tesla er tilkoblet 100 % til Tesla sitt system som laster opp det meste av data. Dette har både positive og negative sider. Den positive siden er at selskapet kan lære og kontinuerlig utvikle programvaren sin og oppdatere bilens programvare. Mange Tesla-eiere har opplevd det. Den negative delen er at Elon Musk vet alt du gjør, og det kan brukes til andre formål. Det er betingelser når det gjelder data sikkerhet som kan være tvilsomme.

Værstasjoner som samler værdata. Smarthus. Elektriske målere har vært et slikt tilfelle. Moderne elektriske målere sender data til strømleverandørene, slik at de kan sende deg en faktura for strømforbruket. Mange har protestert mot dette, men de fleste har gått over til det. Ved å gjøre det, trenger man ikke noen til å lese av måleren, og du trenger heller ikke å gjøre det selv. Strømleverandøren kan sette prisen for strømmen annerledes. Du kan ha forskjellige priser for strøm gjennom dagen basert på forbruket. Dette kan gi deg billigere strøm over tid. Forhåpentligvis.

Mannen bak Internett of Things er Kevin Ashton, som jobber ved MIT, Massachusetts Institute of Technology. Det han utviklet var konseptet og ordene "Internett of Things." Han sier at IoT kan transformere verden til data som kan brukes til å ta store beslutninger om ressursutnyttelse. Ved å kontrollere ting rundt deg kan vi optimalisere måten vi bruker ressurser på, gjøre det bedre og fordele ressurser bedre. Informasjon kan redusere avfall og øke effektiviteten. IoT gjør dette mulig.

IoT gjør også smarte vinflasker, bikinier og vannflasker mulig. Dette er ikke IoT, sier Kevin Ashton, men søppel. Vel, man kan undre seg over verdien av noen av disse sakene som kan kobles til Internet.

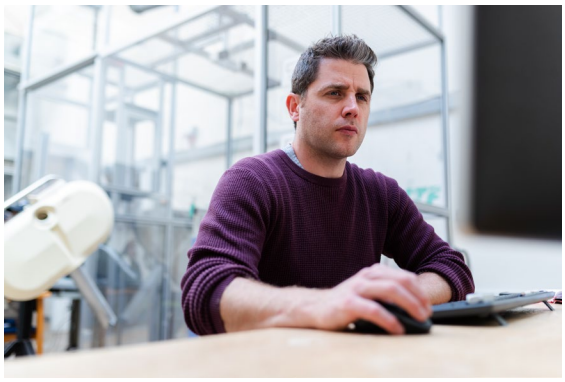
En ting jeg tvilte på lenge, var å plassere sensorer i stoler og koble dem til Internett.

Jeg lurte på hvorfor vi ville ønske å gjøre det. Så møtte jeg en mann som leide ut kontorplass. Han sa at det var viktig for ham å vite hvordan og hvor stolene ble brukt. På den måten kan han optimalisere kontorområdet og tilpasse det til hvordan det brukes i stedet for å ha stoler der som ingen bruker. Ved å bruke denne dataen kan dette forbedres. Det kunne være nyttig å ha en datamaskin i stolen som er koblet til Internett.

4. ERP og MES systemer

By Andreas S. Hernandez

Dette kapittelet handler om ERP, eller Enterprise Resource Planning, og MES, eller Manufacturing Execution System.



Figur 18: ERP Enterprise Resource Planning.

Først skal vi se på hvordan alt dette fungerer sammen. Vi skal se på Automatiseringspyramiden.
Automatiseringspyramiden beskriver de forskjellige konseptene og systemene. Vi ser at ERP-programvaren er øverst. Dette er Enterprise-nivået, som er det høyeste nivået i hele organisasjonen. Dette brukes vanligvis av ledelsen og nedover gjennom operasjonene. Det er ikke spesifisert hvor langt ned, men selv operatører kan bruke det. MES er nivået under ERP. MES er det som kalles styringsnivået. Vi kommer tilbake til hva dette er. De to første er programvaredrevne, der vi ser på omgivende systemer og hvordan data håndteres av disse systemene.

SCADA er enda nærmere produksjonen, mens PLC og PAC er kontrollerne for sensorene. Deretter går vi ned til sensorene og aktuatorene, og annet utstyr som utgjør de fysiske delene av produksjonen.

Hvis vi starter nederst, ser vi at alle sensorene i produksjonen gjør ting, sensorer utstyret, og signalene deres går opp til neste nivå, som bare kontrollerer dataen, registrerer og lagrer den. De forteller bare sensorene eller aktuatorene hvor de skal gå. Så går vi videre opp til SCADA-nivået. Dette er hvor vi får datahåndtering. Men den virkelig store datahåndteringen skjer ikke før vi kommer til MES-nivået. Det er her vi får en oversikt over de forskjellige systemene. Dette er hvor vi kan aggregere data til noe større, slik at vi kan se det større bildet. Men på SCADA-nivået ser vi bare hvor de forskjellige linjene går.

På ERP-nivået ser vi organisasjonens store linjer. Ting som finans, planlegging, tilgang til materialer, tilgang til forskjellige ressurser. Dette er ERP-nivået.

Så hva er den store forskjellen mellom ERP, Enterprise Resource Planning, og MES, Manufacturing Execution System? Den største forskjellen, i hvert fall slik jeg ser det, er at ERP dreier seg om et overordnet perspektiv. Vi ser på måneder, uker og dager. Mens MES er opptatt av hendelser

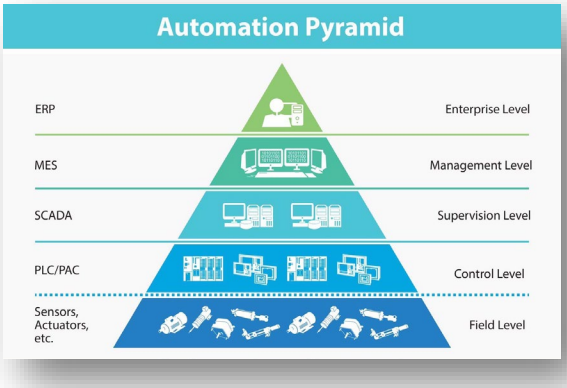


Figure 19: The automation pyramid.

som skjer akkurat nå. De overvåker

produksjonen som pågår øyeblikkelig og den informasjonen vi trenger. Mens ERP kan være mer relatert til rapportering, gir det en oversikt over det totale bildet. MES dreier seg mer om hva som skjer her og nå.

Noen av områdene som har med ERP å gjøre, inkluderer salg, økonomi, regnskap, HR, produksjon, planlegging, lagring, innkjøp, service, for å ikke nevne kundeservice. Mens MES har noe mer overlappende funksjonalitet. Det tar for seg ting som SPC (Statistisk prosesskontroll), kvalitetskontroll, rapportering og håndtering av ressurser i øyeblikket. Det svarer på spørsmålet: Hva trenger vi for denne oppgaven? Ikke minst prosesser og utstyr som vi trenger. Ordre og håndtering av ordre, og selvfølgelig levering.

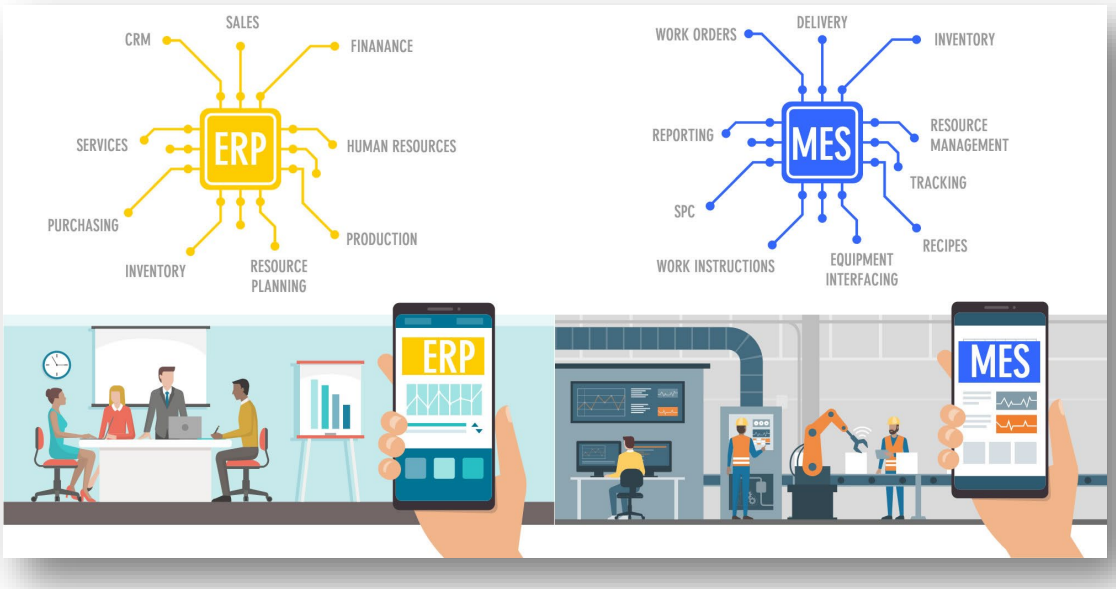
Dette er to forskjellige detaljnivåer. Dette betyr at ERP er et tregere system. Vi kan ikke ha samme oppdateringsfrekvens som vi har i MES. I MES snakker vi om dager, timer og minutter. Så det er en tidsforskjell i oppdateringen av de to systemene.

På 1960-tallet var vi i begynnelsen av bruk av datamaskiner og databasert assistanse. Det begynte selvfølgelig med lagring og håndtering av lagring. Ressursplanlegging kom litt senere, nærmere 70-tallet. Ikke å glemme produksjonsplanlegging.

Vi ønsker at disse systemene skal kommunisere med andre typer systemer. Vi ønsker mer hjelp for dem. Ikke bare at vi hadde lagring, og hvor mye vi hadde på lager. Og hvor mye vi burde bruke, hvor mye produksjonen trengte.

Dette er alt bra, men hva med alle de andre tingene? På 1980-tallet ønsket vi å ta det ett skritt videre. Vi introduserte det vi kaller produksjonsressursplanlegging. Dette omhandler ikke bare materialer, men også tilgjengelig maskineri. Vi snakker om andre ressurser, som operatører. Og verktøy, og alt som trengs for produksjon.

På 1960- og 1970-tallet var det noe som het MRP. Materialressursplanlegging. På 1980-tallet hadde vi fortsatt MRP, men vi kalte det MRP II. Så ,det har vært en utvikling fra det som var på 60 and 70 tallet. So even



Vi må også se på bakgrunnen. Hvorfor opprettet vi et ERP-system på et tidspunkt? though we had resource planning for our

production, it doesn't really address the overall demand in the business.

På 90-tallet ønsket de å knytte ting enda tettere sammen. Selv om vi hadde ressursene, ønsket vi å se hvor mye penger vi brukte. Så finans ble en del av ERP (Enterprise Resource Planning). Ikke å glemme human resources (menneskelige ressurser).

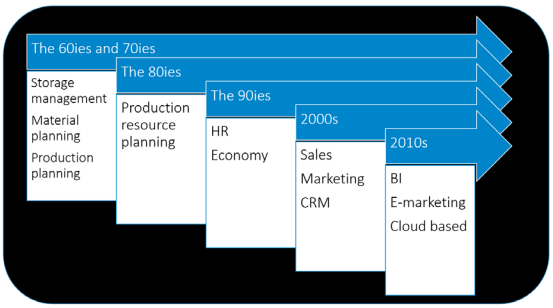


Figure 20: Historical development.

