OT DESIGN

TEMANUMMER FOR DAu-BLADET

DAu

NO 3 • DECEMBER 2018

TILBAGEBLIK PÅ 2018 OG FORVENTNINGER TIL 2019

AF FRANK FAURHOLT, FORMAND FOR DANSK AUTOMATIONSSELSKAB (DAu)

Hovedhjørnestenen i Dansk Automationsselskab er fire store årlige konferencer, hvor vi præsenterer den nyeste viden og nyeste teknologi inden for automation belyst af internationale talere og gennem konkrete cases fra danske virksomheder, der er fremme i skoene.

ÅRET DER GIK 2018

Nu, hvor året er ved at gå på hæld, kan vi se tilbage på 2018 med fire velbesøgte konferencer: "Human Machine Interface" hos Schneider Electric i Ballerup i februar, "Digitalisering af store infrastrukturanlæg" i samarbejde med Sund & Bælt på Sprogø i maj, "Integrated Engineering 4.0 – Fra vision til virkelighed" hos Schneider Electric i Kolding i september samt "OT netværk: Design, drift og fejldiagnosticering" hos Ørsted i oktober.

HVAD BYDER 2019 PÅ?

Programmet for den første DAu-konference i 2019 er allerede på plads. Temaet er "Edge, Fog og Cloud Computing" og bliver holdt den 27. februar. Her stilles der skarpt på Edge, Fog og Cloud Computing som mulige alternativer til de klassiske PLC'er (Controller) og SCADA systemer.

Derudover har vi planlagt at holde en konference i maj om, hvordan vi bedre kan udnytte al den data, som vi får adgang til fremover i form af Big Data, AI og Analytics. Herefter følger i september en konference om, hvordan vi får robotterne bedre integreret i automationsløsningerne. På årets sidste konference i november ser vi nærmere på, hvordan AR og VR fremover vil påvirke vores engineerings (design) processer. Med disse temaer håber vi, at vi også i 2019 kan bidrage med ny viden og eksempler, der kan være med til at give vores medlemmer indblik i de nyeste trends inden for automationsløsninger.

GODT NYTÅR OG PÅ GENSYN I 2019

LÆS DAu-BLADET ONLINE

Ønsker du ikke at modtage bladet i papirform, men vil hellere læse det på telefon, tablet eller computer?

Så send en besked med dit navn og e-mail til dau@dau.dk.

Herefter får du fremover tilsendt en mail med link til bladet.

INDHOLD

DAu **DANSK AUTOMATIONSSELSKAB** • **SEKRETARIAT** DI DIGITAL • 1787 KØBENHAVN V • TELEFON 3377 3377 • DAU@DAU.DK • WWW.DAU.DK •
REDAKTION JETTE NØHR, MADS RASMUSSEN, SIMON NIELSEN • **LAYOUT** FRU NIELSENS TEGNESTUE • **TRYK** KAILOW GRAPHIC A/S • ISSN 1601-6750

FOKUS PÅ OT NETVÆRK

AF KARSTEN HVALKOF ANDERSEN,
SENIOR MANAGER
SCADA WIND POWER,
ØRSTED A/S

Automationsbranchen er på fremmarch i disse år, hvor stadig flere arbejdsprocesser digitaliseres i industrien. Softwaremarkedet boomer både inden for administrative systemer og systemer til automation af produktionen. Udbredelsen af IIoT vokser også støt, og data, der genereres af alle disse systemer, skal kategoriseres og opsamles på en struktureret måde, enten i traditionelle serverparker eller i skyen. De skal samtidig gøres let tilgængelige for de tiltænkte applikationer og brugere, og utilgængelige for de uautoriserede.

Når behovet for sikring af systemer og dataveje tillige tiltager pga. stigende trusler om cyber-crime, peger mange pile på OT netværket som en kritisk ressource. Virksomhedens toplinje er tæt koblet til en stabil og ubrudt drift af datavejene, herunder OT netværket. Der er derfor god grund til at fokusere på forskellige aspekter i design, drift og vedligehold, der tilsammen sikrer pålideligheden. Nogle af de vigtigste faktorer er:

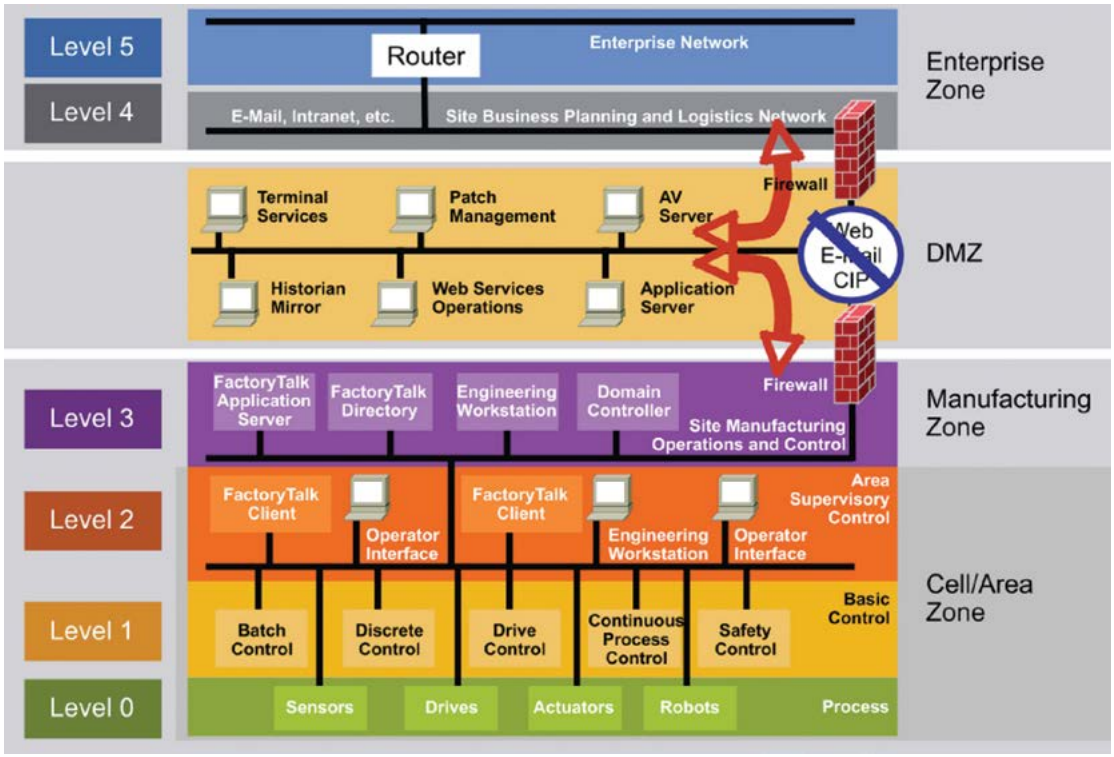
- Arkitektur, herunder Interface mellem OT netværket, OT systemerne, dataservere og evt. administrative netværk
- Redundans
- Realtids performance
- Administration, konfigurationsstyring og maintainability
- Multi-purpose anvendelse, understøttelse af protokoller, segmentering, VLAN, VRF osv.
- Firewalls DMZ og andre barrierer

OVERORDNET ARKITEKTUR

OT netværkets arkitektur skal understøtte de krav til transport af information, som de tilkoblede systemer og applikationer har brug for. Purdue-modellen beskriver en overordnet arkitektur, som de fleste moderne OT netværk-designere inspireres af og forsøger at efterleve:

Netværkene adskilles, som vist i modellen nedenfor, af en såkaldt Demilitarized Zone (DMZ), der mod både det administrative net og OT netværket afgrænses med firewalls. Reglerne i disse firewalls sikrer, at kun de nødvendige porte og IP adresser er åbne for at nå applikationerne i DMZ'en, og at data ikke kan flyde direkte mellem de to net.

FORTSÆTTES NÆSTE SIDE



PURDUE REFERENCE MODEL FOR KONTROL HIERARKI, KILDE: ROCKWELL AUTOMATION

FORTSAT FRA FORRIGE SIDE

UDVIKLING I OT NETVÆRKS ARKITEKTUREN

Edge og Fog Computing er nu ved at gøre sin entre i de moderne produktionsprocesser. Beregningerne og algoritmerne flytter helt ud i komponenterne, eller i centralt placerede gateways i OT netværket. Den udvikling vil føre til en omlægning af datatrafikken og belastningen af netværket, der skal tænkes ind i design af OT netværket. Automations-pyramiden vil "skrumpe på midten", idet mange af de lokale SCADA systemer bliver overflødiggjort, eller erstattet af simple HMI-klienter, der enten betjenes af de centrale servere, eller direkte af servere indbygget i komponenterne på det nederste niveau i automations-pyramiden.

