# Dansk Standard

Elektro-dag 31.1 2024, 16.20-16.50

Tema 3, Sikker udførelse af OT

# Agenda

1. Kort om os
2. Hvilke offentlige cybersikkerhedsstrategier omfatter el-, gas- og fjernevarmesektorerne
3. Hvad er forskellen på OT og IT
4. Forskellige reguleringer
5. Kan standarder understøtte arbejdet med at modne OT-cybersikkerheden

# 1. Oplægsholdere

**Søren Storm**
Senior Konsulent, Dansk Standard
Udvalgssekretær, DS
Industriel Automatisering, S-565

E: sst@ds.dk
T: 3996 6208

**Henriette Brandstrup**
Konsulent, ejer, CyberWorks.dk
Udvalgsmedlem i DS Cyber- og informationssikkerhed, S-441 og Industriel Automatisering, S-565

E: henriette.brandstrup@cyberworks.dk
M: 3061 3929

# 2. Strategier, relevante for el-, gas- og fjernevarmesektor

Ønsker man det store overblik over sammenhængen mellem samfundsudvikling, grøn omstilling, behov for robust elnet og sammenhængen til cybersikkerhed, - ja, så er et sted at starte at rette blikket mod eksisterende nationale strategier og trusselsvurderinger.

Centrale dokumenter er:

- National strategi for cyber- og informationssikkerhed, 2022-2024
- Cyber- og informationssikkerhedsstrategi for el-, gas- og fjernvarmesektorerne, 2022-2025
- Regeringens Digitaliseringsstrategi – Ansvar for den digitale udvikling, fra november 2023
- Cybertruslen mod energisektoren fra feb 2023, CFCS

# 3. Hvad er OT, Operationel Teknologi?

OT er en betegnelse for det fysiske produktionsapparat på en fabrik, i et vandværk, kraftvarmeværk, lager, svømmehal mm, og det, der holder driften i gang.

OT ses ofte i samfundskritisk infrastruktur.

I produktionsapparatet er industrielle enheder som industrirobotter, vandpumper, termostater, ventilationsanlæg, kontrolcentre mm. Alle med grader af software og internet-forbundenhed.

ICS (Industrial Control System), PLC (Programmable Logic Controller), SCADA (Supervisory Control And Data Acquisition) er gængse termer i OT.

Dele af elnets-værdikæden er også OT.

# De væsentligste funktionsmæssige forskelle mellem IT og OT

- It-systemer processerer, transmitterer og gemmer data via computere og netværk
- Confidentiality, integrity, availability (CIA) er i fokus
- It-systemer har typisk kortere levetid
- Geninstallering af software og genskabelse af data

- OT styrer noget i den fysiske verden; opererer, kontrollerer og overvåger
- Der er et sikkerhedsaspekt omkring produktionsapparatet, da mennesker bevæger sig rundt i produktionsmiljøet
- Oppetid, availability, integrity, confidentiality er i fokus
- Systemer har længere levetid uden indbyggede sikkerhedsfeatures

- Gamle systemer ses ofte i infrastrukturen, hvor der sættes smarte enheder på, uden det oprindeligt var designet til det
- Der ses ofte distribuerede systemer
- Konsekvensen af tab af funktionalitet er en fysisk effekt, måske hardware skade
- Reparation /genstart kan tage lang tid
- Større risici forbundet med softwareopdatering af OT-enheder end ved øvrige typer af udstyr
- Mange leverandører og eksterne parter har adgang, fysisk eller remote
- Stabilitet - "If it ain't broken, don't fix it" er mantra

# Digitaliseringen af OT

Den voldsomme teknologiudvikling og digitalisering i samfundet ses naturligt også i OT.

Industry 4.0 har bragt interconnectivity ind i OT med IoT devices mm., hvor det før var air gapped. Sammenhængen med it øges hurtigt.

Fra Bottom-up til Top-down, ledelsers ønske om at udnytte teknologi i driften til bl.a.

