Af: Jan Stentoft, professor i Supply Chain Management, Syddansk Universitet Business School og Jørgen Hartig, adm. direktør, SecuriOT.

OT er kritisk for driften – men mangler fortsat strategisk forankring

Denne artikel præsenterer resultaterne fra en mini-undersøgelse gennemført i SCM.dk og produktion.dk panelerne med fokus på Operational Technology i praksis. Panelerne er oprettet i et samarbejde mellem scm.dk og produktion.dk og SCM-forskere fra Syddansk Universitet Business School. Formålet med undersøgelsen er at belyse relevante udfordringer inden for produktion og Supply Chain Management, som de opleves i praksis, og dernæst skabe et overblik, der kan hjælpe læserne med at vurdere kompetencebehov i egen organisation.

1. INTRODUKTION

Operational Technology (OT) har i de seneste år bevæget sig fra at være et relativt isoleret teknologisk område til at blive en central del af den moderne dagsorden for cybersikkerhed. Hvor OT tidligere primært blev anvendt i lukkede industrielle miljøer med fokus på stabil drift og fysisk kontrol, er systemerne i dag i stigende grad forbundet med IT-netværk, cloud-løsninger og eksterne leverandører. Denne udvikling har skabt nye muligheder for effektivisering, automatisering og dataudveksling, men samtidig åbnet døren for en voksende mængde cybertrusler rettet mod kritisk infrastruktur og industrielle processer.

OT dækker blandt andet over industrielle kontrolsystemer såsom SCADA-systemer (Supervisory Control and Data Acquisition), PLC'er (Programmable Logic Controllers) og andre teknologier, der styrer fysiske processer i eksempelvis produktion og transport. I modsætning til traditionelle IT-systemer, hvor fokus ofte er på databeskyttelse og fortrolighed, handler OT-sikkerhed i høj grad om tilgængelighed, driftssikkerhed og fysisk sikkerhed. Et cyberangreb mod OT-miljøer kan derfor få alvorlige konsekvenser, ikke blot digitalt, men også i den virkelige verden gennem produktionsstop, miljøskader eller fare for menneskeliv.

Samtidig er grænsen mellem IT og OT blevet mere flydende. Mange virksomheder integrerer i dag deres produktionsmiljøer med administrative IT-systemer for at opnå bedre overvågning, analyse og styring af driftsdata. Denne konvergens mellem IT og OT betyder, at traditionelle cybertrusler som ransomware, phishing og kompromittering af netværk nu også kan ramme industrielle kontrolsystemer. En væsentlig udfordring inden for OT-sikkerhed er, at mange industrielle systemer er udviklet uden moderne sikkerhedsmekanismer. Mange anlæg er designet til at fungere i årtier og benytter ældre hardware og software, som kan være vanskelige at opdatere uden at forstyrre driften. Derudover har OT-miljøer traditionelt været administreret af driftstekniske specialister frem for eksperter indenfor cybersikkerhed, hvilket kan skabe organisatoriske barrierer i arbejdet med sikkerhed. Resultatet er ofte komplekse miljøer med begrænset netværkssegmentering, svag adgangskontrol og utilstrækkelig overvågning.

I takt med den stigende digitalisering og de voksende geopolitiske spændinger er OT-sikkerhed blevet et strategisk fokusområde for både virksomheder og myndigheder. Internationale standarder som IEC 62443 (krav til cybersikkerhed for industrielle automations- og kontrolsystemer) og regulativer som NIS2-direktivet understreger behovet for en mere systematisk tilgang til beskyttelse af kritisk infrastruktur. Virksomheder er derfor nødt til at tænke cybersikkerhed ind som en integreret del af deres OT-miljøer gennem risikovurderinger, segmentering, overvågning, beredskabsplaner og tættere samarbejde mellem IT- og OT-afdelinger.

OT-sikkerhed handler således ikke længere kun om at beskytte maskiner og industrielle processer, men om at sikre samfundets fundamentale funktioner i en stadig mere digital og sammenkoblet verden. Denne artikel behandler resultaterne af et-minisurvey i SCM.dk og produktion.dk panelet, hvor der er spurgt ind til OT-praksis.

