TEMANUMMER FOR DAu-BLADET

GODE DATA

9898AA

DAu
NO 3 • SEPTEMBER 2017

VIGTIGE DATA, RIGTIGE DATA OG USIKRE DATA

AF JACOB HERBST, CTO, DUBEX A/S

I gennem de sidste 20 år har mit arbejde været at passe på data, og på alle måder er det en endnu vigtigere opgave i dag end nogensinde før. Mængden af data er eksploderet, og vi har i dag uendelig mængder data, om næsten hvad som helst. Mange virksomheder har fået øjnene op for, at disse data kan bruges til at udvikle forretningen og målrette produkter og services til den enkelte kunde. Samtidig kan data bruges til at optimere arbejdsprocesser og trimme systemerne og dermed være med til at spare tid og penge. I mange situationer er data desuden nødvendige for at dokumentere, at vores produkt er, som det skal være – og uden disse data har vores produkt ingen værdi. For mange virksomheder kan data altså være mere værd end guld.

> Vi mangler ikke data. Udfordringen er derimod, at finde ud af, hvordan vi får brugt vores data bedst muligt – og hvordan vi beskytter dem. For når data bliver så vigtige, betyder det også, at hvis vi ikke har adgang til data eller data er forkerte, bliver vores beslutninger også forkerte – og potentielt ganske bekostelige.

Jeg arbejder til hverdag med it-sikkerhed og har traditionelt arbejdet med databeskyttelse ud fra den i sikkerhedskredse så kendte CIA-model: Confidentiality, Integrity og Availibility. Modellen tager udgangspunkt i at,

- data er fortrolige, kun dem vi ønsker må kende data gør det
- data er korrekte, så vi kan stole på dem
- data er tilgængelige, når vi skal bruge dem.

Det er tre simple og dybest set ret banale krav at stille til vores data, men det er også vigtige krav, hvis vi skal have værdi af vores data.

CIA-modellen fokuserer primært på, hvordan vi beskytter de data, vi allerede har, og ikke så meget på hvordan data skabes. Erfaringen viser dog, at det kan være en meget stor udfordring i sig selv. Som regel er vi i en situation, hvor der er flere sider af virkeligheden – de opsamlede data er ikke entydige, og afhængig af hvor og hvordan vi måler, risikerer vi at få forskellige resultater. Disse variationer kan vi måske leve med, når data bliver brugt passivt til eksempelvis rapportering, men efterhånden som flere og flere processer fungerer automatisk i realtid baseret på data der opsamles, er det vigtigt, at vi har styr på kvaliteten af data. Med forkerte data tager vi de forkerte beslutninger.

En anden udfordring, jeg ofte støder på er, at virksomheder har store mængder data, som de aldrig ser på. Eksempelvis har mange virksomheder nærmest uendelige mængder logdata fra deres systemer, men der er aldrig nogen, der ser på dem. Det betyder, at vigtig information om aktivitet på netværket ikke opdages. I it-sikkerhedsbranchen oplever vi nærmest dagligt virksomheder, der er blevet kompromitteret eller har mistet data – ofte igennem en længere periode. Det er hændelser, der med den rette overvågning kunne være forhindret eller i hvert fald stoppet meget hurtigere.

Behovet for overvågning og behandling af data bliver ikke mindre fremover, da hele udviklingen frem mod Internet of Things og Industri 4.0 er drevet af dataopsamling. Før vi når dertil, skylder vi os selv at stoppe op og tænke på, hvordan vi får kvalitet i vores data og rent faktisk får udnyttet dem. Jeg er sikker på, at der findes eksempler fra alle brancher på, at vi ikke bruger vores data ordentligt og dermed ikke får værdi af dem. Skal vi udover det problem, skal der investeres ligeså meget energi i at udnytte vores data som i at fremstille dem.

> Vi mangler ikke data. Udfordringen er at finde ud af, hvordan vi får brugt vores data.

DAU **DANSK AUTOMATIONSELSKAB** • **SEKRETARIAT** DI DIGITAL • 1787 KØBENHAVN V • TELEFON 3377 3377 • DAU@DAU.DK • WWW.DAU.DK
REDAKTION HENRIK VALENTIN JENSEN • DI DIGITAL • **LAYOUT** FRU NIELSENS TEGNESTUE • **TRYK** KAILOW GRAPHIC A/S • ISSN 1601-6750

STOL TRYGT PÅ DE ANDRES DATA

DU KAN VÆRE SIKKER PÅ ÆGTHEDEN AF DE DATA DU FÅR VED AT BRUGE BLOCKCHAIN.

AF FRANK FAURHOLT, SIEMENS, FORMAND FOR DAU

Blockchain er en teknologi, der kan være interessant i mange sammenhænge, også indenfor automation og produktion. Særligt i disse Internet of Things (IoT) tider, er Blockchain et vigtigt tema.

Det, der gør Blockchain interessant, er at det er en teknologi, der kan være med til at sikre, at vi stoler på ægtheden af data, også når de udveksles automatisk mellem kommercielle parter. Parter der både kan være privatpersoner, virksomheder og "ting", og så er vi jo tilbage til Internet of Things.

Blockchain er en teknologi, der via komplekse algoritmer og en decentral valideringsmekanisme, sikrer, at de data der udveksles mellem medlemmerne af en Blockchain gruppe, ikke er blevet manipulerede og dermed fortsat er valide. Det er en teknologi, der overflødiggør den berømte "trusted middleman" som fx kunne være en bank, og gør at reelle kommercielle værdiersåsom penge men også kommercielle kontrakter, beskrivelser indeholdende IP rettigheder etc. an udveksles direkte mellem deltagerne i Blockchain gruppen.

Teknologien og ikke mindst use cases er på et tidligt stadie indenfor vores område, men fx indenfor Smart Grid (energi produktion, transmission, distribution og forbrug) dukker de første spændende eksempler nu op. Eksempler hvor private el-biler og private solcelleanlæg indgår i en kommerciel sammenhæng, og hvor afregning mellem de deltagende parter sker automatisk og i realtid.

Et andet interessant eksempel er, hvor en gruppe af Blockchain deltagere fx ønsker at følge kvaliteten under produktion, transport og drift af en given vare, komponent eller maskine.

Kunden ønsker valide data (dokumentation) på, at det indkøbte produkt er produceret jf. de aftalte design og kvalitets specifikationer, og at produktet er transporteret jf. specifikationerne (temperatur, fugtighed, stød/vibrationer, tid etc.).

Leverandøren ønsker at sikre at transportfasen forløber korrekt og at kunden arbejder korrekt med maskinen. Dette kan være meget relevant i forhold til fx garantiforpligtelser.

Transportleverandøren ønsker at kunne dokumentere, at transporten er forløbet jf. specifikationerne, for derved at kunne håndtere eventuelle transportskader og reklamationer på en endnu mere professionel måde.

En Blockchain gruppe indeholdende disse tre parter, kan være med til at sikre at håndteringen af ovenstående scenarie sker automatisk, elektronisk, billigt og i realtid og at troværdige data er tilgængelige for alle tre parter.

Her vil de enkelte automationsløsninger, med det nødvendige måleudstyr og kommunikationsmuligheder, være forudsætningen for en Blockchain anvendelse.