For å opprettholde produksjonen trengte vi ansatte med riktig kompetanse til riktig tid, og i riktig mengde. Så alle disse tingene kom nærmere hverandre gjennom ERP (Enterprise Resource Planning).

På 2000-tallet gikk det fra organisasjonens indre liv, der vi prøvde å integrere alt i ERP, til å se på omverdenen også. Dette inkluderte salg, markedsføring og det vi kaller CRM (Customer Relationship Management).

På 2010-tallet og fremover begynte vi å snakke om data og databehandling av dette. På den tiden hadde mengden av ulike data blitt for stor for én person å håndtere, så vi trengte hjelp til å visualisere det. Derfor ble Business Intelligence, som først dukket opp på 1980-tallet, integrert i vår ERP-løsning. Slik kan vi få en god oversikt over organisasjonens status.

Videre ser vi at e-markedsføring og skylagring er noe vi ønsker å inkludere i ERP. Spørsmålet er: Hvorfor trenger vi virkelig ERP-løsningen? Fordi vi ønsker at ERP, Enterprise Resource Planning, skal inkludere alt som har med virksomheten vår å gjøre. Slik at vi har ett program som håndterer all dataen. Noen av de største ERP-leverandørene i Norge er Visma, Oracle ERP, Microsoft Dynamics, Baan og SAP. SAP er kanskje den største ERP-leverandøren vi kjenner til, og den har vært her siden den først startet på 1960-tallet. Nykommere som Microsoft Dynamics har også sine løsninger.

La oss gå videre og spørre: Hvem trenger ERP? Det er for ledelsen. Ledelsen trenger å vite alt som skjer. For eksempel, bruker vi penger på riktig måte? Er det andre måter å utnytte ressursene våre bedre på? Vi ønsker å ha kontroll over produksjonen. Leverer vi tilstrekkelig? Har vi nok verktøy? Har vi nok utstyr? Nok folk? Har vi riktig kompetanse? Selvfølgelig ønsker ledelsen å vite dette.

Og den økonomiske siden har sine egne krav. Så vi bruker ikke for mye penger, eller for lite. Hvis vi ikke bruker nok penger, kan vi mangle noe, og produksjonen kan stoppe. Vi må fokusere på kvalitetsprodukter. De må være en del av prosessen. Håndtering av databrudd bør kanskje være en del av ERP. Når det skjer et brudd, kan vi ikke fortsette produksjonen av produktene våre før de er registrert i ERP-systemet. Så vi ser at alt samarbeider. Det er ikke bare én informasjon som hjelper oss med å se det store bildet, men det er helhetsbildet.

Vi må innse at ingen systemer i dag kan operere isolert. Vi trenger det store bildet med en kobling mellom alle systemene

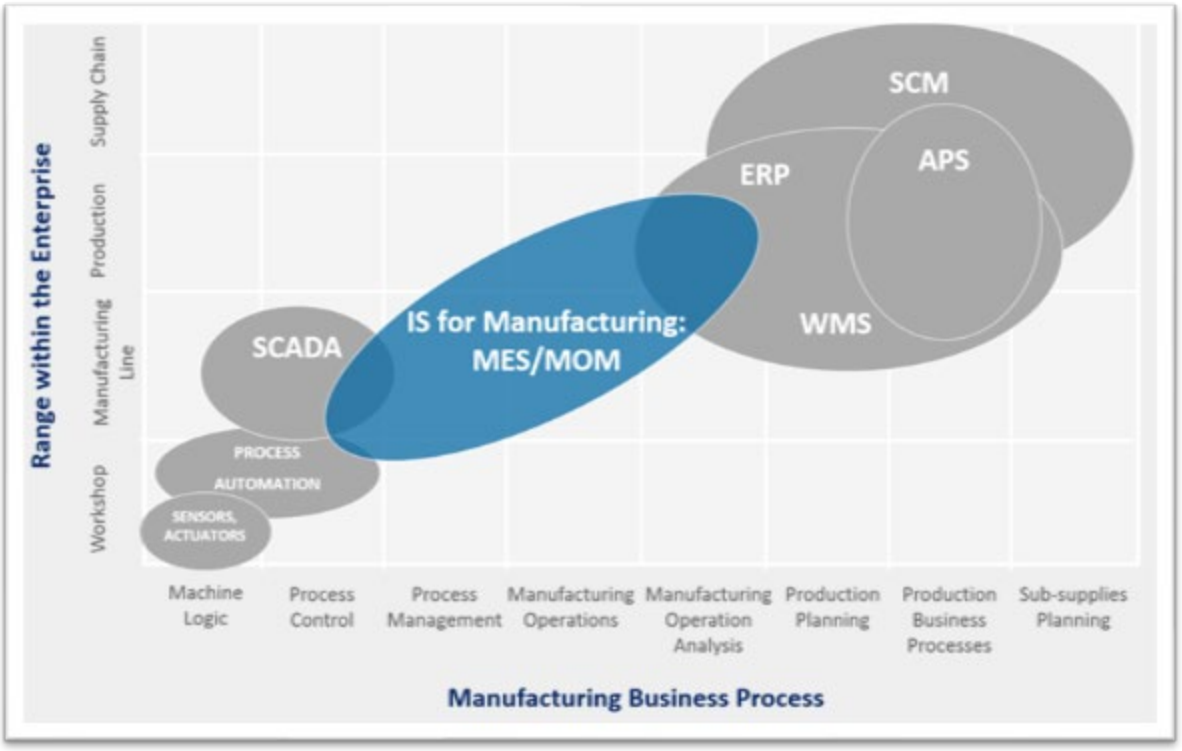


Figure 21: The MES domain.

våre. Dette er det ERP har forsøkt å oppnå siden 1960-tallet. At vi har en felles plattform der vi kan se alt som angår organisasjonen vår. Når vi ser på de ulike områdene for både ERP og MES (Manufacturing Execution System), ser vi at produksjonsplanlegging og det vi kaller forretningsprosesser, det vil si de overordnede prosessene for virksomheten vår, er plassert i ERP-området. Hvordan utfører vi innkjøp? Hvordan håndterer vi kunder? Og lignende ting. Dette er plassert i ERP-systemet.

ERP kan også grense mot MES-systemet, spesielt i de mer operative delene. Dette skjer gjennom operasjonell analyse, for eksempel "hva hvis"-scenarioer. For eksempel, hvis vi har det vi trenger. Når vi ser på MES, ser vi at det starter med prosesser. Hvordan den fysiske delen blir laget, er en del av MES-området. Dette omfatter hele operasjonskjeden. For eksempel, når vi har laget en del, hvor går denne delen? Det faller under MES-systemet. For å oppsummere ERP: Det dreier seg om det store bildet. Salg, innkjøp. Det håndterer logistikk, det håndterer mennesker. Det håndterer leveranser. Det håndterer produksjon. Og integrasjonen mellom alle disse områdene, blant annet.

La oss ta en titt på MES (Manufacturing Execution System). Hva er MES? For å forenkle ting, i fortiden hadde vi mange papirdokumenter. Når formannen tildelte en oppgave, hadde han en bunke med papirer. Skjemaer, arbeidsinstruksjoner, leveranser, materialer. Alt dette var inkludert i en haug med papirer. Dette er omtrent det MES ønsker å erstatte.

Vi har et dataprogram som sier at når jeg legger inn denne delen i datamaskinen min, kan jeg få en oversikt over alt jeg trenger. Ikke å glemme hva som må gjøres. Alle produksjonsdokumenter, skjemaer, arbeidsbeskrivelser, verktøy og så videre. Jeg kan også få informasjon om tidligere versjoner, hvis vi har hatt problemer. Og en

liste over prioriteringer. Hvilken jobb starter jeg med? Hvis jeg har fire produkter, hvilket av dem skal jeg starte med?

Spørsmålet er: Hvem er ansvarlig for ERP? Hvem er hovedbrukeren, eller superbrukeren, av MES-systemet? Vi

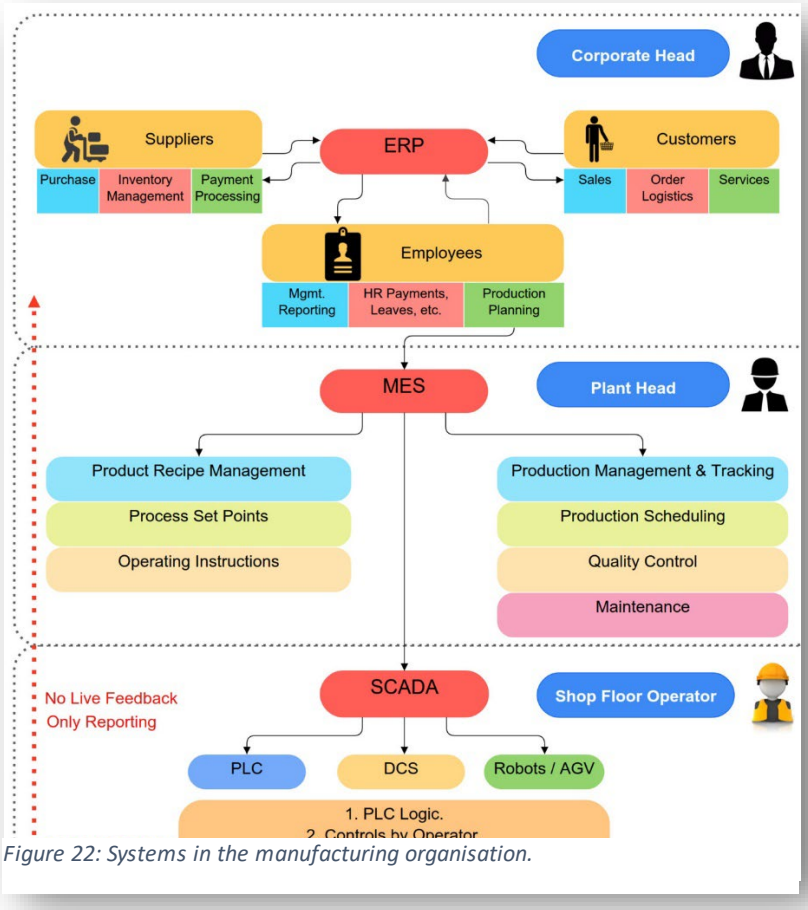


Figure 22: Systems in the manufacturing organisation.