Vi ser også en trend imod, at selve OT netværket i mange produktionsprocesser går mod stigende geografisk udbredelse. F.eks. er der i offshore vindmølle-industrien meget store og komplekse OT netværk, hvor der er behov for realtidsperformance mellem komponenter, der er fysisk adskilt af store distancer. Et beskyttelsesrelæ til et eksportkabel kan f.eks. være op til 180 km langt og have brug for kommunikation mellem hver ende med en forsinkelse på under 5 millisekunder. Det er muligt, men stiller store krav til OT designet.

Den voksende kompleksitet samt fokus på Cyber Security, Intrusion Prevention (IPS) og Intrusion Detection (IDS) – også i OT netværket – betyder, at Security Operation Center (SOC) også kigger ind i OT netværket. Det betyder samtidig at grænserne mellem det administrative netværk og OT netværket langsomt udviskes. De "gamle OT dyder" som realtid og determinisme er imidlertid stadig centrale. Struktur, overblik, gennemtænkt design og fokus på driften, er derfor fortsat det bedste svar på disse udfordringer.

Vil du vide mere? En udvidet udgave af denne artikel kan læses på dau.dk

EDGE, FOG, CLOUD, 5G OG IIoT – NU MÅ DET ALTSÅ SNART STOPPE!

AF FRANK FAURHOLT, FORMAND FOR DANSK AUTOMATIONSSELSKAB (DAu) OG SALGSDIREKTØR I SIEMENS A/S

Vi har efterhånden brugt rigtigt mange ressourcer på at strukturere vores automationssystemer efter f.eks. ISA 88 og ISA 95 standarderne, der pænt indordner de enkelte komponenter og funktioner i veldefinerede lag og moduler.

I bunden har vi sensorer og handleorganer, dernæst følger Controller-laget med de klassiske PLC'er, oven på det har vi MES-laget, og øverst er ERP-laget.

Vi har styr på tingene, og alt er i sin skønneste orden.

Men nu kommer Industry 4.0, digitalisering, Industrial Internet of Things (IIoT) og Cyber-Physical Systems (CPS) og vender op og ned på det hele.

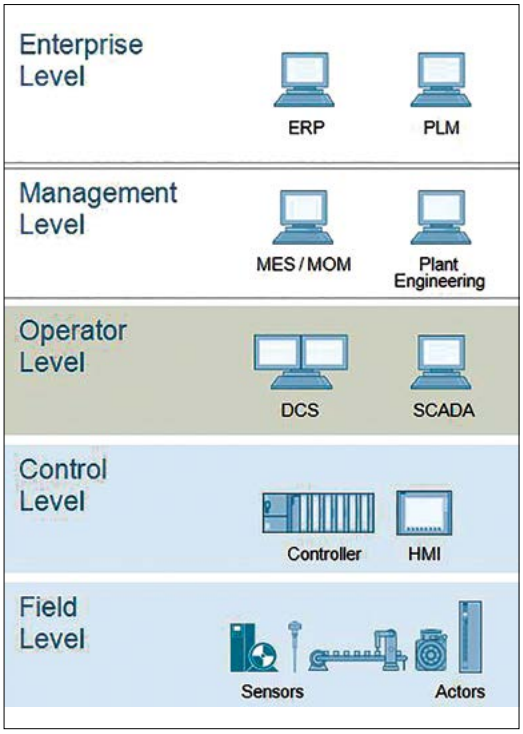
AUTOMATIONS-TREKANTEN ER BLEVET FIRKANTET

Al den moderne teknologi udfordrer vores klassiske måde at tænke industriel automation på.

Vores første modangreb var at begynde at tale om Manufacturing Operations Management (MOM) i stedet for Manufacturing Execution System (MES).

Nu taler vi også om Operational Technology (OT) i stedet for Automation og Industrial IT.

Grafisk er trekanten nu blevet til en firkant.



Deltag på næste DAu konference omkring Edge, Fog, Cloud, 5G og IIoT

Sæt allerede nu kryds i kalenderen onsdag den 27. februar 2019.

Læs mere omkring konferencen på www.dau.dk

ANGREBET PÅ STATUS QUO

Angrebet på status quo fortsætter, idet vi nu også skal til at forholde os til Edge Computing, Fog Computing og Cloud Computing. For slet ikke at tale om 5G og IIoT.

Det er ligesom i skakspillet. Her er det bare PLC'en, der er vores konge, og som nu er under direkte angreb.

Det grundlæggende spørgsmål er, om PLC'en, som vi kender den i dag, er ved at blive slået skakmat?

PLC'EN SKAL NOK OVERLEVE – I MODIFICERET FORM

Hvis vi tager "ja-hatten" på, er det rigtigt, at den klassiske automationstrekant er udfordret, men det er ikke nødvendigvis dårligt.

I disse digitaliseringstider er det på tide at ryste posen lidt, så vi virkelig kan få værdi af de nye teknologier, der nu kommer stormende.

Vi skal ikke hårdnakket holde fast i traditioner og standarder. Men vi skal samtidig have et kritisk syn på anvendelse af den nye teknologi i en industriel sammenhæng.

NYE UDFORDRERE TIL TRONEN

Nu er der andre udfordrere til tronen, der stiller sig op i køen. Spørgsmålet er, om PLC'en endnu en gang vil overleve, måske dø, eller eventuelt genopstå som Fugl Føniks i en endnu stærkere skikkelse.

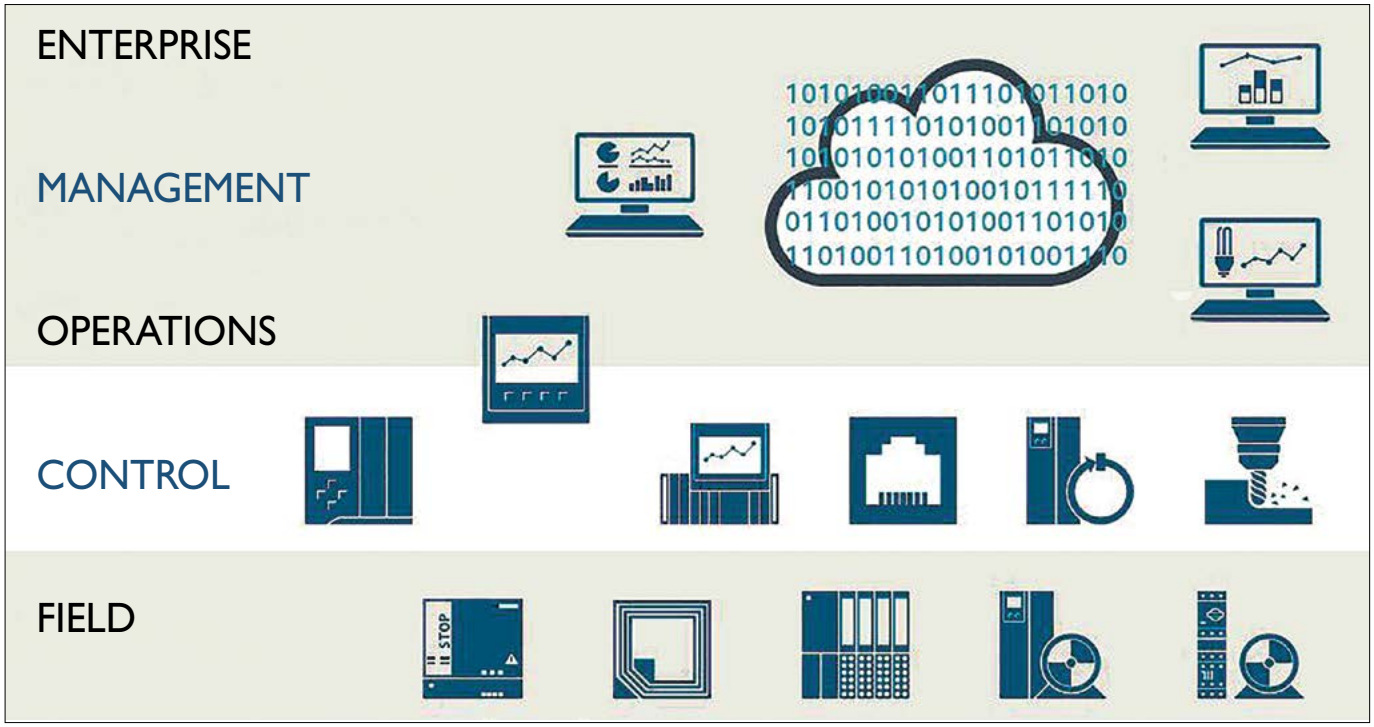
Edge-, Fog- og Cloud Computing vil under alle omstændigheder få stor indvirkning på fremtidens Controller (PLC) platform. Spørgsmålet er blot hvordan.

PLC'EN SOM EDGE CONTROLLER

I min verden vil PLC'en overleve. Den vil faktisk blive en endnu mere central del af fremtidens OT-arkitektur, som en Industrial Edge Controller. Den har alle forudsætningerne for det. Den skal blot opgraderes med den nyeste teknologi i forhold til Cloud connectivity og management.