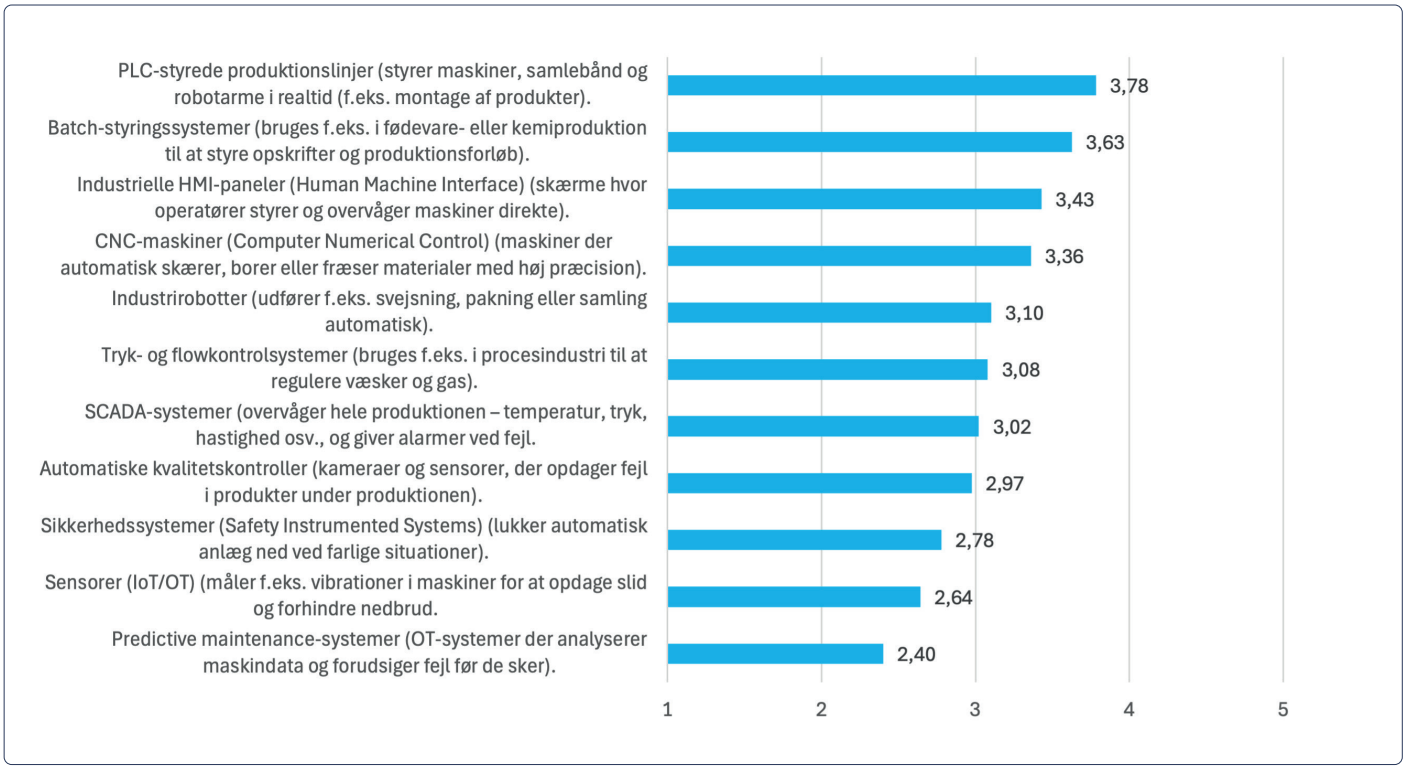
2. OT-SYSTEMER I BRUG

Respondenterne er blevet bed om at tage stilling til den konkrete anvendelse af en række listede OT-systemer indenfor produktion. Som det fremgår af figur 1, opnås de højeste gennemsnit ved teknologierne PLC-styrede produktionslinjer, batchstyringssystemer, og industrielle HMI-paneler og CNC-maskiner med gennemsnit fra 3,78 til 3,36. Industrirobotter anvendes kun i nogen fra med et gennemsnit på 3,10. I den anden ende finder vi predictive maintenance-systemer med et gennemsnit på 2.40. Den lave anvendelse kan skyldes, at predictive maintenance-systemer ofte kræver avanceret dataanalyse, AI-løsninger og store mængder driftsdata for at fungere effektivt. Mange virksomheder befinder sig stadig i en tidlig digitaliseringsfase og har derfor endnu ikke implementeret

sådanne løsninger bredt. Systemerne kræver desuden betydelige investeringer i både software, sensorer og kompetencer. Sensorer opnår et gennemsnit på 2,64 og de anvendes typisk forskelligt fordi behovet varierer mellem brancher og produktionsformer. Virksomheder med højt automatiseringsniveau benytter ofte mange sensorer til overvågning og dataindsamling, mens mere traditionelle produktioner fortsat baserer sig på manuel overvågning. Implementeringen afhænger også af omkostninger, kompleksitet og graden af digitalisering. Resultaterne indikerer generelt, at anvendelsen af OT-systemer varierer afhængigt af branchens automatiseringsgrad, produktionskompleksitet, økonomiske ressourcer og behov for præcision og overvågning. Traditionelle og modne teknologier som PLC'er, HMI-paneler og CNC-maskiner er mere udbredte, mens nyere og mere avancerede teknologier som predictive maintenance og omfattende IoT-løsninger fortsat anvendes i mindre grad.

Respondenterne er også spurgt ind til deres brug af OT indenfor lager og transport (se figur 2). Den højeste anvendelse ses ved automatiske palleteringsrobotter (med et gennemsnit på 3,71), hvilket kan skyldes deres store betydning for effektivisering af tunge og repetitive arbejdsopgaver. Mange virksomheder anvender disse robotter for at reducere fysisk belastning, forbedre arbejdsmiljøet og øge produktiviteten i lager- og produktionsmiljøer. Transportbånd er blandt de mest etablerede og udbredte OT-teknologier inden for logistik og produktion. Den høje score på 3,54 skyldes sandsynligvis, at teknologien er relativt billig, driftssikker og effektiv til håndtering af kontinuerlige vareflows i både små og store virksomheder. Det tredje højest gennemsnit på 3,21 opnås af automatiserede