- Automatisering og optimering af produktionen
- Remote styring
- Bruge data til realtids monitorering til hurtigere beslutningsprocesser og forudsigelig vedligehold
- Bedre synlighed over produktionssystemet
- Minimering af omkostninger
- Brug af lejede maskiner, hvor leverandør servicerer via internettet kan nedbringe omkostninger

# De store udfordringer med digitaliseret OT

Blandt de store udfordringer med digitaliseret OT ses, at fokus på OT-cybersikkerhed ikke følger med.

- Manglende fokus på området fra topledelsen og manglende politikker, der udstikker mål og mandat – ved I, hvem der er ansvarlige i jeres organisation?
- Manglende ejerskab mellem it og OT teams vedrørende OT-cybersikkerhed
- Manglende faguddannede specialister og mangel på medarbejdere generelt
- Gamle systemer og nye systemer i én og samme infrastruktur
- Dårlig dokumentation og overblik over komponenter i infrastrukturen
- Umodne leverandører og third-party risici

# Øget fokus på OT cybersikkerhed

**Eksterne faktorer for øget fokus**

- Geopolitisk dynamik med fx angreb på forsyningssektor med Ukrainekrigen
- Nye lovningsmæssige krav til fx kritisk infrastruktur, enheder mm
- Stærkere dækning af OT rettede cyber-angreb i mainstream presse og medier, fordi OT understøtter ofte national kritisk infrastruktur, hvor impact ses straks.

  SektorCERTs rapport er fx nået ud i bredere kredse

**Interne faktorer**

- Bevidstheden og forståelsen for OT cybersikkerhed er øget i organisationerne
- Forstår, at stigning i antal og mere sofistikerede cyber-relaterede angreb giver omkostninger
- Ansvar flyttes fra driften til CISO i forhold til en strategisk tilgang og autonomi reduceres
- Nye lovningsmæssige krav til fx kritisk infrastruktur og enheder tvinger organisationerne til handling
- Leverandører mødes med øgede krav fra både upstream og downstream

# 4. Eksisterende reguleringer og værktøjer

IT-ROS Trusselscenarier

BEK nr 2646 af 28/12/2021
Bekendtgørelse om beredskab for elsektoren

**§ 11.**

1) *Klasse 1* : Anlæg af væsentlig betydning for at opretholde elforsyningen for
2) *Klasse 2* : Anlæg af væsentlig betydning for at opretholde elforsyningen på
3) *Klasse 3* : Øvrige anlæg.

**§ 13.** For anlæg i klasse 1 og 2 efter § 11, stk. 1, skal virksomhederne sikre,
1) at anlægget har lav sårbarhed over for funktionssvigt af offentligt udbudte
2) at anlægget har lav sårbarhed over for funktionssvigt af væsentlige it-syster
3) at anlægget har nødstrømsforsyning, som i tilfælde af strømafbrydelse sikre

*Stk. 2.* For ubemandede anlæg i klasse 1 efter § 11, stk. 1, skal virksomheden si elektroniske sikrings- og overvågningsforanstaltninger. Sikringen skal omfatte en g væsentligste dele af anlægget. Det skal herunder sikres, at der ved sådan uautorise kontrolrum eller en af Rigspolitiet godkendt kontrolcentral. Virksomhederne skal f information og skal sikre, at dette arbejde foretages hurtigt og kvalificeret.

**§ 32.** Sårbarhedsvurderinger og klassificering efter § 11, stk. 1 og 2, samt kritisk behandles fortroligt og må ikke komme uvedkommende i hænde. Materialet kan c sletning, ødelæggelse, ændring og offentliggørelse forhindres.