Opgraderingen er reelt allerede ved at ske, og vi kan derfor snart se en række spændende nye hardwareplatforme og softwarekoncepter på markedet.

Jeg er overbevidst om, at Edge, Fog og Cloud vil ændre vores måde at arbejde med OT på, og det på den gode måde. Automationstrekanten er nu blevet til en sky.



FEJLDIAGNOSE PÅ ETHERNET: HVORFOR 1+1 OFTE ER FORSKELLIG FRA 2

**AF MADS LAIER,
TEAM LEADER
COMMERCIAL ENGINEERING
DENMARK,
ROCKWELL AUTOMATION A/S**

Lad os få det ud med det samme: Langt størstedelen af de fejl, vi ser på Ethernet, relaterer sig til det fysiske medie. Dvs. uhensigtsmæssig montering og terminering og/eller, at de anvendte ethernetkabler ikke er egnet til det miljø, de bliver installeret i. Den nemme løsning på det problem er at følge automationsleverandørens anvisninger.

Når vi så har styr på det rent fysiske i installationen, begynder udfordringerne.

For år tilbage var det de traditionelle fieldbus-systemer, der var dominerende. Hos Rockwell Automation var det f.eks. ControlNet, DeviceNet, DH+ og RIO. På disse netværk var der nogle helt klare begrænsninger for, hvordan man strikkede et system sammen, hvilke kabler man anvendte, og i det hele taget krævede det viden for at få hul igennem.

STANDARD ETHERNET/IP

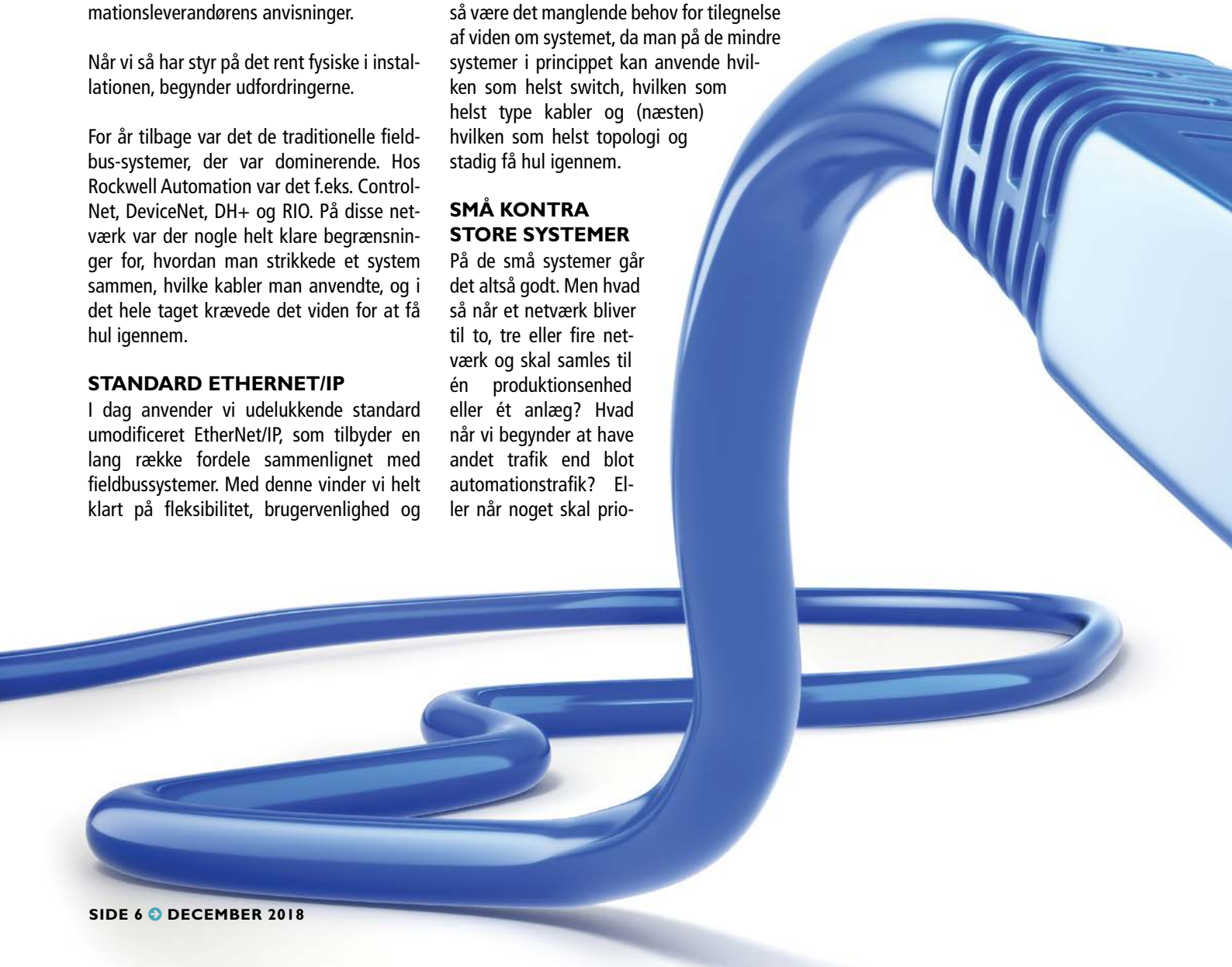
I dag anvender vi udelukkende standard umodificeret EtherNet/IP, som tilbyder en lang række fordele sammenlignet med fieldbussystemer. Med denne vinder vi helt klart på fleksibilitet, brugervenlighed og ikke mindst, at det ikke er et dedikeret netværk kun til automationssystemet, men et netværk til hele virksomheden. Kravet om at tilegne sig viden, der gjorde sig gældende på de gamle fieldbussystemer, er således ikke helt så akut på standard umodificeret EtherNet/IP. Ulemper i den forbindelse kan så være det manglende behov for tilegnelse af viden om systemet, da man på de mindre systemer i princippet kan anvende hvilken som helst switch, hvilken som helst type kabler og (næsten) hvilken som helst topologi og stadig få hul igennem.

SMÅ KONTRA STORE SYSTEMER

På de små systemer går det altså godt. Men hvad så når et netværk bliver til to, tre eller fire netværk og skal samles til én produktionsenhed eller ét anlæg? Hvad når vi begynder at have andet trafik end blot automationstrafik? Eller når noget skal prioriteres mere end andet? Det er her at "1+1 ofte er forskellig fra 2", kommer ind i billedet.

APPLIKATIONSKRAV

Når netværket designes, er der nogle spørgsmål, man med fordel kan stille sig



selv. For eksempel: "Løser mit netværksdesign applikationskravet og lever det op til min kundes forventning og brug? "

Applikationskrav kan være ting som trafiktype (IO, safety og motion), topologi (stjerne, lineær, ring, mixed), belastning, robusthed og cybersikkerhed, håndtering af flere identiske maskiner i samlet anlæg osv.

KUNDENS FORVENTNINGER

Slutkundens forventninger og brug kan være vanskeligt at få klarlagt, og her er det en rigtig god idé med dialog. Derudover skal det specificeres helt præcist, hvad kunden får, og hvilke begrænsninger der eventuelt måtte være på trafik, som ikke er decideret automationstrafik. Specifikation er i den forbindelse mere end netværksoversigt og IP-adressering. Det er ikke usædvanligt, at man med sit design har fået sat alle de rigtige flueben og løst applikationskrav, men bliver udfordret, fordi kunden har andre forventninger til f.eks. robusthed og cybersecurity.