I en Industry 4.0 sammenhæng, er fokus også på at "ting" arbejder smart, autonomt og kommunikerer via internettet. Her har vi jo – med god grund fokus på Industrial Cyber Security – men det er også vigtigt, at vi kan stole på validiteten af de data, der kommunikeres på en sikker måde. Vi taler ofte om "as a service" som en af de kommende forretningsmodeller,. As a service forretningsmodellen forudsætter, at leverandøren og kunden har et fælles billede af den serviceydelse, der leveres, og at de begge stoler på hinanden.

Blockchain er med til at sikre et fælles billede og tillid – ingen kan snyde. I dag vil man jo bl.a. skulle stille en bankgaranti, eller deponere penge hos en "trusted middleman". De skal begge online og i realtid kunne se kvaliteten af denne service, og evt. også afregne kommercielt via Bitcoin. Når vi taler om digitalisering, den 4. industrielle revolution, taler vi også om den digitale tvilling. Når fysiske ting har en digital tvilling (eller er det omvendt?) skal både mennesker og "andre ting" kunne stole på den digitale tvillings data. Også her bliver anvendelsen af Blockchain en central del af videreudviklingen af Internet of Things teknologierne og forretningsmodellerne. Man taler fx ofte om "værdikæder", men så skal vi igen kunne stole på, at data har en valid værdi.

Træerne vokser som bekendt ikke ind i himlen, og der er fortsat mange spørgsmål forbundet med anvendelsen af Blockchain. Dette både relateret til teknologi, omkostninger, jura og forretningsmodeller. Blockchain bygger på konsensus princippet, der i teorien skal forhindre, at en deltager snyder, da de andre deltagere i Blockchain gruppen vil opdage det, men hvad nu hvis 51 % af deltagerne beslutter sig til i fællesskab at manipulere med valideringsmekanismerne Ligeledes giver en digital sikkerhed via Blockchain jo ingen mening, hvis deltagerne ikke kan stole på, at den grundlæggende fysiske måling er foretaget efter forskrifterne (kalibrering etc.) og at konverteringen til den digitale repræsentation er sket korrekt.

Det bliver spændende at følge udviklingen indenfor dette område, fordi Blockchain er med til at kommercialisere den nye teknologi, og dermed skabe nye forretningsmodeller

GEM DE DATA ORGANISATIONEN KAN FÅ BRUG FOR

VED AT GIVE ANSVAR OG EJERSKAB FOR EGNE DATA OG ET GOVERNANCE FORUM, KAN MAN BEDRE SIKRE, AT DATA DER ER RELEVANTE UD I FREMTIDEN, BLIVER GEMT.

AF KARSTEN HVALKOF ANDERSEN, DONG

I automationsbranchen er der mere og mere opmærksomhed på Big Data, og dagens tekniske ICS systemer og databaser understøtter i høj grad indsamling og storage af meget store datamængder, der ofte viser sig værdifulde i optimeringen af forretningen. Dette gælder ikke kun data fra administrative systemer, men også realtids data, som kan hentes fra ICS systemerne.

ICS systemer er f.eks. SCADA systemer til styring og overvågning, PLC (Programmable Logic Controller), RTU (Remote Terminal Unit) eller BCU (Bay Control Unit)

En stor udfordring ved Big Data er, at man ikke nødvendigvis ved hvilke data der kan skabe værdi for forretningen i fremtiden, og det er derfor svært at definere, hvad der skal opsamles og ikke opsamles i databaser på tidspunktet for design og engineering af ICS systemerne. Derfor vil der være en naturlig tendens til at gemme alle tilgængelige data "for en sikkerheds skyld", gerne med så stor opsamlingsfrekvens og med så stor præcision som muligt.

Det vil naturligvis fordyre ICS systemerne, og det er meget svært at lave en business case, der anviser et optimum for opsamlings-scope. Men en endnu større udfordring ligger i at sikre overblik og datakvalitet for alle disse data, der muligvis ikke er forretningskritiske til en start, men sidenhen kan vise sig at blive det.

Som eksempel kan jeg nævne availability data for power-produktion i en vindfarm. Gennem tiden er availabilty beregningen blevet forfinet, for at give et mere retvisende billede af anlæggenes oppetider, og for at kunne placere og fordele ansvar for nedetid hos hhv. driften og leverandøren af

> En stor udfordring ved Big Data er, at man ikke nødvendigvis ved hvilke data der kan skabe værdi i fremtiden. Derfor vil der være en naturlig tendens til at gemme alle tilgængelige data "for en sikkerheds skyld".

vindturbiner. Det har betydet, at data, som i starten var ukritiske, er gået hen og blevet en kritisk del af beregningen. Konkret drejer det sig om alarmdata, der viser om der er tale om en fejl på turbinen, hvor ansvaret ligger på leverandørsiden eller ej. Det har så vist sig, at nogle af disse data ikke er blevet opsamlet robust, men at der er store huller i datamaterialet, og at teknikken til data-opsamling er baseret på skrøbelig og ufleksibel OPC teknologi.

Man kan naturligvis rette op på det og opdatere systemer og data-strategi, men det viser sig i praksis, at der er et konstant behov for at modernisere og tilpasse dataprotokoller og databaser, for at få kvaliteten forbedret på de nødvendige data. Desuden vil historikken for de nye beregninger være svær at etablere, eftersom den baserer sig på gamle fejlbehæftede data, der ikke kan genskabes. Denne historik er vigtig for at kunne spore performance af anlægsdriften ud fra disse data, så man kan vurdere effekten af forbedringer i anlægsdriften på konkrete og sammenlignelige data.

Hvorfor er dette problem så opstået, og hvordan kan man undgå at gentage fortidens synder. Her er mit svar, at det altid er nødvendigt at tilknytte et organisatorisk data- og system-ejerskab til alle data, der opsamles og til alle ICS systemer, der installeres, og dette skal ske selv om der ikke er et øjeblikkeligt behov for alle de opsamlede data i organisationen. Grunden til, at problemet er opstået, er at et sådant data-ejerskab ikke er blevet defineret i sin tid, hvor data-opsamlingen blev etableret.

Konceptet har flere fordele:

1. Den dataansvarlige skal sige god for alle data-opsamlinger, og eftersom vedkommende bliver gjort ansvarlig for specifikation, kvalitet og tilgængelighed vil der komme en meget sund beslutningsproces om hvad der skal opsamles, og hvad der kan have fremtidigt potentiale. Organisationen tvinges til at tænke fremad, og der kommer en naturlig begrænsning på hvad der opsamles og med hvilken opløsning, kvalitet og robusthed det skal gøres, så ICS og databaser ikke under- eller overdimensioneres.
2. Overblik over tilgængelige data, og planer for udbygning vil være placeret ét sted i organisationen, hvorved alle nuværende og kommende interessenter har ét sted at henvende sig.
3. Èt sted hvor Lessons Learnt og parkerede ønsker til kommende systemopdateringer og datastrategi kan samles sammen til "næste version"

Funktionen vil nok være bedst placeret det sted i organisationen, der har økonomisk og forretningsmæssigt ansvar, idet man her har incitament til at sikre gevinst af Big Data ar-

bejdet, og balancere det med omkostningen ved ICS og database engineering. Hvis man placerer data og system ansvaret f.eks. i IT afdelingen, vil der ikke være samme incitament til en balanceret beslutningstagen. Det kræves naturligvis at der ikke kun kigges på den øjeblikkelige drift, men at virksomhedens forventede strategi og KPI'er i en god tid fremover tages med i beslutningen om dataopsamlings-scope.

