**Kim Visby**
PROCOS & MES, CGI Danmark

# Cyber Security - SESAM 2021

# Kim Visby

- 2015 – CGI, Ledelse af SCADA system PROCOS samt opstart af en MES afdeling med fokus på Life Science
- 2001 – 2015 – NNE, MES konsulent, OT Infrastruktur konsulent, Projektledelse og Director for Manufacturing IT
- 1998 – 2001 – Microsoft MCSE, IIS, MS Exchange, Symantic Raptor Firewall certificeret, samt opbygning og drift af infrastruktur til hosting

Mest interessante opgave omkring Cyber Security:

- Sikring af energiselskab efter incident
  - Baseret på NSA guideline for sikkerhed for Windows miljøer, IIS og SQL samt 2 forskellige firewall produkter inklusiv fysisk sikring af hardware.

# CGI at a glance

Founded in 1976
45 years of excellence

CA$12.1 billion revenue

78,000 consultants

400 locations in 40 countries

5,500 clients benefiting from end-to-end services

170+ IP-based solutions serving 50,000 clients

# Truslen for OT miljøer

- Ifølge CGI's cyber security center er chancen for en cyber angreb i OT miljø lavere end i IT miljøer, til gengæld kan effekten være enorm når det sker
- OT miljøer har historisk set haft ensidet fokus på høj oppetid og tilgængelighed
- For mange er cyber security i OT miljøer noget med begrænsning i fysisk adgang og begrænsning i integrationen med det administrative netværk også kaldet perimeter sikkerhed

Stuxnet – Duqu – Night Dragon

- For at øge effektiviteten og kontrol med produktionen er OT i højere grad eksponeret for det administrative net og forbundet med internettet

CGI's cyber security center beretter om svagheder i OT udnyttes i stigende grad

# Et dansk SCADA system

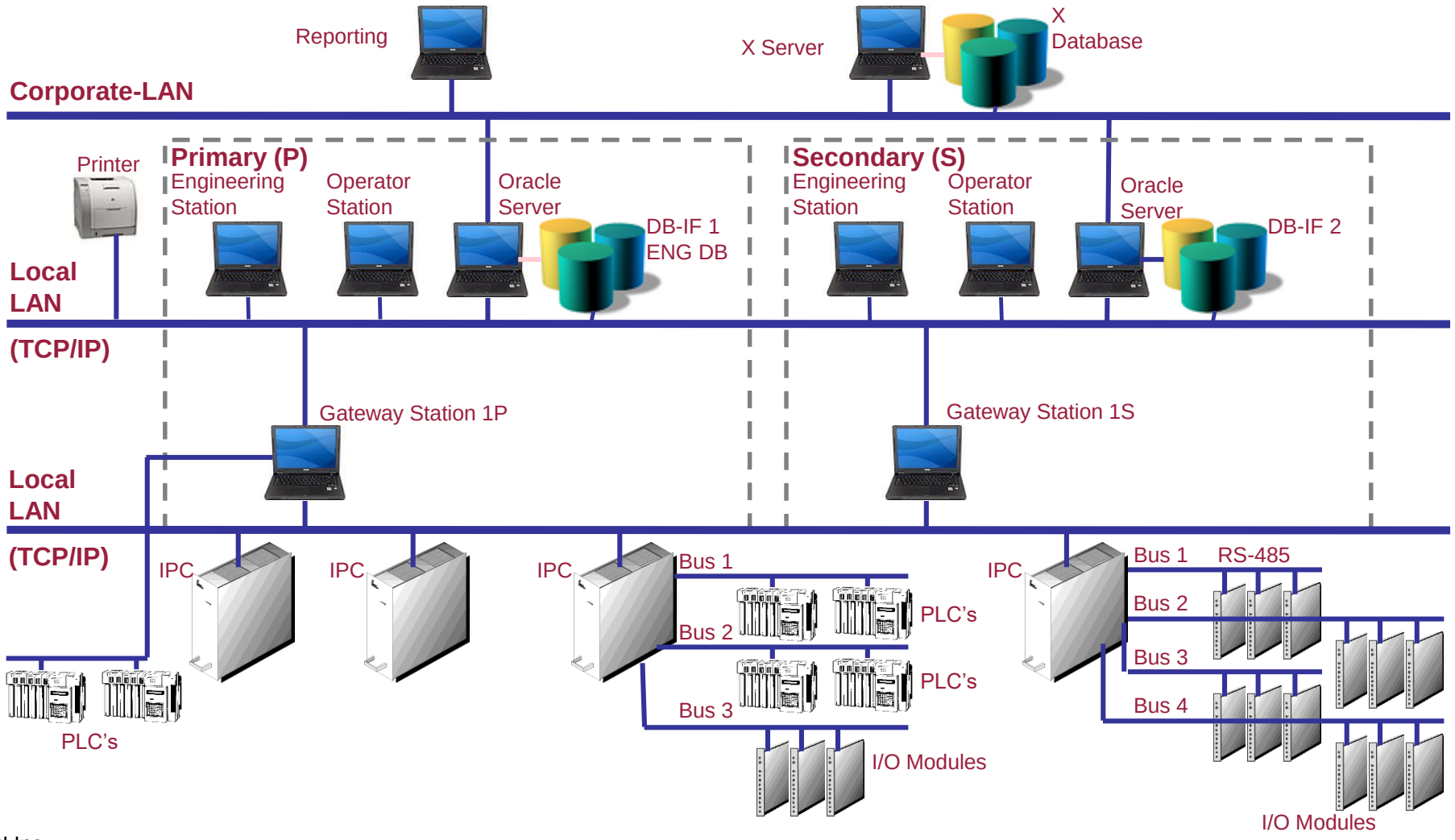
“PROCOS er resultatet af en dansk vision om at skabe en platform, som understøtter en automatiseret produktion som var langt forud for sin samtid”

