Region Syddanmark

Delstrategi for digitalisering af det tekniske område og bygningsstyring

Indledning

Bygningsstyring og tekniske installationer spiller en afgørende rolle i moderne sygehuse. De danner rygraden i en drift, der sikrer optimale forhold for både patienter, personale og pårørende. De tekniske installationer spænder bredt og har indvirkning på alt fra indeklima og energiforbrug til patientsikkerhed og arbejdsforhold for sundhedspersonalet.

De seneste år har budt på en øget digitalisering, som har medført nye muligheder for overvågning, styring, automatisering og optimering af de tekniske systemer. Smarte løsninger og intelligente bygningsinstallationer bidrager til en mere effektiv og bæredygtig drift, samtidig med at de understøtter en høj standard for patientsikkerhed og komfort.

Mange af de tekniske installationer i sygehusbyggeri har en levetid på 20-30 år, hvilket stiller store krav til både planlægning, vedligeholdelse og opgradering. Langsigtet tænkning er derfor afgørende for at sikre, at de tekniske løsninger forbliver tidssvarende og i stand til at understøtte den konstante udvikling inden for sundhedssektoren.

Den øgede digitalisering bringer også nye udfordringer i form af cybersikkerhed. Særligt trusselsbilledet for ot og it har ændret sig markant. (OT er en forkortelse for Operationel Teknologi, der fungerer i tæt samspil med it – se *figur 1* nedenfor).

Ot-systemer, der styrer kritiske funktioner såsom ventilation, strømforsyning og medicinsk udstyr, er i stigende grad forbundet med it-infrastrukturen. Dette øger risikoen for cyberangreb, hvor hackere potentielt kan kompromittere både patientdata og vitale bygningsinstallationer.

En særlig sårbarhed findes i grænsefladen mellem it-systemer og ot teknologien, der anvendes til at styre automatiserede processer i bygninger, eksempelvis PLC'er (Programmable Logic Controllers).

Ot komponenter er som regel designet til stabilitet og lang levetid, men mangler ofte de avancerede sikkerhedsfunktioner, der findes i moderne it-systemer. Når eksempelvis PLC'er kobles op mod netværk, cloud-platforme eller andre digitale systemer, skabes en potentiel angrebsflade, som kan udnyttes, hvis ikke der implementeres tilstrækkelige sikkerhedsforanstaltninger.

Derfor er det afgørende at etablere sikre kommunikationsveje mellem it og ot, herunder segmentering af netværk, brug af firewall-løsninger og adgangskontrol for at minimere risikoen for uautoriseret adgang. Ved at sikre en robust integration mellem it og ot kan sygehuse opnå en mere stabil og sikker drift, samtidig med at de udnytter fordelene ved digitalisering og automatisering.

Udviklingen inden for bygningsstyring og tekniske installationer er desuden stærkt påvirket af nationale og europæiske regulativer. Både dansk lovgivning og EU-direktiver stiller stadig større krav til energieffektivitet, bæredygtighed og datasikkerhed i offentlige bygninger, herunder sygehuse. For eksempel vil EU's NIS2-direktiv skærpe kravene til cybersikkerhed i kritisk infrastruktur, mens strammere krav til energieffektivitet og klimamål understreger nødvendigheden af bæredygtige løsninger i byggeriet. Samtidig reguleres persondatasikkerhed strengt gennem GDPR, hvilket har konsekvenser for, hvordan digitale systemer håndteres og sikres i regionen.

It har historisk set været sekundært ved anskaffelse af nye tekniske systemer eller ved nybygning. Opgaven omkring anskaffelse af tekniske løsninger er typisk placeret lokalt på enheden, medmindre der er tale om større anlægsprojekter. En evt. it-understøttelse har derfor ofte mundet ud i en lokal løsning, hvorfor der findes mange udgaver af samme type it-system på de forskellige enheder.