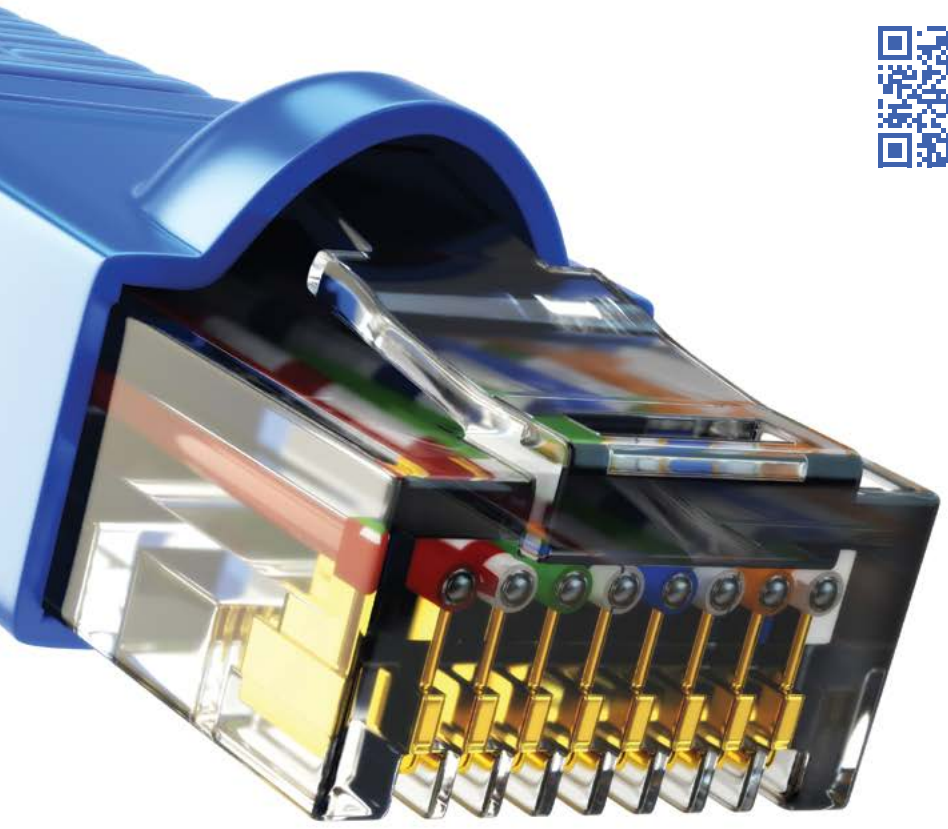
I forhold til fejlfinding på netværket, er det i virkeligheden også her, man bør starte. Hvad var applikationskravet? Topologierne man valgte? Den beregnede belastning? Og matcher det tænkte nu også den faktiske installation og konfiguration? Netværkets øvrige brug kan også nemt have ændret sig over tid, og hvis man ikke har taget forbehold for dette i konfigurationen af sit netværk, vil det også have mulig indflydelse på automationssystemet.

SPØRG AUTOMATIONS-LEVERANDØREN

Information tilgås via automationsleverandørens programmeringssoftware eller netværksmanager. Den kan typisk også ses direkte i de enkelte enheder via Internet browser, men kan også med fordel integreres som en naturlig del af automationssystemets diagnosemuligheder i operatørpanel eller SCADA. Hvis man i sit design har gjort brug af managed switches med integration direkte i automationssystemet, er man godt stillet. Både når man skal diagnosticere, men også fordi man får mulighed for at prioritere trafikbelastning på de enkelte porte. Dette kan bl.a. være i form af benchmarking af trafik, som kan være en stor hjælp i fejldiagnose, hvor benchmark kan sammenholdes med aktuel trafikbelastning eller ved, at der alarmeres ved overskridelse af fastsatte grænser.

Alle disse diagnose- og styringsmuligheder fokuserer primært på OT-anvendelse, men det vil også være naturligt at integrere med IT, og her hjælper det rigtigt meget, hvis den valgte switch hardware understøtter de traditionelt anvendte interfaces og værktøjer for både OT og IT.

Der er masser af hjælp at hente hos automationsleverandøren, som typisk vil kunne være behjælpelig med eksempler på verificerede topologier – vejledninger/White Papers på specifikke emner som f.eks. redundant setup, trådløs, cybersikkerhed og applikationseksempler til automationssystemet. Automationsleverandøren tilbyder naturligvis også kurser omkring OT/IT. Derudover er der meget materiale tilgængeligt online, f.eks. på Industrial IP Advantage (http://www.industrial-ip.org).



Langt størstedelen af de fejl, vi ser på Ethernet, relaterer til det fysiske medie. Det vil sige uhensigtsmæssig montering og terminering og/eller, at de anvendte ethernetkabler ikke er egnet til det miljø, de bliver installeret i. Den nemme løsning på det problem er at følge automationsleverandørens anvisninger.

NETWORK MANAGEMENT OG DIAGNOSTICERING I INDUSTRIAL ETHERNET

AF MORTEN KROMANN,
TECHNOLOGY SPECIALIST,
SIEMENS A/S

Industrial Communication er en central del af alle industrielle automationsløsninger. Det har det faktisk været længe. Men efterhånden som krav og ønsker til kommunikation mellem enhederne i automationsarkitekturen stiger, vokser også udfordringerne.

INDUSTRIAL CYBER SECURITY

Temaet for denne artikel er ikke specifikt Industrial Cyber Security, men ingen artikel om Industrial Communication uden at komme ind på Industrial Cyber Security.

Også i en OT sammenhæng gælder det, at hvis du ikke har styr på din it-sikkerhed, giver det hele ikke nogen mening.

Industrial Cyber Security er naturligvis et spørgsmål om at bruge de rigtige komponenter på den rigtige måde, men det er meget mere jf. IEC 62443, der er "Bibelen" inden for arbejdet med Industrial Cyber Security.

Læs mere om IEC 62443 og andre relevante standarder her: https://en.wikipedia.org/wiki/Cyber_security_standards

INDUSTRIAL COMMUNICATION

Den optimale IT og OT kommunikations infrastruktur kan diskuteres.

Idéen om, at alt skal på ét og samme netværk, lyder besnærende, men er reelt ikke en farbar vej. Både i forhold til IT-sikkerhed, men også i forhold til performance og tilgængelighed, er vi nødt til at segmentere på en struktureret måde.

Jeg vil i denne artikel ikke gå i detaljer omkring OT netværksstrukturer, men blot fremhæve nogle hovedpunkter.

INDUSTRIAL BACKBONE

IT og OT opdeles og adskilles via Firewalls. På OT-siden designes et såkaldt "Industrial Backbone" netværk, der både sikrer kommunikationen til IT-siden og kommunikationen mellem industrielle software applikationer som MES/MOM. Dette sker typisk på Level 3 niveau.

FACTORY FLOOR DISTRIBUTION

Her sker der yderligere en segmentering, særligt når det drejer sig om større OT systemer. Et større distribueret produktionsanlæg kan opdeles i fabrikker og fabriksafsnit. Det sikrer en høj grad af Industrial Cyber Security og tilgængelighed, men sikrer også performance og overskuelighed.

MACHINE / PRODUCTION CELL

Nu nærmer vi os den enkelte maskine, og hermed stiger kravet til realtime. Det gælder også i forhold til nøjagtigheden af maskinens enkelte funktioner. Nogle gange arbejder man med kommunikation i mikrosekunder.

Industriel trådløs kommunikation (IWLAN) anvendes også ofte i denne del af OT arkitekturen, da maskinens bevægelige dele håndteres bedst via denne teknologi.

Maskinsikkerhed (personsikkerhed) er selvfølgelig underforstået, og i dag foregår kommunikation relateret til maskine- og personsikkerhed via OT kommunikationsnetværket.

Det er også her, at klassiske automationskomponenter, som PLC'er og HMI Paneler, bliver koblet på OT netværket.

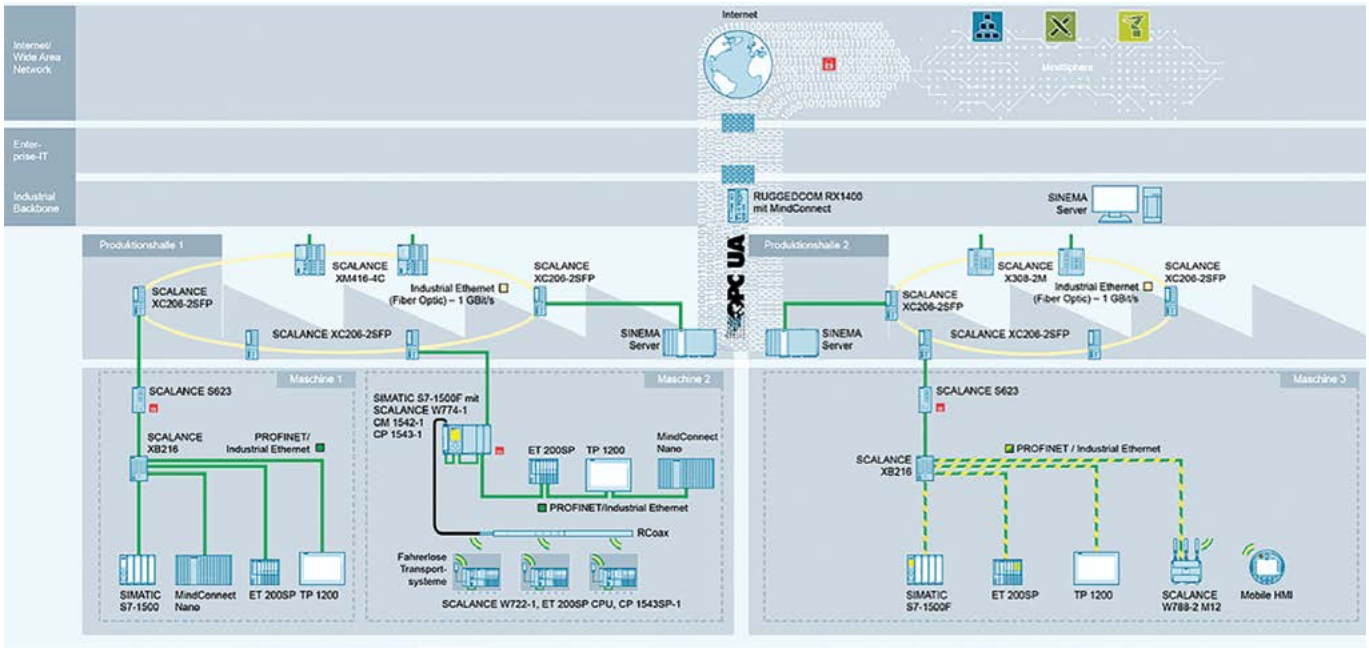
HVAD BETYDER INDUSTRIAL?

