CYBERSECURITY I INDUSTRIEN

HVAD BØR ELEKTRIKEREN I INDUSTRIEN KUNNE?

PROGRAM

- Velkomst og introduktion
- Hvad er Operational Technology (OT)?
- Kernekomponenter i et OT-system
- Virkelige OT-cyberangreb
- Hvordan kan vi sikre os?
- Opsamling og evaluering
- Afslutning

VELKOMST OG INTRODUKTION

- Cyber-In: Cybersecurity in the interconnected industry
  - Projektet har til formål at skabe en cybersikkerhedskultur i industrielle miljøer gennem tværfagligt samarbejde mellem IT- og OT-profiler.
  - Det sigter mod at udvikle kompetencerne hos erhvervsskolelærere i første omgang og herefter overføre disse kompetencer til den fremtidige arbejdsstyrke, der uddannes på erhvervsskolerne
  - Lignende kurser kommer til at køre i Spanien, Italien, Holland og Estland

LÆRINGSMÅL

- Identificere elektrikeres stadig vigtigere rolle i at bidrage til digital sikkerhed i industrien
- Beskrive arkitekturen i et Operational Technology (OT)-miljø, herunder dets nøglekomponenter og deres roller
- Skelne mellem de primære cybersikkerhedsprioriteter og sårbarheder i OT-systemer sammenlignet med IT-miljøer
- Analysere virkelige OT-cyberangreb ved at identificere udnyttede sårbarheder, anvendte metoder og lærte lektioner
- Identificere og forklare de primære cybersikkerhedsudfordringer i OT-kontekster
- Beskrive Purdue segmenteringsmodellen, herunder forklare koncept og mål med netværkssegmentering i OT-miljøer

Erasmus+

Roskilde Tekniske Skole

TILRETTELÆGGELSE

- Kurset er så vidt muligt tilrettelagt så I selv kan bruge oplæg, øvelser og opgaver til jeres egne elever
- Booklet – med forkortelser!
- I er særdeles velkommen til selv at byde ind med viden og spørgsmål ☺
- Kurset slutter med en test og en evaluering

HVORFOR ELEKTRIKERE?

- Elektrikere taler it'sk
- Elektrikere spiller en central rolle ift. digital sikkerhed i industrien:
  - Forståelse af OT-systemer og deres sårbarheder
  - Sikker installation og konfiguration
  - Vedligeholdelse og opdatering
  - Systematik ift. afvigelser
  - Uddannelse og kompetenceudvikling

Cyber-In

Erasmus+

Roskilde Tekniske Skole

HVORFOR ELEKTRIKERE?

- Elektrikere spiller en central rolle ift. digital sikkerhed i industrien:
  - **Forståelse af OT-systemer og deres sårbarheder**
  - Sikker installation og konfiguration
  - Vedligeholdelse og opdatering
  - Systematik ift. afvigelser
  - Uddannelse og kompetenceudvikling

- Kendskab til netværk og protokoller
- Identifikation af sårbarheder
- Adgangskontrol

Cyber-In

Erasmus+

Roskilde Tekniske Skole

HVORFOR ELEKTRIKERE?

- Elektrikere spiller en central rolle ift. digital sikkerhed i industrien:
  - Forståelse af OT-systemer og deres sårbarheder
  - **Sikker installation og konfiguration**
  - Vedligeholdelse og opdatering
  - Systematik ift. afvigelser
  - Uddannelse og kompetenceudvikling

- "Security by Design" og "Privacy by Design"
- Korrekt segmentering af netværk
- Sikre kabelføring og fysisk beskyttelse
- Dokumentation og versionsstyring

Cyber-In
Erasmus+
Roskilde Tekniske Skole

HVORFOR ELEKTRIKERE?

- Elektrikere spiller en central rolle ift. digital sikkerhed i industrien:
  - Forståelse af OT-systemer og deres sårbarheder
  - Sikker installation og konfiguration
  - **Vedligeholdelse og opdatering**
  - Systematik ift. afvigelser
  - Uddannelse og kompetenceudvikling

- Firmware og sikkerhedsopdateringer
- Regelmæssig inspektion
- Automatiske back-up

Erasmus+
Roskilde Tekniske Skole

HVORFOR ELEKTRIKERE?

- Elektrikere spiller en central rolle ift. digital sikkerhed i industrien:
  - Forståelse af OT-systemer og deres sårbarheder
  - Sikker installation og konfiguration
  - Vedligeholdelse og opdatering
  - **Systematik ift. afvigelser**
  - Uddannelse og kompetenceudvikling

- Identifikation af afvigelser
- Assistance i genoprettelse

Cyber-In

Erasmus+

Roskilde Tekniske Skole

VELKOMST OG INTRODUKTION

- Elektrikere spiller en central rolle ift. digital sikkerhed i industrien:
  - Forståelse af OT-systemer og deres sårbarheder
  - Sikker installation og konfiguration
  - Vedligeholdelse og opdatering
  - Systematik ift. afvigelser
  - **Uddannelse og kompetenceudvikling**

- Specialiseret viden (fx IEC 62443 standarden)
- Tværfunktionelt samarbejde
- Bevidsthed om trusler

Cyber-In

Erasmus+

Roskilde Tekniske Skole

HVORFOR ELEKTRIKERE?

- Elektrikere taler it'sk
- Elektrikere spiller en central rolle ift. digital sikkerhed i industrien:
  - Forståelse af OT-systemer og deres sårbarheder
  - Sikker installation og konfiguration
  - Vedligeholdelse og opdatering
  - Systematik ift. afvigelser
  - Uddannelse og kompetenceudvikling
- **Er dette noget I kan genkende? Diskutér 5 min. med sidemanden/damen.**

HVAD ER OPERATIONAL TECHNOLOGY (OT)?