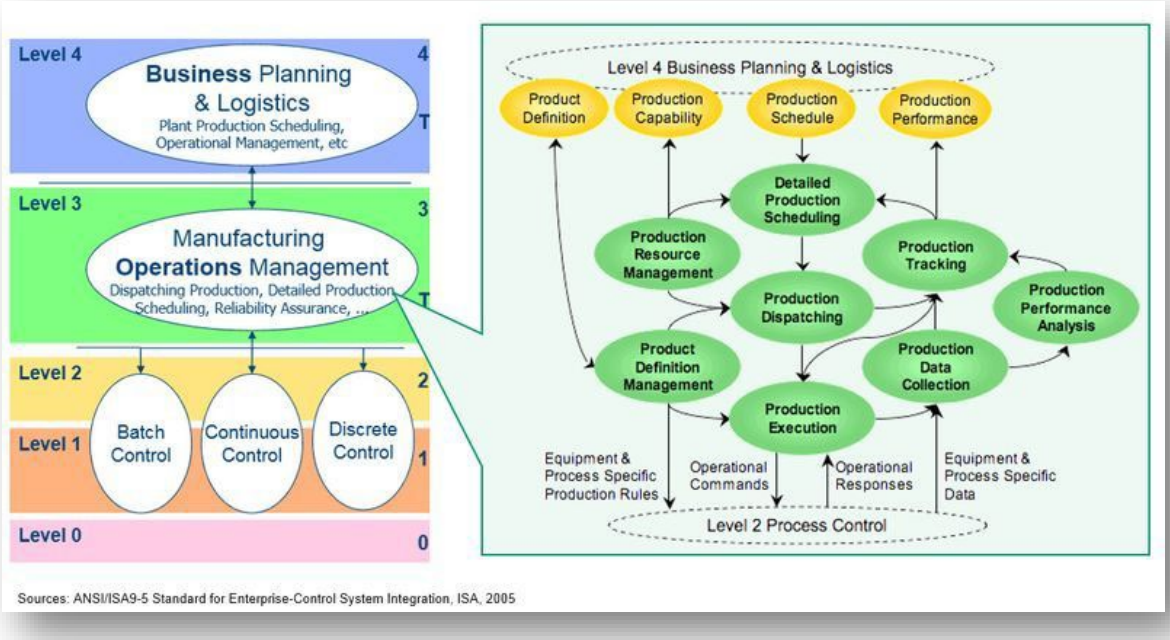
nevnte at sluttbrukeren av ERP er ledelsen. Det er der all dataen skal ende opp og kan brukes som en oversikt og for rapportering til ledelsen. MES-systemet gjør mye av de samme tingene, men det ser ikke på de store trendene. Det er mer for seksjonsledere. Her kan han kontrollere produksjonen og områdene sine. Vi har kontroll på daglige rapporter og daglige behov for ressurser. Som for eksempel personellvurdering, som hvor mange personer trenger jeg i år? Dette faller under ERP. Men hvem trenger jeg for jobbene denne uken? Det utføres i MES-systemet.

Det er det samme med vedlikehold. Vedlikeholdet planlegges i MES-området. Det samme gjelder for kvalitet og kvalitetskontroll. Alt dette er i MES. Mens håndtering av brudd og bruddhåndtering kan skyves opp til ERP.

Hva med nivået under? Hva gjør det? Nivået som kalles SCADA er for operatørene. Der har vi alle rapporter og lignende ting for alle våre PLC-er, roboter og slikt. Der har vi tilbakemeldinger om hvordan en maskin fungerer akkurat nå.

MES gir mer en oversikt over hele produksjons-prosessen vår. Dette er det som skiller MES fra nivået under. Nivået under ser på den nåværende statusen til hver enkelt maskin. Mens MES fokuserer mer på dag-til-dag og uke-til-uke aktiviteter. Men det er også mulig å se på time-til-time.

Det neste bildet er fra en standard kalt ISA-95. Her ser vi på ISA-95-modellen. Hvordan ser dette området ut, og hva er MES ment å gjøre? Det er fire forskjellige områder. Dette er det vi kaller produksjonsstyring. Planene for en uke eller en måned kommer ned fra det som kalles MRP (Material Requirements Planning).

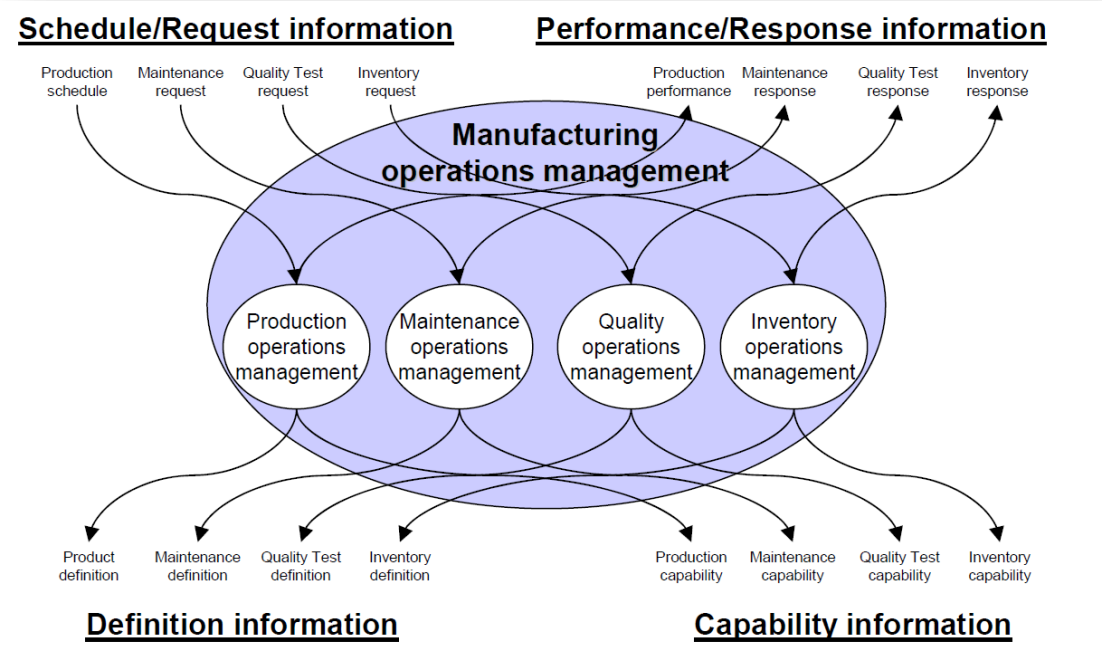


Planene for de kommende ukene og månedene kommer fra ERP-systemet. Dette er hva kunden trenger. Dette går ned til MES-systemet. Hvordan bryter vi ned de store planene slik at vi vet nøyaktig hva vi skal gjøre? Den første delen kalles detaljert produksjonsplanlegging. Dette betyr at vi tar en plan... La oss si at vi skal lage 100 deler på en uke.

Så hvordan deler vi disse 100 delene? Vi går ned til den første delen kalt detaljert produksjonsplanlegging. Deretter blir dette distribuert. Hvilke maskiner, hva trenger vi for å fullføre disse jobbene? For å gjøre dette trenger vi det som kalles produksjonsressursstyring. Vi må vite hvilken type utstyr vi trenger for å håndtere produktene våre og produsere delene vi trenger. Når vi vet hvor mye vi skal produsere i de forskjellige områdene, går vi videre til produksjonsdisponering. Dette betyr at vi har delt opp planen vår, og vi må sende planen til alle maskinene som lager delene. MES-systemet gjør dette for oss.

Når vi har sagt at vi utfører en jobb, trenger vi et grunnlag for jobben. Dette kalles produksjonsdefinisjonsstyring. Med andre ord er det formelen for hvordan vi skal utføre jobben. Dette legges til jobben og sendes til maskinen. Å sende dette ut kalles produksjonsekskursjon. Å utføre jobben. Her ser vi to piler. En går ned til nivå to, og en går tilbake til produksjonsekskursjon. Dette er den utførende delen. Dette er der det faktisk skjer. Men når vi har fullført ordren, er vi ikke ferdige. Vi trenger en tilbakekoplingsløkke for å få informasjon tilbake til systemet vårt. Når jobben er fullført, ønsker vi å samle data. Hvordan gikk jobben? Holdt vi oss til planen? Planla vi materialene riktig? Ressursene og lignende. Dette går opp til det som kalles produksjonsdatainnsamling. Dette samler bare data. Men vi må også gjøre noe med dataen også.

Det er to områder. Det første er produksjonsytelsesanalyse. Dette forteller hvordan vi har gjort det. Hvordan utførte vi jobben? Og er det tilstrekkelig? Dette er



bare en analyse. Dette samler bare data og plotter det. Det siste er produksjons-sporing. Vi har en analyse som sier om det er riktig eller galt. Og vi trenger noe som sier om det går etter planen eller ikke. Produksjonssporing gjør dette. Der ser vi om planen vi har fulgt, samsvarer med målet for uken. Hvis den gjør det, trenger vi ikke å endre planen. Hvis vi ligger langt bak planen, er det en pil som går tilbake til detaljert planlegging. Da starter vi løkken på nytt. Vi er i konstant "bevegelse".

Vi må ha informasjon som går inn i systemet vårt, men det sender også informasjon tilbake til systemet slik at vi kan reagere... Vi må reagere på eventuelle feil som oppstår, slik at vi kan være proaktive. Ved slutten av uken vil vi ikke si: "Beklager, vi klarte ikke å levere i henhold til planen." Vi ønsker informasjon gjennom hele uken slik at vi kan justere planen deretter. Slik at vi kan se om vi gjør det bra eller dårlig.

Dette var en del av MES-nivået. Vi ser at vi får informasjon fra ERP, de store overordnede bildene. Og du får også produksjonsytelse. Så vi får de store bildene tilbake. Hvordan går det i henhold til planen? Og kan vi nå ukens mål? Dette kommer fra MES og opp til ERP-nivået.

Som jeg nevnte, dette er en av fire områder. Vi har produksjonsoperasjons-styring, som vi nettopp har snakket om. Det samme gjelder for vedlikehold. Der har vi den samme logikken bak det og bildet vi nettopp har sett. Det samme gjelder for kvalitet og kvalitetsprosesser. Der har vi den samme løkken. Det samme gjelder for lager og lagerhåndtering.

Så vi har fire forskjellige systemer innenfor MES med samme struktur. Der MES er mellomnivået som går opp til ERP, og også ned til gulvet og våre sensorer. Nå har vi snakket omtrent om hva ERP er, og hva MES er. Og hvordan vi bruker MES, og hvordan vi kan forstå disse to begrepene.

5. Informasjonssikkerhet

By Emil Moholt

That sounds like important and challenging work, especially in the defense and aerospace industry where data security is of paramount importance. If you have any specific questions or topics, you'd like to discuss related to security in computer systems or any other aspect of your work, please feel free to ask, and I'll do my best to provide information and insights.

Jeg kommer til å begynne med å snakke om sikkerhet generelt. Og jeg skal definere noen begreper og metoder vi bruker innen sikkerhet, som vil være universelle for datamaskinsystemer, andre systemer eller andre prosjekter der sikkerhet er nødvendig. Deretter kommer jeg til å snakke om informasjonssikkerhet, eller tradisjonell datasikkerhet. Dette er fordi datasikkerhet har kommet lenger i utviklingen enn det har innen operasjonelle systemer. Deretter skal jeg snakke om sikkerhetsmekanismer, metodene vi bruker for å beskytte tradisjonelle IT-systemer, tradisjonelle datamaskin-systemer.

Deretter vil vi gå over til operasjonelle systemer. OT-systemer, systemer knyttet til fysiske prosesser. Og hvordan sikkerhet er håndtert i slike systemer. Jeg kommer til å avslutte med noen lysbilder der vi skal se på konsekvensene av å kombinere IT-systemer, OT-systemer og IoT-systemer. Og hvordan dette påvirker sikkerheten til systemet.

Det er tre sentrale sikkerhetsbegreper. Først av alt: Hva er verdien? Hva prøver vi å beskytte når vi snakker om sikkerhet i denne sammenhengen? For det andre: Hva er truslene mot verdien vi prøver å beskytte? Hvem ønsker å ødelegge den, stjele den eller bare bruke den feil? Det siste begrepet er sårbarhet. Hvordan kan en trussel utnytte verdien vi beskytter? Dette betyr at det er en feil i måten vi beskytter verdien vår på.

"Verdi" og "trussel" er relativt statiske

> *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)

Figur 23: Sikkerhetsbegreper.

begreper. Så hvis du har identifisert verdiene dine, er de kjente. Med mindre du endrer måten du jobber på, forblir verdiene de samme. Truslene er også mer eller mindre konstante. Det kan hende at en ny trussel oppstår eller at en annen forsvinner, men de er mer eller mindre konstante. Vi vet hvem som prøver å stjele verdiene våre. Når det kommer til sårbarhet, er det mye mer dynamisk. Vi kan føle at vi beskytter verdiene våre slik at de er trygge mot alle trusler. Men låsene vi bruker, kan ha sårbarheter som truslene kan utnytte.