Figur 1. OT-systemer i brug i produktionen



Figur 2. OT-systemer i brug lager og transport

lagersystemer, som indikerer et fokus på lageroptimering, pladsudnyttelse og automatisering. AS/RS-systemer anvendes særligt i virksomheder med høje lageromkostninger eller stort vareflow, hvor automatisering kan skabe betydelige effektivitetsgevinster. I den nedre ende finder RDIF-porte og scannere, temperatur og miljøsensorer og dock management-systemer med gennemsnit fra 2,67 til 2,55. RFID-teknologi kræver investeringer i både tags, scannere og infrastruktur. Derfor anvendes løsningen oftest i virksomheder med store varevolumener og behov for hurtig sporing af produkter og paller. Mange virksomheder anvender stadig traditionelle stregkodesystemer, som er billigere og enklere at implementere. Temperatur- og miljøsensorer anvendes især i brancher med krav til overvågning af klima og opbevaringsforhold, såsom fødevare-, medicinal- og køleindustrien. I andre brancher er behovet mindre kritisk, hvilket kan forklare den moderate anvendelse. Omfanget afhænger ofte af regulatoriske krav og produkternes følsomhed. Den relativt lave anvendelse af dock management-systemer kan skyldes, at sådanne systemer primært benyttes i større logistikcentre og distributionsvirksomheder med komplekse vareflows. Mindre virksomheder håndterer ofte læsning og losning manuelt eller med enklere planlægningsværktøjer. Implementeringen kræver desuden integration med lager- og transportsystemer, hvilket kan være både dyrt og organisatorisk komplekst. Resultaterne antyder generelt, at OT-teknologier med høj modenhed, klare effektivitetsgevinster og bred anvendelighed såsom transportbånd og palleteringsrobotter opnår højere gennemsnitsværdier. Mere specialiserede eller investeringskrævende teknologier anvendes mere selektivt afhængigt af virksomhedsstørrelse, branche og logistikkompleksitet.

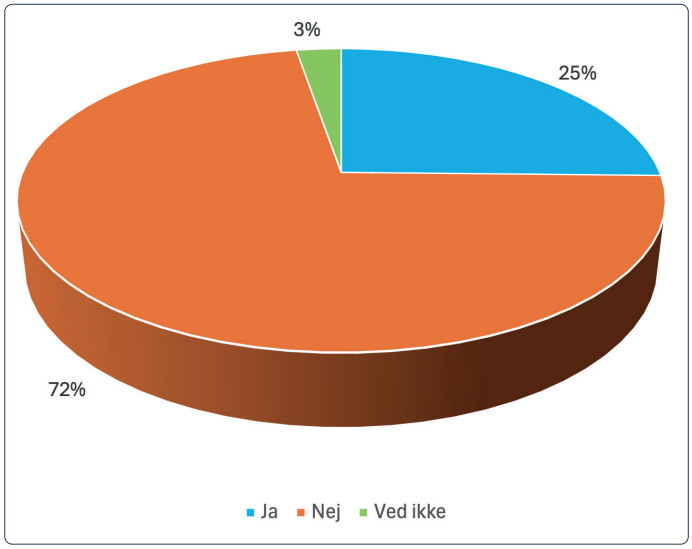
Der er desuden blevet undersøgt den generelle bevidsthed omkring OT-systemernes betydning for den daglige drift. Som det fremgår af figur 3, opnås et gennemsnit på 2,47, hvilket placerer sig under niveauet "i nogen grad". Dette kan indikere, at der endnu ikke er en fuld forståelse af, hvor stor afhængighed der eksisterer af operationelle teknologier i de daglige arbejds- og driftsprocesser. En mulig forklaring er, at OT-systemer ofte fungerer som en integreret og stabil del af produktionen eller logistikken og derfor sjældent tiltrækker særlig opmærksomhed, så længe driften forløber uden problemer. Først ved nedbrud eller driftsforstyrrelser bliver systemernes betydning tydelig. Som følge heraf kan OT-systemer i højere grad blive

Figur 3. Grad af bevidsthed om hvor kritiske OT-systemerne er for driften

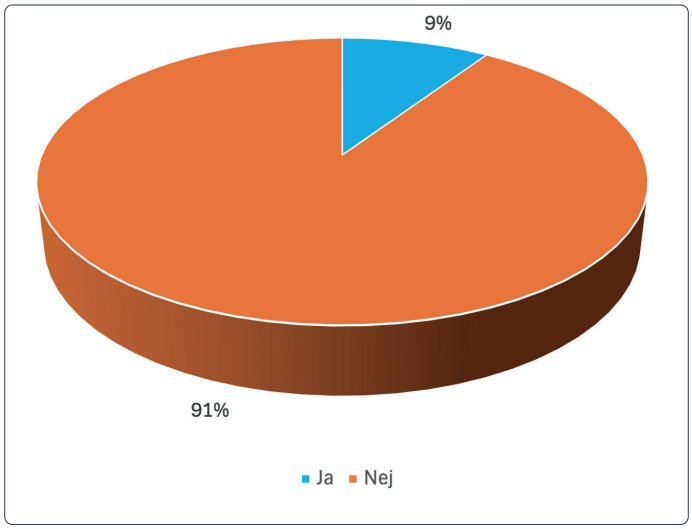
opfattet som tekniske støttefunktioner frem for centrale og forretningskritiske elementer i driften.