Den data-ansvarlige skal derfor samarbejde bredt i virksomheden med såvel IT afdelingen som forretningsudviklerne, så han kan producere en data-strategi.

De samme betragtninger som ovenfor gælder meget enslydende for placering af ICS systemansvar i organisationen. Udførelse af teknisk vedligehold i driften af ICS systemerne kan uddelegeres med diverse SLA aftaler med interne og eksterne IT support organisationer, men ansvaret for funktion og vedligehold bør ligge hos den forretningsansvarlige.

Endelig skal man ikke glemme linket mellem ICS system- og data-ansvar. Dette skal være synligt på den måde at de datagenererende ICS systemer skal linkes sammen med de data, de genererer, så man let kan lave en konsekvensanalyse, når man opdaterer enten ICS systemet eller den tilknyttede data-opsamling.

En vigtig fællesnævner for data og ICS systemer er security. Her er det vigtigt, at man igen har en central funktion med en tilknyttet Governance-model, der rækker såvel ud i omverdenen som ind i organisationen så man tilgodeser såvel:

1. Eksterne krav, standarder og lovgivning
2. Behovet for én Intern myndighed, der fastsætter ICS security requirements og kan tage dialogen om fortolkninger af disse med alle interessenter i organisationen

Dette organ skal så samarbejde med udnævnte security ansvarlige i de forretningsgrene der bruger ICS systemerne i dagligdagen, så man lokalt kan udfærdige de nødvendige disaster-recovery planer, processer for fysisk og remote ICS system-adgang, opdatering og patch-planer, brugeradministration, risikovurdering osv. Der skal udfærdiges et operationelt og compliant regelsæt, en procesbeskrivelse og en uddannelse, som medfører en passende høj KSI score på ICS security samtidig med en smidig systemadgang til de autoriserede brugere.

Ovenstående anbefalinger om sikring af ejerskab og governance for data, systemer og security udspringer af, at de fleste moderne virksomheder konstant udvider deres system og dataanvendelse i driften og forretningsudviklingen, og i højere og højere grad bliver afhængige af dette. En manglende koordinering af aktiviteterne som beskrevet ovenfor viser sig for det meste som root-cause for data-tab, ukompatible ICS systemer og security mangler. Indsatsen er beskeden og gevinsten er stor.

ICS: Industrial Computer Systems.
OPC: OLE for Process Control
OLE: OLE/COM teknologi fra Microsoft indenfor datakommunikation.

AF FLEMMING HØJSKOV ANDERSEN, SEKTIONSCHEF FOR FORRETNINGSUDVIKLING, BANEDANMARK

DIREKTØREN SKAL BYGGE BRO MELLEM OT OG IT

SUCCES MED AT KOMBINERE OT OG IT STARTER I ORGANISATIONEN FREM FOR I MASKINRUMMET.

Driver man en automatiseret produktionsvirksomhed og ser på trends som Industri 4.0, er man næppe i tvivl om, at man har en af de større ledelsesudfordringer. Diskussionen om OT vs. IT er intens og dagsordensættende emner som Big Data, Analytics og IoT, flytter gradvist virksomhedsperspektivet fra en produktionscentreret i retning af en informationscentreret aktivitet.

OT OG IT – HVORFOR FORSKELLEN?

Typiske OT- og IT-miljøer adskiller sig ved at have forskellige formål, operative procesmodeller og arkitekturer. Ingen er mere rigtige eller forkerte, for de har udviklet sig i årtier som funktion af forretningsbehov og muligheder.

IT har imidlertid haft stor vækst i anvendelse og performance efter årtusindeskiftet og ledelserne ser nu et behov for at "digitalisere" forretningen og skabe eller indgå i informationsbårne økosystemer fordi det har potentiale.

De tekniske implikationer er ikke ligetil at løse. Historisk er OT f.eks. præget af operativsystemer som først var indlejrede og proprietære (60'erne og 70'erne), derpå kommercielle operativsystemer men proprietært indpakket og beskyttet (80'erne og 90'erne) og sidenhen blev de IP-adressable (00'erne). Det sidste betød løbende indtog af teknologier fra IT-domænet. Typisk dog stadig med et netværksmæssigt "luftgap" mellem OT- og IT-systemer, som sikrede OT's fokus – oppetid og tilgængelighed. En afgørende udfordring er nu, at OT bliver forbundet til internettet og øvrige systemer, som i formål, driftsprocessser og arkitektur har deres oprindelse i IT-domænet hvor tænkningen har været en anden.

BROBYGNING

Situationen er mange steder, at topledelsen har besluttet, at gøre sin virksomhed datadreven og "IoT-enabled". Nu bliver den videre færd nemt til en teknologidiskussion. Historiske forskelle og fordomme mellem OT og IT ses som barrierer. Spørgsmålet er dog om ikke den administrerende direktør skal starte et andet sted end teknikken?

Skal han lykkes med konstruktiv koordinering og sidenhen integration af OT og IT for at nå sine mål, skal han først kigge på organisering, kompetencer og driftsprocesser. Virker organiseringen fremmende eller blokerende for at opnå målet? Det giver ikke mening at have organisatoriske ansvar, som er silo-opdelt på OT og IT, hvis værdikædens infrastruktur og informationsstrømme reelt forekommer i et kompliceret mix fra de to verdener. Ejheller virker det befordrende for, at medarbejderne forlader respektive ståsteder og udvikler mere hybride kompetencer.

Man ændrer ikke med et snuptag OT-miljøets fornyelsescyklus på 10-15 år til de 4 år, som er typiskfor, hvornår IT har skiftet det meste af butikken. Men via anderledes organisering og ændrede kompetenceprofiler kan man gradvist mindske modsætninger og finde løsninger. Kunne man forestille sig, at en IT-chef og en Teknisk Chef blev til én rolle – en Teknologichef – blot ét eksempel på konstruktiv kortslutning af konkurrerende silo-ansvar. Ville Teknologichefen have bedre incitament for at kigge på værdikæde og opdyrke hybridkompetencer hos medarbejderne? Ja.

Den administrerende direktør skal arbejde med sin organisation, for at opnå drømmen om, at der flyder nær-realtidsdata mellem produktionen og hans ERP-system. Dernæst skal han sikkert igennem frustrationen over, at data er elendige. Så gode, at de kan føre til effektiv planlægning, er de først når der ikke længere er nogen i organisationen, som diskuterer konflikten mellem OT og IT, men fokuserer på de anvendte teknologiers bidrag til virksomhedens værdikæde. Når det sker, er der indtruffet en tilstand, hvor det eksistentielle formål, de tekniske procesmodeller og de anvendte arkitekturer er mere ensartede end dengang OT og IT blev defineret som modsætninger.