# PROCOS produkt strategi

Funktioner og målsætninger

- Batch Management – ét samlet integreret system til overvågning og kontrol af batch produktion
- Effektivitet – Let at anvende og høj produktivitet
- Åbenhed – I forbindelse med integration til planlægning, administration og vedligeholdelses systemer
- Robusthed – Stabilitet i platform
- Continuity – Bagud kompatibilitet er kernen i PROCOS lange levetid
- Flexibilitet – Tilpasning til enhver proces uden at foretage customiseringer i PROCOS kerne
- Uafhængig – Følge med udviklingen indenfor SW og HW

# PROCOS system arkitektur



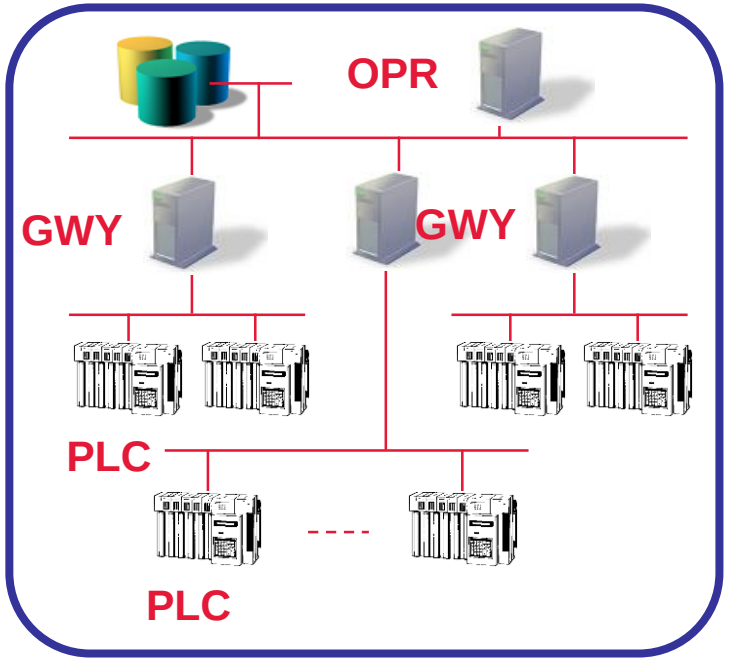
# PROCOS anvender tredjeparts HW som IPC

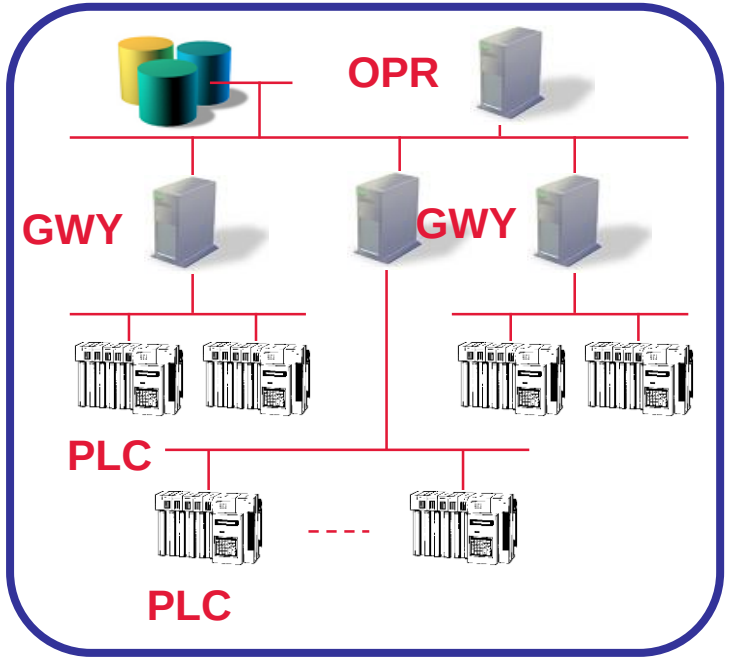
CGI anvender Beckhoff som leverandør af proces interface platform