3. OT-STRATEGI OG GOVERNANCE

Figur 4 viser at kun en fjerdedel af respondenterne oplyser, at der arbejdes ud fra en formel strategi for OT-sikkerhed. Dette kan skyldes flere forhold. En mulig forklaring er, at OT-sikkerhed i mange virksomheder fortsat betragtes som et teknisk eller driftsmæssigt ansvarsområde frem for et strategisk ledelsesområde. Fokus har traditionelt været rettet mod stabil drift, oppetid og produktionseffektivitet, mens systematisk sikkerhedsstyring af OT-miljøer først i de senere år er blevet et større fokusområde. Derudover kan manglen på en formel strategi hænge sammen med, at virksomhederne stadig befinder sig i en tidlig modenhedsfase inden for OT-styring og digitalisering. Særligt mindre virksomheder kan opleve begrænsede ressourcer, manglende specialiseret viden eller usikkerhed omkring, hvordan en OT-sikkerhedsstrategi konkret skal udvikles og implementeres. En anden mulig forklaring er, at OT- og IT-funktioner i mange organisationer historisk har været organisatorisk adskilt. Dette kan medføre uklar ansvarsfordeling og gøre det vanskeligt at etablere fælles strategiske rammer for OT-sikkerhed. Samtidig er mange OT-systemer ældre og udviklet uden moderne sikkerhedskrav, hvilket kan gøre arbejdet med strategiudvikling mere komplekst. Resultatet kan betragtes som relativt kritisk, da fraværet af en formel strategi kan medføre manglende overblik over risici, uklare ansvarsområder og utilstrækkelig prioritering af OT-relaterede sikkerhedsinitiativer. Uden en strategisk tilgang kan virksomheder have vanskeligere ved at håndtere driftsforstyrrelser, teknologiske ændringer og stigende afhængighed af automatiserede systemer. Samtidig kan manglende strategisk forankring gøre det udfordrende at skabe sammenhæng mellem OT, IT og den overordnede forretningsstrategi.



Figur 4. Formel strategi for OT-sikkerhed

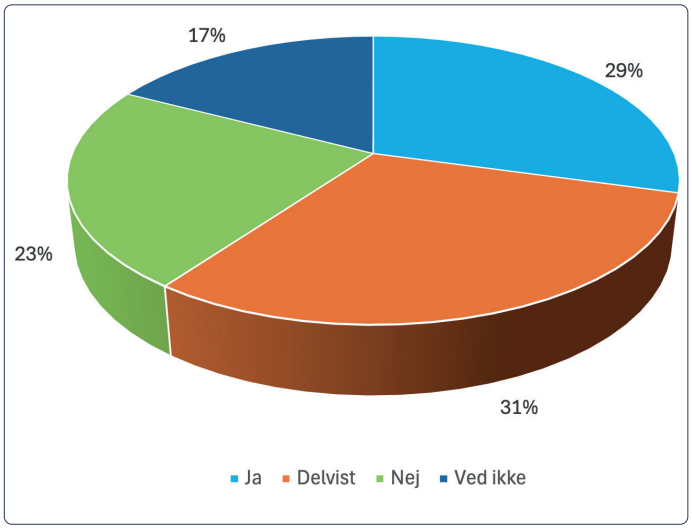


Figur 5. Oplevet sikkerhedshændelser i OT-miljøet

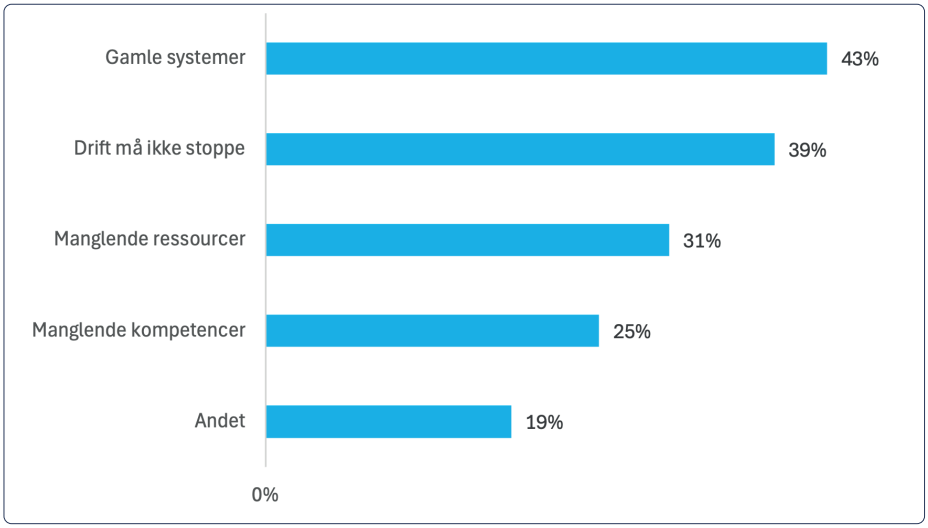
Som beskrevet ovenfor er der ikke den store fokus på strategier for OT-sikkerhed. Dette kan hænge sammen med at kun 9% af respondenterne har oplevet sikkerhedshændelser i deres OT-miljø. En undersøgelse af cybersikkerhed i danske produktionsvirksomheder afslørede, at de 20% der havde haft et cyberangreb have et langt større strategisk fokus og konkret praksis omkring cybersikkerhed end dem, der ikke havde været ramt af et cyberangreb (Stentoft et al., 2024). Man kan sige, at virksomhederne lærte det på den hårde måde. Man kan frygte, at det samme møsner gør sig gældende for OT-sikkerheden.