- Definition på Operational Technology (OT):
  Hardware og software til overvågning, styring og automatisering af fysiske processer i industrielle omgivelser
- OT's kerneformål: Tilgængelighed, sikkerhed og realtidskontrol
- Typiske anvendelsesområder: Automatiserede produktionslinjer, pipeline management, kemisk forarbejdning, energiproduktion og -distribution
- Særpræg ved OT-miljøer: Lang levetid for udstyr, proprietære protokoller, begrænset båndbredde, minimal nedetidstolerance
- Ofte ældre protokoller uden kryptering og autentificering
- OT udstyr er som regel opsat, programmeret og vedligeholdt af folk fra produktionen (og IKKE it-folk)
- OT ligger ofte organisatorisk i en gråzone. Der er sjældent en OT-chef
- IT og OT taler sjældent samme sprog

Erasmus+

Roskilde Tekniske Skole

SAMMENLIGNING AF OT OG IT

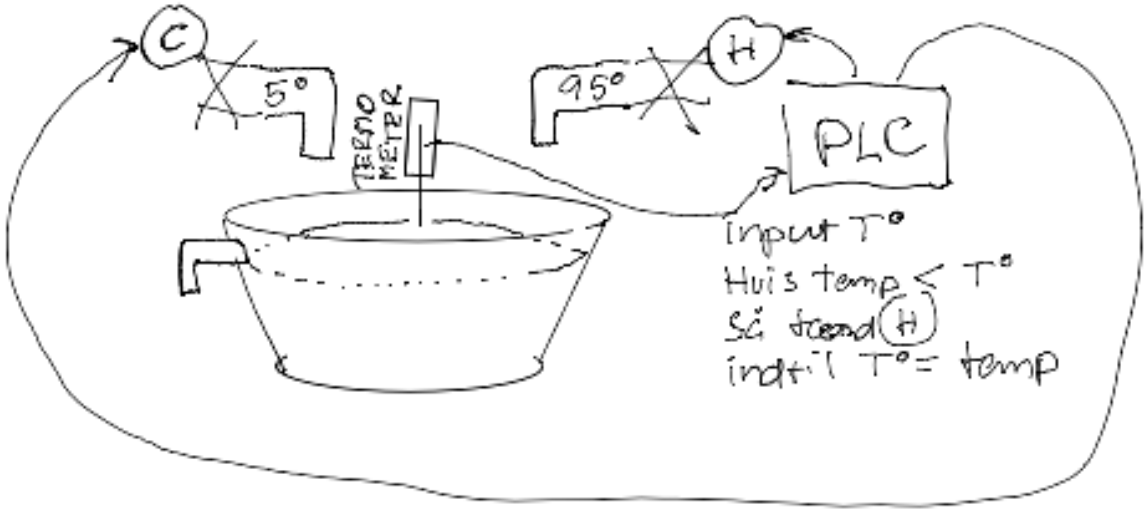
	OT	IT
Mål og prioriteter	Styring af den fysiske verden	Styring og beskyttelse af information
Driftsikkerhed	Nul nedetid	Hyppig vedligeholdelse
Arkitektur og kommunikation	Lukkede netværk	Åbne netværk
Livscyklus	Sjældne opdateringer	Automatiserede opdateringer
Sikkerhedsfokus	Tilgængelighed	Databeskyttelse
Hardware	Lang levetid	Kort levetid

HVAD ER OPERATIONAL TECHNOLOGY (OT)?

Opgave 1A:

Lav et automatiseringsprogram

- Formål: at skabe bevidsthed omkring udfordringer ved automatisering
- Form: gruppearbejde - varighed: 20 min.
  - Gruppestørrelse: 3 eller 2
- Tegn en model der viser en PLC-funktion/styring



Erasmus+

Roskilde Tekniske Skole

HVAD ER OPERATIONAL TECHNOLOGY (OT)?

Opgave 1B:

Giv tegningen til en anden gruppe

- Den anden gruppe prøver at ”obstruere” PLC funktionen. Fx: Der kravler en edderkop ind foran bevægelsessensoren. Kom med to-tre eksempler
- Varighed: 5 min

HVAD ER OPERATIONAL TECHNOLOGY (OT)?

Opgave 1C:

Giv tegningen (med noter om obstruktionerne) tilbage til første gruppe

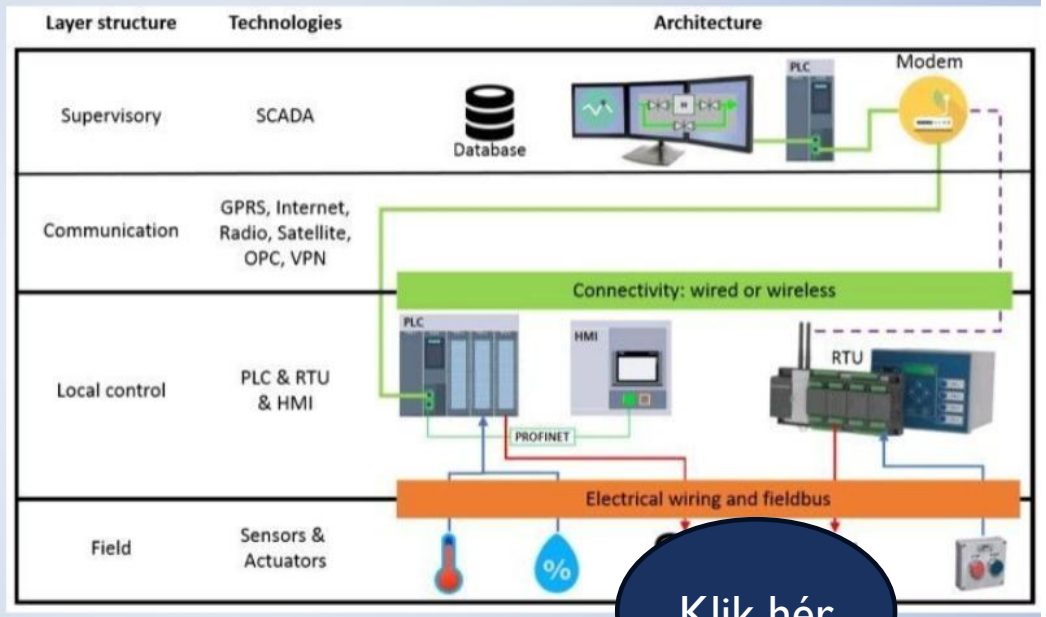
- Første gruppe skal nu forbedre sikkerheden i ”programmet” så uhensigtsmæssigheder undgås
- Varighed: 10 min

PAUSE

KERNEKOMPONENTER I ET OT-SYSTEM

OT-systemer: En integreret tilgang til industriel kontrol

Operationelle teknologisystemer (OT-systemer) spiller en afgørende rolle i styring og overvågning af industrielle processer. Disse systemer består af flere essentielle fysiske komponenter som sensorer, aktuatorer, PLC'er, HMI'er, RTU'er og SCADA-systemer, der arbejder sammen for at skabe en effektiv og responsiv infrastruktur.