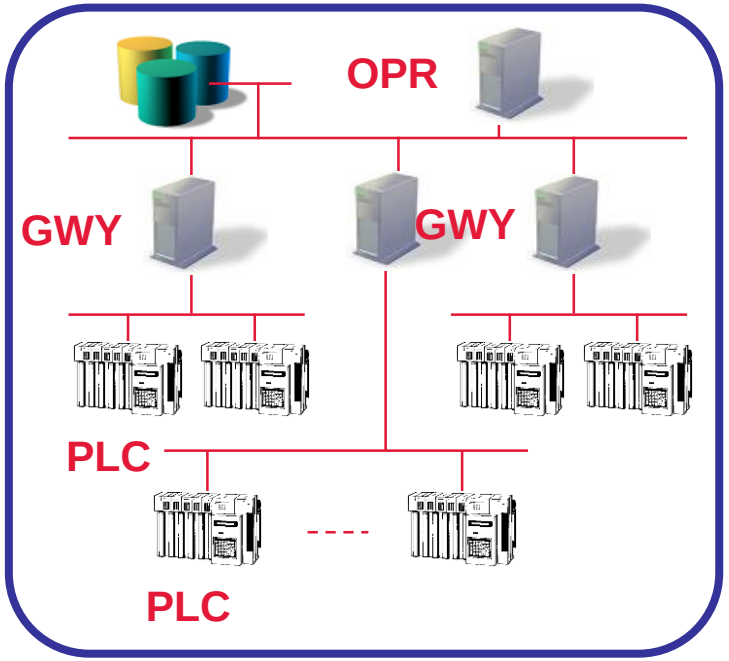
- Global leverandør af industriel HW
- PC baseret arkitektur
- Understøtter en del bustyper
- Understøtter relevante I/O typer
- Udbredt i life science industrien

# PROCOS oprindelige netværks-arkitektur

Isoleret separate ø-installationer med mindre ikke-forbundene netværk, og i øvrigt samme netværk indenfor øen, og naturligvis ingen AD