Hvad angår opfattelser af udfordringer med de nuværende OT-systemer svarer 43%, at der opereres med gamle systemer (se figur 6). 39% svarer at driften ikke må stoppe, 31% at man mangler ressourcer og 25% svarer at man mangler kompetencer. Under "andet" er der givet svar som, manglende hardware til gamle systemer og styresystemer på CNC opdateres ikke.

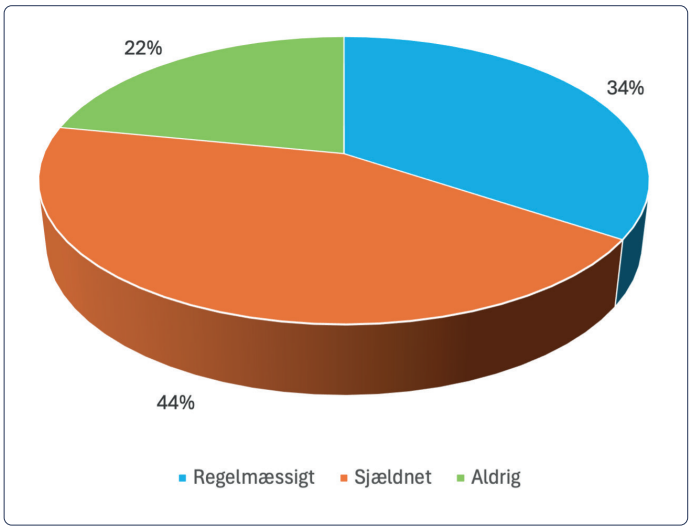
Figur 7 viser respondenters svar på spørgsmålet om hvorvidt OT-systemerne er adskilt fra IT-netværk. Det betyder kort, OT holdes adskilt fra de almindelige administrative IT-systemer og netværk. Formålet er at begrænse, hvordan data, brugere og systemer kan kommunikere mellem netværkene, så problemer eller angreb i ét netværk ikke automatisk spreder sig til det andet. 29% svarer, at dette er adskilt. 31% svarer, at det kun delvist er adskilt, mens 40% ikke har denne adskillelse eller ikke ved om det er adskilt. Dette punkt indikerer et behov for et indsatsområde med henblik på at vurdere, om der opereres med et tilstrækkeligt sikkerhedsniveau.



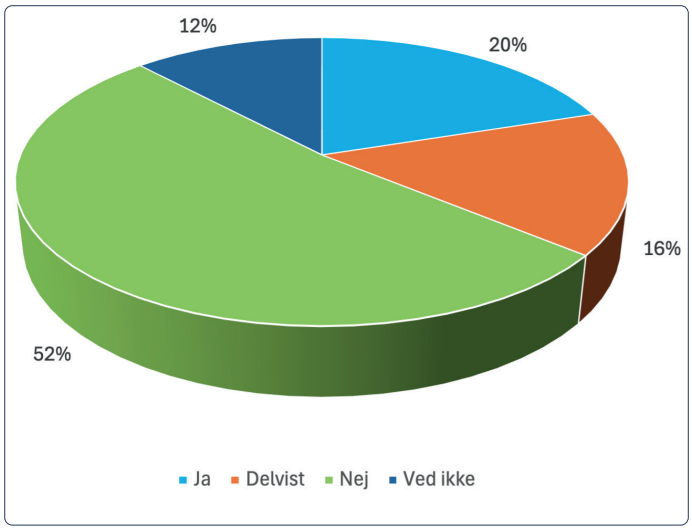
Figur 7. OT-systemers adskillelse fra IT-netværk (netværkssegmentering)