Med "trusler" mener jeg tyver og hackere. Jeg har lagt ved en lenke til en PDF. Dette kom fra noen studenter ved MIT. For å vise folk hvordan de kan komme seg inn i laboratorier utenfor åpningstid. Denne lenken fungerer. Hvis den ikke gjør det, kan du bare søke på "MIT Guide to Lock Picking". De har tatt vanlige låser som ble brukt på MIT på 80- og 90-tallet og laget en guide for hvordan man kan låse opp disse låsene. Så selv om universitetet følte at laboratoriene deres var sikre, da folk visste hvordan de kunne komme forbi låsene, var ikke laboratoriene lenger sikre. Fordi de fant sårbarheter i låsene i laboratoriene.

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.*

Figur 24: Sikkerhetstiltak - mottiltak.

Dette er bare et generelt overblikk over sikkerhet. Du har verdier og trusler, og du beskytter dem på en eller annen måte. Deretter er det sårbarheter som truslene kan bruke for å utnytte det du prøver å beskytte. I populærkulturen er det normalt å utnytte sårbarheter. Jeg antar at noen av dere kanskje har sett Olsenbanden-filmene. Der låser folk med verdier dem inn i den beste safen de kan finne. Det er en Franz Jäger-safe fra Berlin. De vet ikke at det er en Egon Olsen som kan åpne alle Franz Jäger-safene med et stetoskop. Fordi det er hans spesialitet. Så denne safen har ingen verdi hvis Egon Olsen er den som prøver å stjele verdiene dine. Du må gjøre noe annet.

Når det gjelder trusler, er det delt i tre. Og du er bare interessert i den verste delen. Det er tre typer mennesker eller organisasjoner som er trusler mot verdiene dine. Du har de som bare er nysgjerrige. De sier: "Hva er dette? Kan jeg bruke det eller tjene penger på det?" Så har du opportunistene, som går rundt som mink. "Hva er dette? Kan jeg ta noe? Kan jeg oppnå noe?" Så har du de målrettede truslene. De sier: "Jeg vet at det er noe av verdi her." "Hvordan kan jeg komme til disse verdiene?" "Hvordan er disse verdiene sikret?"

Om det er gullstenger eller et produksjonssystem, spiller egentlig ingen rolle. De prøver å få tak i de verdiene du prøver å beskytte hele tiden. Det du ser når du lager sikkerhetssystemer, enten det er for gullstenger, produksjon eller informasjon, er at hvis du klarer å beskytte mot de målrettede truslene, kan du også beskytte deg mot nysgjerrige mennesker og opportunistene.

Hvis du ser på hvem som prøver å åpne dører, vinduer og skap, er det ofte nysgjerrige mennesker eller opportunistene. Du ser sjelden de målrettede truslene. Men de prøver vanligvis mye hardere når de vil stjele verdiene dine. Når det gjelder verdier, er det ett kontrollspørsmål: Hvorfor ville du ikke ønske å legge eiendelene dine ubeskyttet ute på gaten? Hvorfor skulle du ikke ønske å legge eiendelene dine ubeskyttet ute på gaten? Hva skjer med

deg og din forståelse av verdien hvis den blir liggende ubeskyttet ute på gaten? Ville den bli ødelagt eller stjålet? Ville det påvirke deg eller organisasjonen din hvis den blir stjålet?

Hvis svaret er: "Ja, jeg ville ikke kunne produsere noe." "Ja, jeg ville miste forretningshemmeligheter." Eller noe lignende. Dette betyr at tingen som ligger ute på gaten, har en verdi for deg. Da må du spørre: Hvem ønsker å ødelegge den? Og hvordan kan jeg sikre den mot disse truslene? Sikkerhetstiltak. Dette er det vi gjør for å beskytte verdier. Den mest tradisjonelle måten å beskytte verdier på, er å bygge sikre hus. Gamle banker laget av stein med vinduer høyt oppe på veggene. Det er vanskelig å komme inn i bygningen, og inne i bygningen er det et hvelv som er enda vanskeligere å bryte seg inn i. Dette er tradisjonelle sikkerhetstiltak når du har håndfaste verdier som du ønsker å beskytte.

I dag, når vi snakker om håndfaste verdier, har vi hus eller bygninger der vi legger ting. Og inne i dem har vi låste skap eller til og med safes som gjør det vanskelig å komme til verdien. Vi har andre verdier som vi ikke låser ned. Dette er ting vi bærer med oss. De fleste av oss har en lommebok. Noen av oss har kontanter, vi har kredittkort. Vi har en telefon, bilnøkler og så videre. Dette er verdier, og du sikrer dem ved å bære dem med deg. Slik at ingen kan komme til dem uten at du merker det. Vi er litt skeptiske til fremmede. Når vi er på arbeidsplassen eller et sted der det er mange fremmede, er vi på vakt og prøver å passe på folk som prøver å stjele vesker eller lommebøker. Hvis du er på stranden, er du på vakt overfor folk som ser på vesker.

Det samme gjelder for bedrifter. Mange bedrifter har en resepsjonsdisk. Etter arbeidstid har de sikkerhetsvakter. Du må komme forbi flere låser før du kan komme til bedriftens verdier. Så det å være på vakt overfor fremmede er en viktig del av sikkerhetsarbeidet.

Så er det en annen aspekt. Og det er: Hva er verdien av et sikkerhetstiltak hvis du ikke tar vare på det? Ethvert sikkerhetstiltak du har, alle slags sikkerhetstiltak, har ingen verdi med mindre du tar vare på dem. For å se om noen manipulerer sikkerhets-tiltaket.

Hvis vi går tilbake til "MIT Guide to Lock Picking". I det øyeblikket den guiden ble publisert, betydde det at hver dør som var sikret med en gammel Yale-lås, ikke lenger var trygg. Du må oppgradere låsen din til noe bedre. Dette gjelder generelt. Hvis du ser at sikkerhetstiltaket ditt ikke lenger er trygt, må du bytte det ut med noe bedre.

Din egen hukommelse er et veldig viktig sikkerhetstiltak. Som passord. Noen viktige passord og PIN-koder skal du ikke skrive ned. De skal være helt utilgjengelige, slik at bare du kjenner dem, og uansett hva som skjer, vil ingen andre finne dem ut. Dette er de viktigste delene. Bli kjent med verdier, trusler og sårbarheter.

Det neste jeg skal snakke om, er risikovurdering. Hva er vi redde for å miste? Og hva er konsekvensene av å miste det? Du må veie dette opp mot: Hvem er interessert i det vi har? Med hensyn til verdien vi har og den mulige trusselen, hvor mye bør vi gjøre for å hindre noen i å ta verdien vår?

Et godt eksempel på dette er: Hva gjør du med hytta di på fjellet? Hvis du har en hytte på fjellet, hvor mye beskyttelse trenger du? Dette er konsekvensene: Hvis du har en veldig sterk lås, kan en innbruddstyv trenge 30-45 minutter for å bryte seg inn. Men han vil ødelegge både dørkarmen og døren, og kanskje mer, for å komme inn i hytta. Hvis du har en mindre lås, kan han bare ødelegge dørkarmen eller bare låsen. For å komme inn. Hvis låsen er så sterk at det tar en time å komme inn, og han ødelegger en dyr dørkarm og dør, men han kommer fortsatt inn, er hyttas verdier tryggere enn hvis du hadde hatt en billigere lås?

Problemet er at så lenge ingen passer på denne låsen, spiller det ingen rolle hvor sterk den er. Da trenger du en annen sikkerhetstiltak. Slik at før noen klarer å bryte seg gjennom låsen, gir en slags alarm beskjed til en sikkerhetsvakt som kan komme til hytta før de er inne. Da er det sikkert.

Så hvis du har noe som er veldig verdifullt, må du vurdere hvilke sikkerhetstiltak du trenger. Bare en lås oppe i fjellet gir ikke veldig god beskyttelse. Du må tilpasse tiltakene til verdien du prøver å beskytte. Og hvor bestemt trusselen er for å komme til verdien. Hvis noen vet at du har gullstenger i hytta di, spiller det ingen rolle om du omgir dem med 20 mm stålplater. En bestemt innbruddstyv vil klare å komme gjennom uten å bli forstyrret med mindre du også har gjort noe annet.

Vi kan se på dette i andre sammenhenger. Hva prøver vi å beskytte? Hva skjer hvis vi mister det? Du trenger balanserte sikkerhetstiltak slik at du kan stoppe

- *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?*

Figur 25: Sikkerhet – risikovurdering.

trusselen. Avhengig av hvor bestemt han er før han kommer til verdien.

Jeg har nå dekket det innledende materialet om sikkerhet. Vi har snakket om de tre viktige begrepene, verdi, trussel og sårbarhet. Og at du trenger en risikovurdering for å ha balanserte sikkerhetstiltak for verdiene du prøver å beskytte.

Nå skal jeg snakke om sikkerhet i IT-systemer. Grunnen til at vi starter med IT-systemer er fordi datasikkerhet er mer avansert her enn i andre datamaskinområder. Sikkerhetspersoner som meg selv liker å kalle IT-systemer for CIA. Vi snakker ikke om den amerikanske etterretningsorganisasjonen, vi snakker om Konfidensialitet. Og informasjonen må være korrekt. Det er Integritet. Og informasjonen må være tilgjengelig, det er Tilgjengelighet. Dette utgjør CIA.

Dette er de tre begrepene vi skal snakke om. Vi starter med konfidensialitet. Hva er konsekvensene hvis informasjonen blir tilgjengelig for inntrengere? Gjør dette informasjonen mindre verdifull for oss? Vil det skade oss? Dette inkluderer ting som produksjonsdokumenter, immaterielle eiendeler. Hvis noen stjeler designdokumentene for produktene dine, kan de lage kopier av samme kvalitet som dine. Hvis det blir stjålet, vil det ha mindre verdi for oss etterpå fordi vi må senke prisene våre for å konkurrere med produsenter med forskjellig etikk enn vår når det gjelder respekt for andres immaterielle eiendom.

Neste aspekt er integritet. Er informasjonen vi jobber med korrekt? Det neste vi skal snakke om er sabotasje. Hvis du har muligheten til å endre produksjonsdokumentene du lager delene dine fra, eller som du tar beslutninger basert på, vil dette gjøre informasjonen mindre verdifull? Ja, det kan føre til direkte økonomisk tap. Dette inkluderer ting som bankinformasjon, personlig informasjon. Omtrent all informasjon du har i et IT-system. Hvis den er feil, har den ingen verdi for brukeren.

Det siste begrepet er tilgjengelighet. Vi blir stadig mer avhengige av datamaskinsystemer i livene våre. Hvis du

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.

Figue 26: Security in IT-systems - valuables.

betaler for noe, bruker du et kredittkort. Du bruker nettbank for banker og offentlige tjenester. Det er knapt noe som

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 27: Security in IT-systems - threats.

fortsatt er på papir. Hvis du mister datamaskinsystemene, vil du ikke kunne gjøre alt du vanligvis gjør. Hvis en bedrift mister datamaskinsystemet, stopper

normalt alt til systemene er oppe igjen. Du kan ofte bare sende arbeiderne hjem til IT-avdelingen har fikset systemet. Når du gjør en verdianalyse av et IT-system, må du se på alle disse tre parameterne og si: Hva er konsekvensene når det gjelder konfidensialitet? Hva er konsekvensene når det gjelder om informasjonen er korrekt eller ikke? Og hva er konsekvensene når det gjelder tilgjengelighet?