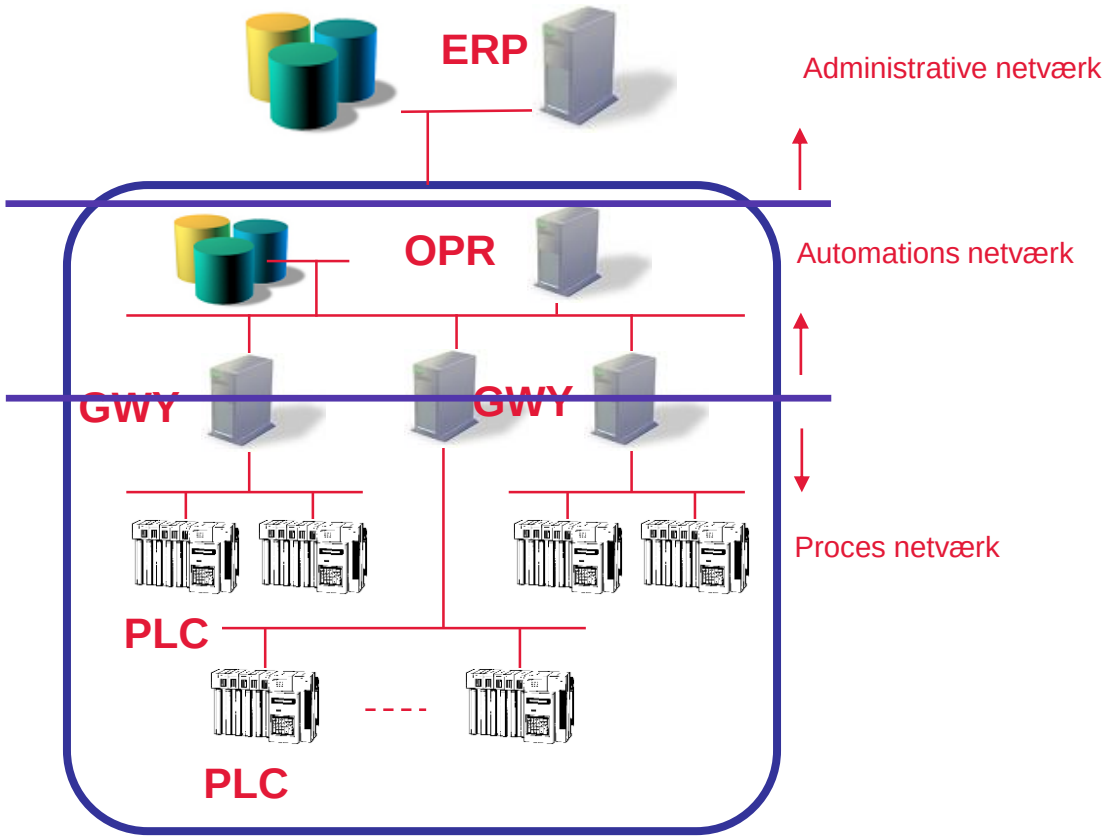


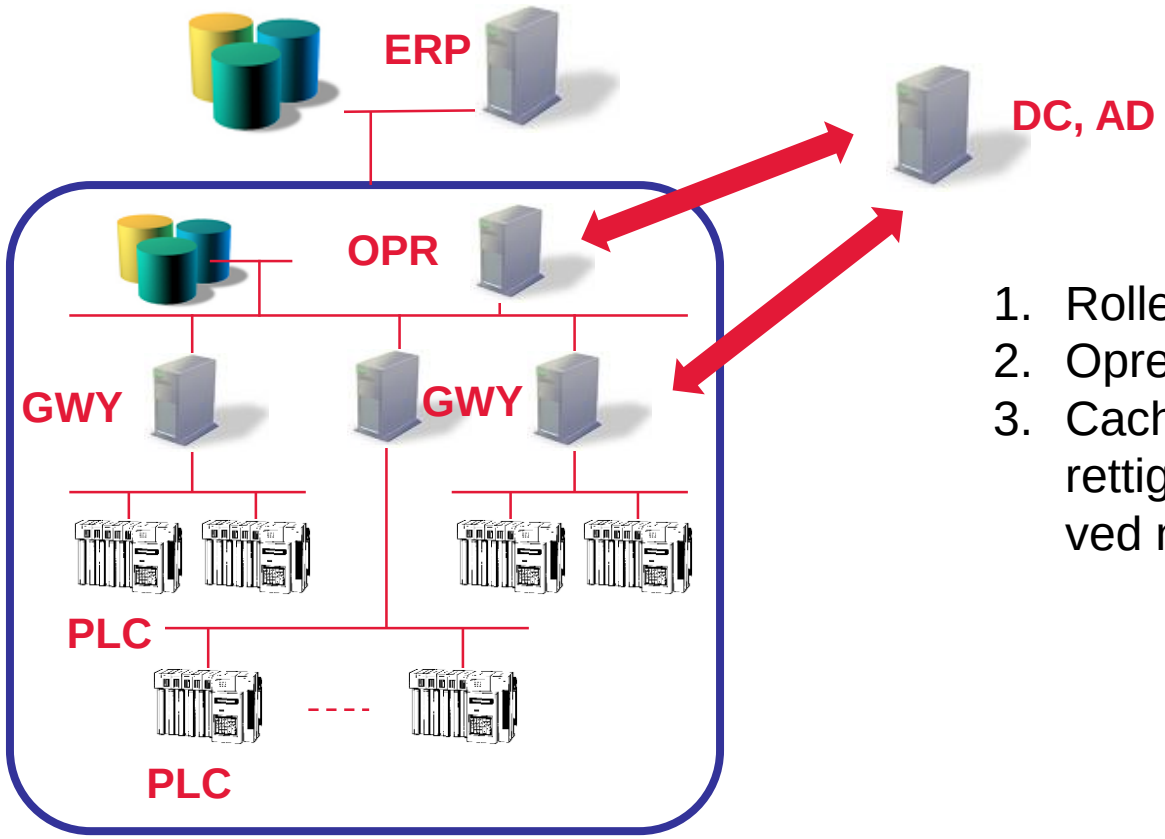
# PROCOS topologi netværk

Opdeling af netværk, så proces nettet ikke ligger på samme net som automations net, oprindeligt for netværks optimering.
Senere kom integration med supply chain



# PROCOS topologi domæne

Oprindelig var der ikke nogen rolle til en domæne controller i PROCOS systemet.