Figur 6. Oplevede udfordringer med OT-sikkerhed



Figur 8. Risikovurderinger af OT-systemer



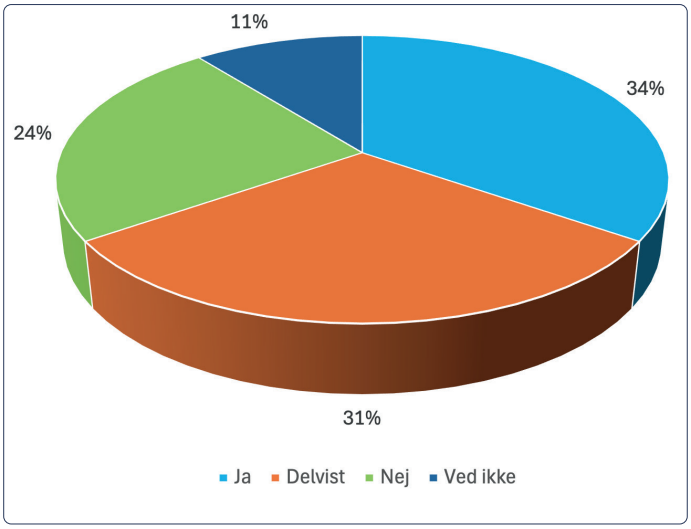
Figur 9. Dokumenteret OT-beredskabsplan

Det har været relevant at undersøge, i hvilket omfang der foretages risikovurderinger af OT-systemer. Som det fremgår af figur 8, svarer 34% af respondenterne, at dette sker regelmæssigt, mens 66% angiver, at det kun sker sjældent eller aldrig. Resultatet tyder på, at systematiske risikovurderinger af OT fortsat er begrænsede i mange virksomheder. Dette kan være problematisk, da OT-systemer ofte understøtter centrale drifts- og produktionsprocesser. Uden løbende risikovurderinger kan det være vanskeligt at identificere sårbarheder og konsekvenser ved fejl eller nedbrud. Samtidig kan manglende vurderinger medføre, at beslutninger om vedligeholdelse og sikkerhed bliver mere reaktive end forebyggende. Resultatet kan desuden indikere, at OT fortsat betragtes som et teknisk driftsområde frem for et strategisk risikoområde. Den store andel, der sjældent eller aldrig gennemfører risikovurderinger, kan derfor ses som udtryk for en relativt høj risikoappetit og peger på behovet for større ledelsesmæssigt fokus på OT-relateret risikostyring.

Når respondenternes praksis med risikovurderinger sammenholdes med deres praksis med dokumenterede OT-beredskabsplaner findes et lignende mønster. Figur 9 viser, at 20% har en OT-beredskabsplan, 16% har delvist en beredskabsplan men 64% svarer at ikke har det eller ikke ved det.

4. DOKUMENTATION AF OT-SYSTEMER

Set i lyset af det relativt begrænsede strategiske fokus på OT-sikkerhed og beredskab er det interessant at undersøge, i hvilket omfang der foreligger opdaterede oversigter over organisationernes OT-systemer. Som det fremgår af figur 10, er det positivt, at godt en tredjedel af respondenterne (34%) angiver, at de har sådanne oversigter, mens yderligere 31% svarer, at de delvist har dette overblik. Samlet set indikerer det, at en betydelig del af organisationerne allerede arbejder med kortlægning og dokumentation af deres OT-miljøer. Dette kan ses som et vigtigt første skridt mod en mere struktureret styring af OT-området, da overblik over systemer og aktiver ofte er en grundlæggende forudsætning for både drift, vedligeholdelse og videre udvikling. Resultatet antyder samtidig, at der er en begyndende erkendelse af behovet for større indsigt i

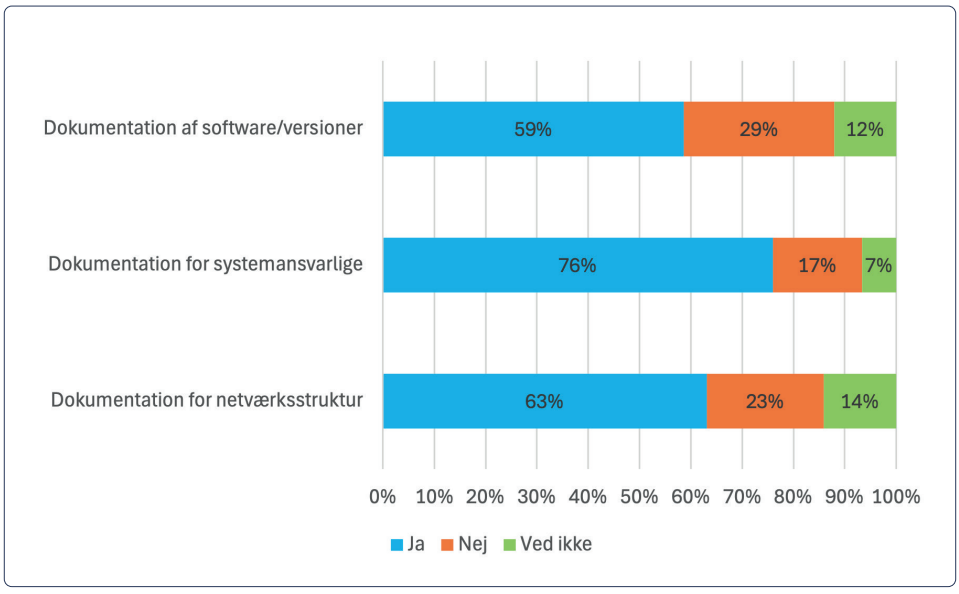


Figur 10. Opdateret oversigt over alle OT-systemer

OT-infrastrukturen. Samtidig viser resultatet dog også, at 35% enten ikke har dette overblik eller er usikre på, om det eksisterer. Dette peger på, at der fortsat er potentiale for at styrke dokumentation og transparens omkring OT-systemerne i mange virksomheder.

Figur 11 viser resultaterne af spørgsmål angående om der foreligger dokumentation af software/versioner, systemansvarlige og netværksstruktur. Dokumentation af OT-systemer omfatter typisk registrering af software og systemversioner, ansvarlige personer samt netværksstruktur og forbindelser mellem systemerne. Formålet er at skabe overblik over OT-miljøet og understøtte drift, vedligeholdelse, fejlhåndtering og organisatorisk koordinering. Ca. 60% svarer, at software/versioner er dokumenteret, mens godt 40% svarer nej eller ved ikke. Bedre ser det ud med dokumentation for de systemansvarlige, hvor 76% svarer at dette foreligger, mens 24% svarer nej eller ved ikke. Hvad angår dokumentation af netværksstruktur er dette til stede hos 63% af respondenterne mens 37% svarer ned eller ved ikke.