Truslene mot IT-systemer er annerledes enn for fysiske systemer, som bygninger. Det er fordi de fleste trusler prøver å angripe IT-systemet ditt via internett. Dette betyr at de er relativt usynlige mens de angriper. Hvis du ikke legger til IT-sikkerhetsmekanismer i systemet ditt, selv om du er inne i en bygning eller et datasenter, er det litt som å legge informasjonen ut på gaten. Så alle som passerer kan se på den og leke med den. Mange har nok kunnskap om datasikkerhet til å bare spille seg gjennom systemet ditt. Si at du har målrettede trusler. Det er mange forskjellige grupper, ofte drevet av utenlandske etterretningsorganisasjoner. De prøver å bryte seg inn i bedrifter og private datamaskiner for å finne informasjon. Når de angriper private datamaskiner, er det ofte for å stjele prosessorkraft. De vil ikke ha bildene dine, men nettverkstilkoblingen din. De bruker dette til å angripe sine virkelige mål senere. De som er strukturerte og bestemte og vil komme seg inn, prøver å finne ut hvilke sikkerhetsmekanismer du har. De mest sofistikerte blant dem, når de angriper bedrifter og andre stater, bruker agenter for å prøve å finne ut hva målene har gjort. Deretter prøver de å vurdere hvordan sikkerhetsmekanismene i bedriften din fungerer utenfra. Deretter kjøper de den samme programvaren og prøver å finne sårbarheter. Så truslene mot IT-systemer fra internett er mye større enn for fysiske systemer. Både fordi du ikke kan se dem, og fordi hele verden prøver å angripe deg.

I Norge har vi stor grad av tillit. Denne tilliten eksisterer ikke på internett. Så truslene mot IT-systemer er normalt større enn mot fysiske verdier. Mot bygninger i Norge. Jeg skal snakke litt om IT-sikkerhetsmekanismer. Vi vil bruke flere av dem senere, så jeg vil guide deg gjennom dem. Hvis du vil fysisk beskytte noe, bruker du en lås. Du bygger et hus med en dør og en lås. Den er da sikret på et minimumsnivå. For IT-systemer bruker du flere ting samtidig. Det første du gjør med et stort system, er å sette opp det vi kaller en brannmur. En brannmur i et IT-system er litt som en telefonutveksling. Den ruter informasjonen til rett sted, men den kan også kontrollere hvem som snakker med hvem. Hvem du har lov til å ringe innenfor et telefonsystem. Det er funksjonen til en brannmur i et IT-system.

Hvem har du lov til å kontakte gjennom dette nettverkspunktet? De fleste av dere

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.

Figure 29: Security in IT-systems – counter measures.

har bredbånd hjemme. Når du kobler datamaskinen din til nettverket via en bredbåndsforbindelse hjemme, fungerer denne forbindelsen som en brannmur med mindre du har gjort noe for å unngå dette. Dette betyr at de som prøver å kontakte hjemmenettverket ditt via bredbåndet, stoppes av bredbåndsruteren. Den fungerer som en brannmur.

Det spiller ingen rolle hva noen prøver å gjøre med hjemmenettverket ditt; de stoppes av bredbåndsruteren. Så dette fungerer som en brannmur hjemme.

En bedrift har ofte systemer innenfor IT-nettverket som systemer utenfor har lov til å kontakte. Så du må sette opp en brannmur og definere reglene for denne brannmuren, slik at du har lov til å kontakte serveren. Du lager et hull i brannmuren. Så hvis du ikke konfigurerer brannmuren riktig, kan du skape store hull i brannmuren slik at den ikke lenger fungerer. Dette gjør systemene mer sårbare.

En brannmur er en svært viktig sikkerhetsmekanisme i ethvert datasystem som har mer enn én datamaskin.

Et IT-system har også tilgangskontroll. Dette betyr at du vet hvem som har lov til å bruke systemet. For å få tilgang til systemet må du identifisere deg med brukernavn og passord før du kan bruke ressursene i nettverket. Tilgangskontroll er et svært viktig konsept i store bedrifter og organisasjoner.

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

Figur 28: Sikkerhet i OT-systemer – verdier – trusler.

Alle vil ikke ha tilgang til alt. Og de som logger seg på utenfra, kan ha mer begrenset tilgang enn brukerne på innsiden. Tilgangskontroll er også en svært viktig sikkerhetsmekanisme i et IT-nettverk. Så har vi kryptering. Så lenge det er innenfor et IT-nettverk, er dette en mekanisme du bruker fordi du antar at noen har kommet seg inn i nettverket.

Hvis vi krypterer all trafikk i nettverket, vil inntrengere ikke kunne se passord, brukernavn og informasjon i nettverket. Du kan bare se det som er på datamaskinen du har brutt deg inn på. Så har vi dedikert maskinvare. Dette er kanskje mindre viktig. Kjernen er at hvis hver datamaskin i et nettverk bare gjør én ting, og noen klarer å bryte seg inn i én enkelt datamaskin, kan de bare se hva som skjer på denne datamaskinen. De kan ikke se resten.

Med brannmurer, tilgangskontroll og kryptering er skaden minimal. Akkurat som hytta. Å legge til sikkerhetstiltak uten å overvåke dem hjelper deg ikke i det hele tatt. Så hvis noen prøver å komme gjennom brannmuren din, må dette loggføres, og noen må sjekke loggen. Det samme gjelder for tilgangskontroll. Hvis noen prøver å logge seg på med ulike passord hele tiden, må dette registreres slik at du kan se at noen har prøvd å komme inn. Hvis du har en brannmur og tilgangskontroll, og du ikke sjekker om noen har prøvd å bryte seg inn, vil de til slutt lykkes. Og du har ingen måte å se om de har prøvd og når de klarte å komme inn. Jeg går nå over til operative systemer.

OT-systemer, eller operasjonell teknologi. Den viktigste forskjellen mellom OT-systemer og IT-systemer er at de samhandler med fysiske prosesser. Disse systemene har direkte samhandling med den ytre verden og snakker ikke bare med andre IT-systemer og mennesker. I industriell kontroll har du ofte såkalte SCADA-systemer. Systemkontroll og datagrabbing. Du styrer produksjonen.

Når vi snakker om verdien av et OT-system, er verdien at systemet faktisk fungerer. Systemet er satt opp til å håndtere fysiske prosesser slik at folk ikke trenger å gjøre det. Det er ofte ingen reserveordninger for disse systemene. Så hvis et OT-system stopper, stopper også aktivitetene i en bedrift. Hvis du har jobbet i industrien og sett produksjonen stoppe, blir det alltid veldig stille veldig fort. Alle jobber hardt for å få dette i gang igjen.

Truslene mot OT-systemer er de som ikke ønsker at du skal gjøre jobben din. Så hvis du har en konkurrent som vet at en ny kontrakt vil bli tildelt basert på leveringsytelse, vil de forsøke å stoppe produksjonen din av og til, og leveringsytelsen din vil falle, og du kan miste fremtidige kontrakter. Samtidig, hvis de kan stoppe produksjonen din over tid, vil du miste forretninger. Og du er svekket i møte med fremtidige utfordringer.

Jeg har et eksempel på noen som ønsket å ødelegge et OT-system. Stuxnet er navnet på plattformen de brukte. Den ble brukt en gang. De vet ikke hvem som gjorde det, men de mistenker amerikansk etterretning. Dette er et målrettet angrep mot Irans kjernefysiske program i 2010. Det var mye sikkerhet i kjernefysiske systemer, men de overførte denne skadevaren til SCADA-systemet via en USB-pinne. Én bestemt anlegg ble målrettet. De fant kontrollprogramvaren for sentrifugene som beriket uran. Og de fjernet topphastigheten, slik at mellom en fjerdedel og en femtedel av sentrifugene ved kjernefysisk anlegg brøt sammen på grunn av dette målrettede angrepet med programvare på SCADA-systemet.

Det er lite sannsynlig at noen vil bruke så mange ressurser på å angripe norsk industri, men vi har ting som kraftselskaper. Hvis noen ønsker å skape uro i samfunnet, kan de bruke mange ressurser for å stoppe vann- og

strømforsyningen i Norge. Dette gjelder

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*

Figur 30: Sikkerhet i OT-systemer – mottiltak.

alle systemer som kan stoppe en bedrift eller kritisk infrastruktur.

Du trenger sikkerhetstiltak her fordi vi kan bli angrepet. Tradisjonelt er sikkerheten i OT-systemer basert på at de er individuelle systemer. De er ofte enkeltmaskiner som ikke er koblet til et nettverk, og de er plassert i fabrikker bak låste dører.

For å programmere CNC-maskiner bruker du spesielle USB-minnepinner. I nyere systemer bruker du datamaskiner som er koblet sammen for programmering, men disse datamaskinene er ofte ikke koblet til andre datamaskiner.

Hvis disse datamaskinene er koblet til internett eller et annet nettverk, introduserer du en sårbarhet i et OT-system. Dette er på generelt grunnlag. Verden er ikke svart eller hvit. Det er mange OT-systemer som er koblet sammen, men tradisjonelt har sikkerheten i OT-systemer innebåret at de ikke er koblet til noe. De er ofte ikke engang koblet til produksjonsnettverket.

Så lenge de er individuelle systemer i et låst rom, er det enklere for de som driver systemene å se hvem som kommer inn og gjør noe med systemet. Så det er lettere å se hvem som skader systemet så lenge det ikke er koblet til noe.

Når du kobler datamaskiner til produksjonsutstyr, er det noen vanlige sårbarheter. Dette skyldes at når produksjonssystemene er i drift, rører vi dem ikke. Fordi hver gang du vedlikeholder systemet uten å oppdatere produksjonen, er det en risiko for at produksjonen kan endre seg.

"Om det fungerer, ikke rør det" er en normal tilnærming til dette. Det er veldig skadelig hvis maskinen er koblet til internett. Så hvis du har datamaskiner knyttet til produksjonssystemet, og tilnærmingen din er "om det fungerer, ikke rør det", er det en liste med ti punkter.

Check Point, en av de største

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 31: Sikkerhet i OT-systemer – sårbarheter.

leverandørene av datamaskinsikkerhet, har utarbeidet denne sjekklisten. Det første punktet er gammel maskinvare. Gamle operativsystemer og gamle applikasjoner på en datamaskin er litt som

en gammel Yale-lås på hytta. Noen vil til slutt lage en veiledning for hvordan man kan bryte gjennom sikkerhets-mekanismene på gamle systemer. Hvis du ikke oppdaterer det, vil systemet inneholde sårbarheter.

Punkt 2: For at ting skal være lette å bruke, bruker folk fabrikkinnstillingene på utstyret. De bruker standard-konfigurasjonen med et passord. Dette betyr at alle som bruker utstyret, vet nøyaktig hva de skal gjøre. Men hvis det er koblet til internett, vet alle internettbrukere også hvordan de skal bruke utstyret. På produksjonsutstyr er det normalt å ikke kryptere data. Dette skyldes rett og slett at du må inkludere krypterings-informasjon som en del av konfigurasjonen av utstyret. Dette gjør det mye mer komplekst, slik at det ofte unngås. Dette betyr at du kan begynne å lete etter passord og brukernavn i trafikken inn og ut av dette utstyret.

Virkelig gammelt produksjonsutstyr, utstyr som fortsatt fungerer, er ofte koblet til et modem for vedlikehold. Sikkerheten er ofte basert på at hvis du har telefonnummeret, er du inne. Sikkerheten dreier seg om at telefonnummeret skal være hemmelig. Så når du har nummeret til et gammeldags modem, kan du gå inn og endre og konfigurere utstyret. Dette er ikke en sårbarhet knyttet til internett. Det er bare en vanlig sårbarhet for operativ-systemer som bruker et modem for konfigurasjon.