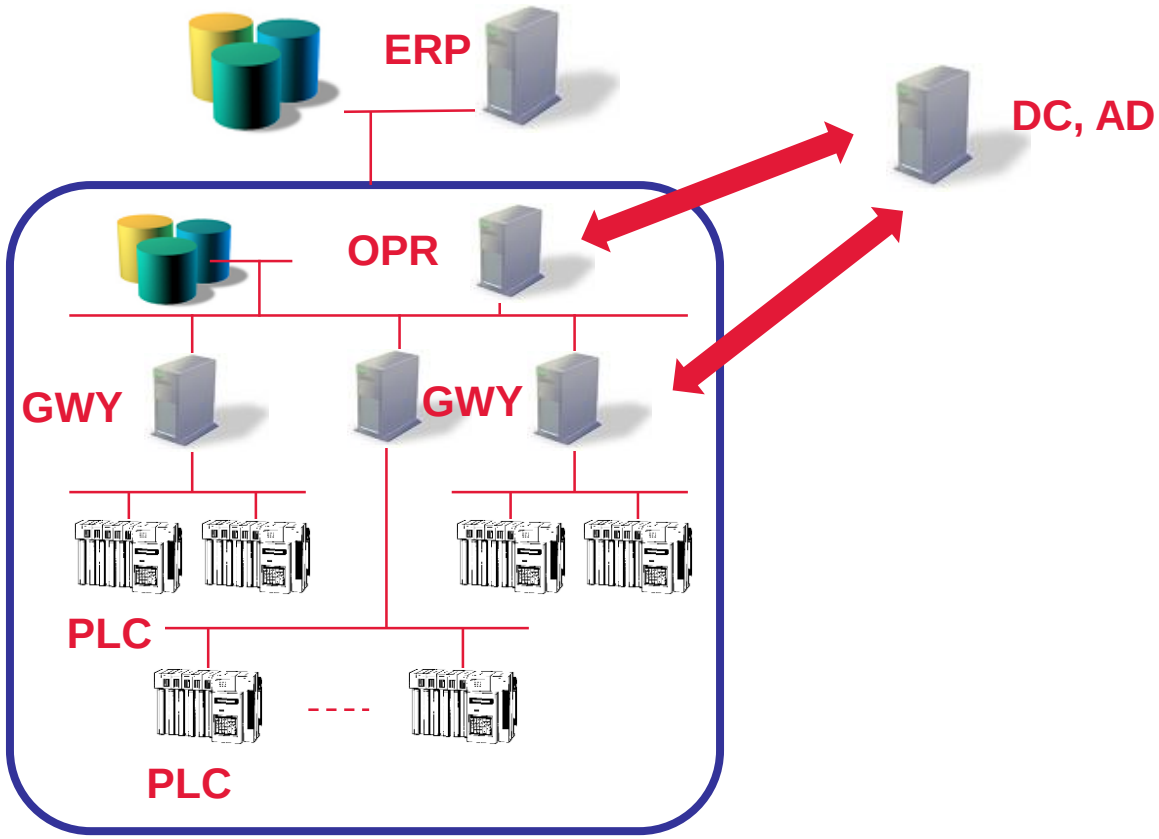



1. Roller og rettigheder
2. Opret/nedlæg brugere
3. Cache roller og rettigheder i PROCOS ved netværks svigt

# PROCOS topologi services

Ikke nødvendige services og funktioner
reduceres til absolut minimum

- Remote desktop
- Remote registry
- Mail
- Internet adgang
- O.m.a.



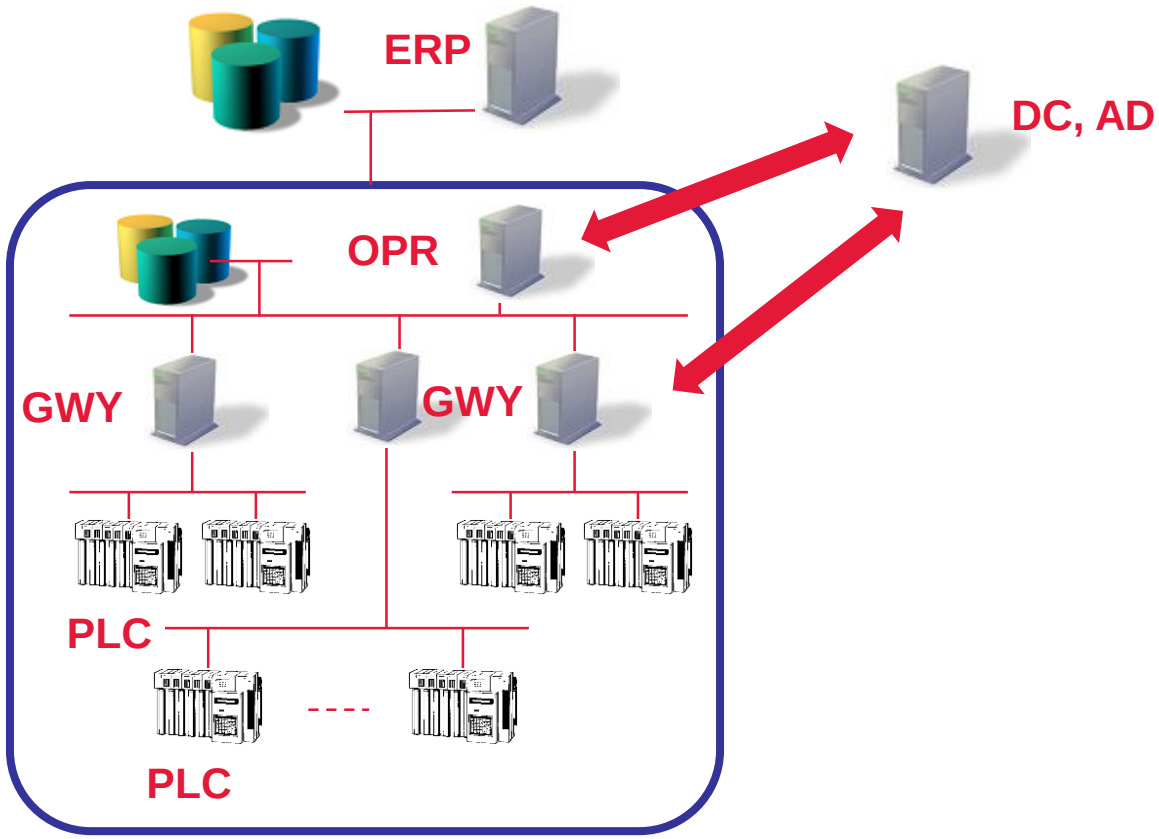
# PROCOS topologi firewall, whitelisting/blacklisting