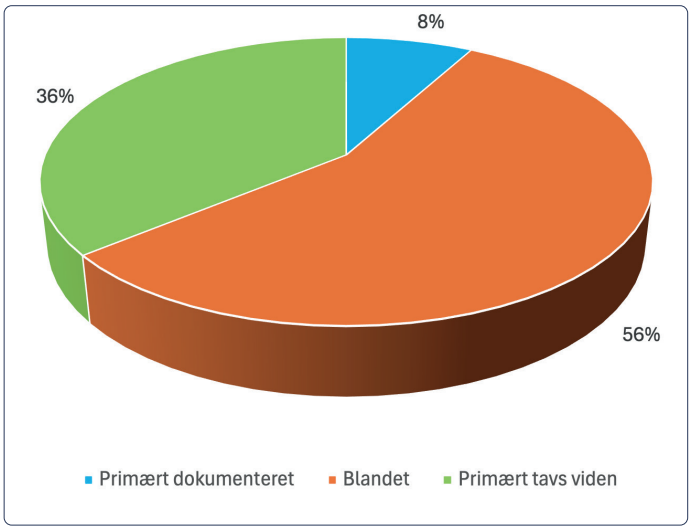
På spørgsmålet om hvor ofte dokumentationen opdateres opnås der er gennemsnit på 2,55 som det kan ses af figur 12. Behovet for opdatering hænger naturligvis sammen med, hvor ofte der reelt sker ændringer. Gennemsnittet på 2,55, dvs. lavere end "i nogen" grad kan således være udtryk for, at der ikke er det store behov for opdateringer.



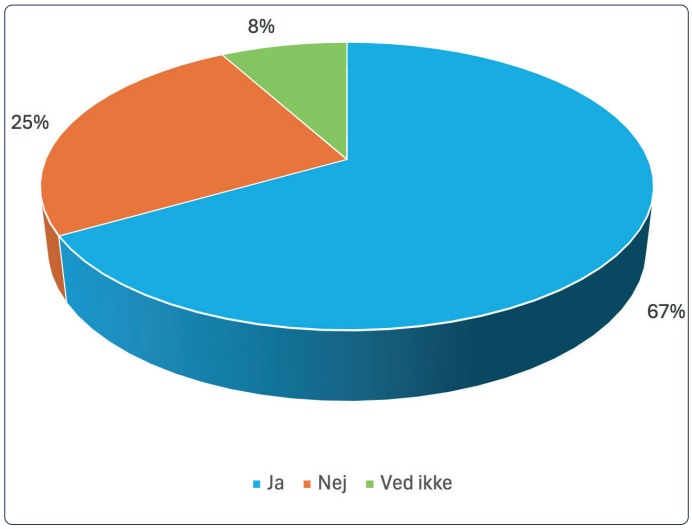
Figur 11. Dokumentationspraksis

Som det kan ses af figur 13, svarer kun 8% af respondenterne, at deres OT-systemer er dokumenteret, mens 56% svarer at noget er dokumenter, mens 36% svarer, de er udokumenteret (tavs viden). Dette indikerer, at vigtig viden om systemernes opbygning, konfiguration og drift i mange tilfælde er knyttet til enkelte medarbejdere frem for at være systematisk dokumenteret. En sådan afhængighed af tavs viden kan skabe udfordringer i forbindelse med vedligehol-

Figur 12. Dokumentationens opdateringsgrad



Figur 13. Dokumenteret viden om OT-systemer vs. tavs viden

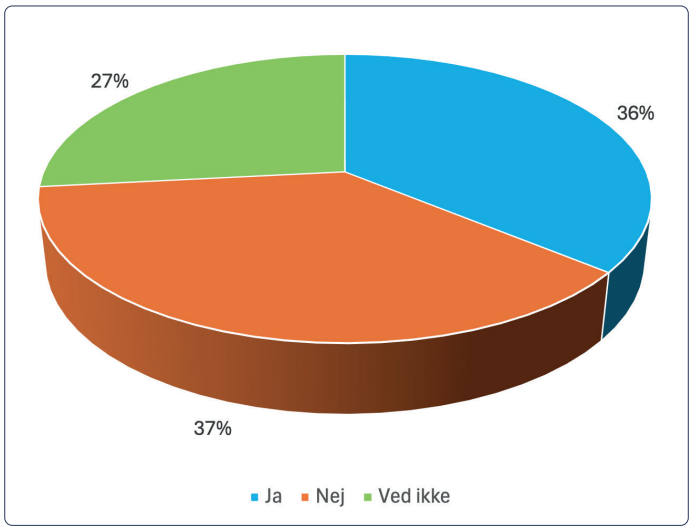


Figur 14. Medarbejdere ligger inde med kritisk viden

delse, fejlhåndtering, oplæring af nye medarbejdere og organisatorisk kontinuitet. Resultatet understreger derfor behovet for en mere struktureret tilgang til dokumentation af OT-systemer.