Bekendtgørelse af lov om elforsyning
LBK nr 1248 af 24/10/2023:

**§ 85 c.** Virksomheder, som er bevillingspligtige efter §§ 10 og 19 eller har tilladelse til elproduktion fra anlæg med en kapacitet på over 25 MW efter § 29 i lov om fremme af vedvarende energi eller § 11, Energinet og dennes helejede datterselskaber samt virksomheder, der yder balancering af elsystemet, skal opretholde et it-beredskab, herunder planlægge og træffe nødvendige foranstaltninger for at sikre **beskyttelsen af kritiske it-systemer, der er af betydning for elforsyningen.**

*Stk. 2.* Klima-, energi- og forsyningsministeren kan ved manglende opfyldelse af et påbud efter § 85 d om at overholde stk. 1 påbyde virksomheder at foretage en it-revision af kritiske systemer ved en uafhængig revisor godkendt af tilsynsmyndigheden.

*Stk. 3.* Klima-, energi- og forsyningsministeren kan påbyde virksomheder at gennemføre tiltag, som på baggrund af en it-revision, jf. stk. 2, skønnes nødvendige for at opretholde et it-beredskab, jf. stk. 1.

*Stk. 4.* Informationer, herunder vurderinger, planer og data, vedrørende sikkerhedsforhold for kritiske it-systemer i virksomheder omfattet af stk. 1 er fortrolige, hvis oplysni
sammenhængende elsystem.

*Stk. 5.* Klima- energi- og forsyningsministeren fastsætt
ng af virksomhedens it-beredskab og evne
ng og beredskabsarbejde, som virksomhe
rnes pligt til at videregive oplysninger til E
dernes risikostyring, herunder inddragels
til en it-sikkerhedstjeneste, der yder vars
varetagelse af overordnede, koordinerer
stk. 1, og
holdet og planlægningen af en it-revision
energi- og forsyningsministeren fastsætt

LBK nr 314 af 03/04/2017 § Gå til paragraf

Kapitel 5

*Beredskabsplanlægning m.v.*

**§ 24.** De enkelte ministre skal hver inden for deres område planlægge for opretholdelse og videreførelse af samfundets funktioner i tilfælde af større ulykker og katastrofer, herunder udarbejde beredskabsplaner.

*Stk. 2.* Planerne skal revideres i det omfang, udviklingen gør dette nødvendigt, dog mindst én gang hvert fjerde år.

*Stk. 3.* Planerne og revisioner heraf sendes til Beredskabsstyrelsen.

**§ 25.** Kommunalbestyrelsen skal udarbejde en plan for kommunens beredskab. Planen skal vedtages af kommunalbestyrelsen i et møde.

FORORDNINGER, EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2019/941 af 5. juni 2019 om risikoberedskab i elsektoren og om ophævelse af direktiv 2005/89/EF (EØS-relevant tekst)

*Artikel 10*

**Udarbejdelse af risikoberedskabsplaner**

1. På grundlag af de regionale og nationale elkrisescenarier, der er opstillet i henhold til artikel 6 og 7, udarbejder hver medlemsstats kompetente myndighed en risikoberedskabsplan efter høring af distributionssystemoperatører, der af den kompetente myndighed betragtes som relevante, transmissionssystemoperatørerne, de relevante producenter eller deres brancheorganisationer, el- og naturgasselskaberne, de relevante organisationer, der repræsenterer industrielle og ikkeindustrielle elkunders interesser, samt den regulerende myndighed, hvor denne ikke er den kompetente myndighed.

2. Risikoberedskabsplanen skal bestå af nationale foranstaltninger, regionale og, hvor det er relevant, bilaterale foranstaltninger som fastlagt i artikel 11 og 12. I overensstemmelse med artikel 16 skal alle foranstaltninger, der planlægges eller er truffet med henblik på at forebygge, forberede sig på og afbøde elkriser, fuldt ud overholde reglerne for det indre elmarked og systemdriften. Disse foranstaltninger skal være klart defineret, gennemsigtige, forholdsmæssige og ikkediskriminerende.

3. Risikoberedskabsplanen udarbejdes i overensstemmelse med artikel 11 og 12 og med skabelonen i bilaget. Medlemsstaterne kan om nødvendigt medtage yderligere oplysninger i risikoberedskabsplanen.