Firewall regler på netværk:

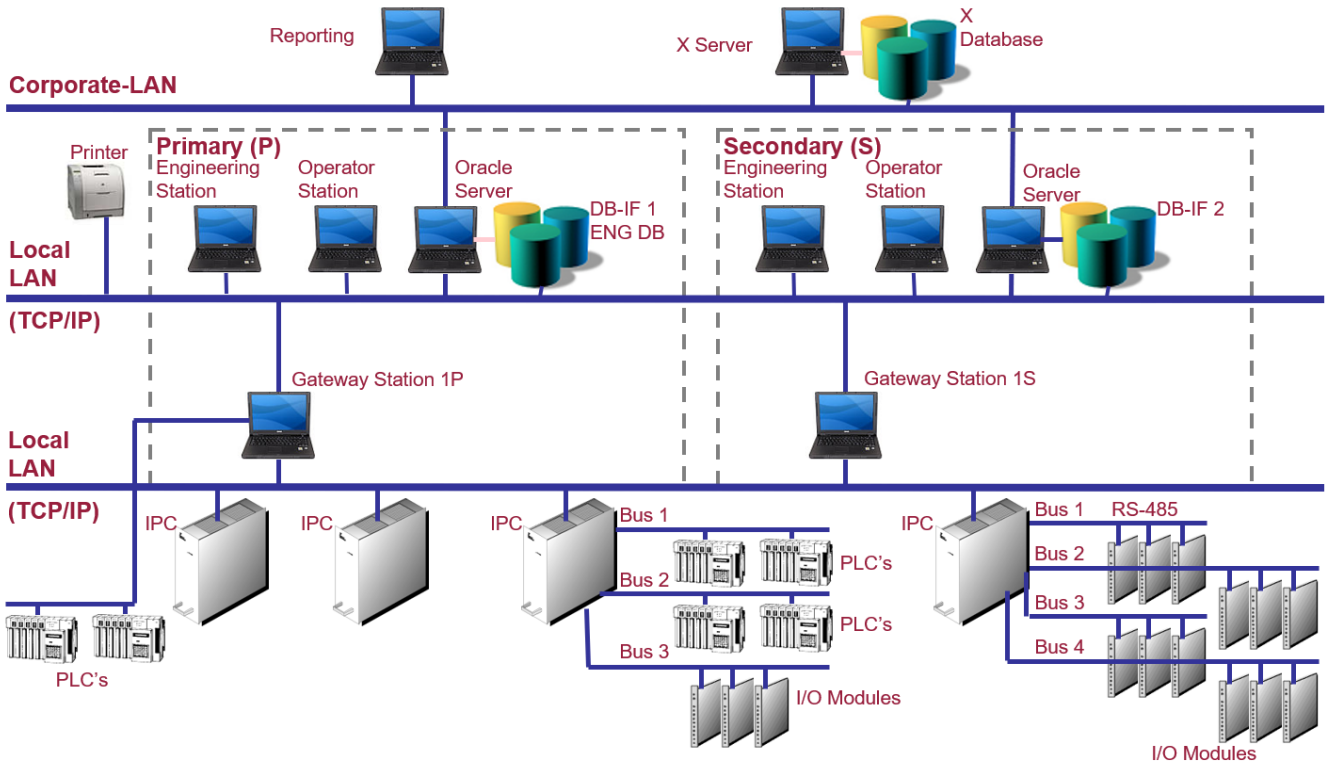
- Only allow IP xx.xx.xx.xx, port xx ↔ IP xx.xx.xx.xx, port xx
- Monitorering af ”unormal” trafik