Respondenterne har også skulle svare på, hvorvidt medarbejdere ligger inde med kritisk viden om OT-systemerne. Resultatet, som vist i figur 14, indikerer, at kritisk viden om OT-systemerne i høj grad er forankret hos medarbejderne, idet 67% af respondenterne vurderer, at dette er tilfældet. Selvom dette afspejler en betydelig intern ekspertise, kan det samtidig skabe sårbarhed, hvis viden ikke dokumenteres og deles systematisk. Virksomhederne kan dermed blive afhængige af nøglepersoner i forbindelse med drift, vedligeholdelse og fejlretning.

Figur 15 viser et delt billede af de fremtidige investeringer i OT-sikkerhed. Mens 36% af respondenterne planlægger investeringer på området, angiver 37%, at der ikke er planer herom, og 27% er usikre. Dette kan indikere, at OT-sikkerhed endnu ikke er et entydigt prioriteret indsatsområde i alle virksomheder, og at der fortsat er forskelle i både modenhed, fokus og strategisk prioritering af området.



Figur 15. Planlægning af investeringer i OT-sikkerhed

KONKLUSION

Undersøgelsen viser, at OT-teknologier i dag udgør en central del af moderne produktions- og logistikvirksomheder, men at anvendelsen varierer betydeligt mellem forskellige typer teknologier. Traditionelle og modne løsninger som PLC-styrede produktionslinjer, HMI-paneler, CNC-maskiner, transportbånd og palleteringsrobotter er bredt implementeret, mens nyere teknologier som predictive maintenance-systemer, sensornetværk og RFID-løsninger fortsat har en mere begrænset udbredelse. Dette tyder på, at virksomhederne primært investerer i teknologier med dokumenterede driftsmæssige gevinster og høj modenhed.

Samtidig peger resultaterne på, at den organisatoriske og strategiske opmærksomhed omkring OT-området fortsat er begrænset. Bevidstheden om OT-systemernes kritiske betydning for driften er relativt lav, og kun en mindre del af virksomhederne arbejder ud fra en formel strategi for OT-sikkerhed. Hertil kommer, at mange virksomheder fortsat opererer med ældre systemer, begrænsede ressourcer og mangel på relevante kompetencer, hvilket kan vanskeliggøre både modernisering og sikkerhedsmæssige forbedringer.

Undersøgelsen viser desuden, at centrale elementer som netværkssegmentering mellem OT og IT, systematiske risikovurderinger og dokumenterede OT-beredskabsplaner kun er implementeret i begrænset omfang. Dette kan indikere, at OT i mange virksomheder fortsat primært betragtes som et teknisk driftsområde frem for et strategisk risikoområde. Samtidig kan det forhold, at relativt få virksomheder har oplevet konkrete OT-sikkerhedshændelser, bidrage til en oplevelse af, at området endnu ikke kræver samme ledelsesmæssige opmærksomhed som andre forretningskritiske områder.

På den positive side viser resultaterne, at mange virksomheder allerede har taget de første skridt mod en mere struktureret styring af OT-miljøet. En betydelig andel har etableret overblik over deres OT-systemer og dokumenteret centrale forhold som softwareversioner, systemansvarlige og netværksstruktur. Dette udgør et vigtigt fundament for videre udvikling af governance, risikostyring og beredskab. Samtidig fremstår dokumentation og videndeling som væsentlige forbedringsområder. Kun få virksomheder har fuldt dokumenterede OT-systemer, og kritisk viden er i høj grad forankret hos nøglemedarbejdere. Denne afhængighed af tavs viden kan skabe sårbarheder i forbindelse med vedligeholdelse, fejlretning og organisatoriske ændringer.

Samlet set tegner undersøgelsen et billede af virksomheder, som i stigende grad er afhængige af OT-systemer for at understøtte produktion og logistik, men hvor den strategiske styring, risikohåndtering og organisatoriske forankring endnu ikke er fuldt udviklet. Der synes derfor at være et betydeligt potentiale for at styrke ledelsesmæssigt fokus, dokumentation, risikostyring og beredskabsarbejde, så OT-området i højere grad understøttes som et forretningskritisk og strategisk aktiv.

FAKTA

Industriens Fond har støttet en portefølje på fem projekter, der har fokus på cybersikre værdikæder. Mere information om projekterne kan findes her:

Cybersikkerhed og Forretningskontinuitet – Syddansk Universitet og Forsvarsakademiet
Cybersikre Fødevareværdikæder – Food & Bio Cluster Denmark, SecuriOT og Syddansk Universitet.
Cyber Safe Robotics – Odense Robotics.
Styrket cybersikkerhed for SMV'er – Erhvervshus Midtjylland.
Cybersikre Forsyningskæder – Copenhagen Business School.

REFERENCER

Stentoft, J., Mikkelsen, O.S, Schmitt, O., Keating, V., Theussen, A., Peressotti, M., Mayer, P., Kankam-Boateng, J. & Tumchewics, L. (2024), Cybersikkerhed i små og mellemstore danske produktionsvirksomheder, Institut for Erhverv og Bæredygtighed/Center for War Studies/Institut for Matematik og Datalogi, Syddansk Universitet samt Forsvarsakademiet. **Læs rapporten her.**