



6076736363376510606
76801176786868 3-87
765786106 0126 81
765761701961 838
496196065477 87-10

2632372727732176262
32467732342424 7 43
321342762 6782 47
32132736752 DATA-03 8
05275262103



OT-sikkerhed

**Undgå cyberangreb og -trusler
med NIRAS' ekspertise og
løsninger til OT-sikkerhed.**

OT-sikkerhed

NIRAS forbedrer din sikkerhed med indsigt i din virksomheds svagheder og styrker. Målet er konkrete, designede indsatser og løsninger til din OT-sikkerhed for at undgå cyberangreb og -trusler.

Operational teknologi

OT (Operational teknologi) er software og hardware, der anvendes til at styre industrielle anlæg, hvor der ofte sker en interaktion med fysiske objekter. OT involverer normalt miljøer, som omfatter industrielle kontrolsystemer (IACS) og SCADA/PLC systemer. Det kan eksempelvis være industrielle systemer med overvågningskontrol- og dataindsamling.

OT-sikkerhed

Ved OT-miljøer forstås et samarbejde mellem systemer og komponenter, som kan blive udsat for eventuelle sikkerhedsangreb udefra. Af den årsag skal OT-miljøerne altid inddrages i sikkerhedsprocesser og -protokoller. Ellers får det store konsekvenser, hvis der sker nedbrud. OT-sikkerhed er dermed mere kompleks og påvirker ofte økonomi, produktion, dataintegritet, mv. NIRAS tager udgangspunkt i CER- og NIS2-direktiverne, med brug af f.eks. ISO/IEC 27000 og ISA/IEC 62443 serier. NIRAS tilbyder den

nødvendige ekspertise og kommer med konkrete indsatser og løsninger til OT-sikkerheden alt efter virksomhedens behov og givne situation.

Implementering af OT-sikkerhed

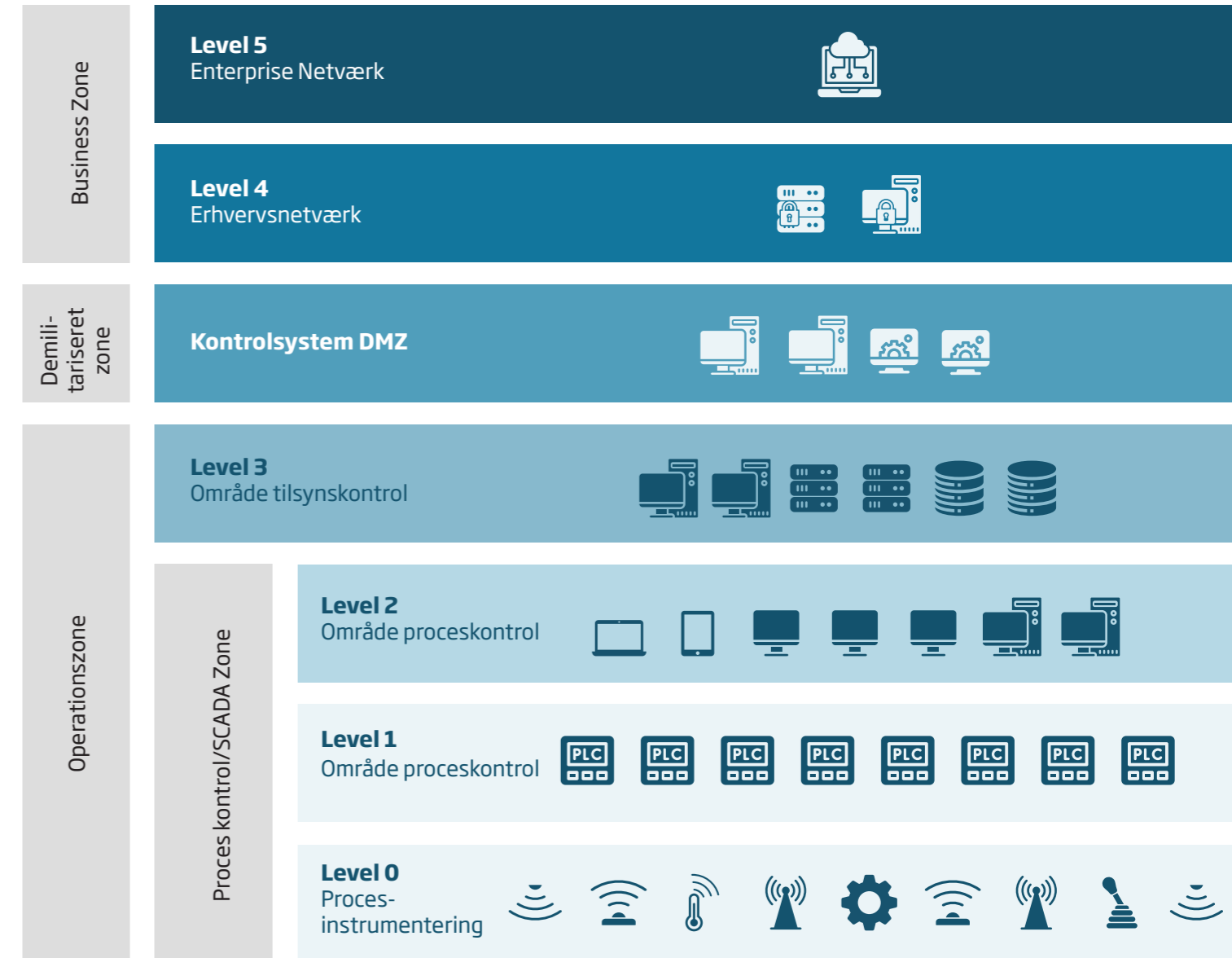
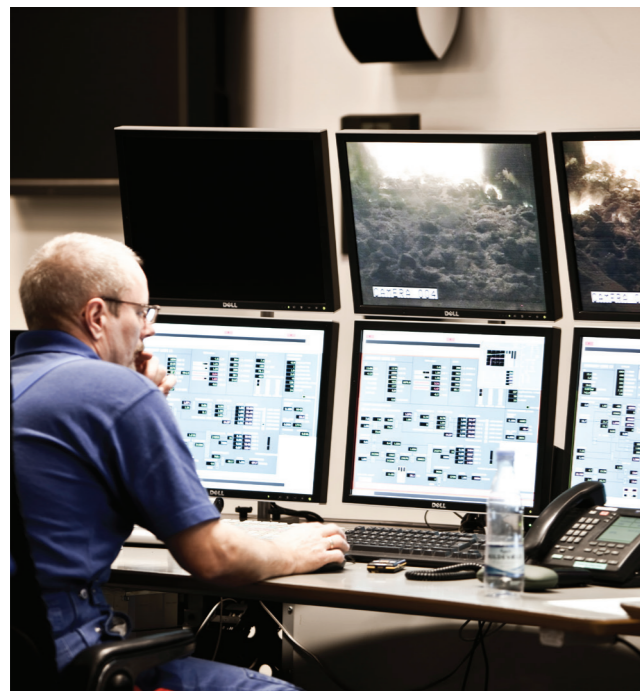
NIRAS tilbyder flere eksperter på området, der står klar til at afdække sikkerheden på dit procesanlæg. Med vores erfaring i og kendskab til IACS og SCADA systemer er vi en kompetent og effektiv samarbejdspartner på OT-sikkerhedsopgaver uanset virksomhedsstørrelse.