Whitelisting:
Tilladte applikationer
Konfigurationsstyring på fil niveau
Tilladte IP adresser range

Blacklisting:
Fobudte applikationer
Forbudte filer såsom (.exe., bat etc.)
Eksklusion IP adresse range



# PROCOS patch strategi

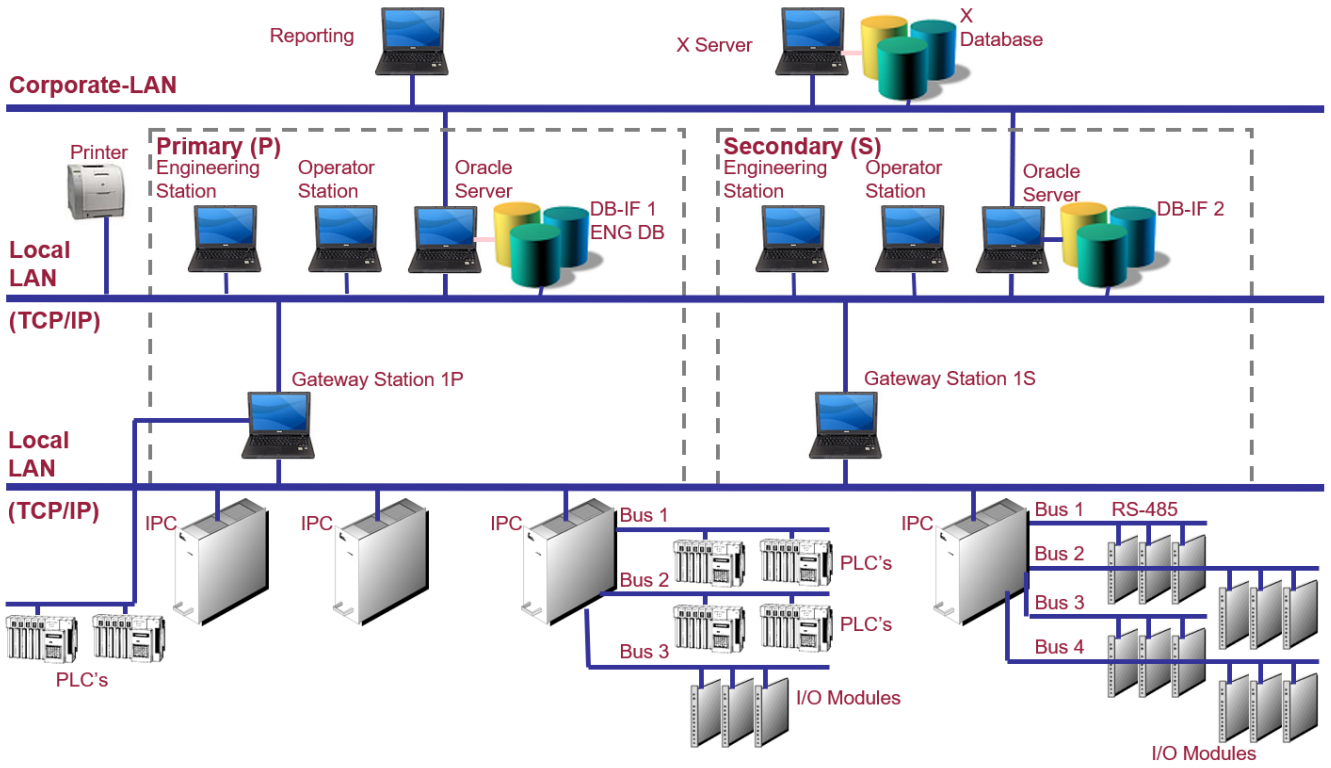



Årlig PROCOS patch cyklus
PROCOS hovedrelease udgives årligt, scope bliver fastlagt og opdateres flere gange årligt

- Teknologi
- Funktion
- Sikkerhed

Dernæst udgives et antal mindre patches som løser mindre problemer eller af sikkerhedshensyn
CGI frigiver efter grundig test vores anbefaling af Microsoft patches, og der bør anvendes manuel WSUS
Alle PROCOS komponenter er i scope for patches

