



Energistyrelsen

Vejledning: Kontrolelementer og vurdering af kompetencer inden for OT

Checkliste

Kontor/afdeling
Beredskab

Dato
06-07-2026



Energistyrelsen

Energistyrelsen

Carsten Niebuhrs Gade 43
1577 København V

T: +45 3392 6700
E: ens@ens.dk

www.ens.dk



Versionshistorik

Versions-nr.	Ændret	Ændret af	Kommentarer
1	08.07.2025	Søren Egede, konsulent	Dokumentet blev oprettet.
1.1	17.11.2025	Stine Buemann	Tydeliggørelse af fortrolighedsgrad i materialet i sidefod og på forsiden.
1.2	06.07.2026	Stine Buemann	Fortrolighedsstempel fjernet.



Indhold

Indledning	4
Certificeringer	4
Kurser	5
Erfaring	6
Tjekliste til vurdering af kompetencer	6



Indledning

Denne vejledning har til formål at hjælpe virksomhederne i energisektoren med at vurdere, om personer, der arbejder med OT-cybersikkerhed, har de rette kompetencer. Dette gælder, uanset om vedkommende skal ansættes som medarbejder i virksomheden, eller om vedkommende skal fungere som ekstern konsulent i en periode.

Da der findes mange måder at opnå kompetencer på inden for dette område, skal vejledningen betragtes som en checkliste og informationskilde – ikke som en udtømmende liste.

Det kan være svært at vurdere, om en person har de rette kompetencer. Dette er en generel udfordring, som ikke kun gør sig gældende inden for industriel cybersikkerhed, men også på tværs af mange brancher. Der findes dog nogle områder, som kan give gode indikationer på en persons kompetencer og erfaring inden for dette felt. Dette dokument eksemplificerer disse kompetencer og erfaringer.

Certificeringer

Certificeringer giver en form for verifikation af, at en person på tidspunktet for certificeringen har forstået og kan anvende den viden, som certificeringen dækker. Det er dog vigtigt at forstå, hvad indholdet af certificeringens tilhørende kurser er, og om dette stemmer overens med det kompetenceområde, der er behov for i den konkrete situation.

Kendte certificeringer inden for OT-sikkerhed er:

SANS GIAC ICS-certificeringer

SANS, i samarbejde med GIAC¹, udbyder tre certificeringer inden for OT-sikkerhed. Én af disse er relateret til amerikanske lovkrav (NERC-CIP) og er derfor ikke relevant for alle, men er alligevel inkluderet nedenfor for fuldstændighedens skyld.

SANS GIAC-certificeringer anses generelt for at være blandt de mest anerkendte inden for OT-sikkerhed og er kendt for deres høje faglige kvalitet.

SANS GIAC OT-certificeringer:

- Global Industrial Cyber Security Professional Certification (GICSP)²

¹ SANS Institute har et samarbejde når det gælder certificeringer til deres kurser. Dette er GIAC (giac.org).

² GICSP-certificeringen er for SANS ICS410 kursus (ICS/SCADA Security Essentials).



- GIAC Critical Infrastructure Protection Certification (GCIP) – NERC-CIP³
- GIAC Response and Industrial Defence (GRID)⁴

IEC 62443-certificeringer

ISA/IEC (International Society of Automation) har udarbejdet den mest kendte og udbredte standard inden for industriel cybersikkerhed – IEC 62443. I den forbindelse har ISA/IEC oprettet en række certificeringer, der er målrettet personer, som arbejder med eller implementerer IEC 62443-standarden, som er en standard, der omhandler cybersikkerhed i industrielle miljøer.

Der findes i alt fem forskellige certificeringer fra ISA/IEC, som er:

- ISA/IEC 62433 Cybersecurity Fundamentals Specialist⁵
- ISA/IEC 62433 Cybersecurity Risk Assessment Specialist⁶
- ISA/IEC 62433 Cybersecurity Design Specialist⁷
- ISA/IEC 62433 Cybersecurity Maintenance Specialist⁸
- ISA/IEC 62433 Cybersecurity Expert⁹

Kurser

Der findes mange udbydere af OT-sikkerhedskurser, både i Danmark og internationalt.