Region Syddanmarks beslutning om en central konsolidering af it-systemer nødvendiggør, at der skal etableres et tættere samarbejdet mellem enhederne og Regional IT. Et samarbejde der skal sigte mod anskaffelse af fælles it tekniske løsninger, der understøtter driften på enhederne og samtidig effektiviserer forvaltningen af disse.

Den fælles strategi for it-forvaltning, drift og anskaffelse vil samtidig kunne sikre, at enhedernes teknologiske løsninger forbliver fremtidssikrede, overholder gældende lovgivning og sikkerhedskrav og derigennem sikrer en stabil, sikker og fremtidssikret infrastruktur, der understøtter både patienter, personale og pårørende.

Aktuel status og udfordringer for teknik og byggestyring i Region Syddanmark

It-landskabet inden for teknik og bygningsstyring består af ca. 175 it-systemer gående fra meget kritiske systemer til systemer uden væsentlig driftsmæssig betydning.

I modsætning til de kliniske områder, hvor systemer anvendes på tværs af enheder, er systemerne inden for teknik og bygningsstyring typisk anskaffet til et konkret formål på den enkelte enhed, og ofte i forbindelse med et anlægsprojekt, hvor omkostningerne til it indgår som en mindre delmængde af en samlet kontrakt uden nærmere specifikation.

Det har typisk været medvirkende til at driftsøkonomien og forvaltningsansvaret for it-systemerne efterfølgende er landet hos de tekniske afdelinger, og indgår i en samlet prioritering i forhold til alle øvrige opgaver inden for det tekniske område.

Fokus er derfor ofte rettet mod nødvendige tiltag i relation til driftssikkerhed og generelt har tiltagene karakter af reaktive handlinger frem for proaktive handlinger.

I forhold til den gældende governance for it-systemer i regionen er området som helhed underforvaltet, og der mangler fokus på kompetencer og ressourcer inden for it- og ot-sikkerhed.

I forbindelse med en gennemgang af områdets it-systemer har det vist sig, at selv om flere enheder anvender systemer fra samme leverandør/producent, kan der være forskel på de kontraktlige vilkår enhederne imellem.

Der eksisterer generelt kun support- og produktvedligeholdelsesaftale på en begrænset del af it-systemerne, hvilket stiller afdelingerne i en vanskeligere situation i forhold til leverandøren, når handlinger er påkrævet.

Samarbejde mellem Regional IT og enhederne i forbindelse med anskaffelse og forvaltning af it- og ot-systemerne har traditionelt været begrænset. Der er derfor både synergi og potentiel effektivisering i at bringe de faglige kompetencer sammen.

Tendenser

Den almindelige teknologiske udvikling, herunder meget billig produktion af komplekse elektroniske komponenter, udvisker til en vis grad grænserne mellem it- og ot-udstyr. Selv styringselektronik til enkle opgaver (f.eks. dørlåse) er i dag udstyret med avanceret teknologi i form af netværkskommunikation, hurtig processor, stor hukommelse osv. Det er ikke forkert at sige, at en lille mikroprocessor i dag på mange områder kan sammenlignes med en PC fra ’90erne.

Dette giver mulighed for opbygning af ot-løsninger, hvor operationelle enheder selvstændigt kan træffe beslutninger, der optimerer driften i realtid. Edge computing er f.eks. en teknologi, hvor data behandles på

opsamlingsstedet i stedet for at sendes tilbage til en central server. Et eksempel på dette er en sensor, der selv afgør, hvornår en maskine skal stoppe pga. slitage i stedet for at vente på en central godkendelse.

Det er en ny erkendelse, at ot-området skal betragtes som en kritisk infrastruktur, på lige fod med it-området, men med nye udfordringer. Hvor it-området er præget af få, men store leverandører, er ot-området fragmenteret med både store og mindre leverandører. Desuden er leverandørkæderne ofte lange og komplekse og domineret af proprietære løsninger.