Grundlæggende taler vi om Ethernet, så hvad er det lige, der gør det industrielt?

I en fejlfindings- og diagnosesammenhæng er det relevant at kigge på grundlæggende komponenter som kabler og stik. På kontoret virker det meste, men i et industrielt miljø er det ofte noget helt andet. Temperatur

IT versus OT

Se YouTube-video fra Siemens, der kortfattet forklarer forskellene på IT og OT netværk, herunder opbygning, drift og diagnosticering https://youtu.be/V9K3hZgkVRc



og vibrationsforhold spiller ind, men også elektromagnetisk støj fra f.eks. frekvensomformere og andre komponenter.

Det samme gør sig gældende for switches og andet hardware, der indgår i et Industrial Ethernet.

Både i forhold til driftssikkerhed og fejlfinding kan det anbefales at anvende udstyr, der er designet til industriel brug. Også fordi det typisk indeholder diagnoseinformationer og funktionaliteter, der passer i en industriel sammenhæng.

OG SÅ ER DER ALLE DE FRÆKKE UDTRYK

Media Redundancy Protocol (MRP), High Speed Redundancy Protocol (HRP) og Rapid Spanning Tree Protocol (RSTP) er alle teknologier, koncepter og standarder, der kan implementeres i en Industrial Ethernet OT netværksstruktur.

Typisk er der tale om koncepter, der netop øger driftssikkerheden og tilgængeligheden, men som ikke nødvendigvi s gør fejlfinding og diagnosticering nemmere.

NETWORK MANAGEMENT SOFTWARE

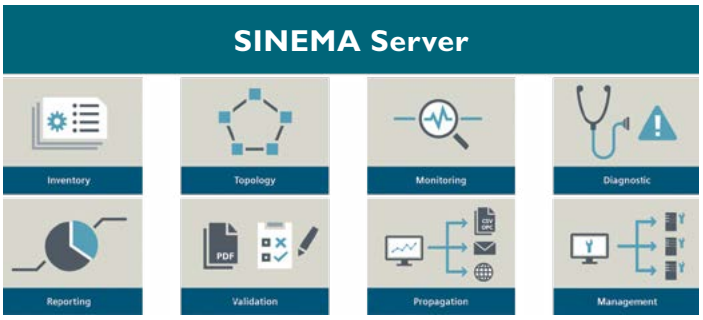
Tiden, hvor fejlfinding kunne klares med et potentiometer, er endegyldig forbi. Selv mange af de oprindelige teknologier kommer til kort. Det kan fortsat være nødvendigt at bruge f.eks. Wireshark til at analysere netværkstrafikken og individuelle telegrammer, men denne form for fejlfinding kan ikke stå alene.

Der er brug for en Network Management software til at holde styr på det hele.

I Siemens arbejder vi med SINEMA Server, som er en software, der bl.a. kan håndtere følgende funktionaliteter:

NETVÆRKSTOPOLOGI

Det er altafgørende for en hurtig og effektiv fejlfinding at kunne udlæse netværkstopologien mere eller mindre automatisk. Det gælder særligt, hvis du som ekstern servicemedarbejder bliver tilkaldt som ekspert. Kun herved kan du få det nødvendige overblik over et typisk komplekst OT netværk.



DIAGNOSE INFORMATIONER

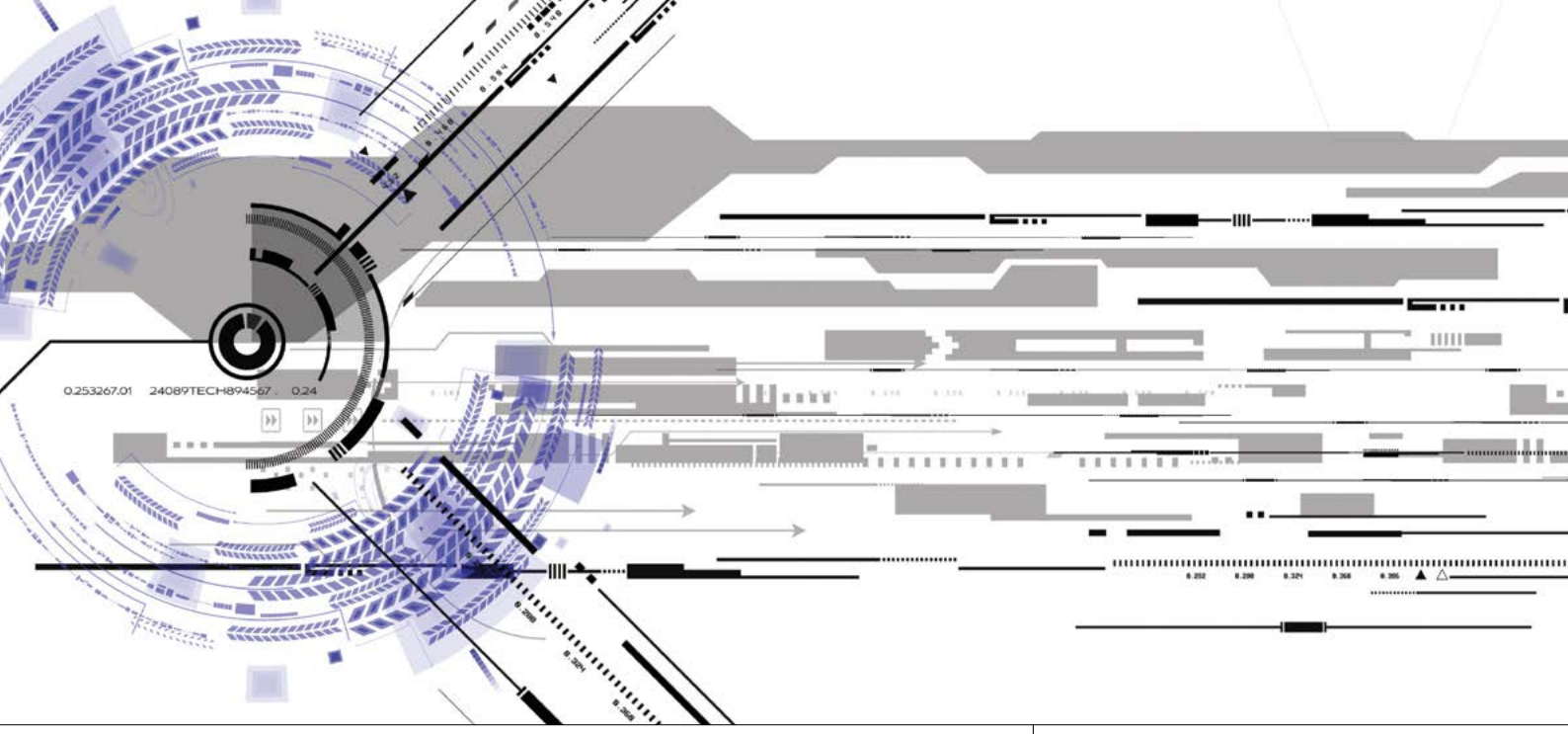
Diagnosemuligheder, bl.a. ved anvendelse af Simple Network Management Protocol (SNMP), giver unikke muligheder for hurtig og effektiv fejlfinding. Igen er det vigtigt, at komponenterne kan håndtere SNMP. Det er dog endnu vigtigere, at Network Management systemet kan præsentere diagnoseinformationerne på en intuitiv måde. Det gælder både i forhold til det lokale drift- og vedligeholdelsespersonale, men også i forhold til eksterne eksperter.

RAPPORTER OG DOKUMENTATION

I rigtigt mange sammenhænge er det vigtigt at kunne udskrive en rapport over netværket. Det lyder "gammeldags", men det er fortsat et grundlæggende og relevant krav i mange sammenhænge. Det gælder både for netværksstrukturen, men også for de komponenter, der indgår.

FIRMWARE UPDATE

Tiden, hvor en hardware blev produceret og installeret, og herefter driftet uændret gennem hele anlæggets levetid, er forbi. Det er et grundvilkår, at der skal opdateres firmware til komponenterne på netværket.