4. For at sikre sammenhæng i risikoberedskabsplaner fremlægger de kompetente myndigheder, inden de vedtager deres risikoberedskabsplaner, udkastet til disse planer med henblik på høring for de relevante medlemsstaters kompetente myndigheder i regionen og, hvis de ikke befinder sig i samme region, for de kompetente myndigheder i direkte forbundne medlemsstater samt for elektricitetskoordinationsgruppen.

# Kommende lovgivningsmæssige krav

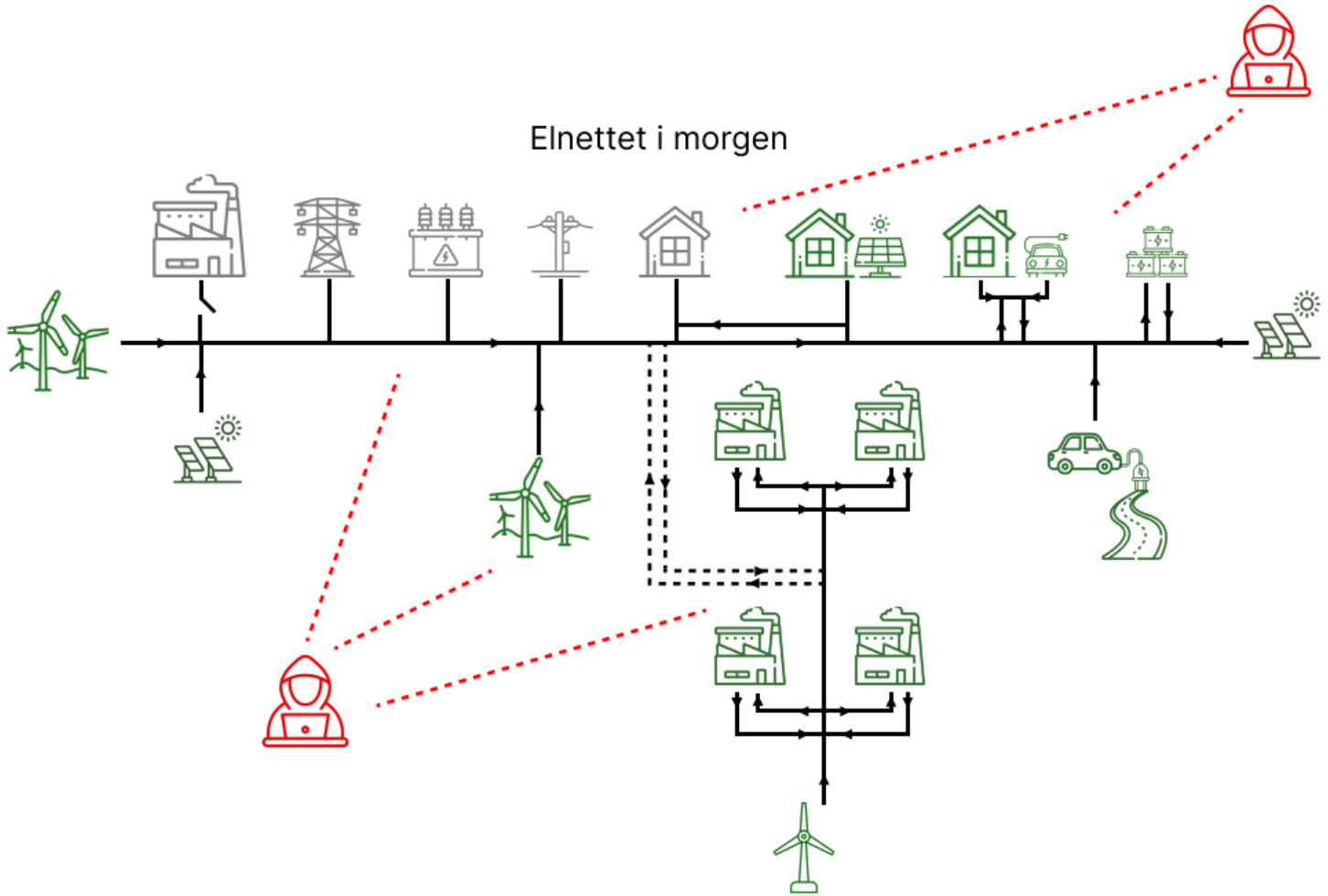
EU's Digitale strategi og dens direktiver og forordninger stiller krav, der udrulles i disse år. Det er stilhed før storm på det område - også for OT med fx NIS2, Cyber Resilience Act, Maskinforordning mm.