Deretter har vi samspillet mellom datamaskiner og datamaskinsikkerhet. Du har nå funksjonelle forbindelser mellom IT- og OT-systemer, men det har ikke vært en felles strategi når det gjelder sikkerhetsfunksjoner. Dette betyr at du kan omgå IT-sikkerhetssystemene ved å angripe OT-systemene. Dette betyr at du kan angripe IT-funksjonene fra OT-systemene. Og vice versa. Så lenge du ikke bruker de samme sikkerhetsstrategiene, kan du angripe ett system fra de andre systemene.

Så har vi brannmuren. En brannmur i et nettverk sørger for at bare riktige enheter kan kommunisere sammen. Når du setter opp et produksjonsnettverk, blir dette ofte gjort uten brannmurer og uten noen kontrollmekanismer i nettverket. Dette betyr at hvis du får en inntrenging, kan de få tilgang til hele produksjonssystemet, selv om bare én maskin har blitt kompromittert. Hvis du ikke bruker funksjonaliteten til en brannmur, blir det lettere å bryte seg inn i produksjonssystemet.

Det samme gjelder for det neste punktet: Stansing av produksjon. Hvis du er koblet til internett og ikke har en brannmur, og du har gammel programvare, vil du være svært sårbar for tjenestenektangrep (DoS-angrep). Dette vil stoppe alt. Det er veldig fristende å unngå å oppgradere et OT-system som fungerer, fordi det fungerer. Dette betyr at du til slutt ender opp med maskinvare som er 10, 15 eller 20 år gammel, med tilsvarende gammel programvare. Dette betyr at det ikke engang er mulig å oppgradere programvaren for disse maskinene. Så de vil alltid være sårbare for angrep fra utsiden.

Det siste punktet: Hvis du er koblet til omverdenen, kan du bli angrepet av virus eller skadelig programvare. Ofte finnes det ingen antivirusprogramvare i en maskin i et OT-system. Og hvis det er, blir signatur-filene ofte ikke oppdatert. Dette gjør deg sårbar for angrep fra utsiden.

Nå kommer konklusjonen. Hva skjer hvis noen bryter seg inn i et OT-system?

Dette er parametermanipulasjon. Du kan ødelegge selve produksjonen eller kvaliteten på produktene ved å endre produksjonsparametrene. De kan også stjele parameterne slik at de kan produsere det samme som deg, eller noe veldig likt med samme kvalitet fordi de har alle detaljene om produksjonen din.

Vi begynner å snakke om IoT-systemer. IT-systemer, OT-systemer og IoT-systemer møtes i en smeltedigel. IoT-systemer, tingenes internett, er basert på små enheter som er sensorer eller aktuatorer som arbeider med fysiske systemer. De er koblet til systemene ved hjelp av nettverksteknologi. Så du må bruke IT-sikkerhetstiltak for å beskytte IoT-systemene. Samtidig må du koble disse IoT-enhetene til kontrollsystemet.

Dette skaper en smeltedigel der du har IT-systemer, OT-systemer og IoT-enheter som jobber sammen i ett stort system. Dette har ofte begrensninger for oppdatering av de forskjellige systemene. Når du jobber med slike systemer, bør du alltid installere en brannmur, slik at du vet hvem som snakker med hvem.

Det finnes flere eksempler på at folk har satt opp små IoT-enheter hjemme, og dette har blitt brukt til å få tilgang til nettverket. Hvis du har en feilaktig IoT-enhet og kobler den til hjemmenettverket ditt, opprettes det en tilkobling til et eksternt system. Så trusler kan bruke denne tilkoblingen for å komme inn på IoT-enheten din.

Og deretter gå videre til hjemmenettverket ditt. IoT-enheten oppretter et hull i brannmuren din uten å rekonfigurere brannmuren. Så hvis du har et tradisjonelt produksjonssystem, et OT-system, må du låse dem ned på samme måte som før. Det er naturlig at et OT-system skal plasseres i et begrenset område. Nettverket som peker ut mot internett, skal gå gjennom en datamaskin med høyt sikkerhetsnivå.

- *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*

Figur 32: Sikkerhet i IT/OT/IOT-systemer II.

- *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*

Figur 33: Sikkerhet i IT/OT/IOT-systemer II

Og du trenger brannmurer i nettverket med en streng konfigurasjon, slik at du kan oppdage eventuelle inntrengere på et tidlig stadium. Du kan gjøre alt dette uten å endre OT-systemene. Du bruker bare de sikkerhetsfunksjonene som er tilgjengelige.

Dette er en kort oppsummering. Dette gjelder alle verdier; håndfaste verdier, IT-systemer, OT-systemer og systemer som er en blanding av IT, OT og tingenes internett.

Du må balansere sikkerheten din. Et IT-system som står ute på gaten med alle slags sikkerhetstiltak, er ikke balansert. Du trenger fysisk sikkerhet rundt IT-systemene dine og OT-systemene dine. Sikkerhetsnivået bør gjenspeile nivået på IT-systemet og OT-systemet. Sikkerhetsnivået bør gjenspeile nivået av IT-sikkerhet i det samme systemet. Og sikkerhetssystemer har feil.

Hvis du bruker en fysisk lås, bør du også ha sikkerhetsvakter. Så hvis noen plukker låsen, vil det bli oppdaget. Det samme gjelder for et IT-system. En kombinasjon av brannmurer og tilgangskontroll betyr at du må bryte gjennom brannmuren og tilgangskontrollen før du kan få tilgang til verdier i systemene. Så å ha mer enn én sikkerhetsmekanisme i nettverket, eller mer enn én sikkerhetsmekanisme rundt det du vil beskytte, er avgjørende.

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*

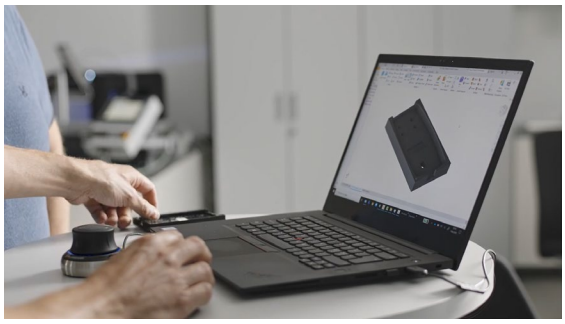
Figur 34: Prinsipper for sikkerhet.

Uansett hva du gjør, hvis du ikke overvåker sikkerhetstiltakene, har de ingen funksjon i det hele tatt. Uansett hvilke typer sikkerhetsmekanismer du har, hvis noen er fast bestemt på å komme inn, vil han klare det gitt nok tid. Det tar bare mye tid. Med overvåking kan du stoppe ham før han når verdiene.

6. En samtale om produktutvikling

By Endre Jamtveit and Tommy Hvidsten

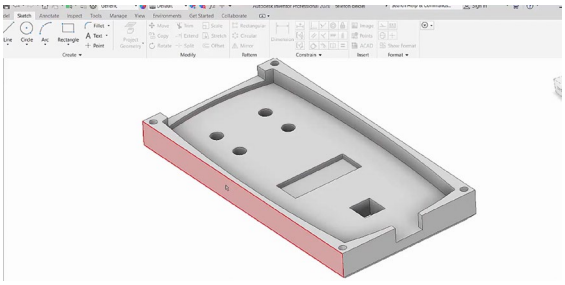
Jeg har med meg Endre Jamtveit i dag. Vi skal snakke om produktutvikling og en smart måte å gjøre dette på. Vi skal se på 3D-modellering, som er et av Endres kjerneområder. Vi vil se på hvordan dette kan bli til fysiske produkter.



Endre, hva skjer på skjermen akkurat nå?

Du har sett dette mobildekselet tidligere. Det er modellert på en datamaskin ved hjelp av et 3D-program som Inventor, som vi bruker nå. Først tegner vi delen, hvordan vi vil at den skal være. Deretter bygger vi den, akkurat som vi har gjort her. Her er dekselet. Vi kan gjøre mange endringer på hullstørrelser, hullmønster, tykkelse og ulike varianter.

Dekselet på skjermen ser nøyaktig ut som det fysiske dekselet. Hvordan kan du endre dette nå?



-Her har vi en lignende modell, og hvis vi ønsker at hullene på siden her skal være større, - kan vi enkelt endre dem i programmet. Hvis vi vil endre de 3 mm hullene til 4 mm, kan vi bare endre dem. Deretter kan du overføre dataene til en 3D-skriver for å lage en prototypedel. Når du har gjort det, og alt passer, og du er fornøyd med produktet, kan du sende det til en CNC-maskin, der det får CNC-dimensjoner. Deretter kan du masseprodusere det.

-Først lager du maskineringsbanene, for å gi CNC-maskinen noe å jobbe med. Deretter lager den det. Så er det bare plug-and-play. Det er et fantastisk produkt, spesielt for prototypetesting. Noen ganger trenger du en fysisk del for å sjekke om den er slik du hadde forestilt deg. Dataverdenen er ikke akkurat som den virkelige verden.

-Hvis du skal montere den på et trangt sted, er det bra å sjekke det med en prototype først for å forsikre deg om at den passer.

Denne er ferdig, men hvordan ville du begynne å bygge en 3D-modell?

-Vi starter med en type "del" i en 3D-virtuell verden. Og så må vi tenke i 3D. Først tegner vi i 2D, og deretter drar vi det ut i 3D. Hvordan ville du for eksempel lage en støpeform? Her er de tre planene som skal

gjøres om til 3D. Hvis vi starter med denne her...

- Vil du ha en kube? Ja, for eksempel. Her tegner vi den i 2D. Først spesifiserer vi størrelsen nøyaktig, med mange desimaler. Du kan ha det så presist du vil. Her bruker vi 3 mm. Nå har vi en 2D-modell, som er en støpeform eller en side av støpeformen. Deretter drar vi den oppover. Dette er 3D-modelleringen. Så velger jeg et verktøy, jeg velger å løfte det området der. Jeg vil dra det opp 25 mm. "Ok." Så nå har jeg en 3D-modell.

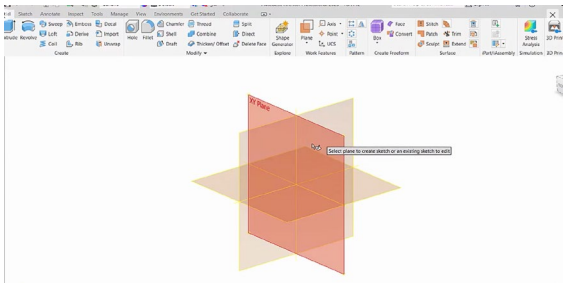
Figur 35: Endre bruker 3D-musen..

Jeg ser at du har to verktøy på datamaskinen din, en mus og noe annet også?

Ja, dette er en vanlig mus, og dette er en 3D-mus. Det er et verktøy for manøvrering i programmet. Når jeg vrir på den, roterer jeg modellen i Inventor, jeg løfter den og zoomer den. Med den kan du jobbe mye raskere, men du trenger ikke å ha den. Du kan også bruke en vanlig mus. Slik. Men hvis du gjør mye tegning, er den virkelig nyttig. Hvordan ville du få tegninger fra dette?

Jeg er så gammel at jeg fremdeles husker å tegne med blyant på papir. Er det mulig å få 2D-tegninger fra en 3D-del?