SIKKERHED VIA OVERBLIK I OT NETVÆRKET

**AF JACOB HERBST,
CTO/CHIEF TECHNICAL OFFICER,
DUBEX A/S**

Når OT netværket baseres på standard teknologier og er forbundet til IT netværket og Internettet, ændres risikobilledet. Man bliver nødt til at forholde sig til, at de samme sårbarheder og trusler, der rammer normale administrative IT netværk, også rammer OT netværk.

Selvom sårbarheder og trusler er de samme i OT og IT netværk, er problemerne – og dermed prioriteringen af løsningerne – forskellig. I IT netværk er fokus primært at sikre integritet og fortrolighed, og mindre udfald på den bekostning kan godt tolereres. I OT netværket er det omvendt. Her er fokus på sikkerheden i den fysiske verden og at sikre tilgængeligheden. Det betyder en langt mindre tolerance over for forstyrrelser og udfald. Konsekvensen af den prioritering er f.eks., at sårbarheder eksisterer væsentligt længere, da det er sværere at komme til at installere opdateringer, ligesom sikkerhedsværktøjer som f.eks. antivirus og IPS konfigureres mindre rigidt for at undgå falske positiver, hvorved potentielle angreb og kompromitteringer opdages og blokeres mindre effektivt.

OVERVÅGNING ER ET KRAV

Da risikoappetitten i forhold til OT netværket normalt er minimal, er man nødt til at etablere andre metoder og kontroller for at sikre OT netværket. Desværre er det ikke nok blot at etablere en ordentlig arkitektur med segmenteret netværk, sikker konfiguration af enhederne m.m., da erfaringen fra normale IT netværk viser, at man uanset forholdsregler på et tidspunkt vil blive ramt af en sikkerhedshændelse. Det kan f.eks. være et tilfældigt angreb med krav om ransomware eller anden malware eller ved et egentlig angreb, hvor der målrettet gøres forsøg på at trænge ind i netværket.
For at kunne opdage og håndtere den type hændelser, er man nødt til at holde øje med dem, hvilket kræver en overvågningsløsning. I praksis gøres det ved at etablere en Security Information and Event Management (SIEM) løsning, dvs. en løsning der opsamler log-data fra alle enheder. Den information kan også suppleres med data fra eksempelvis netværksprober, IDS-systemer o.lign. Selve SIEM løsningen er dog kun en tredjedel af løsningen, da der også kræves kvalificerede menneskelige ressourcer til at holde øje med, kvalificere og håndterer de potentielle alarmer. Den sidste del af løsningen er at have processer og procedurer på plads til at vide, hvordan der skal reageres, når der konstateres en utilsigtet hændelse.

KONKLUSION

Når man ændrer teknologi, bliver man også sårbar over for andre typer angreb. Det er vigtigt konstant at vurdere, om man har et passende sikkerhedsniveau set i forhold til den fastlagte risikoappetit. Det er også vigtigt at være opmærksom på, at sikkerhed i et moderne OT netværk ikke kan opnås udelukkende ved passiv beskyttelse. Det kræver konstant årvågenhed og aktiv overvågning, således at utilsigtede hændelser kan opdages hurtigt og effektivt for at mindske den potentielle skade mest muligt.

IIoT FOR DUMMIES

MARTIN HEIDE JØRGENSEN ER PROGRAMLEDER FOR INDUSTRI 4.0 VED SYDDANSK UNIVERSITET OG NYT BESTYRELSESMEDLEM I DAu. VI HAR BEDT HAM INTRODUCERE SIG OG KORT FORKLARE, HVAD IIoT (INDUSTRIAL INTERNET oF THINGS) EGENTLIG ER.

MARTIN HEIDE JØRGENSEN, PROGRAMLEDER, SYDDANSK UNIVERSITET OG NYT BESTYRELSESMEDLEM I DAu

HVEM ER DU?

Jeg er uddannet maskiningeniør og har haft hele min karriere i forskning og universitetsverdenen – altid med et klart industrirettet perspektiv. Jeg har stor erfaring som gruppe- og institutleder, hvor jeg bl.a. har arbejdet med at udvikle samarbejder på tværs af de forskellige ingeniørdiscipliner. I de seneste to år har jeg arbejdet med digitalisering af produktion/Industri 4.0. I min nuværende funktion som programleder for I4.0 ved SDU er en af kerneopgaverne at opbygge industrielle samarbejdsrelationer og et dynamisk laboratoriemiljø, der skal understøtte I4.0 aktiviteter på det tekniske fakultet. SDU har investeret mere end 100 mio. kr. i den aktivitet.

1 HVAD ER IIoT EGENTLIG?

I produktionssammenhæng betyder IoT eller "cyper physical systems", at alle komponenter og processer i en produktion er forsynet med signalgivere og sensorer, så de kan identificeres og afgive signal om status og tilstand. Enhederne er forbundet til et samlet system, hvor alle enheder er digitalt synlige og forbundet.

2 HVAD ER FORSKELLEN PÅ KLASSISK AUTOMATION OG IIoT?

I klassisk automation fungerer de enkelte produktionsceller og -grupper individuelt, men er forbundet til et centralt SCADA og MES system. I IIoT er det samlede system forbundet, så der er digital transparens gennem hele systemet.

3 HVORDAN KAN IIoT GØRE EN FORSKEL?

Når et system er digitaliseret og transparent, giver det mulighed for en højere grad af systemoptimering via dataunderstøttet kontakt mellem organisationens enheder. Det er bl.a. muligt at håndtere mere komplekse produktionsopgaver med stor effektivitet og effektiv kvalitetssikring. IoT betyder også, at der kan etableres forbindelse til brugeren og dermed mulighed for et mere brugerspecificeret design. Det er også muligt at følge produktet i brugssituationen, hvor det giver større forståelse for anvendelse, funktionalitet samt behovstilpasset vedligehold.

4 ER DET SVÆRT AT KOMME I GANG FOR VIRKSOMHEDER?

Digitaliseringen giver store muligheder, men rummer også markante ændringer. Det kan virke uoverskueligt, men behøver ikke at være svært. Det vigtigste er at have en klar strategi og nogle opnåelige delmål. Det er afgørende, at man forholder sig til såvel de tekniske muligheder som de forretningsmæssige potentialer. Nye tiltag skal understøttes både organisatorisk og ledelsesmæssigt. En god digital løsning skal bidrage til en intern kostoptimering samtidig med, at den skal bidrage til at udvikle virksomhedens forretningsplan. Derfor vil en digitaliseringsstrategi i sin natur være unik for den individuelle virksomhed.

5 KENDER DU NOGLE EKSEMPLER PÅ IIoT I DRIFT?

Der findes flere virksomheder, som har taget udfordringerne op, men meget få har en fuldt digitaliseret produktion. De større virksomheder arbejder generelt målrettet med udfordringen. Mindre virksomheder kan ikke umiddelbart kopiere metoden fra de større virksomheder. De bør i stedet digitalisere udvalgte forretningsgange eller produktionsområder.

6 HVAD BLIVER DET NYE HOTTE IIoT?

Radikal innovation ses ofte, når nye teknologier kobles i nye sammenhænge. Noget af det, der virkelig spås en kraftig udvikling, er kunstig intelligens. Jeg glæder mig til at se, hvordan det kan bidrage til nyskabelser inden for automation og produktionsindustrien.

7 HAR IIoT SLET IKKE NOGLE NEGATIVE SIDER?

Jo, der er flere. En af dem er, at man, for at kunne agere i det digitale rum, naturligt må indføre nogle virksomhedsstandarder. Det er nøglen til at håndtere en stor grad af kompleksitet. Der ligger en vigtig opgave i at holde standarder opdaterende, så de ikke skaber unødige begrænsninger i muligheder eller udviklingen. En anden problemstilling er virksomheder, der ønsker at bevare en håndværksmæssig tilgang, eller hvor tillægsværdien fra digitaliseringen vil være begrænset. De vil opleve en øget konkurrence fra de virksomheder, der effektivt kan udnytte digitaliseringens muligheder. Jeg er dog overbevist om, at alle virksomheder kan skabe øget forretningspotentiale ved at forholde sig strategisk til mulighederne og sætte fokus på at implementere de værktøjer og løsninger, der giver mening for den enkelte virksomhed.

FEJLFINDING OG DIAGNOSE I IOT-SYSTEMER

AF ANDERS P. MYNSTER, SENIOR SPECIALIST PRODUCT COMPLIANCE, FORCE TECHNOLOGY

I takt med at IoT-teknologier vinder frem, vil fremtidens systemer være distribuerede over større områder. De vil være heterogene med mange forskellige typer af sensorer og kommunikationsteknologier, og de vil dele data gennem API'er (Application Programming Interface) – altså deling af data gennem et rent IT-interface. Men hvordan diagnosticerer vi IoT-systemer, når der er tale om heterogent distribuerede og API-forbundne systemer?