Den stadig stigende specialisering betyder, at fremstilling af ot-komponenter sker som samling af delkomponenter, leveret gennem kæder af underleverandører i lande uden for EU. Hermed er markedet stort for slutprodukter med samme virkemåde, men kan være stærkt påvirket af forhold fra uventet side, herunder lovgivningen i lande, der ligger uden for EU.

Med de nye muligheder følger også ændringer i trusselsbilledet. Intelligente ot-enheder kan angribes gennem flere trådløse netværksprotokoller, hvis de ikke er korrekt afkoblet. Derudover kan ot-enheder fra producentens side være påført skjulte kanaler eller bagdøre, som en udefra kommende kan bruge til fjernovervågning og -kontrol eller overtagelse. For eksempel har overvågningssystemer været under mistanke for at sende informationer til en fremmed magt.

Endelig kan selve kompleksiteten af ot-enhederne ”overvælde” leverandøren, så risikoen øges for fejl og sikkerhedshuller under udvikling. Dette kan i sidste ende føre til uforudsigelig drift og øget sårbarhed over for angreb, hvilket stiller nye krav til sikkerhed og risikostyring i ot-miljøer.

Selv om intelligente løsninger åbner for nye muligheder, medfører de også øgede sikkerhedsrisici. Trusler som netværksangreb, skjulte bagdøre og udviklingsfejl kræver en højere grad af opmærksomhed på sikkerhed og risikostyring. Derfor er det afgørende at betragte ot som en kritisk infrastruktur og sikre robuste forsvarsmekanismer for at beskytte både drift og data mod uforudsete trusler.

Værdiskabelse

Delstrategien for teknik og bygningsstyring skaber værdi ved at adressere både sikkerhed, effektivisering og governance i grænselandet mellem it og ot – et område der traditionelt har været underforvaltet, men som i stigende grad betragtes som en kritisk infrastruktur.

Den primære værdiskabelse knytter sig til fire centrale effekter:

1. Øget sikkerhed og robusthed i OT-miljøet
   Med et trusselsbillede i hastig udvikling og nye lovkrav som NIS2 og CER-direktivet er det afgørende at etablere et acceptabelt og vedvarende sikkerhedsniveau. Delstrategien bidrager til at styrke regionens modstandsdygtighed ved at opbygge viden, anvende internationale rammeværker (ISO 27001 og IEC 62443) og sikre segmentering af ot-systemer efter kritikalitet. Det styrker regionens evne til at modstå cybertrusler og beskytte både drift, data og patientnære funktioner.

2. Effektivisering gennem konsolidering og standardisering
   Med ca. 175 registrerede it-systemer og op mod 100.000 ot-enheder er der et betydeligt potentiale for effektivisering. Konsolidering af systemporteføljen – med principper som "én opgave, ét system" – skaber overblik og reducerer både kompleksitet og fremtidige driftsomkostninger. Samtidig sikres bedre datagrundlag for beslutningstagning og en mere ensartet tilgang på tværs af regionens enheder.

3. Ensartede processer og stærkere leverandørstyring
   Strategien lægger op til etablering af fælles og gennemskuelige processer for nyanskaffelser og forvaltning, i tæt samarbejde mellem de tekniske afdelinger, it-området, bygningsområdet og indkøbsområdet. Det muliggør regionale løsninger, attraktive driftsaftaler og bedre overholdelse af

sikkerheds- og kvalitetskrav. Derudover styrkes leverandørstyringen, så eksisterende kontrakter understøtter serviceklassificering og ansvar er tydeligt placeret.

4. Kompetenceløft og kapacitetsopbygning i forvaltningen
   Strategiens indsatser skal bidrage til at opbygge en stærkere forvaltningskapacitet – både i Regional it og i de tekniske afdelinger – med varig forankring af ny viden og erfaring. Etableringen af et fælles videns- og læringsmiljø og dedikerede forvaltningsressourcer skal sikre, at regionen fremadrettet kan agere proaktivt og professionelt i et stadig mere komplekst og reguleret teknologilandskab. Forankringen af projektressourcer i Regional IT sikrer, at den opbyggede viden bevares og videreføres i den varige drift.