- Beskytte borgere i EU direkte
- Øge cybersikkerhedsmodenheden og opbygge kapaciteter
- Harmonisere tilgangen på tværs af EU
- Bidrage til EU's sikkerhed, og at økonomi og samfund kan fungere effektivt

F.eks lovgivningsmæssig fokus for leverandører af kritisk infrastruktur og deres leverandører, sikkerhed i produkter/enheder mm

# Elnettet

Hele elnets-værdikæden har mange stakeholders med mange forretningsformål, kontrakttyper, markeder, reguleringer og lag fra generering af el til distribution. Hackere er ligeglade med dette og rammer, hvor de kan.



# 5. Kan standarder understøtte arbejdet?

Standarder skaber en ramme, der kan sikre:

- At brugerne – internt såvel som eksterne leverandører - har det samme sprog og en harmoniseret tilgang
- En struktur at arbejde efter
- Konkrete krav om f.eks. hvilke security levels, der skal arbejdes efter
- Tekniske specifikationer og konkret vejledning i, hvordan man kan udføre aktiviteter
- Imødekomme krav/ opfordringer i lovgivninger
- Visse standarder kan man blive certificeret i, hvilket styrker organisationen f.eks. i samarbejdsrelationer

ISO 27001/2
www.iso.org

ISA/IEC 62443
www.isa.org/

IEC 62443
www.iec.ch/

www.nist.gov

www.nerc.com

EN IEC 62443
www.iec.ch/

# ISO27001+2 er en kendt IT-sikkerhedsstandard

It-folk vil ofte være meget fortrolige med ISO27000 serien. Den anerkendt internationalt og er udbredt i Danmark og fx statslige organisationer skal følge den.

Man kan blive certificeret for hele organisationen eller dele. Personer kan blive fx ISO27001 Lead Implementor, Lead Auditor mm

Man kan fint anvende standard uden certificering

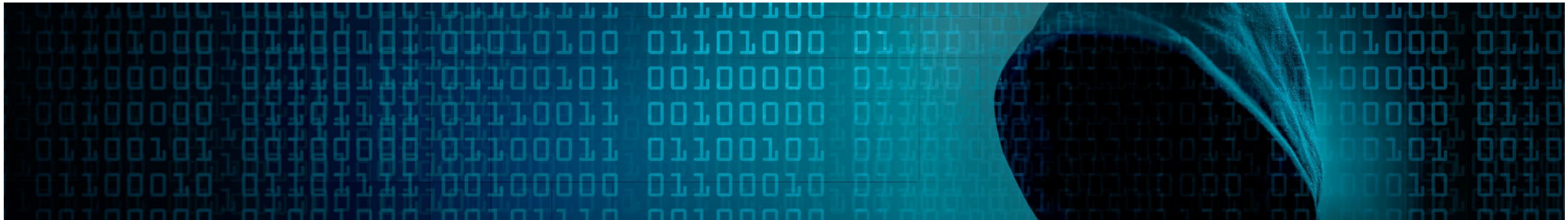
Især ISO27001+2 er bredt anvendelige og blev opdateret i :2022.

Opdatering har medført:

- Struktur er ændret og præsenterer foranstaltningerne ved hjælp af en simpel taksonomi og tilhørende såkaldte attributter.
- Nogle foranstaltninger er sammenlagt, nogle er slettet og nye foranstaltninger er blevet indført.