KERNEKOMPONENTER I ET OT-SYSTEM

Som elektriker er du afgørende for den fysiske integritet af OT-systemer

- Installation og vedligeholdelse: Korrekt installation og kabling af PLC'er, SCADA-komponenter og HMI'er er fundamental for deres funktion og sikkerhed
- Fysisk sikring: Du er (med)ansvarlig for at sikre, at programmeringsporte på PLC'er og RTU'er er utilgængelige for uautoriseret adgang. Det kan inkludere installation af låse, forseglinger eller andre fysiske barrierer
- Sensorintegritet: Sikring af korrekte installationer af sensorer og aktuatorer, herunder kabelføring, for at forhindre signalmanipulation eller uautoriseret adgang til feltkabling. Regelmæssig kontrol af fysisk tilstand
- Håndtering af ældre udstyr: Rapportering af ældre, upatchede systemer og deltagelse i implementering af kompenserende kontroller som fysisk isolation og sikker kabling omkring disse enheder
- Strømforsyning: Sikring af stabil og beskyttet strømforsyning til disse kritiske komponenter for at undgå uplanlagte nedlukninger, der kan udnyttes af angribere
- Overvågning og rapportering: At bemærke og rapportere enhver fysisk manipulation, usædvanlig adfærd eller skade på kabinetter, der huser disse enheder
- Kommunikationsinfrastruktur: Forståelse af krav til redundans (backups) og Quality of Service (Ydeevneprioritering) i netværksopsætningen

Erasmus+
Roskilde Tekniske Skole

VIRKELIGE OT-CYBERANGREB

- **Stuxnet (2010):** Et avanceret angreb rettet mod Irans atomanlæg, hvor en computerorm blev brugt til at forårsage fysisk skade på anlæggets maskineri via USB-drev og Windows-sårbarheder.
- **Angrebet på det ukrainske elnet (2015):** Et cyberangreb, der resulterede i en stor strømafbrydelse for over 230.000 mennesker og afslørede sårbarheden i kritisk infrastruktur.
- **Industroyer / CrashOverride (2016):** Et angreb på Kyiv's el-transmissionsnet, som resulterede i et black-out af dele af Kyiv's el-forsyning
- **Triton Malware (2017):** Dette angreb var rettet mod et petrokemisk anlæg i Saudi-Arabien og specifikt mod anlæggets sikkerhedssystem (SIS). Det viste, hvordan cyberangreb kan skabe reelle fysiske farer.

Erasmus+

Roskilde Tekniske Skole

VIRKELIGE OT-CYBERANGREB

Cyber-In

Stuxnet (2010)

- Mål: Irans Natanz-anlæg til uranberigelse
- Angrebsvektor: Inficerede USB-drev introducerede ormen i et netværk uden internetforbindelse (air-gapped).
- Mekanisme: Stuxnet ændrede specifikt Siemens Step7 PLC-kode for periodisk at få centrifugerne til at rotere ved ødelæggende hastigheder, mens den viste falske normale aflæsninger til operatørerne.
- Påvirkning: Over 1.000 centrifuger blev ødelagt, hvilket satte Irans berigelsesprogram flere år tilbage.
- Betydning: Første bevis på, at et cybervåben kunne bryde igennem netværksisolering og forårsage fysisk ødelæggelse gennem målrettet PLC-manipulation.

Erasmus+
Roskilde Tekniske Skole

VIRKELIGE OT-CYBERANGREB

BlackEnergy (2015)

- Mål: Ukraines el-distributionssystem
- Angrebsvektor: Phishing-e-mails leverede malware med ondsindede makroer, som indsamlede loginoplysninger.
- Mekanisme: Hackere brugte de stjålne legitimationsoplysninger til at logge ind på SCADA-arbejdsstationer og betjente afbrydere for at afbryde strømmen. De deaktiverede også backupsystemer og korrumperede firmware for at forsinke genopretningen.
- Påvirkning: Næsten en kvart million indbyggere mistede strømmen i flere timer midt om vinteren.
- Betydning: Viste, at relativt enkel social engineering kombineret med adgang til OT kan lamme kritisk infrastruktur.

VIRKELIGE OT-CYBERANGREB

Industroyer / CrashOverride (2016)

- Mål: Kyivs eltransmissionsnet
- Angrebsvektor: Specialudviklet malware, der udnyttede industrielle protokoller (IEC 101/104).
- Mekanisme: Malwaren kommunikerede direkte med afbrydere og koblingsudstyr via native kommandoer og lancerede derefter et destruktivt modul, der slettede enheders firmware.
- Påvirkning: Midlertidigt strømsvigt i dele af Kyivs elnet; manuel indgriben var nødvendig for at genoprette driften.
- Betydning: Viste angribernes dybe forståelse af IEC-protokoller og transformerstationers arkitektur — et skridt videre end de generiske ICS-værktøjer, der blev set i tidligere angreb.

VIRKELIGE OT-CYBERANGREB

Triton / HatMan (2017)

- Mål: Petrokemisk anlæg i Mellemøsten
- Angrebsvektor: Sandsynligvis spear-phishing for at infiltrere ingeniørarbejdsstationer, der kørte Triconex Safety Instrumented System (SIS)-controllere.
- Mekanisme: Malwaren manipulerede SIS-logikken for at deaktivere sikkerhedsfunktioner, hvilket potentielt kunne få anlægget til at køre usikkert uden at udløse nødstop.
- Påvirkning: Driften blev standset, da ingeniører opdagede uregelmæssigheder; der skete ingen fysisk skade, men hændelsen afslørede risikoen for en masseulykke.
- Betydning: Den første kendte malware, der specifikt var designet til at angribe sikkerhedssystemer, hvilket markerede et nyt niveau af hensigt om at forvolde fysisk skade.