AUTOMATION SIKRER AT CHR. HANSEN PRODUCERER I DANMARK

AF HENRIK VALENTIN JENSEN, DI DIGITAL

ROBOTTERNE KLARER DET KEDELIGE ARBEJDE OG MEDARBEJDERNE DET SJOVE. DET GIVER VÆKST OG FLERE ARBEJDSPLADSER FOR CHR. HANSEN.

Ikke alene sikrer Chr. Hansen's robotter og automationsanlæg, at virksomhedens produktion kan forblive i Danmark, de har også udvidet deres kapacitet.

FRYGT UBEGRUNDET

Chr. Hansen investerer i automation for at være konkurrencedygtig, og det får virksomheden til at vokse og skabe arbejdspladser. Frygten for at miste jobbet, som medarbejderne kunne have i forbindelse med robotter, har virksomheden taget fat på:

- I starten har vi brugt en del kræfter på at forklare vores medarbejdere, at robot og teknologi ikke nødvendigvis er en trussel mod deres arbejdspladser og det har vi fået overbevist vores medarbejdere om ved, at de kan se, at vi faktisk lykkes med at skabe arbejdspladser, siger Torsten Steenholt, Executive Vice President, Global Operations, Chr. Hansen i en youtube video DI's digitaliseringsindsats har lagt på nettet.

Uden dette havde Chr. Hansen ikke kunne blive i Danmark på lidt længere sigt, forklarer Torsten Steenholt i videoen, og understreger, at udviklingen kommer af automatik og robotløsninger. For medarbejderne har det været en positiv udvikling. I stedet for det trivielle og gentagede fysiske arbejde, robotterne nu udfører, overtager medarbejderne mere administrative processer, overvåger processerne og kvalitetssikrer dem.

FORDOBLER KAPACITETEN

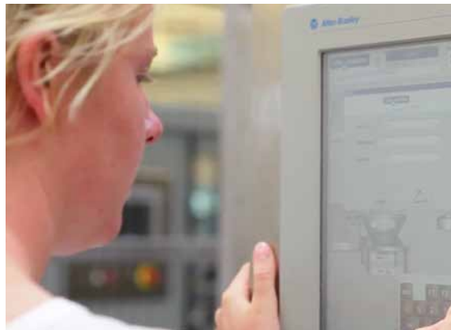
Chr. Hansen vil med de seneste tiltag fordoble outputtet og kapaciteten fra deres fabrik i Danmark. Den er allerede nu verdens største til at producere mælkesyrebakterier. Med mere og mere teknologi, mere og mere automatik, får virksomheden flere og flere arbejdspladser i Danmark.

Dermed indgår eksemplet fra Chr. Hansen i den løbende debat af, om automatisering og robotter skaber arbejdsløshed som vi ser denne udvikling af teknologi i dag. De positive erfaringer kan genfindes i en række andre virksomheder, og generelt er der ifølge Erhvervsministeriet en positiv sammenhæng mellem digitalisering og produktivitet i danske virksomheder. Noget af forklaringen kan være, at der også skal mennesker til at betjene robotter og at robotter og automatisering gør medarbejdere mere produktive. Det er vigtigt, eftersom produktivitet er en af de vigtigste faktorer i konkurrencen.

ANBEFALINGER

DI's Digitaliseringsindsats med det slående navn 'Vind fremtiden' skal frem mod udgangen af 2017 indsamle og udvikle politiske og virksomhedsrettede anbefalinger, som kan løfte digitaliseringen i Danmark og sikre, at disse anbefalinger fører til konkret handling.

Videoen fra DI's Digitaliseringsindsats kan ses på: youtube.com/watch?v=bOokx_4QGWY



DE SOCIALE KONSEKVENSER AF INDUSTRI 4.0 SKAL KENDES

DEN SOCIALE KAPITALFOND SER PÅ, HVAD DER KAN GØRES FOR MENNESKER PÅ KANTEN AF ARBEJDSMARKEDET.

AF KRISTIAN THOR JAKOBSEN, ANALYSECHEF OG
RUNE RIISBJERG THOMSEN, PROJEKTLEDER,
BEGGE DEN SOCIALE KAPITALFOND

Den fjerde industrielle revolution, tegner sig som en potentielt voldsom og disruptiv kraft på det danske arbejdsmarked. Analyser viser, at op mod 40 pct. af danske arbejdsfunktioner indeholder mange opgaver, der indenfor en overskuelig periode kan overtages af teknologier, vi allerede kender i dag. I en ny undersøgelse sætter Den Sociale Kapitalfond, i samarbejde med TrygFonden og Det Centrale Handicapråd, i 2017-18 fokus på konsekvenserne for de mennesker, der allerede nu er på kanten af arbejdsmarkedet og hvilke nye muligheder, der byder sig for dem på fremtidens arbejdsmarked.

UDSATTE GRUPPER

Vores indledende analyser viser, at udsatte unge, ufaglærte og mennesker med handicap er i særlig risiko for at se mange af deres arbejdsopgaver blive overtaget af digitale løsninger og robotter i fremtiden. Det er nemlig de rutineprægede opgaver, der ofte er trinbræt ind på arbejdsmarkedet, der står først for, når der introduceres nye teknologiske løsninger. Analysen bygger på nyeste registerdata samt samfundsvidenskabelig forskning inden for automatisering (Frey og Osborne).

Den indledende analyse bekræfter, i samklang med tidligere analyser fra McKinsey, Kraka og Cevea, at 40 pct. af danske jobs indeholder mange opgaver, der kan klares med teknologi, vi allerede kender i dag. Det svarer til omtrent 820.000 jobs, der primært består af repetitive arbejdsopgaver og ikke kræver særlige kreative evner eller sociale kompetencer. Den slags stillinger findes der mange af inden for f.eks. industriproduktion, kontor- og sekretærarbejde samt salgsarbejde.

UNGE PÅ KANTEN

For udsatte unge – det vil sige gruppen af ca. 20.000 unge uden uddannelse og med svag tilknytning til arbejdsmarkedet – gælder det, at 60 pct. af dem, som er er i arbejde, har et job med mange opgaver som kan overtages af ny teknologi. Også personer i fleksjob er i høj grad (47 pct.) ansat i jobs, der kan automatiseres. Disse jobs er især inden for administrativt sekretærarbejde og salgsarbejde.

Analysen har også kigget på grupper af mennesker med fysiske eller psykiske barrierer for at være en del af arbejdsmarkedet.

Ser vi på mennesker med muskelsvind, som et eksempel på en fysisk barriere, eller ADHD som eksempel på en psykisk, gælder det, at begge grupper har svært ved at finde fodfæste på arbejdsmarkedet. Samtidig har dem, som faktisk lykkes med at få job også i højere grad end gennemsnittet opgaver, der kan løses af teknologi.

Som samfund står vi altså med en udfordring, når de stillinger, der tidligere har givet adgang til arbejdsmarkedet for unge udsatte og personer uden uddannelse med stor sandsynlighed vil blive forandret radikalt eller helt forsvinde.

ET SKÆVT DANMARK

Vi finder samtidig, at en stor del af de job, der lettest kan erstattes med teknologi, ligger i Vestjylland og Vestsjælland – op mod 50 pct. af de beskæftigede borgere i nogle af disse kommuner. I den modsatte ende af skalaen finder vi storbykommuner og kommuner tæt på hovedstaden.