Vi assisterer med sikker og central brugerstyring, rådgivning om fysisk adgang til anlæg, tjek af software og indstillinger, definition af backup og genetablering, dokumentation af dit system-setup, udførelse af fuld audit af dit system og meget mere.

NIRAS anbefaler grundlæggende ti trin, som der også tages udgangspunkt i.

Kom godt i gang med implementering af OT-sikkerhed

1. Erkend, der er en OT-udfordring, og skab forståelse i virksomheden
2. Afsæt nødvendige ressourcer
3. Udpeg medarbejdere med sikkerhedsansvar
4. Skab bevidsthed hos medarbejderne
5. Skab overblik over OT-systemer
6. Udfør risikovurdering
7. Udarbejd en plan for nøddrift (Redundans)
8. Opdatér systemer og udfør nye sikkerhedstiltag
9. Etablér beredskab og handlingsplan
10. Udfør løbende opfølgninger og systemovervågning



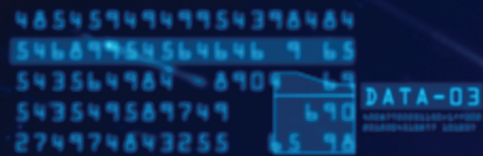
Sikkerhed i industrielle kontrolsystemer

Industrielle kontrolsystemer er designet til at være robuste og pålidelige. Men de er ikke immune over for angreb udefra. Der er tale om komplekse systemer, og dette kræver proceserfaring og proceskendskab. NIRAS tilbyder OT-sikkerhed, der ligger i operationszonen, nærmere bestemt: Level 0,1,2 og 3. De andre Levels tilhører IT-sikkerhed, som ofte ligger i egen IT afdeling.

Vi assisterer blandt andet med:

- Sikker og central brugerstyring
- Rådgivning om fysisk adgang til anlæg
- Tjek af software og installationer
- Definition af Backup og genetablering
- Dokumentation
- Fuld audit af system

Og meget mere.



Michael Svend Rørby Petersen

Project Manager
+45 2968 7180
mrp@niras.dk



Klaus Christensen

Afdelingsleder - Automation og Data
+45 2948 3391
kch@niras.dk



Anni Offersgaard

Sales & Market Director
+45 4299 0309
aoff@niras.dk

Følg NIRAS:

Bliv opdateret på nyheder, de nyeste metoder og løsninger på www.data.niras.dk.