Strategiens samlede værdiskabelse skal ses i lyset af dens tværgående karakter: Ved at skabe synergi mellem teknik og it styrkes både modstandsdygtighed og driftssikkerhed, og Region Syddanmark bringes tættere på målet om en mere sikker, effektiv og bæredygtig hospitalsinfrastruktur.

Strategiske ambitioner

Der er identificeret tre strategiske ambitioner, som tilsammen skal gøre området effektivt og modstandsdygtigt. Ambitionerne sætter retning for den overordnede vision fra digitaliseringsstrategien og understøttes via målrettede indsatsområder, som forventes gennemført over en 2-årig periode og udmøntes ved hjælp af konkrete handleplaner. Handlingsplanerne tages løbende op til revision i takt med, at teknologien, lovkrav, digitale løsninger, risikobilledet, miljøkrav m.m. forandrer sig.

1. Effektivisering gennem styrket tværgående samarbejde
   Regionens tekniske afdelinger skal arbejde hen mod ensartede arbejdsgange og processer, og der skal etableres et fællesskab i grænselandet mellem it og ot.
   Regionens tekniske afdelinger skal have fokus på omkostningsbesparelser og effektiviseringer via tværgående samarbejde omkring indkøb og forvaltning af it og ot.

   De tekniske enheder har hver især arbejdet på at skabe de bedste rammer for det enkelte sygehus eller institution, og har derfor løbende anskaffet udstyr og tilhørende it i takt med behovet hos den enkelte enhed.

   Dette har medført en mangfoldighed inden for it-systemer og deres anvendelse, og med udsigt til øget ressourceanvendelse og øget økonomi grundet et stigende trusselsbillede og en stadig større afhængighed til it, er det nødvendigt at styrke samarbejdet på tværs af organisationen og derigennem opnå stordriftsfordele og professionalisering inden for indkøb, forvaltning, automatisering mv.

2. Øge sikkerheden på det tekniske område via en risikobaseret tilgang
   Med et øget trusselsbillede over for bl.a. kritisk infrastruktur og med afsæt i bl.a. den kommende NIS2 lovgivning skal der foretages en målrettet forebyggende indsats mod udefra kommende trusler. Øget sikkerhed inden for de tekniske områder indbefatter både forebyggende aktiviteter og aktiviteter, der understøtter den daglige driftssikkerhed, herunder beredskabshåndtering.

   Regionen blev berørt af et hackerangreb mod en af dens leverandører i 2024, og oplevede i den forbindelse, hvilke konsekvenser et cyberangreb kan have.

   Hændelsen har medvirket til aktiviteter, som nedsætter risici inden for it-organisationen generelt, men der er et særligt behov for at have fokus på aktiviteter, der kan tage højde for de specielle forhold, der findes inden for det tekniske område og især omkring integrationen mellem it og ot.

Dette omfatter et nærmere kig på processen omkring risikovurderinger for teknisk udstyr samt gennemgangen af beredskabsplaner for de mest kritiske systemområder.

3. Sikre høj driftsstabilitet til gavn for personale, patienter og pårørende
   De tekniske afdelinger og Regional IT skal i samarbejde udarbejde krav for anskaffelse af ot-teknologi og sikre at disse opretholdes i forbindelse med projekt- og anlægsarbejde, så der skabes de optimale forudsætninger for, at der i hele driftsperioden kan opretholdes høj driftsstabilitet og sikker drift.
   Indsatsen omkring leverandørstyring skal øges som et aktivt bidrag til at skabe høj driftsstabilitet.