Kurserne er generelt kompetencegivende og giver et solidt grundlag, som kan danne basis for videre erfaring og specialisering. Kurser er vigtige for at opnå en forståelse af de grundlæggende principper og teknologier, der anvendes inden for OT-cybersikkerhed, og de fungerer som et godt fundament at bygge videre på i praksis.

³ GCIP-certificeringen er for SANS ICS456 kursus (Essentials for NERC CIP).

⁴ GRID-certificeringen er for SANS ICS515 kursus (ICS Visibility, Detection and Response).

⁵ Grundlæggende certificering med fokus på introduktion, roller, ansvar, terminologi, risiko, zoner og segmentering.

⁶ Fokus på risikovurdering i OT. Områder er aktiver og trusler, sårbarhedsanalyse, sikkerhedsniveau og mål.

⁷ Fokus på design med elementer som zoner og conduits, sikringsprincipper, netværk, arkitektur og adgangsstyring.

⁸ Fokus på drift, overvågning og vedligeholdelse. Elementer som patching, logning, hændelseshåndtering.

⁹ Denne certificering kræver, at man har alle de andre. Se mere på

<https://www.isa.org/certification/certificate-programs/isa-iec-62443-cybersecurity-certificate-program>



For at kunne give mere præcise informationer om kurser er det vigtigt at vide, hvad for et område inden for OT-cybersikkerhed, der er behov for. Derfor er der her givet et generelt overblik over kompetencer inden for OT-cybersikkerhed, der vurderes at være relevante, og som personer bør have viden om eller bør tilegne sig:

- Grundlæggende forståelse for industriel automation (mekanik, formål og risici)
- Forskelle mellem IT og OT og deres grundlæggende komponenter
- Netværk og systemforståelse
- Arkitektur i relation til cybersikkerhed i OT (fx Purdue-modellen)
- OT-protokoller og hvad de bruges til
- Standarder og lovgivninger i OT
- Logning og monitorering i industrielle miljøer
- Angreb og angrebs vektorer mod OT-miljøer
- ICS Kill Chain
- Sårbarheder og kendte angreb på OT

Erfaring

Erfaring er en vigtig faktor, særligt i kombination med kurser og certificeringer. Dog kan erfaring være vanskelig at vurdere alene, da det ofte fremgår i et CV uden dybere kontekst.

Det er vigtigt at se på, hvad personen konkret har arbejdet med, og om arbejdet har været kontinuerligt. Fx kan en person have syv års erfaring med OT-sikkerhed, men kun have brugt 100 timer på området i alt. I så fald er erfaringen begrænset. Hvis en person omvendt har arbejdet med OT-sikkerhed i syv år og anvendt eksempelvis 80 % af sin arbejdstid på området årligt, er der tale om en stærk og anvendelig erfaring – dog kan denne være begrænset til det specifikke område, som vedkommende har arbejdet med.

En meget vigtig erfaring for at kunne lave OT-cybersikkerhed er forståelsen for OT. Det er derfor meget vigtigt, at en person har været på et eller flere produktionssteder (OT) og har fået en god rundvisning, fået en god forståelse af det og snakket med personer i produktionen.

Tjekliste til vurdering af kompetencer

Denne tjekliste er udarbejdet på baggrund af informationen beskrevet i de foregående afsnit. Det er vigtigt at understrege, at listen kun fungerer som en vejledning og ikke er fuldstændig dækkende.

- Har personen en certificering?



- Hvornår er certificeringen opnået, og inden for hvilket område?
- Hvilke kurser inden for OT har personen gennemført?
 - Hvad for nogle relaterede kurser har personen gennemført?
 - Er der løbende aktiviteter som fx tillægskurser, konferencer eller andre kompetencegivende opkvalificeringer?
- Hvor lang tid har personen arbejdet med OT-sikkerhed?
 - Er der oplysninger om omfanget og kontinuiteten i arbejdet med OT-cybersikkerhed?
 - Er der konkrete projekter eller anden relevant erfaring, der underbygger kompetencen? Dette bør være beskrevet i CV'et.
- Har personen været fysisk på en produktionslokation?
- Kan personen forklare generelle OT-termer og begreber samt demonstrere forståelse for deres anvendelse?