Erasmus+
Roskilde Tekniske Skole

VIRKELIGE OT-CYBERANGREB

Opsummering

- Initial adgang via IT-vektorer: Phishing, ondsindede e-mailvedhæftninger og kompromitterede VPN-legitimationsoplysninger er udbredte indgangspunkter og udnytter IT/OT-konvergens til at springe fra forretningsnetværk ind i kontrolmiljøer.
- Lateral bevægelse og privilegieeskalering: Når angribere først er inde, bruger de legitime administrative værktøjer eller protokolbevidst malware til at kortlægge netværket, indsamle servicelegitimationsoplysninger og opnå kontrol over PLC/HMI-servere.
- Protokolmanipulation: Angriberne udformer native Modbus-, DNP3- eller IEC-meddelelser for at udsende uautoriserede kommandoer direkte til feltudstyr og dermed omgå højere niveauers sikkerhedsforanstaltninger.
- Supply-chain- og USB-spredning: Målrettede malwarevarianter (som Stuxnet) udnytter flytbare medier til at trænge ind i netværk uden internetforbindelse, mens supply-chain-angreb kompromitterer leverandørers softwareopdateringer for at distribuere ondsindet kode.
- Destruktive payloads og wipers: Avancerede værktøjssæt indeholder moduler, der kan slette firmware, overskrive kritiske konfigurationstabeller eller ødelægge proceshistoriske databaser — hvilket i høj grad forlænger nedetid og genopretning.

Cyber-In
Erasmus+
Roskilde Tekniske Skole

VIRKELIGE OT-CYBERANGREB

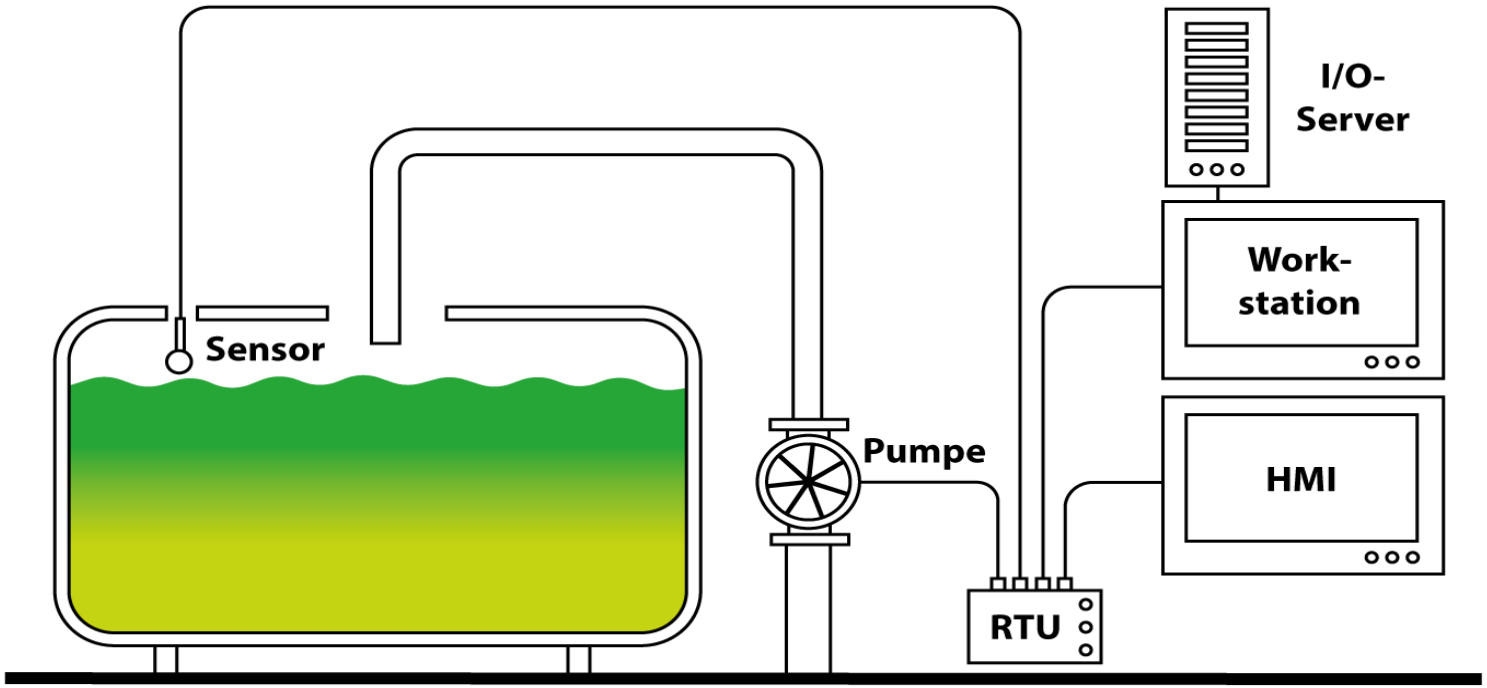
Elektrikerens rolle

- Sikkerhedsbevidsthed: Forståelse af de alvorlige konsekvenser af et cyberangreb understreger vigtigheden af din rolle i at opretholde fysisk sikkerhed og følge procedurer (f.eks. at være forsigtig med USB-enheder for at undgå at introducere malware som Stuxnet)
- Rapportering af anomalier: Din opmærksomhed på uregelmæssigheder i udstyr eller netværk (f.eks. usædvanlig adfærd, forkert kabling) kan være afgørende for tidlig detektion af et angreb.
- Hurtig inddæmning: I tilfælde af en hændelse kan din evne til hurtigt og sikkert at udføre fysisk isolering af kompromitterede segmenter, afbryde strømmen til kritiske enheder eller skifte til manuel kontrol være afgørende for at inddæmme angrebet.
- Rapportering: Deltag i "no-blame"-politikker og rapporter straks mistænkelig fysisk aktivitet eller nær-ved-ulykker. Din observation kan give værdifuld information til sikkerhedsteamet.
- Deltagelse i øvelser: Deltag i regelmæssige øvelser og simuleringer for at teste responstider og koordination mellem IT og OT-personale.

OPGAVE I CYBER-AWARENESS

Opgave

- En pumpe har til opgave at opfylde en udendørs tank med miljøfarlige væsker. Der er derfor installeret en sensor som sender signal, hvis tanken er ved at blive overfyldt. Hvilke sikkerhedsmæssige overvejelser skal elektrikeren gøre sig, når han/hun skal lave installationen? Brug 10 min. til at diskutere i gruppen, og herefter plenum.