# PROCOS anti-virus strategi



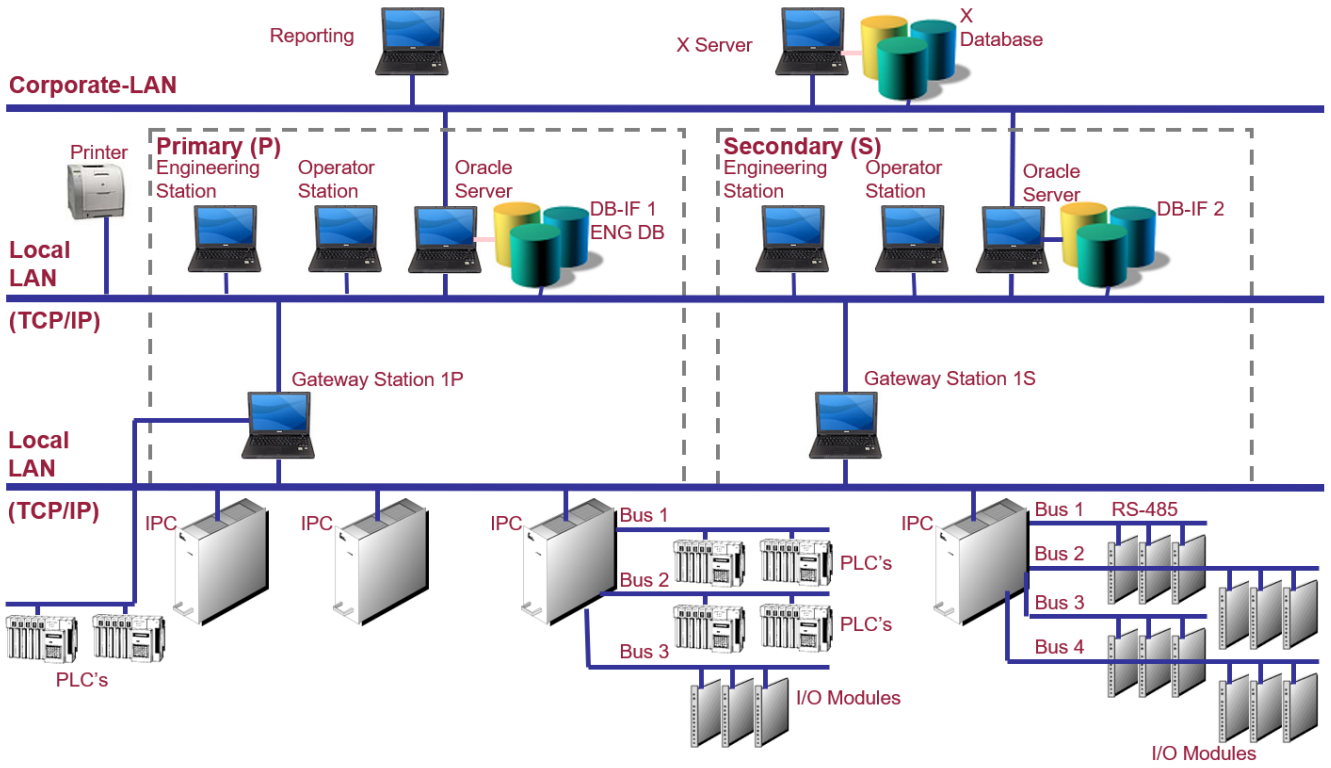

CGI anvender anti-virus på alle test og udviklingssystemer.
CGI forbehold mod anti-virus er af performancemæssige årsager

1. I SCADA systemer er det ikke super genialt at fil skanning låser filer som anvendes i realtids systemer

2. Visse anti-virus programmer har vist sig at identificere visse komponenter som ondsindet, og dermed skaber ”false-positive” som låser filer og systemer

Flere installationer anvender anti-virus, men det kræver en længere prøve periode for at identificere udfordringer, og ved anti-virus patching bør udvises forsigtighed og test!

# PROCOS fysisk sikkerhed




I stort set alle PROCOS installationer er der anvendt fysisk begrænsning til udstyret, især adgang til drev, USB.

Fun fact:
Den historiske årsag er nok overraskende.

De kraftige PROCOS Workstations, som engang ikke var udbredt i den private husholdning, var velegnet til spil, og der blev spillet på livet løs på disse maskiner, og de blev derfor låst inde i kabinetter og i adgangskontrolleret server rum.

# Opsummering af PROCOS tiltag i forbindelse med Cyber Security

- Netværk
- AD, domæne services såsom DNS, WINS
- Services og funktioner
- Firewall, whitelisting/blacklisting, perimeter sikkerhed
- PROCOS Patch strategi samt produkt patches til Microsoft og andre teknologier
- Anti-virus strategi
- Fysisk sikkerhed
- Whitehat sikkerheds analyse

# Q & A

# Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world. We are insights-driven and outcomes-based to help accelerate returns on your investments.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally

**cgi.com**

CGI