TO MULIGHEDER I IIoT

Der er for tiden to bølger af industriel IoT. Den ene går ud på at forbinde de traditionelle automationssystemer (OT) direkte til nettet, for derved at kunne indhente data og lave analyser på driftsstatus i systemet. Den anden handler om at opbygge parallelle systemer, der indhenter data vha. systemer, som ikke er forbundet til automationssystemet direkte. Dvs. et parallelt system, der kun er indrettet til at samle data om driften, og som dermed ikke en del af selve reguleringssystemet. Herved undgår man at forbinde OT direkte til nettet og de dertilhørende cybersikkerhedsudfordringer. Samtidig indebærer det, at der ikke er krav om styring helt ned på millisekunder. I stedet er der ofte tale om dataindsamling på minutbasis. Derudover undgår man den mere kritiske godkendelse af systemet som helhed, og det bliver muligt at opbygge et mere eksplorativt system, hvor sensorer hurtigt kan flyttes hen, hvor de giver mest mening. Samtidig betyder det, at de fleste systemer ofte kan benytte trådløse systemer, hvor transmissionerne er pålidelige, men ikke helt så pålidelige som ved kablede installationer.

MONITORERING AF DRIFTEN

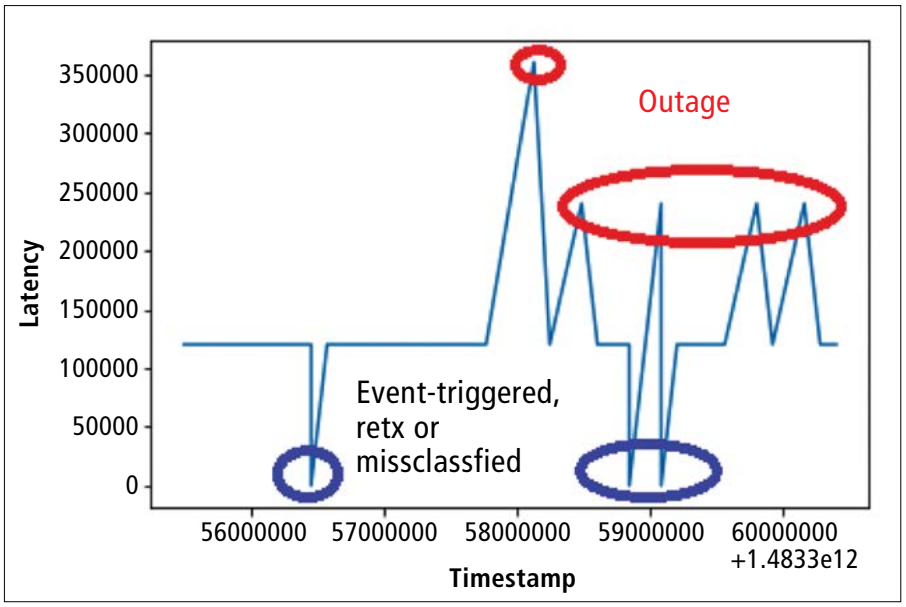
Når IoT-systemet er agilt, er der også behov for agile systemer til at monitorere driften. FORCE har i samarbejde med Aalborg Universitet udviklet et dashboard-baseret testsystem til netop det. Systemet kan, ved blot at analysere tidsstempler og pakkestørrelser, dissekere driften af et IoT-system, og det konfigureres ved at abonnere på de datapakker, der kommer ud af systemet. Dette sker vel og mærke uden at få adgang til krypteringsnøgler. Derfor er der som udgangspunkt ikke adgang til data. Ved at bruge algoritmer til at detektere periodiciteten, dvs. hvor ofte en periodisk sensor sender data, kan systemet beregne, hvor stor datakapacitet der bliver udnyttet på den enkelte enhed og på systemet overordnet set. Samtidigt kan det evaluere, om der er udfald i en pakkedata, og hvilke sensorer der er særligt påvirkede. Det essentielle er, at det også kan detekteres, hvis sensoren holder op med at sende, eller begynder at sende forkerte data pga. manglende batteri, fugtindtrængning eller andre klassiske fejl, som kan få elektronik til at holde op med at fungere.

Grunden til at der ikke er adgang til de data, der bliver overført fra sensoren, er, at de fleste virksomheder ikke umiddelbart vil dele disse for at analysere på driftsstabilitet. Hvis det alligevel ønskes, kan man vha. grafisk programmering hurtigt også analysere på disse data. Det kan f.eks. være data omkring signalstyrke og signal-støjforhold for de trådløse signaler. Ved at plotte disse to imod hinanden kan man identificere transmissioner, hvor der har været en høj signalstyrke, men lavt signal-støjforhold, hvilket indikerer tilstedeværelse af interferens – altså forstyrrende radiosignaler.

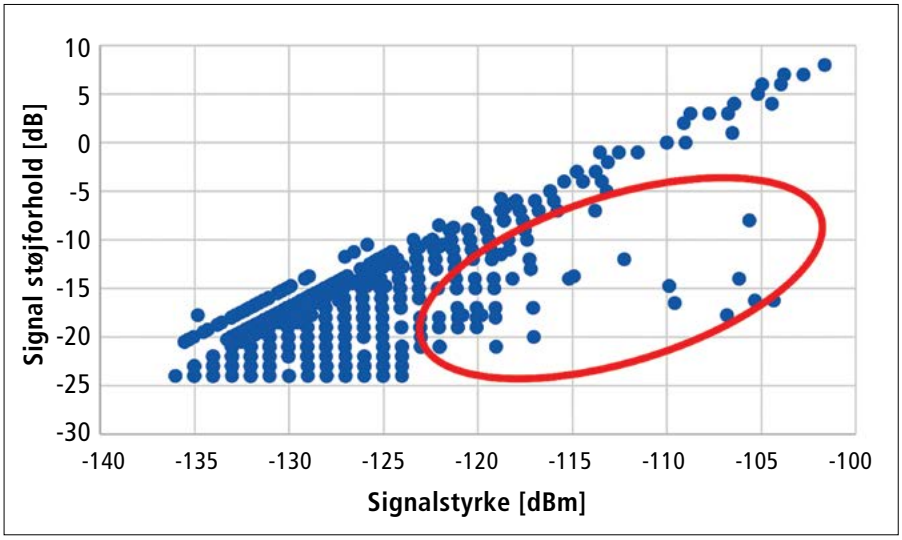
Det er vigtigt, fordi mange IoT-løsninger baserer sig på det trådløse 868 MHz bånd, jf. artikel fra Aalborg Universitet: "Interference Measurements in the European 868 MHz ISM Band with Focus on LoRa and SigFox", der præsenterede interferensmålinger i 868 MHz båndet.

Det essentielle er naturligvis at danne sig et overblik over, hvordan de tabte pakker kan påvirke systemets overordnede funktionalitet. Hvis der f.eks. er tale om, at funktionen af indholdet i pakken blot er at rapportere, at temperaturen stadig er 20°C, har det ikke den store effekt. Hvis det imidlertid er en pakke, der indeholder en alarm om, at temperaturen nu er 45°C, kan det være essentielt, at slutbrugeren bliver opmærksom på alarmen. Ergo kan det have katastrofale følger, hvis pakken ikke kommer frem pga. interferens.

FORCE kan nu, efter at have evalueret forstyrrelsen i praktiske netværk, opbygge et simuleret spektrum. Det kan afspilles, så man kan teste indvirkningen på brugeroplevelsen i ens eget system.



FIGUR 1 ANALYSE AF EVENTDREVNE PAKKER ELLER TABTE PAKKER VIA DASHBOARD ANALYSEN UDEN ADGANG TIL PAYLOAD DATA



FIGUR 2 SIGNALSTYRKE VS. SIGNAL-STØJFORHOLD, HVOR INTERFERENSRAMTE PAKKER ER MARKERET I DEN RØDE CIRKEL.

I takt med at IoT-teknologier vinder frem, vil fremtidens systemer være distribuerede over større områder. De vil være heterogene med mange forskellige typer af sensorer og kommunikationsteknologier, og de vil dele data gennem API'er (Application Programming Interface) – altså deling af data gennem et rent IT-interface. Men hvordan diagnosticerer vi IoT-systemer, når der er tale om heterogent distribuerede og API-forbundne systemer?

NYT FRA DAU'S NETVÆRK FOR AUTOMATIONSUDDANNELSER

MØDE I DAU'S UDDANNELSESNETVÆRK. I FORGRUNDEN TIL HØJRE SES FORMANDEN NETVÆRKET, LEIF POULSEN, DER ER GLOBAL TECHNOLOGY PARTNER I AUTOMATION & IT HOS NNE OG MEDLEM AF DAU'S BESTYRELSE.

AF JETTE NØHR, SEKRETARIATSLEDER FOR DAu

DAu etablerede for knap tre år siden et netværk for automationsuddannelser.

Formålet med netværket er at styrke samarbejdet mellem DAu's medlemsvirksomheder og uddannelsesinstitutioner inden for automation og industriel IT.