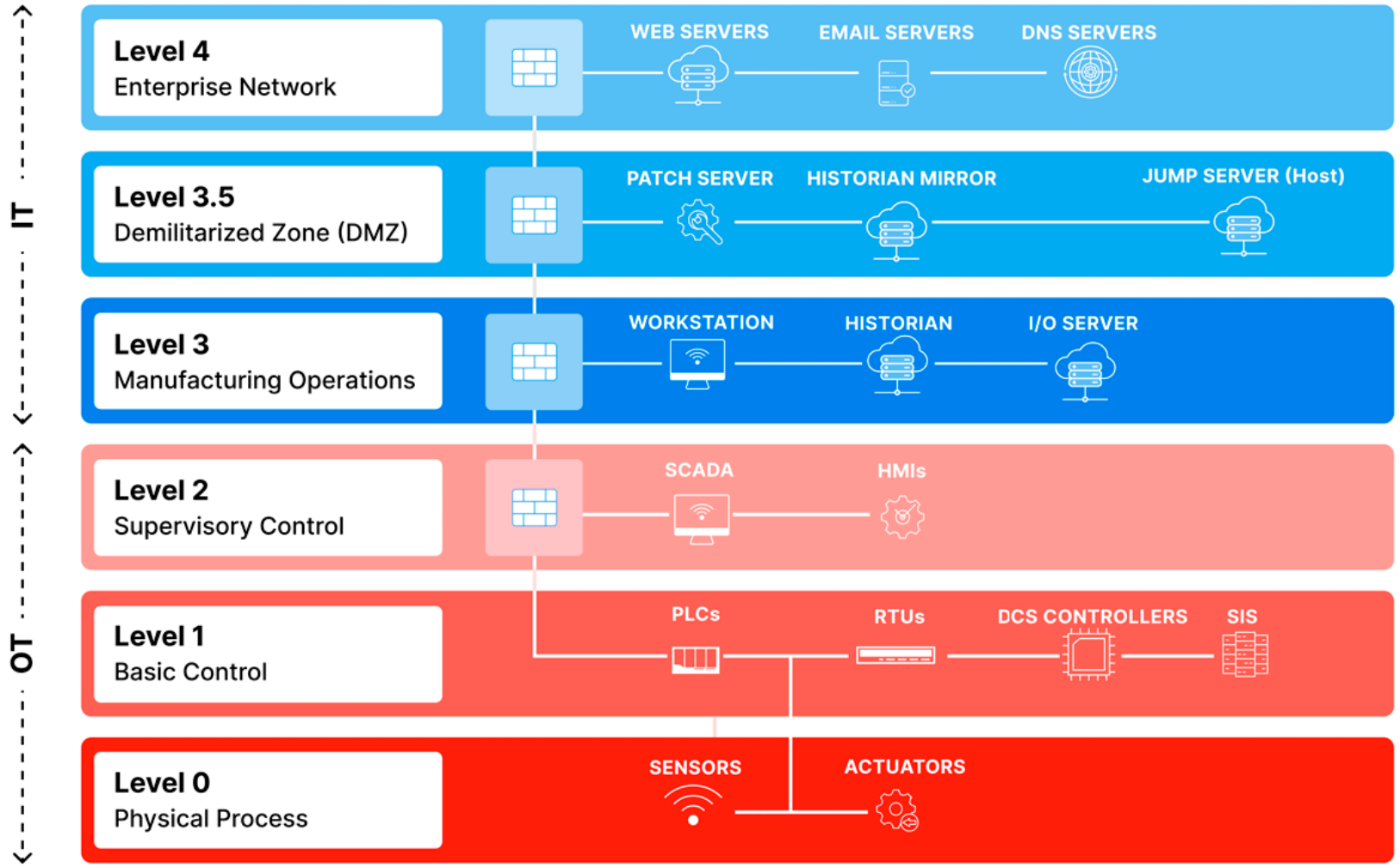
Cyber-In

Erasmus+

Roskilde Tekniske Skole

PAUSE

PURDUE-MODELLEN: EN RAMME FOR OT-SIKKERHED

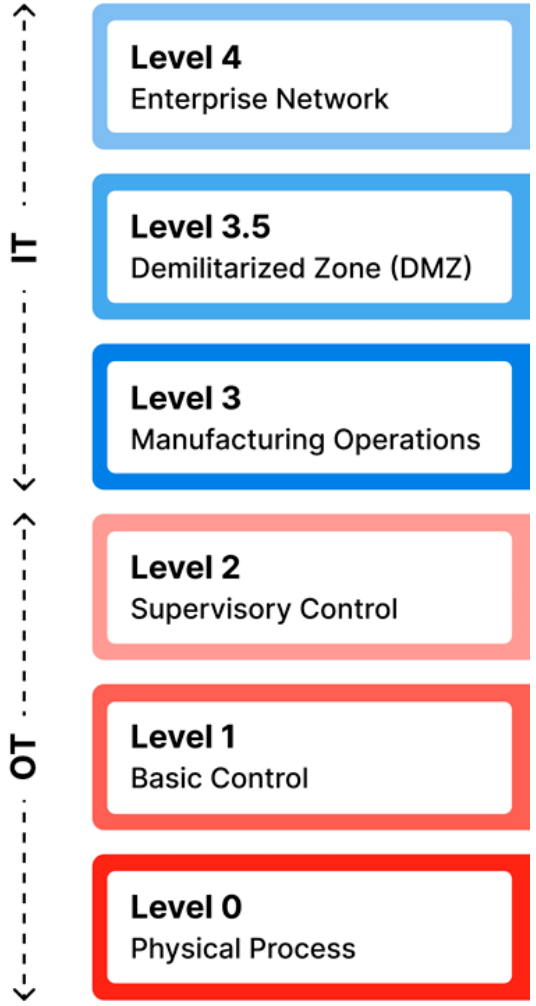


Cyber-In

Erasmus+

Roskilde Tekniske Skole

PURDUE-MODELLEN: EN RAMME FOR OT-SIKKERHED



Purduemodellen blev udviklet i 1990'erne af Theodore J. Williams på Purdue University