Det er et resultat af den danske erhvervsdemografi, hvor især industri- og produktionsjobs i små og mellemstore virksomheder findes i "udkantsområderne", mens de videnstunge jobs findes i de større byer.

Det betyder samtidig, at nogle vestsjællandske og nordjyske kommuner står med en dobbeltudfordring. De har både en stor gruppe borgere, der allerede står uden job, og samtidig har mange af dem opgaver, som kunne forventes ville blive automatiseret.

NYE MULIGHEDER

Der er således store udfordringer, men vi ved også, at nye teknologier vil betyde nye muligheder for personer på kanten af arbejdsmarkedet. Augmented og virtual reality vil give mulighed for opkvalificering af folk, der ikke finder sig godt til rette på skolebænken. Co-bots vil give muligheder i produktionsvirksomheder, for personer der ikke tidligere har haft fysisk mulighed for at tage disse jobs. Tale-til-tekst og virtuelle assistenter vil give nye muligheder for personer med bevægelses- og kommunikationshandicap.

CASES EFTERSPØRGES

Alt dette er noget, vi kigger nærmere på i resten af 2017. Vi eftersøger derfor cases fra virksomheder, der gør brug af teknologier til at inkludere flere medarbejdere eller opkvalificere nuværende, så også de kan få en plads på fremtidens digitaliserede arbejdsmarked.

> Det er de rutineprægede opgaver, der står først for, når der introduceres nye teknologiske løsninger.

REDAKTIONELT
STANDARDISERING

INGEN DIGITALISERING UDEN STANDARDISERING

Historisk har vi flyttet data fra analoge værdier henholdsvis papirform til digitale medier. Vi har skannet tonsvis af papirdokumenter og vi har opbygget utroligt mange specifikke databaser til alle vores data. Vi har "case by case" fortaget en 1:1 konvertering og vi har fokuseret målrettet på det specifikke scenarie. Vi har opbygget en masse digitale siloer, nogle vil kalde dem "black boxes".

Data skabes i mange situationer, fx både under engineeringsfasen og i driftsfasen. Vi har været rigtigt gode til at udvikle specifikke softwareværktøjer, der lige netop løser en specifik opgave. Vi har også opbygget vores organisationer, således at virksomhederne bliver specialiserede i at løse de konkrete opgaver som stilles.

SAMMENHÆNGEN GLEMT

Digitalisering er ikke et spørgsmål om at have fokus på den enkelte teknologi, proces eller indholdet i den enkelte database, det er et spørgsmål om at kunne se sammenhængen.

Der, hvor digitalisering bliver interessant, er når data bliver tilgængelige for andre dele af organisationen. Digitalisering er altså mindst lige så meget et spørgsmål om det digitale dataflow og workflow, som det er et spørgsmål om de enkelte data.

Det er lidt som at opleve at tågen letter, pludselig kan du se sammenhængen og træffe sikre og effektive beslutninger. Ting, der før var usynlige, og situationer der var umulige at finde hoved og hale på, optræder nu klare og tydelige.

Når vi taler om tåge, er det lidt sjovt at man nu bl.a. taler om fog (tåge) og cloud (sky) computing som væsentlige dele af Internet of Things. Her hentydes dog ikke til sigtbarheden, men mere til hvordan teknologierne anvendes i relation til den klassiske automationstrekant.

Formålet med at få sine data og evt. også sine applikationer op "i skyen" er bl.a. at gøre sine data transparente og tilgængelige for andre. Det er en mulighed for at frigøre data fra de klassiske on-site databaser, og få dem op, hvor man kan se sammenhængene.

Digitale data er blot en masse bits og bytes, Når dine digitale data i dag er nøje forbundet med den applikation, som du har installeret på din pc, og formatet er optimeret til netop denne applikation, så bliver tingene lidt tunge at arbejde med. Blot at flytte disse data op i skyen hjælper heller ikke meget. Det er først, når vi kan blive enige om fælles definitioner på dataformater, applikationsgrænseflader (API'er) og sikre kommunikationsformer, at skyen begynder at give mening.

Det er derfor, at standardisering er forudsætningen for digitalisering og derfor, vi i DAu har stor fokus på det felt.

RAMI 4.0 FOR INDUSTRI 4.0

Industri 4.0 er en ny og meget kompleks størrelse, som vi først nu er begyndt at kunne se konturerne af her i morgentågen. Vi har derfor brug for nogle fælles rammer for at kunne beskrive og forstå hvad der reelt gemmer sig bag Industri 4.0

Reference Architectural Model for Industry 4.0 (RAMI 4.0) er et nødvendigt skridt for at definere de enkelte komponenter i sammenhængen, samt hvordan de interagerer. Det er en fælles referenceramme, der gør at vi kan begynde at arbejde konkret med Industri 4.0 og gøre konceptet relevant for kommercielle automationsprojekter.

INDUSTRIAL CYBER SECURITY

Industrial Cyber Security er meget mere en blot at installere en firewall. Det er en kompleks størrelse, der omfatter både teknologier og politikker (governance). Det er noget som både produktleverandører, systemintegratorer og slutbrugere skal være enige om at håndtere på en ensartet og veldefineret måde.

GOD FORMIDLING

Nogle synes, at standarder er guds gave til menneskeheden, andre det er noget fanden har skabt. Uanset, hvad du mener, er der ingen vej udenom at sætte dig ind i de relevante standarder indenfor automation og produktion. At læse standarder og artikler omkring standarder er ikke nødvendigvis som at læse en "læse let bog", men nødvendigt. Vi har fået nogle af de eksperter, der er gode til formidle standarder til at fortælle om RAMI 4.0 og IEC 62443. Læs med på de følgende sider.

STANDARDISERING

VI SKAL STANDARDISERE FLEKSIBILITET

AF ANDERS P. MYNSTER,
SENIOR SPECIALIST,
FORCE TECHNOLOGY

INDUSTRI 4.0 STANDARD GIVER ALLE DE FRIHEDSGRADER INDUSTRIEN BEHØVER UDEN AT SÆTTE CONNECTIVITETEN OVER STYR.

Fra tid til anden bliver jeg kontaktet af virksomheder, der skal i gang med Industri 4.0. De tænker som regel på robotter, sensorer, trådløse netværk og connectivity – men bliver nogle gange trætte i blikket når talen falder på standarder, selvom de også ved, at connectivity ikke kan eksistere uden. Det er den første og simpleste del af standardiseringen altså den basale forklaring om hvordan de forskellige elementer af et system passer sammen. Ganske som det er beskrevet i en standard, hvordan en møtrik og en bolt passer sammen, er det beskrevet hvordan en mobiltelefon og en basestation gør det.

Industri 4.0 bliver af mange forstået som robotter, der laver det samme igen og igen. Men industri 4.0 handler i høj grad om fleksibilitet til at kunne producere produkter som er individualiseret til en bestemt bruger gruppe, eller en enkelt bruger. Dette skal vi gøre gennem modularisering; ved at sammensætte et væld af devices med vidt forskellige udbydere og brugere, så de kan tale sammen. Men det skal naturligvis sættes i system. Sagt enkelt er udfordringen ikke møtrik-bolt fittet, men hvordan vi kan standardisere fleksibilitet.