- Ja, det er også mulig. Da må du åpne en 2D-tegning. "Ny". Vi velger deretter at vi vil ha en tegning. Vi er ikke interessert i en modell nå. Vi ønsker heller ikke en gruppe, som også er et alternativ. Vi velger tegning,

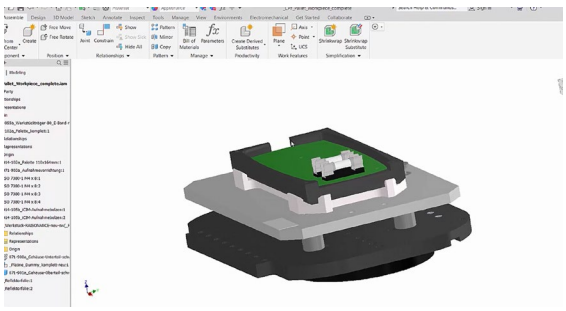


og vi åpner den. Nå får vi et tomt ark, som du kjenner igjen fra gamle dager. Det ser kjent ut. Ja. Så åpner jeg modellen jeg vil ha. Den er ikke blitt lagret ennå. Jeg må gjøre det først.

- Her kan du markere dimensjonene, lage produksjonstegninger, tilbudstegninger, monteringstegninger om installasjon og så videre. Det ser litt enklere ut enn blyant og papir. Og så har du Montering. I dette monteringseksempelet modellerer du hver del og monterer den slik den skal være.

Kan du ta dette fra hverandre?

-Ja. Her kan jeg plukke ut spesifikke deler. Som denne telefonen her. For å se på kretskortet, kan jeg finne riktig del, slik, og gjøre den usynlig. Så har jeg tilgang til den. Her kan vi sjekke at alt passer. At layouten er som forventet. Det er enkelt å gjøre justeringer. Det er et utmerket verktøy for å arbeide med prototyper og første produksjon.



Hvis du har et produkt og vil lage en variant av det, er det enkelt å gjøre det? Ganske raskt?

- Ja, og det er viktig å ha i bakhodet når du modellerer, at du kanskje må gjøre endringer senere. Du må dimensjonere det fornuftig, siden hull, veggtykkelse osv. vil endre seg. Og det er den vanskelige delen. Det er ikke lett å jobbe med noen andres modell, fordi du har en idé om hvordan du vil at den skal være. Så når du modellerer den, gir det mening å gjøre den lett justerbar.

Jeg antar at erfaring hjelper?

-Ja. Da lærer du hvordan du kan gjøre det lettere å justere ting senere.

Ja, det ser jeg. Er det andre ting vi kan se på som demonstrerer kraften til et verktøy som dette når det kommer til produktutvikling?

-Jeg er ikke helt sikker på hva du sikter til, men du kan gjøre styrkeberegninger, for eksempel. For disse delene har det mindre relevans. Men hvis du modellerer noe som må tåle trykk eller kraft, kan du legge inn den informasjonen i Inventor og få en analyse.

Forteller du Inventor hvilke materialer du har?

-Ja, du legger inn materialer, kraft, hvor kraften påføres, osv. Dette er en tilleggsmodul.

En plug-in?

-Ja. Da kan du få mye informasjon om tykkelse osv. Du vil ikke bruke mer materiale enn nødvendig, spesielt når du skriver ut det i 3D. Du bør holde det til et minimum. Jeg har modellert ganske mange trykkbokser for subsea-produksjon. Da er det avgjørende å gjøre styrkeevalueringer på forhånd. Det er viktig å sjekke at ting fungerer før de sendes til havbunnen. Du legger bare til alle sikkerhetsfaktorene og informasjonen du trenger.

Vi snakket om forskjellige utganger, som

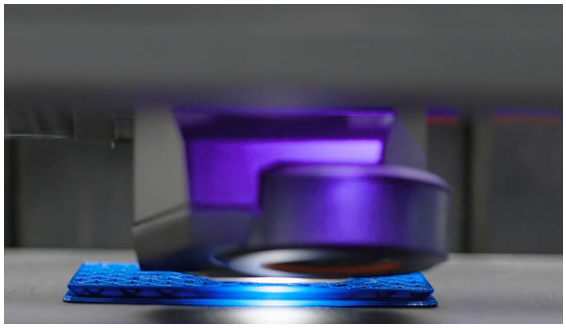


Figure 36: 3D-skriverens dyse ekstruderer plast på en oppvarmet overflate.

CNC. CNC-teknologi er så gammel at selv jeg vet hvordan den fungerer. CNC-er er verktøymaskiner, og jeg tror de første kom ut så tidlig som på 50- eller 60-tallet. Computer Numerical Control. Er verktøybanene ganske enkelt tilgjengelige fra dette programmet?

- Ja.

Trenger du etterbehandling?

-Ja. Du legger inn informasjon om hvilke verktøy du har, diameter og lengde osv. Du kan legge inn all den informasjonen og få banene, som du deretter kan simulere. Deretter kan du forhåndsvise hvordan verktøyene beveger seg. Du ser hvordan delen lages fra materialet. Og du ser den arbeider med det. Former det ferdige produktet. Dette er et praktisk verktøy for de som bearbeider det.

Her i Kongsberg har vi en lang tradisjon for verkstedproduksjon. Mange selskaper i Teknologiparken gjør det, som GKN, som produserer jetmotorer. Og vi har Servi Group. De produserer hydrauliske ventiler for offshore. Aktuatorer og ventiler. Disse produktene er modellert i et verktøy som

dette. Og deretter produsert direkte.

Bearbeidingsmaskinene er ganske imponerende, komplekse maskiner.

-Ja, med ekstremt høy nøyaktighet. 3D-utskrift er den nyeste teknologien innen produksjon - "additiv produksjon." I stedet for å fjerne ting, legger du til ting. Du former en ny del direkte. Og du nevnte prototyping. Det er det 3D-utskrift brukes mest til nå. Men 3D-skrivere brukes også til produksjon. Den plastskriveren vi har her, er en typisk prototype 3D-skriver. En rask og enkel måte å lage en modell på. Så kan du montere den og sjekke resultatet. For å se om den virkelig er som modellen du ser på skjermen. I 3D-utskrift har du en plasttråd som blir ekstrudert gjennom en tynn dyse. Det finnes mange forskjellige typer 3D-skrivere, men vi har en av disse her.

En plasttråd går gjennom en dyse som smelter plasten, som faller ned på en plate som beveger seg i et 2D-mønster.

- Ja, først én gang, deretter hever den seg litt og legger et nytt lag. Mange tror dette er fremtiden innen produksjonsteknologi. Og noen 3D-skrivere kan allerede produsere brukbare deler. De skriver nå ut titanium, stål og mye plast. De skriver også ut deler med kretskort inni. Der loddet de på komponenter. De printer huset rundt det.

I Ringerike, Norsk Titan, 3D-printer titanium. Deler som er brukbare.

-Ja, de produserer robuste titaniums-braketter. Og Tronrud Engineering, ved siden av dem, har en annen type titan 3D-skriver. De bruker pulver.

Pulver som smelter? - Ja. Lag med pulver. Og en laser smelter pulveret.

Trenger du en spesiell atmosfære for det? Gass eller vakuum?

-Ja, det må være i en kontrollert atmosfære. Og det krever etter-bearbeiding. En av svakhetene til 3D-utskrift er overflaten. Du får en grov overflate. Du trenger ofte etterbehandling av overflaten, som gjenger osv. Men det gjør det mulig å lage dine egne geometrier.

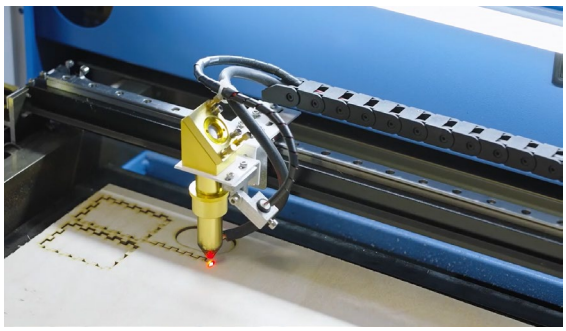
Fordi 3D-utskrift gjør det mulig å produsere deler som du ikke kan produsere med CNC?

-Ja. Det gir deg stor grad av geometrisk frihet.

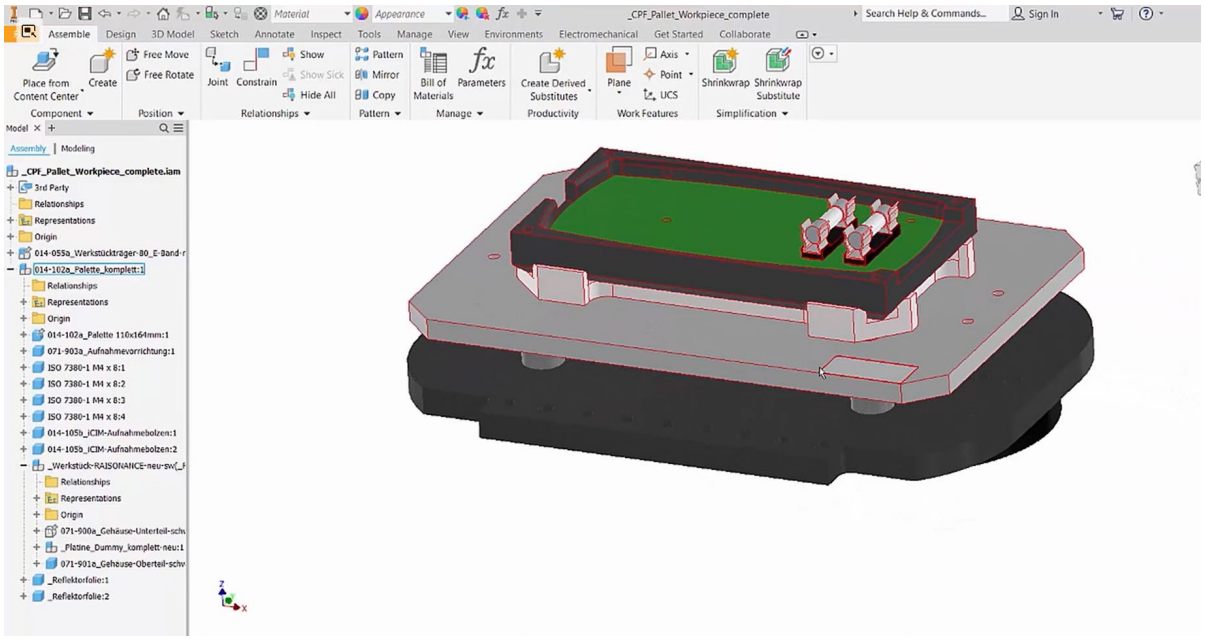
Interessant. En liten avsporing. Jeg var på et møte med hærens tekniske støtteavdeling. I Bjerkvik i Narvik har de en installasjon. Der har de reservedeler for hæren i Nord-Norge. I stedet for å ha store lager vil de bare skrive ut delene de trenger.

-Jeg hørte på en NASA-podcast at når de skal til mars, tar de med seg en 3D-skriver i stedet for reservedeler, og lager dem selv. Data veier ingenting. Og du skriver bare ut det du trenger når du trenger det.

Men mange skrivere er ganske trege, i hvert fall for øyeblikket. Utskriftsprosessen tar tid. Men det spiller ikke så stor rolle hvis du er på ISS og må vente på Space Shuttle. Da må du bare vente til den begynner å fly igjen.



Figur 37: Laser cutting.



Figur 38: Pallerte som danner plattformen for montering av et produktt.

Dette er spennende. Vi nevnte akkurat laserskjæring. Det er en mye brukt teknologi, både for hobbyister og kommersielt.

Ja, både laserskjæring, vannskjæring, plasmaskjæring og 3D-utskrift fungerer på lignende måte. Du har koordinater som det følger, og deretter skjærer du materialene i henhold til deres egenskaper.