   De tekniske enheder skal sammen med Regional IT's forvaltning, indkøbsområdet og det juridiske område øge indsatsen omkring leverandørstyring som et aktivt bidrag til at skabe høj driftsstabilitet. Driftsstabilitet inden for de tekniske anlæg er en nøglefaktor, der bidrager aktivt til en effektiv og sikker hverdag for enhedernes personale samt for patienter og pårørende.

   Anskaffelse af bygningsteknik er oftest en investering, som rækker 20-30 år ud i fremtiden, og inkluderer ofte dedicerede it-systemer, der hen over tid kommer til at udgøre en stigende risiko, hvis ikke der indgås gode vedligeholdelses- og supportaftaler. Fokus skal således være på at sikre disse langtidsinvesteringer bedst muligt og derigennem bl.a. skabe høj driftssikkerhed for systemer og anlæg.
   Inden for den nuværende it-systemportefølje er der kun indgået service- og supportaftaler med leverandører for en meget lille procentdel. Det gælder også de mere kritiske systemer og betyder blandt andet, at det kan være vanskeligt at få leverandører til at opgradere systemer løbende. Serviceaftaler kan være ret bekostelige, og derfor vil en konsolidering af systemporteføljen være en økonomisk gevinst på dette område.

Indsatsområder

De strategiske ambitioner sætter retning. Og for at opnå de strategiske ambitioner er der identificeret syv konkrete indsatsområder, der skal sikre, at Region Syddanmark bevæger sig i den ønskede retning.
De syv indsatsområder er:

1. Styrke sikkerheden omkring ot
2. Konsolidering af den nuværende (systemporteføljen)
3. Fælles processer for nyanskaffelser
4. Samarbejdsfora og ansvarsplacering
5. Bidrage til klimamålsætning
6. Leverandørstyring
7. Fra underforvaltning til tilstrækkelig forvaltning

1. Styrke sikkerheden omkring OT
Teknik og Bygningsstyring omfatter bl.a. adgangskontrol, videoovervågning og alarmkald, som er afgørende for både patienters og medarbejderes sikkerhed. Domænet dækker også energi og miljø, transport og logistik – alle centrale elementer i den kritiske infrastruktur. For at beskytte både drift og data mod uforudsete hændelser og trusler, skal der etableres og vedligeholdes robuste forsvarsmekanismer. Samtidig er det afgørende at øge bevidstheden om trusselsbilledet og sikre et klart overblik over de forretningsmæssige konsekvenser af forstyrrelser i ot-området.

Den stigende trussel fra cyberangreb kræver, at ot-sikkerheden løbende udvikles til at modstå udefrakommende angreb. Lovgivningen understøtter beredskabet, og det er derfor vigtigt at udbrede kendskabet til relevante tiltag. På grund af områdets kompleksitet er en risikobaseret tilgang nødvendig, så de mest forretningskritiske delområder identificeres.

Mål 1: Indsatsen skal sikre at viden omkring lovgivning om cybersikkerhed, særligt NIS2, CER- og Maskindirektivet tilføres relevante personer og funktioner inden for teknik og bygningsstyring, samt sikre at de tilhørende rammeværker (ISO 27001 / IEC 62443) anvendes som regional standard.

Mål 2: Indsatsen skal sikre, at ot-systemlandskabet klassificeres efter forretningsmæssig betydning, og segmenteringen af systemerne skal styrkes i henhold til serviceklassificeringen.

Stram adgangskontrol i ot-netværket er afgørende – både for at imødegå cybertrusler og sikre driftens stabilitet. Hvis en leverandør har adgang til at sende opdateringer eller fjernstyre en ot-enhed, indebærer det en risiko for driftsforstyrrelser. Dette kan minimeres gennem skærpet adgangsstyring samt klare og ensartede krav til leverandørernes handlinger i driftssituationer. Desuden bør det sammen med Operationel Sikkerhed i Regional IT vurderes, hvordan og på hvilket niveau et fælles management-system kan etableres til styring af adgange og data-/filoverførsler til ot-området.