REFERENCEARKITEKTUR

En referencearkitektur, som er generel og kan bruges til Industri 4.0, er ISO/IEC 30141, der i år er ved at blive færdiggjort som international standard.

Den beskriver de byggeblokke, der er i et IoT system, hvilke egenskaber man skal tilstræbe for disse blokke, og hvordan de forbinder sig med systemet. Da standarden er under udvikling er den stadig ikke offentlig, men meget af det arbejde, der danner grundlag for standarden blev udført i det Europæiske forskningsprojekt IoT-A.

Her er der beskrevet en konceptuel model, som kan bruges både i industri 4.0 systemer, og i IoT systemer. Den beskriver hvordan brugerne interagerer med systemet, og hvordan der både er digitale og menneskelige brugere. Desuden de elementer, der skal indgå i det device, der forbinder det fysiske objekt, med den virtuelle infrastruktur. Og til sidst beskriver den, hvordan der er forskel på om viden stammer fra netværks ressourcer eller noget der ligger lokalt på enheden. Altså et kort, der på meget højt abstraktionsniveau viser et industri 4.0 system.

Det vigtige er, at man ikke venter på den "endelige standard" for systemets enkelte elementer, men at man ved at have forståelse af standarden for systemet kan se, hvordan man tilpasser elementerne i forhold til hinanden. Den konceptuelle model og systemarkitektur går ikke i stykker af, at der kommer en ny version af bluetooth eller low power wide area radio teknologi, den bliver forbedret, da det nu giver nye muligheder for at komme på markedet med nye tilbud gennem den eksisterende arkitektur.

Parallelt med den konceptuelle model beskriver standarden 9 forskellige roller, som skal huskes, når man udvikler systemet.

16.000 VARIANTER

VW Golf bliver produceret i mere end 16.000 varianter, når alle de variable parametre tages i betragtning. Dette betyder, at der er ekstreme krav til, at hver bil gennemgår individuelt tilpassede processer, at der indlæses forskellig software, at netop denne bil sendes til den rigtige kunde i Danmark, og at underleverandører har leveret dele, så lageret har lige præcis de dele, der skal bruges til de modeller, som skal produceres i dag. Alt dette er styret af en ekstern salgsorganisation, som bestiller online. Herved bliver det digitale input (bestillingssystemet til sælgere) og digitale output (rekvisitionssystemet til underleverandører) lige så centralt som det fysiske input.

Det koncept ses i RAMI 4.0 standarderne og på den måde bliver produktet gennem standarder ved med at være fleksibelt.

> Udfordringen er, hvordan vi kan standardisere fleksibilitet.

SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

INDUSTRIAL SECURITY STANDARD IEC 62443, FOR AUTOMATION.

BY RAINER FALK AND STEFFEN FRIES, SIEMENS AG, CORPORATE TECHNOLOGY, GERMANY

Protecting industrial automation control systems against intentional attacks is increasingly demanded by operators to ensure a reliable operation, and also by regulation. The industrial security standard IEC 62443 [IEC62443] specifies security for industrial automation and control systems (IACS)

It is applied successfully at different automation domains, including factory and process automation, railway automation, energy automation, and building automation. It covers the setup of a security organization and the definition of security processes as part of an information security management system (ISMS). Furthermore, technical security requirements are specified distinguishing different security levels for industrial automation and control systems, and also for the used components. Industrial security is called also Operation Technology security (OT Security), to distinguish it from general IT security.

Industrial systems have not only different security requirements compared to general IT systems, but come also with specific side conditions that prevent that security concepts established in the IT domain can be applied directly in an OT environment. For example, availability and integrity of an automation system have often a higher priority than confidentiality. High availability requirements, different organization processes (e.g., yearly maintenance windows), and required certifications may prevent the immediate installations of updates.

INDUSTRIAL SECURITY STANDARD

The international industrial security standard IEC 62443 is a security requirements framework defined by the International Electrotechnical Commission (IEC) and can be applied to different automation domains. Specific parts of the standard define security requirements that target the solution operator, the system integrator, but also the component manufacturer. The requirements address both organizational and technical aspects of security.

IEC 62443 OVERVIEW

The different parts of the standard IEC62443 are grouped into four clusters:

- General aspects: common definitions and metrics.
- Policies and procedures: Requirements on the setup of a security organization (ISMS related) for operators and system integrators, as well as on the definition of associated security processes.
- System level: Risk-based methodology for defining security zones and their security level on a system-wide level of an automation and control system. Technical security requirements are defined for a zone, distinguishing different security levels.
- Component level: Requirements on the secure development lifecycle of system components, and technical security requirements for such components.

ZONES AND CONDUITS

According to the methodology described in IEC 62443-3-2, see Figure, a complex automation system is structured into zones that are connected by and communicate through so-called "conduits". Conduits are zones that map for example to the logical network protocol communication between two zones. A risk-based approach is taken to define the targeted security level for each zone and conduit. The zone concept allows handling different zones, depending on the risk to which a zone is exposed.

SECURITY LEVELS

Four Security Levels (SL1, SL2, SL3, SL4) are defined that correlate with the strength of a potential adversary. To reach a dedicated security level, the requirements (SR) and potential requirement enhancements (RE) defined for that security level have to be fulfilled. The standard foresees that a security requirement can be addressed either directly, or by a compensating countermeasure. The concept of compensating countermeasures allows to reach a certain security level even if some requirements cannot be implemented, e.g., as some components do not support the required technical features. This approach is in particular important for existing industrial automation and control systems, so called "brownfield installations", as existing equipment can be continued to be used.

> Protecting industrial automation control systems against intentional attacks is increasingly demanded.

For each security level, IEC 62443 part 3-3 defines a set of security requirements. Seven foundational requirements group specific requirements of a certain category:

- FR 1 Identification and authentication control
- FR 2 Use control
- FR 3 System integrity
- FR 4 Data confidentiality
- FR 5 Restricted data flow
- FR 6 Timely response to events
- FR 7 Resource availability

For each of the foundational requirements, several specific technical security requirements (SR) are defined. In the context of communication security, these security levels are specifically interesting for the conduits connecting different zones.

The security level of a zone or a conduit is more precisely a security level vector with seven elements. The elements of the vector designate the security level for each foundational requirement. This allows defining the security level specific for each foundational requirement. If, e.g., confidentiality is no security objective within a zone, the security level element corresponding to FR4 "Data confidentiality" can be defined to be SL1 or even none, although SL3 may be required for other foundational requirements (e.g., for FR1, FR2, and FR3). So, the resulting security level vector for a zone could be SL=(3,3,3,1,2,1,3) or SL=(2,2,2,0,1,1,0).

Different types of SL vectors are distinguished, depending on the purpose:

- SL-T: A target security level vector is defined by the IACS operator based in his risk assessment, defining which security level shall be achieved by each zone and conduit.
- SL-A: The achieved security level vector designates the current status, i.e., the security level that is actually achieved by each zone and conduit. In particular for brown-field installations, it is common that a targeted security level cannot be set-up immediately. The gap between the targeted and the actually achieved security level can be made transparent.
- SL-C: The security level capability describes the reachable security level a component is capable of, if properly configured, without additional compensating counter measures employed. This also means that depending on the SL-T not all security features of a component may be used in certain installations.