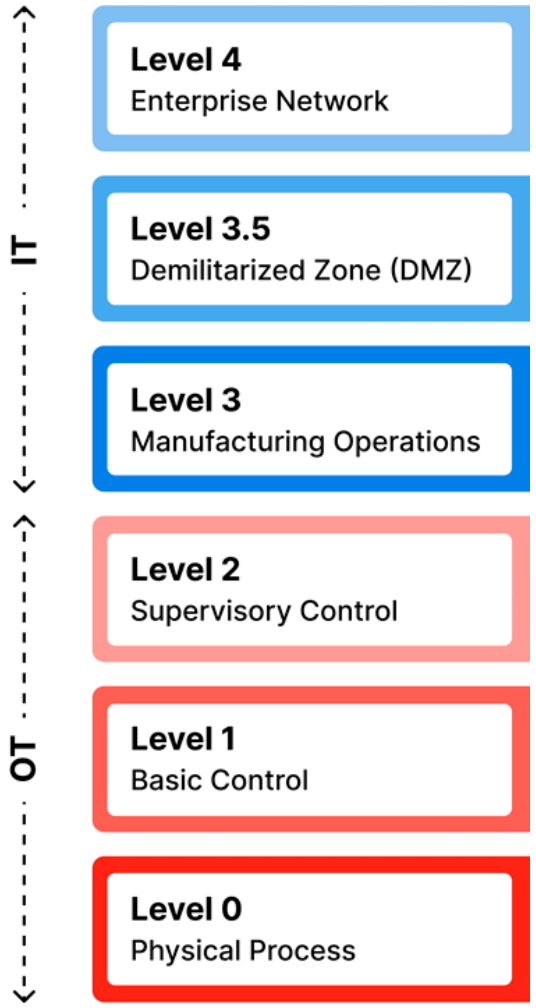
- Den blev udviklet for at skabe en struktureret tilgang til at segmentere og styre industrielle kontrolsystemer og deres integration med forretningsnetværk.
- Målet var at skabe en model, der kunne organisere komplekse systemer i distinkte zoner eller lag med specifikke sikkerhedshensyn.
- Således sætter den standard for hvordan man kan adskille industrielle operationssystemer fra forretningsmæssige IT-systemer, for at forbedre sikkerheden og effektiviteten af industrielle automatiserede processer.

Cyber-In

Erasmus+

Roskilde Tekniske Skole

PURDUE-MODELLEN: EN RAMME FOR OT-SIKKERHED



Elementer der bidrager til sikkerheden i Purduemodellen

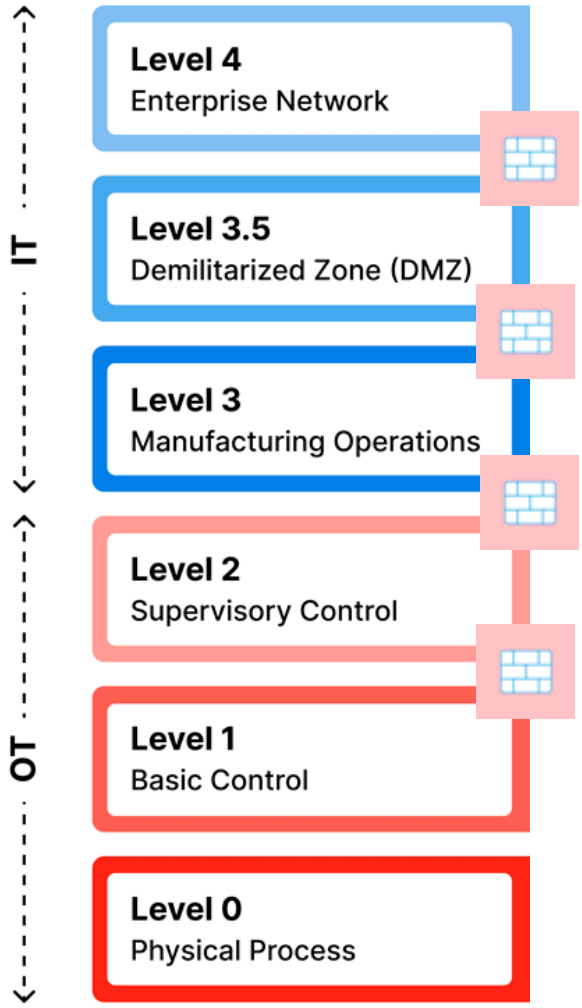
- Firewall's
- Demilitarized Zone (DMZ)
- Data Dioder
- Virtuelle LAN (VLAN'er)
- Overvågning og Trusselsdetektion
- Patch- og ændringsstyring
- Fysiske sikkerhedslag
- Logning og Auditering

Cyber-In

Erasmus+

Roskilde Tekniske Skole

PURDUE-MODELLEN: EN RAMME FOR OT-SIKKERHED



Firewalls

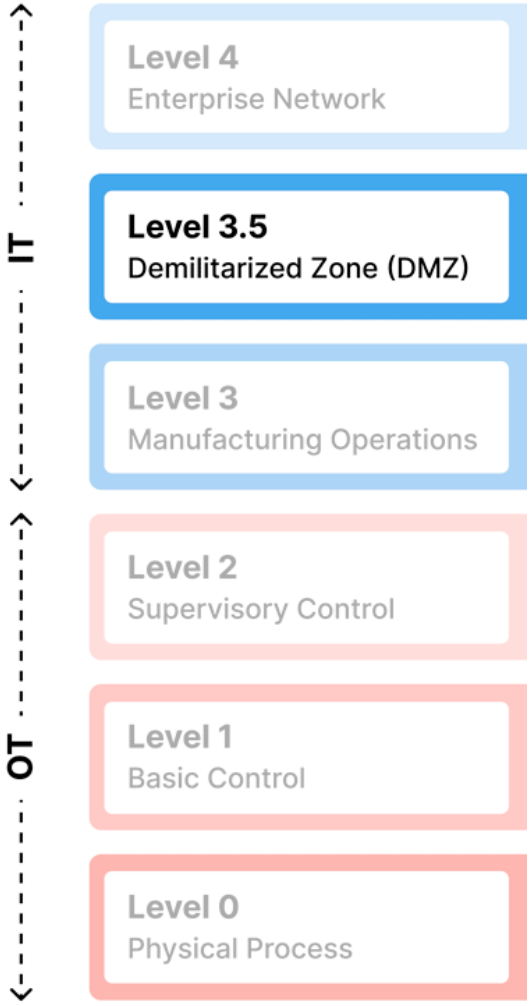
- Firewalls er digitale produkter der typisk er placerede i routere eller servere. De skaber en barriere mellem et betroet internt netværk og ubetroede eksterne netværk, hvilket forhindrer uautoriseret adgang og cybertrusler
- Forskellige typer firewalls:
  - Pakke-filtrerende firewall (Packet Filtering Firewall)
  - Stateful Inspection firewall
  - Proxy firewall
  - Næstegenerations firewall (Next-Generation Firewall – NGFW)
- I purduemodellen er firewalls brugt mange forskellige steder for at skabe sikkerhedsbarrierer mellem de forskellige segmenter.