ISO27001/2
www.iso.org

- Foranstaltningstyper
- Informationssikkerhedsegenskaber
- Cybersikkerhedsbegreber
- Driftsmæssige kapaciteter
- Sikkerhedsdomæner



# Overblik over IEC 62443-serien

| Generelle aspekter | Procedurer & politik | Systemer | Komponenter | Profiler | Evaluering |
|---|---|---|---|---|---|
| **-1-1 (TR)** Terminologi koncepter og modeller | **-2-1** Etablering af sikkerhedsprogram | **-3-1 (TR)** Teknologier | **-4-1** Produktudvikling | **-5-x** Sektor rettede dele af standarden | **-6-x** Evaluering, metoder i forhold til andre kravs-standarder i IEC 62443-serien |
| **-1-5 (TS)** Standardiserings-rammer for profiler | **-2-3 (TR)** Patch styring | **-3-2** Risikovurdering | **-4-1** Krav | | |
| | **-2-4** Service provider | **-3-3** Krav og sikkerhedsniveauer | | | |

# ISA/IEC 62443-5 profil på vej

Ses mod USA er cybersikkerhedsstrategier og udarbejdelse af f.eks cybersecurity baselines for DER, distributed energy resources, igang.

Det har tidligere forlydt, at det amerikanske Department of Energy (DOE) har f.eks sammen med globale leverandører og en række stakeholders annonceret etablering af en "Electric Energy OT Security Profile" arbejdsgruppe understøttet af ISA99, der står bag ISA/IEC62443.

Denne planlagte "Electric Energy OT Security Profile" vil udmønte sig i et anerkendt cybersikkerheds work product og bliver en formel IEC62443 application guide for sikring af forskellige styresystemer i elproduktionen, transmissionen og distributionen.

Det følges tæt, hvordan udmøntningen sker.

Kilde: ISA Leading Development of Electric Energy Operational Technology Security Profile for IEC 62443 Standard

# Standarder i IEC 62351-serien

**- elsystemstyring og tilhørende informationsudveksling – Data og kommunikationssikkerhed**

| | | |
|---|---|---|
| DS/EN IEC | 62351-3:2023 | Kommunikationsnetværkers og -systemers sikkerhed |
| DS/EN IEC | 62351-4:2018 | Profiler indeholdende MMS |
| DS/EN IEC | 62351-5:2023 | Sikkerhed for protokoller |
| DS/EN IEC | 62351-6:2020 | Sikkerhed i IEC 61850 |
| DS/EN | 62351-7:2017 | Dataobjektmodeller til netværks- og systemstyring |
| DS/EN IEC | 62351-8:2020 | Rollebaseret adgangskontrol |
| DS/EN IEC | 62351-9:2023 | Cybersikkerhedsrelateret nøglehåndtering |
| DS/EN | 62351-11:2017 | XML-dokumenters sikkerhed |

**- start med DS/IEC/TS 62351-1:2007 Introduktion til sikkerhedsspørgsmål**

# Hvordan kan man komme i gang? Kursus, introduktion til OT-cybersikkerhed - for personer med IT-forståelse

Den teknologiske udvikling, OT's øgede opkobling til internettet og fremkomst af regulatoriske krav for OT cybersikkerhed som fx EU NIS2 kalder på større fokus i organisationerne, herunder hvordan man kan styrke sin it/OT-organisation

Arbejder du fx med it-sikkerhed, og ser behov for at øge din viden om OT-cybersikkerhed?

Vi har et nyt kursus for personer med it-forståelse, der ønsker mere viden om OT-cybersikkerhed, om ligheder og hvordan, det adskiller sig fra it-området. Det er ikke et meget teknisk kursus, men sætter dig i stand til at stille de rigtige spørgsmål..

## 10. april 2024

# Spørgsmål

**Søren Storm**
Seniorkonsulent | Senior Consultant
Sekretariater, udvalg og netværk I

E: sst@ds.dk
T: 39 96 62 08

**Henriette Brandstrup**
Konsulent, ejer, CyberWorks.dk

E: henriette.brandstrup@cyberworks.dk
T: 30613929