APPLICATION OF IEC 62443

The standard IEC 62443 has been applied successfully by operators and manufacturers in various projects. It is common that documentation and technical designs of real-world deployments are not made public or shared with competitors. However, some examples for applying IEC 62443 are available publicly:

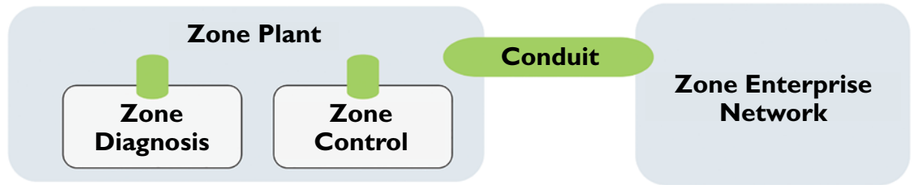
A publication of the IEC 62443 to the Ukrainian power plant gives some insight concerning how the standard can be applied in a concrete setting [BHFF17]. In particular, it shows that a sound, comprehensive security concept is needed that covers security requirements broadly and at a consistent level. It does not help to focus only on certain facets of security. The security requirements defined by IEC 62443 part 3.3 help to ensure that no important aspects are omitted.

The German industrial association ZVEI published an overview document on IEC62443 that includes a simple example, showing the application to a simplified automation system [ZVEI17].

For the integration of decentralized energy resources into the digital grid, IEC 62351-12 [IEC62351-12] maps the described security against the security requirements in IEC 62443-3-3 to argue their comprehensiveness.

REFERENCES

[IEC62443] IEC62443, Industrial communication networks – Network and system security, https://webstore.iec.ch/



SÅDAN KAN ET SCADA-MILJØ HACKES

FÅ INDBLIK I HVORDAN HACKERNE ARBEJDER OG HVAD DU SKAL VÆRE OPMÆRKSOM PÅ, NÅR DU KOBLER DINE SYSTEMER TIL INTERNETTET.

AF MARIE RAABYE,
GRC CONSULTANT,
DUBEX A/S

De it-kriminelle vil gerne tjene deres penge så nemt som muligt. Derfor er de begyndt at automatisere deres arbejde og sælge deres services til andre, mere eller mindre teknisk kyndige, personer. Og de tjener stort på det! Hver dag omsættes der for 12,3 milliarder kr. alene i den anonyme, digitale valuta Bitcoins. Dertil kommer omsætningen i de mere end 750 andre kryptovalutaer, der efterhånden findes. Langt fra alle transaktioner skyldes kriminelle aktiviteter, men en meget stor del gør. Prisen for et exploit, der kan bruges til at lave en bagdør ind i et system, kan svinge fra nogle få tusind kroner til flere millioner, hvis der er tale om fuld overtagelse af en iPhone. Man skal således ikke være i tvivl om den økonomiske motivation, der ligger bag hackernes arbejde. Det er relativt nemt at finde oplysninger på internettet, der kan bruges til at hacke et SCADA-setup, hvis der ikke er styr på den basale sikkerhed.

IoT ER ET SLARAFFENLAND

I dag kobles flere og flere systemer til internettet – oftest uden, eller kun med ringe, sikkerhed. Undersøgelser viser, at langt de fleste aldrig skifter standardkodeordet, der følger med fra deres leverandører til deres enheder og på hovedparten af alle disse enheder anvendes der kun 61 forskellige login- og kodeordskombinationer. Når en enhed er sat på nettet, tager det i gennemsnit 94 sekunder for en hacker at opdage den og prøve hele listen af login- og kodeordskombinationer af. Hvis enheden ikke er sat på et lukket netværk, har du altså i princippet mindre end 100 sekunder til at lave en ny kode, før en hacker vil kunne nå at sætte en bagdør op i dit SCADA-system.

NEMT AT VÆRE HACKER

Der findes et væld af online hackerfora, hvor man kan købe værktøjer og Youtube-videoer, der viser, hvordan man bruger dem. Derudover kan man bruge forskellige søgemaskiner og købe lister over sårbarheder. De lidt mere teknisk kyndig kan lave robotter, der løbende henter de nyeste søgninger.

For at finde de sårbare servere eller pc'ere foretager en hacker typisk en portscanning. Det svarer til, at en indbrudstyv går rundt i et givent område og tager i alle dørhåndtag og vinduer for at se, hvilke der er åbne. I stedet for at gøre det manuelt, bruger hackere søgemaskiner i stil med Google, hvor det også er muligt at lave fokuserede søgninger. Det svarer til, at indbrudstyven kan søge efter alle røde huse med en blå dør, som står åben. Har hackeren båndbredde nok, kan han også selv scanne hele internettet efter bestemte huller på under 5 minutter. En sådan søgning vil kunne vise alt fra private smart tv, kaffemaskiner og selv SCADA-systemer.

I forbindelse med researchen til et indlæg om it-sikkerhed og digitale risici foretog en kollega en portscanning, hvor han faldt over flere SCADA-enheder, der var forbundet direkte til internettet. En af disse viste sig at være kontrolanlægget i en danske svømmehal, hvorfra man at dømme efter skærmbillederne blandt andet kunne kontrollere temperaturerne, tømningen af basinerne samt klor/saltsyre-balancen. Det viste sig desuden, at login og passwords stod i klartekst – og at passwordet var genbrug fra andre installationer, hvilket vi desværre ofte ser. I praksis var det altså muligt for en ekstern at overtage systemet og ændre på indstillingerne. En situation der hurtigt kan resultere i uoverskuelige konsekvenser.

SÅDAN SIKRER DU BEDST DIT SCADA-SYSTEM

Begræns åbninger mod internettet. Hver måned frigives en liste over sårbarheder, der kan udnyttes og hackerne kan automatisere søgningerne på disse.

- Sørg for at leverandørens standardkodeord mv. er skiftet og ikke er lette at knække.
- Sørg for en god netværkssegmentering og brug en god firewall, så informationerne ikke ligger frit fremme.
- Hvis der er åbninger mod nettet, bør data kun kunne tilgås via en krypteret forbindelse, så uvedkommende ikke kan lytte med eller opsnappe data.
- Log al ind- og udgående trafik på netværket. Trafikken bør overvåges løbende og analyseres for uregelmæssigheder, så man kan spore mistænkelig trafik.

Hvis du følger de ovennævnte råd, er du et godt skridt på vej. Dine data ligger ikke frit fremme, du har taget dine forhodlsregler mod "ulåste bagdøre" og har en sensor der vil kunne registrere, hvis der er it-kriminelle, der snuser rundt og så vil du kunne nå at reagere.

DIGIPIPPI FÅR PIGER I GANG MED 3D PRINT

GÅR DET SOM FORENINGEN DIGIPIPPI ØNSKER, VIL VI I FREMTIDEN SE MANGE FLERE PIGER OG KVINDER I IT OG ELEKTRONIK.