Cyber-In

Erasmus+

Roskilde Tekniske Skole

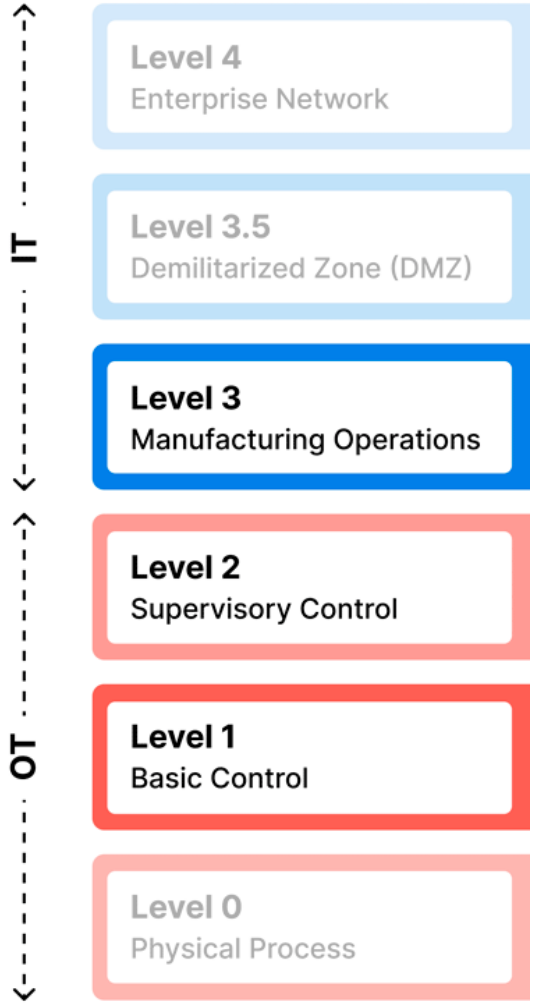
PURDUE-MODELLEN: EN RAMME FOR OT-SIKKERHED



DMZ'er

- DMZ står for Demilitarized Zone, der skal forstås som 'den fredsbevarende styrke' mellem eksterne (4) og interne (3) netværk
- Indgående og udgående trafik gennem DMZ'en er strengt filtreret gennem firewalls og jumpservere
- DMZ hoster tjenester, der skal være tilgængelige udefra, men som ikke skal have direkte adgang til det interne produktionsnetværk, som fx fjernstyrings servere og værktøjer, cloud-baserede sikkerhedstjenester, ERP (Enterprise Resource Planning) og systemer til dataopsamling fra OT-miljøet

PURDUE-MODELLEN: EN RAMME FOR OT-SIKKERHED



Andre sikkerhedssystemer

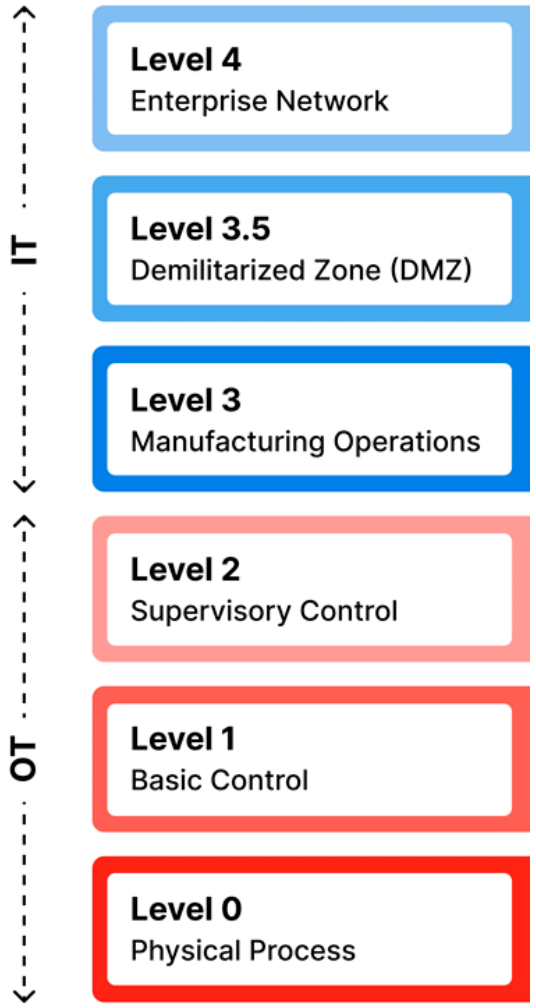
- **Data dioder**: Envejsnetværksenheder, der fysisk eller logisk blokerer returtrafik, hvilket sikrer, at data kun kan flyde fra OT til IT, men ikke omvendt, hvilket giver en ekstrem form for segmentering i højrisikokontekster
- **Virtuelle LAN (VLAN'er):** VLAN'er muliggør oprettelsen af flere logiske netværk på en enkelt fysisk infrastruktur. Ved at tildele forskellige porte eller enheder til særskilte VLAN-ID'er, kan organisationer adskille trafik efter funktion, afdeling eller sikkerhedsniveau
- **Overvågning og trusselsdetektion:** Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Dybdegående pakkeinspektion (DPI), Kontinuerlig overvågning og anomalidetektion, Security Information and Event Management (SIEM)
- **Patch- og ændringsstyring:** Tilpasning af firmwareopgraderinger med planlagte produktionsstop og brug af testlaboratorier til at validere patches på forhånd.

Cyber-In

Erasmus+

Roskilde Tekniske Skole

PURDUE-MODELLEN: EN RAMME FOR OT-SIKKERHED



Andre sikkerhedssystemer

- **Fysiske sikkerhedslag:** Sikring af paneler, låsning af skabe og implementering af manipulationssensorer
- **Logning og Auditering:** Detaljerede logs over kommunikation og konfigurationsændringer vedligeholdes på tværs af alle niveauer for at understøtte detektion og undersøgelse af mistænkelig aktivitet
- **Applikationshvidlistning:** Begrænsning af eksekverbar kode på PLC'er, HMI'er og SCADA-servere til kun godkendte binære filer
- **SSL-inspektion:** Afgørende for at forbedre netværkssikkerheden ved at tillade sikkerhedsværktøjer at inspicere krypteret trafik. Processen involverer at opfange trafik, dekryptere data, analysere for trusler og genkryptere trafikken.
- **Web- og applikationskontrol:** Kombinerer elementer fra firewalls, IDS og IPS for at styre adgangen til specifikke websteder, applikationer og tjenester baseret på sikkerhedspolitikker.