Netværket skal også fremme projekter og praktikforløb på automationsområdet og understøtte mulighederne for, at undervisere og studerende kan få inspiration og den nyeste viden på DAu's fire årlige konferencer. Netværket henvender sig til både uddannelsesinstitutioner og virksomheder, der har interesse i at fremme kompetencer inden for automation og industriel IT.

MØDE 28. NOVEMBER

DAu's netværk for automationsuddannelser holdt møde den 28. november 2018.

Her var der en stor opbakning fra de uddannelsesinstitutioner, der er medlemmer af DAu. Bl.a. var der repræsenteret tre universiteter, to maskinmesterskoler og flere erhvervsskoler og -akademier.

På mødet blev der diskuteret, hvordan DAu kan udvikle og tilpasse sine aktiviteter, så uddannelsesinstitutioner, der er medlem af DAu, kan få endnu større glæde af medlemsskabet.

Det blev besluttet at oprette en LinkedIn-gruppe, hvor medlemmer af uddannelsesnetværket kan dele erfaringer. Alle uddannelsesinstitutioner og virksomheder, der er medlemmer af DAu, kan blive medlem af gruppen.

Kernen i DAu's aktiviteter er de fire årlige konferencer. Der har på hver DAu-konference været et antal fribilletter til studerende. Fremover har undervisere førsteret på fribilletterne. Det skal sikre, at viden fra DAu-konferencen bliver spredt til flere studerende gennem undervisningen.

Desuden blev det besluttet, at uddannelsesinstitutionerne i højere grad inddrages i planlægning af kommende DAu-konferencer. Det skal bl.a. sikre flere oplæg på DAu-konferencerne med den nyeste viden fra uddannelsesinstitutionerne på automationsområdet.

Erfaringer og inspiration fra spændende projekter mellem studerende, uddannelsesinstitutioner og virksomheder kan også indgå på DAu-konferencer. Og endelig kan der pitches forslag til projektforløb og relevante praktikophold, som enten virksomheder eller uddannelsesinstitutioner ønsker at sætte i værk for at skabe konkrete match og samarbejder mellem virksomheder, studerende og uddannelsesinstitutioner.

Bliv medlem af LinkedIn-gruppe for Netværk for uddannelser i DAu
https://www.linkedin.com/groups/13647783/

Kontakt: Tovholder på DAu's uddannelsesnetværk
Christine Bernt Henriksen
e-mail cbh@di.dk eller
telefon 3377 3802

TAG GODT IMOD TO NYE VIDENCENTRE FOR AUTOMATION OG ROBOTTEKNOLOGI

AF CHRISTINE BERNT HENRIKSEN,
TOVHOLDER PÅ DAU'S NETVÆRK
FOR AUTOMATIONSUDDANNELSER

Der er netop etableret to nationale videncentre for automation og robotteknologi på to erhvervsskoler.

De er placeret på Tech College i Aalborg og Syddansk Erhvervsskole i Odense.

Begge videncentre er etableret i et tæt samarbejde med i alt seks andre erhvervsskoler spredt over hele landet.

Formålet med at etablere disse to videncentre er at styrke talentudviklingsarbejdet og tiltrække flere ressourcestærke elever til erhvervsuddannelser som automatikteknikere, industriteknikere eller smede.

Derudover ønsker man politisk at styrke erhvervsskolernes arbejde med at digitalisere erhvervsuddannelserne, så de matcher den teknologiske udvikling, der foregår i virksomhederne.

VIDENSCENTRENES OPGAVER

De centrale opgaver, der ligger i de to videncentre, er:

- Udvikle og afprøve nye former for samarbejde om bl.a. ny teknologi, efteruddannelse og talentudvikling mellem erhvervsskoler, virksomheder og de videregående uddannelser
- Udvikle nye undervisningsforløb og -materialer
- Opbygge og formidle ekspertviden til undervisere i hele landet
- Indkøbe og vedligeholde højt specialiseret udstyr, der kan bruges i undervisningen.

DAu har etableret en dialog med de to videncentre, som også er blevet engageret i vort uddannelsesnetværk med andre uddannelsesinstitutioner inden for automation og digitalisering.

SAMARBEJDE MED VIRKSOMHEDERNE

Videncentrene skal samarbejde med virksomheder i hele landet. Samarbejdet kan tage mange former.

Det kan f.eks. dreje sig om projekter omkring implementering af nyt udstyr og teknologi, undervisning og foredrag eller talentudvikling af lærlinge.

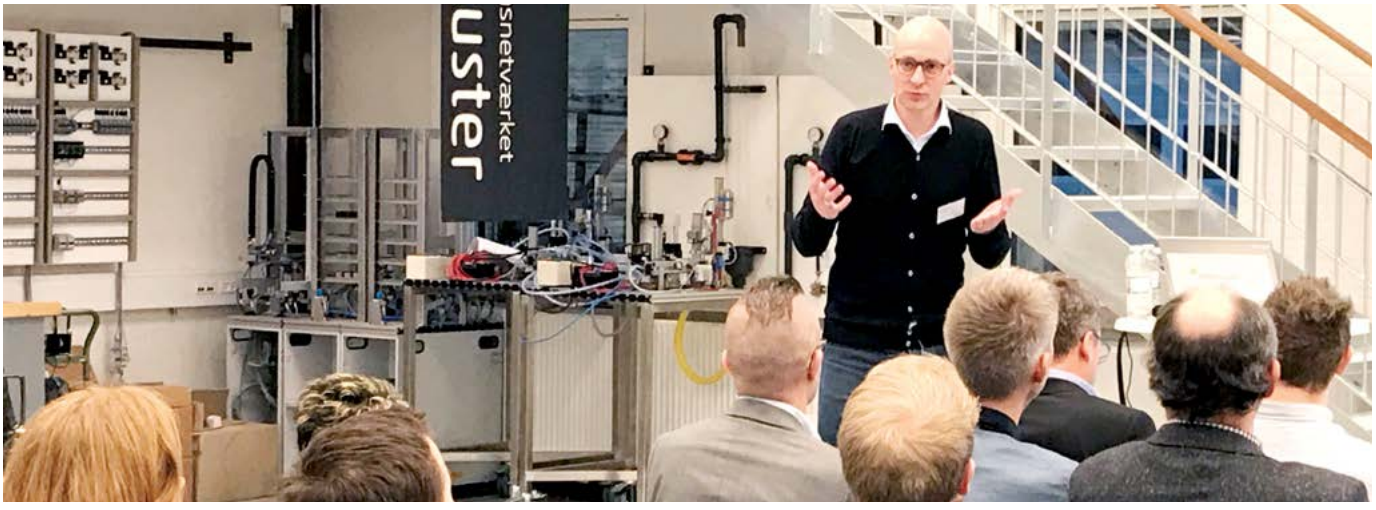
Du er velkommen til at tage direkte kontakt til de to videncentre, hvis du har en ide eller spørgsmål.

Læs mere om de to videncentre her:
https://www.sde.dk/til-virksomheder2/videnscenter/
https://techcollege.dk/virksomheder/videncenter/

KONTAKTPERSON PÅ DE TO VIDENSCENTRE

Videncentret for Automation og Robotteknologi i Aalborg
Christian Ravn Haslam
videncenter@techcollege.dk
telefon 2526 6842

Videncentret for Automation og Robotteknologi i Odense
Lars Mathiesen
lmat@sde.dk
telefon 24225275



SIDEN SIDST

DAu HAR FÅET NY HJEMMESIDE

Se DAu's nye brugeroptimerede hjemmeside på dau.dk. Du kan som sædvanlig finde præsentationer og billeder fra tidligere arrangementer og læse om vores kommende arrangementer.

VÆR MED I DAu GRATIS TRYOUT HELE 2019

Kender du en virksomhed, som ikke er medlem af DAu? Så fortæl dem, at nye medlemmer nu få gratis medlemskab af DAu i 2019. Læs mere om DAu TryOut 2019 på dau.dk under menupunktet "Bliv medlem".

PÅ PROGRAMMET I 2019

KONFERENCER

- **FEBRUAR** Edge, Fog og Cloud Computing: Er PLC'en død?
- **MAJ** Big Data, AI og Analytics: Hvad skal vi med al den data?
- **SEPTEMBER** Robotterne kommer: Og de skal være velkomne!
- **NOVEMBER** AR og VR: På med brillerne, men hvad så?

Vil du hellere modtage DAu-bladet elektronisk?
Så send en besked med dit navn og e-mail til dau@dau.dk

DAu SPONSORER

nne® Focused pharma engineering

OMRON

Rockwell Automation

ROCKWOOL

RAMBØLL

Schneider Electric

SIEMENS

TANGBERG Pro-Consult

ABB

INNOVATION BY EXPERIENCE

COWI

FLSmidth

MASKINSIKKERHED
Rådgivning · Inspektion · Undervisning

VIL DU OGSÅ HAVE DIT LOGO HER?
SÅ BLIV SPONSOR.
SE MERE PÅ WWW.DAU.DK