AF EVA FOG,
STIFTER AF
DIGIPIPPI

20 piger fra 4. klasse sidder helt stille og knokler i et klasselokale. Ikke et helt unormalt syn, hvis ikke det var for det de er i gang med, og det faktum at der ingen hankøn er i lokalet. Det, pigerne fordyber sig i, er et af de områder, vores erhvervsliv i stigende grad har brug eksperter i: 3D design.

Grunden til det er DigiPippi. En forening hvor omdrejningspunktet er teknologi og hvor fokus er på piger i alderen 7 og 13 år. Foreningen er stiftet, fordi andelen af piger og kvinder inden for it og teknologi er faldet voldsomt siden midten af 1980'erne. Dette på trods af at vores samfund generelt er blevet højteknologisk. Dette har medført en skævvridning, hvor alt for mange piger fejlagtigt undlader at udforske teknologiens verden. En skævvridning, der påvirker samfundets udvikling negativt.

SELVSIKRE PIGER

Tilbage i klasseværelset hos 4. klasse har pigerne været i gang i 3x3 timer, og er efterhånden ret hærdede brugere af det gratis 3D program Tinkercad. Programmet er skabt af Autodesk, og her kan man nemt og enkelt sætte nybegyndere i gang med grundlæggende arbejde i 3D miljøer. Modsat da de startede forløbet i DigiPippi Skole, som projektet kaldes, er selvsikkerheden og forståelsen for det de laver, steget voldsomt.

I begyndelsen gav over 60% af pigerne nemlig udtryk for, at de ikke var sikre på, at de kunne finde ud af det, vi skulle i gang med. Den usikkerhed er for længst væk. Sammen med videoer, der demonstrerer hvad 3D kan bruges til i praksis – bygning af huse, kropsdele, smykker og endda kager – er pigerne godt på vej til at kunne skabe deres egen verden, og i fremtiden vores fælles.

DER ER MENING I GALSKABEN

Det kan virke banalt, men når pigerne pludselig forstår 'hvad det skal gøre godt for' og hvad de 'kan bruge det til', har de bevæget sig første skridt videre og fundet en gnist. Dette er netop essensen af DigiPippis arbejde. Vil vi fri os for de stereotype ideer om, hvem der arbejder med teknologien og på hvilke måder man kan arbejde med den. Vi vil fremvise de gode eksempler, den virkelighedsnære praksis, og give pigerne rollemodeller, de kan spejle sig i.

Der er så mange forskellige applikationsmuligheder for teknologien, beliggende mellem social media manageren og den hardcore koder. Desværre er der ikke mange muligheder for at gennemskue hvilke. De rollemodeller der findes, er dem som medierne vælger at skabe i serier og film, og de er sjældent nuancerede men meget stereotype. Med dem i baghovedet som eneste rettesnor, er det svært at gennemskue, hvilke muligheder der rent faktisk er. Oftest er det først på tærsklen af voksenlivet, at de præsenteres for virkeligheden, og det er for sent. Af samme grund er vores målgruppe så ung, for de skal nås, mens de er børn. Ellers er det tit for sent for specielt piger at komme i gang. Show, don't tell, som det engelske ordsprog siger.

VIL GERNE PÅ RUNDVISNING I VIRKSOMHEDER

Derfor samler vi i DigiPippi på kvindelige rollemodeller fra alle slags job med IT. Ved at vise mangfoldigheden af muligheder og at vise pigerne specifikt, at det ikke er deres køn som sætter begrænsningen, så åbnes deres sind for muligheder frem for begrænsninger. De 20 piger har for eksempel mødt en arkitekt, en it-saglig lærer, en med kandidatur i IT Didaktisk Design og undertegnede – en livslang nørd, uden formel træning og med en kæmpe kærlighed for 3D.

For at fuldende billedet ville vi gernehave, at pigerne fik mulighed for at supplere det hele med en rundvisning på en virksomhed, der specialiserer sig i produktion med basis i 3D skabte modeller. Der er vi ikke endnu, men i givet fald, ville sammenhæng for alvor være sunket ind. Så det er en af de ting vi leder efter.

Det ville gå fra teori til virkelighedsnær praksis, og det er en måde at skabe grobund for fremtidens medarbejdere. Virksomheder ville være rollemodeller for de næste generationer, og det er netop, hvad der er brug for. For på den måde fremtidssikrer vi os selv, og skaber bedre muligheder for alle.

Pigerne fra 4. klasse, Dagmarskolen, Ringsted

SIDEN SIDST

GRATIS ADGANG TIL DATAVÆRKTØJ

NY PLATFORM SPARKER 500 VIRKSOMHEDER I GANG MED BIG DATA.

Det er svært at forestille sig en virksomhed, der ikke kan forbedres ved en systematisk brug af data om produktionsprocesser, produkter, kundeadfærd og så videre. En ny platform **#DataForBusiness**, som er gratis at bruge, skal få virksomheder i gang med Big Data. Værktøjet gør det muligt at tjekke, hvordan man kan bruge eksisterende data til at videreudvikle sin forretning.

Værktøjet bygger på den nyeste forskning på området for Big Data analyse på baggrund af studier af databrug i danske virksomheder, gennemført af CBS, Alexandra Instituttet, og Teknologisk Institut. Virksomheder, der deltager, får:

- Adgang til nyeste, forskningsbaserede værktøjer
- 360° analyse af virksomhedens data-potentiale
- Individuel, branche- og performance-benchmark
- Klare handlingsplaner og adgang til certificerede rådgivere (frivilligt!)

Der bliver desuden holdt en række events, herunder en stor inspirations-konference den 18. januar 2018.

DAU KONFERENCE
SÆT KRYDS I KALENDEREN 23. NOVEMBER

BLIV KLAR TIL INDUSTRI 4.0 MED DET ANLÆG DU HAR – **HØR OM** STRATEGIER OG VEJE DU KAN GÅ.

HVER TREDJE ER I GANG MED SENSOR IoT

Det er næsten hver tredje danske virksomhed, der har sensorer koblet til internettet. Det viser nye tal fra Danmarks Statistik. En ret pæn andel er således i gang med måske det første vigtige skridt for at komme i gang med IoT og Big Data. Cloud Computing har også vundet indpas når det handler om data. 28 pct. får således opbevaret data i clouden i dag.

ET EFTERÅR SPÆKKET MED INDUSTRI 4.0

Der er fyldt godt op de kommende måneder, hvor industri 4.0 og hvad dertil hører, er hovedtema på en række events. Emner som Industry 4.0, Digitalization and Big Data, Internet of Things, startups vil være i fokus den 20.-21. september til High Tech Summit, som bliver holdt på DTU. Derpå følger hi-messen i starten af oktober og en ny satsning fra messecenter Herning med Electronic of Tomorrow, EOT sidst i oktober.

DAu SPONSORER

INNOVATION BY EXPERIENCE
COWI
FLSmidth
MASKINSIKKERHED Rådgivning · Inspektion · Undervisning
nne Focused pharma engineering
OMRON
Rockwell Automation
ROCKWOOL
RAMBØLL
Schneider Electric
SIEMENS
TÅNGBERG Pro-Consult
ABB

HAR DU LYST TIL OGSÅ AT SPONSERE DAu, SÅ SE MERE PÅ WWW.DAU.DK