Cyber-In

Erasmus+

Roskilde Tekniske Skole

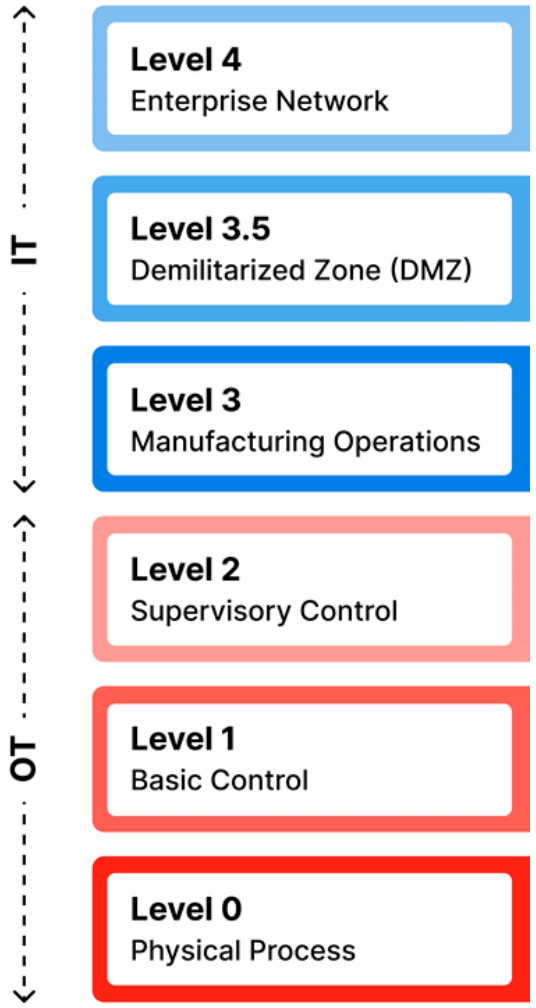
PURDUE-MODELLEN: EN RAMME FOR OT-SIKKERHED

Elektrikerens rolle i forhold til Purdue-modellen:

- Fysisk implementering af zoner: Forståelse af Purdue-modellens niveauer er afgørende for at kunne udføre korrekte installationer og kablinger, der respekterer de definerede sikkerhedszoner. Du skal sikre, at der ikke oprettes "ukontrollerede" forbindelser mellem niveauerne.
- Firewall- og DMZ-installation: Som elektriker kan du være involveret i den fysiske installation af firewalls og andre netværksenheder, der opretholder segmenteringen mellem niveauerne, f.eks. mellem Niveau 3 (drift) og Niveau 4 (forretning) via en DMZ.
- Adgangskontrol for udstyr: At sikre, at fysiske adgangspunkter til udstyr på de forskellige niveauer er beskyttet i overensstemmelse med sikkerhedspolitikken, f.eks. låse på kabinetter. Du skal være opmærksom på usikker adfærd (f.eks. ukendte USB-drev, åbne kabinetter) og rapportere dette, da det kan være indikationer på et cyberangreb.
- Viden om sikkerhedsrisici: Du skal holde dig opdateret i forhold til potentielle trusler, som fx at kunne spotte phishing og usikker USB-praksis
- Dokumentation: Detaljeret dokumentation af netværksforbindelser og kabling er essentiel for at lette fejlfinding og sikre, at segmenteringspolitikker håndhæves korrekt.

Cyber-In
Erasmus+
Roskilde Tekniske Skole

PURDUE-MODELLEN: EN RAMME FOR OT-SIKKERHED



Opgave

Hvordan kunne Purdue-modellen se ud i et olieraffinaderi?

- Hvilke OT-komponenter vil man finde på de tre laveste niveauer, og hvilke opgaver løser de?
- Hvilke sikkerhedstrusler er forbundet med disse niveauer?
- Hvad sker der på de tre øverste lag?
- Hvilke cybersikkerheds-overvejelser bør der være hér?

Cyber-In

Erasmus+

Roskilde Tekniske Skole

PAUSE

ROLLEBASERET ADGANGSKONTROL

Rollebaseret adgangskontrol (RBAC) er afgørende for at tildele tilladelser til brugere baseret på deres rolle i organisationen, hvilket sikrer, at de kun får adgang til de ressourcer, der er nødvendige for deres funktion. Dette omfatter princippet om mindst privilegie og adskillelse af opgaver:

- Definition af roller og ansvar: Identificer jobfunktioner og kortlæg dem til minimumssættet af nødvendige tilladelser.
- Etablering af en tilladelsesmatrix: Udvikl en matrix, der lister ressourcer (PLC'er, SCADA-konsoller) over for roller og tildeler læse-, skrive-, udførelses- og konfigurationstilladelser.
- Implementering af mindste privilegium: Tildel kun de tilladelser, der er nødvendige for en rolles opgaver.
- Adskillelse af opgaver: Undgå interessekonflikter, f.eks. kan samme bruger ikke både konfigurere PLC-logik og godkende dens implementering.
- Audit og compliance: Oprethold detaljerede logfiler over rolletildelinger og adgangsanmodninger.

ROLLEBASERET ADGANGSKONTROL

Hvad betyder det for dig som elektriker?

- RBAC for fysisk adgang: Du skal følge de fastsatte RBAC-politikker for fysisk adgang til serverrum, kontrolrum og kabinetter, der indeholder OT-udstyr. Dette betyder, at du kun bør have adgang til de områder og enheder, der er relevante for din rolle.

OPSAMLING

Hvordan kan vi skabe større awareness hos vores elever omkring cybersikkerhed?

Hvor vil viden fra dette kursus passe ind i UV-planlægningen?

- Diskutér med sidemanden i 10 min.
- Highlights i plenum

EVALUERING OG AFSLUTNING

Knowledge and Skills Evaluation Test, Denmark

EVALUERING OG AFSLUTNING

Cyber-In

Cascade training evaluation form, Denmark

Erasmus+

Roskilde Tekniske Skole

EVALUERING OG AFSLUTNING

- Underskrift af ”List of participants”