På skolen vår har vi laser-skjærere. Det er 2D. Vi skjærer spor i tre, glassfiber eller plexiglass. Deretter kan du gravere. Grunnlaget er det samme, enten det er 3D eller 2D. Forskjellen mellom laserskjæreren og 3D-skriveren er at 3D-skriveren går opp ett trinn av gangen.

-Ja, den bygger lag. De er ganske like, men den har en ekstra dimensjon.

Enda en akse?

-Ja. En av laserskjærerens fordeler er at den er veldig rask.

Er den raskere enn 3D-skriveren?

-Mye raskere. Men jobben er enklere. Den skjærer bare en spor, mens 3D-skriveren må gjøre det mange ganger.

Oppå hverandre?

-Ja. Den jobber raskt, og du kan bygge enkle, fine ting. Internett er fullt av sett som er skåret ut med laser-skjærere. Metall, tre. Du kan lage klokker og mye mer.

Og den er ganske rimelig også, så hobbyister kan kjøpe den. 3D-skrivere og laser-skjærere koster bare noen få tusen kroner nå. Jeg kjøpte en 3D-skriver fra Kina på Black Friday. Den kostet rundt 1000 kroner.

-Dette er spennende. Det er gøy å bruke et 3D-program. Hvis du modellerer noe du har tenkt på og starter fra bunnen av med en idé.

Veien fra en idé til noe nyttig er ganske kort?

-Ja. Og med dette programmet og en 3D-skriver er det ganske enkelt å få det til. Jeg har snakket med mennesker som jobber med produksjon og markedsføring av dette. Det er en parameter som kalles "time to market". Tiden det tar fra du får en idé til produktet er til salgs. Det går raskere

og raskere. Så en av konkurranse-parameterne er å redusere den tiden. Komme til markedet så raskt som mulig. Hvis du er først, vinner du, forutsatt at du har riktig markedskonfigurasjon. Dette er avgjørende i store selskaper. Verktøy som dette reduserer den tiden.

-Ja. Og kostnadene må kuttes.

Hvis du har laget én modell, er det lett å lage en ny modell. En ny versjon av den.

-Ja. Hvis du har et vinnende produkt, bør du oppgradere det ofte for å utvikle markedet ditt. Slik når du nye mennesker og virker ikke gammeldags. Jeg tror vi er på iPhone 10 pluss nå. Men den prosessen går raskt. Du har eliminert mange feil i produksjonen din med all denne forberedelsen. Du kan simulere og beregne styrken. Du kan være ganske sikker på at det første produktet du lager, er førsteklasses.

Å designe produktet er én ting, men du må også tilpasse produksjonsutstyret til det produktet. For eksempel monteringsprosesser. Det er en parameter her. Denne modellen demonstrerer det. Du trenger en palett for at dette produktet skal stå i. Du har nesten designet paletten når du har designet produktet ditt.

Så er det på tide å sette opp produksjons-linjen. Vi har kvalitetssikret at telefonen ligger stødig på paletten sin.

-Riktig. Det er viktig. Paletten er standard. Og vi vil tilpasse den til produktet vårt. Vi kan lage forskjellige versjoner av disse som fortsatt passer.

Forskjellige farger?

-Ja. Og materialer.

Flott! Takk, Endre. Dette var opplysende. 3D-utskrift og 3D-modellering er viktige drivkrefter og teknologier innenfor Industri 4.0.

7. Digital tvilling

By Tommy Hvidsten

Nå skal vi se på dette spennende emnet som kalles "digitale tvillinger". En digital tvilling er en datamodell av et fysisk objekt.

Definisjonen av en digital tvilling er at det er en digital kopi av et bevegelig eller livløst fysisk objekt. En digital tvilling refererer til en digital kopi av fysiske og faktiske objekter, prosesser, mennesker, steder, systemer og enheter som kan brukes til ulike formål.

> *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*

- *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.*

Figur 40: Definisjonn.

Så, en digital tvilling kan være mange ting. Det kan være en digital tvilling av et menneske, deler av et menneske, maskiner eller systemer, men også prosesser, hendelser som skjer i naturen eller i en produksjonsbedrift.

Vi bruker fysiske simuleringer, dataanalyse og i økende grad kunstig intelligens for å vise effektene av endringer eller påvirkninger på et produkt eller et system. På denne måten kan vi teste forskjellige måter et produkt eller en prosess kan

Figur 39: Adferden til en digital tvilling

brukes på, påvirkninger fra miljøet og endringer over tid.

Du kan sjekke slitasje på systemer ved hjelp av en digital tvilling. Dette kan redusere behovet for fysiske prototyper i utviklingsprosessen. Dette kan redusere utviklingstiden og forbedre kvaliteten på det ferdige produktet eller prosessen. So, it can be a tool in a developmental process. Imidlertid kan en digital tvilling brukes gjennom hele levetiden til et produkt eller

en prosess. Vi kan forbedre datamodellen, kjernen til den digitale tvillingen, ved å samle data fra 'den fysiske tvillingen' av datamodellen. På denne måten kan modellen forbedres, vi kan se utviklingen over tid, og vi kan simulere ting som vedlikehold og lignende.

- *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 41: Three main applications of digital twins.

Vi bruker dem for å sikre effektiv utvikling av nye produkter. Vi kan også simulere bruken av produkter, inkludert i perspektivet av levetiden. I produksjon kan vi bruke digitale tvillinger i monterings-prosesser, der vi kan optimalisere prosessene før vi produserer dem på fabrikken. Vi kan teste produkter og kanskje endre dem før de blir produsert. Vi kan simulere hva vi må gjøre i produksjonsutstyret vårt for å lage nye, endrede produkter. Vi kan også simulere flaskehalser, slik at vi kan se hvor ting blir "trange". Og deretter iverksette de riktige tiltakene for å forbedre flyten i produksjonen. Og optimalisere både produksjonsvolum, kostnader og kvalitet.

Ytelse: Digitale tvillinger kan brukes til å samle inn og analysere driftsdata. Dette vil gjøre det mulig for oss å ta beslutninger basert på data fra den digitale tvillingen.

Her er et eksempel: Ved å lage digitale tvillinger av fly og jetmotorer kan du forutsi vedlikeholdsbehov på et helt nytt nivå. Standarden innen luftfart er at etter en viss mengde flytimer, la oss si 500, får jetmotoren sin generelle vedlikehold. Vanligvis kan motoren gå mye lenger enn det, men reglene er slik at du må gjøre det uansett om motoren trenger det eller ikke. Litt som EU-kontroll for bilen din.

Med en digital tvilling kan du forutsi når vedlikeholdsbehovet vil oppstå og planlegge å gjøre det når behovet begynner å oppstå. Denne metoden har vist seg å eliminere mye nedetid for fly, slik at de kan fortsette å fly i stedet for å vente på bakken for "unødvendig" vedlikehold.

Nå, her er noen eksempler. Kunder er viktige for alle selskaper, og de kan påvirke både produkter og hvordan selskapet ditt produserer dem. En digital tvilling kan hjelpe oss med å teste ulike kundeopplevelser. Vi kan bruke den digitale tvillingen til å demonstrere hvordan et produkt vil være. På en måte er det et kommunikasjonsverktøy som du, sammen med kunden, kan bruke til å utvikle både nye produkter og nye tjenester. Optimalisering.

En digital tvilling kan hjelpe deg med å finne alle slags optimale prosesser. Vi vil for eksempel gjøre produksjonsprosessene så effektive som mulig og oppnå høy kvalitet så kostnadseffektivt som mulig. Et annet eksempel på optimalisering som de gjør i et

- ***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 42: Examples for digital twin application.

nytt NASA romprogram, planlegger de å reise til Mars, og ved å bruke digitale tvillinger kan de simulere utstyr om bord i et romskip og teste løsningene på jorden på en digital tvilling før de implementeres i romskipet.

Vedlikehold kan gjennomføres på samme måte. Utstyrets funksjonalitet om bord i romskipet kan også endres underveis. Hvis en digital tvilling hadde vært tilgjengelig da Apollo 13 fikk problemer, ville det ha vært enklere å finne de nødvendige løsningene. I filmen "Apollo 13" samlet de alt om bord for å se om de kunne bruke noe av det til å fikse luftforsyningen og andre problemer. De fant innovative løsninger, som å bruke tape, binders, plast og annet om bord for å løse utfordringene.

På en måte var det "digital tvilling, Industri 2.0", men i dag kan dette gjøres med mye større presisjon ved å bruke egnede digitale tvillinger.

Enda et eksempel er digital maskinbygging der du kan simulere en maskin. Hvis firmaet ditt bygger maskiner, som dette som produserer emballasjemaskiner, så lagde de digitale tvillinger av maskinene sine.

På den måten kunne de, sammen med kunden, sette opp maskinen for å møte en spesifikk kundes behov, fordi du ofte må tilpasse utstyret ditt i henhold til dette. De kunne teste det og deretter vise kunden resultatet. Når den prosessen var ferdig, kunne de bygge akkurat den maskinen kunden ønsket.

Dette forenkler spesifikasjonsprosessen med kunden og hele prosessen blir mer effektiv.

Helsetjenesten bruker digitale tvillinger til å simulere driften av sykehus. Med en datamodell tester de ulike metoder for å drive sykehus. Logistikken på et sykehus er ganske krevende.

Du kan teste ideer på digitale tvillinger først for å finne de beste løsningene. Da får du en ganske god ide om hvordan ting kan gjøres. I medisinsk bruk kan kirurger lage digitale tvillinger av organene de skal operere på. Da kan de øve før de utfører prosedyrene på pasientene. Forholdene de skaper vil være veldig lik virkeligheten. Dette hjelper med å gjøre prosedyrene tryggere.

Byer kan også simuleres. Digitale tvillinger brukes til å undersøke bærekrafts-parametere over tid og rom. Hvordan vil en by utvikle seg over tid? Hvor bærekraftig kunne den være ved å innføre ulike tiltak, som å sortere gjenvinnbart avfall? Hva kunne konsekvensene av slike tiltak være? Hvordan ville det påvirke byens bærekraftighet? I Singapore har de en "virtuell Singapore", det vil si en digital tvilling av Singapore. Det er en del av et program de kaller "Smart Nation Singapore". Det er verdens første digitale tvilling av en bystat, som er hva Singapore er.

Vi har nevnt vedlikehold. Digitale tvillinger kan analysere effektivitetsdata som er lagret over tid under ulike forhold. Du kan lage en god digital tvilling som er "beriket" og optimalisert med data fra virkeligheten. Da kan du simulere driften over tid, og du kan finne ut hvor problemene ligger. Hvilke komponenter vil slutte å fungere først, og når vil det skje? Et utmerket verktøy for vedlikehold.

Dette er noen eksempler på digitale tvillinger. Hva er forskjellen mellom en digital tvilling og en simulering? De har mye til felles. Men en digital tvilling er koblet til virkeligheten ved å samle inn virkelige data, og kan operere under de samme forholdene som sin "fysiske tvilling" av det samme systemet eller produktet. Vi skal se på simuleringsverktøyet Ciros på laboratoriet. Det er ikke koblet til virkelighetsdata, men det viser hvordan en digital tvilling kan fungere. Det er ikke akkurat en digital tvilling, men det demonstrerer godt hvordan laboratoriets fysiske utstyr kan simuleres og kjøres i en datamodell. Og med denne digitale tvillinglæreren her, skal vi dra til laboratoriet for å se hvordan vi kan bruke en "digital tvilling" der.

- ***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 43: Examples for digital twin application.

Appendix

List of figures.