Mål 3: Indsatsen skal sikre, at der udarbejdes og implementeres en klar governance-model for, hvem der har adgang til hvilke ot-zoner, samt hvordan eksterne leverandører får adgang. Modellen skal baseres på en risikovurdering, hvor kritiske systemer underlægges strengere kontrol end mindre følsomme systemer.

Interne trusler kan i ot-miljøet have lige så stor betydning som cyberangreb udefra. De fleste trusler er utilsigtede, såsom menneskelige fejl eller fejlkonfigurationer, men ondsindede handlinger som insider-trusler, sabotage eller datalæk kan ikke udelukkes i en stor organisation. Da stabile systemer er afgørende for forretningen, er det nødvendigt at forebygge, opdage og håndtere disse trusler effektivt.

En stærk adgangsstyring, segmentering af systemer og overvågning af adfærd i ot-netværket er væsentlige værktøjer til at minimere risikoen. Samtidig er det vigtigt at øge bevidstheden om interne trusler gennem træning og kampagner, så medarbejdere kan genkende tegn på uregelmæssig adfærd.

Mål 4: Indsatsen skal medvirke til at medarbejdere trænes i at identificere tegn på interne trusler, og at det, i samarbejde med Operationel Sikkerhed, vurderes, hvordan og på hvilket niveau logning af adfærd i ot-netværket giver mening og kan gennemføres.

Den normale driftssituation kan være udfordret af problemer med driftssikkerhed og -stabilitet. Da der kan opstå fejl i et system på alle tider, er det væsentligt at kunne genskabe en kørende drift så effektivt som muligt. Dette kræver overblik over det miljø, systemet er placeret i, dets kritikalitet og de aftaler, som er gældende i forhold til systemets driftstilstand. Et sådant overblik skal skaffes gennem konsolidering og governance, og det er vigtigt, at det til enhver tid er nemt tilgængeligt for de relevante parter.

Mål 5: Indsatsen skal sikre, at der udarbejdes beredskabsplaner for ot-systemer i forhold til serviceklasserne, og disse planers effektivitet skal afprøves i henhold til serviceklassebeskrivelserne.

2. Konsolidering af det nuværende (systemporteføljen)
Porteføljen af it-systemer inden for teknik og bygningsstyring er historisk set opbygget gennem lokale aktiviteter på enhederne, og indeholder derfor en relativ stor mængde af forskellige it-systemer, der reelt set løser samme opgave.

I forbindelse med den systemgennemgang som blev foretaget i forlængelse af reorganiseringen af it-området, dukkede der mange systemer op, som ikke var blevet underlagt de fælles retningslinjer for forvaltning. Gennemgangen resulterede i, at der er identificeret ca. 175 nye it-systemer inden for teknik og bygningsstyring, og at der inden for visse kategorier, eksempelvis adgangsstyring, findes over 20 registrerede it-systemer.

Indsatsen for konsolidering skal tjene forskellige formål. Den skal blandt andet medvirke til at skabe en mere effektiv forvaltning af it-systemer, og derigennem bidrage til at reducere omkostningerne eller i det mindste begrænse de omkostningsstigninger, der må forventes i forbindelse med opbygningen af forvaltningsfunktionen. Den skal også bidrage til at sikre en bedre udnyttelse af de investeringer, der er

foretaget ved at samle udvalgte it-systemer f.eks. i Regional IT, og stille disse til rådighed for kommende projekter. De nye it-systemer, der er anskaffet i forbindelse med Nyt OUH, vil indgå som et naturligt udgangspunkt ud fra det faktum, at der er tale om nyere teknologier og systemer, der ofte er skalerbare i forhold til hele regionen.

Konsolideringen vil også sikre et bedre datagrundlag for den samlede systemportefølje, skabe overblik og forfølge princippet omkring: én opgave, ét system.

Mål 1: Indsatsen skal bidrage til, at den samlede systemportefølje strømlines ved at reducere i antallet af it-systemer, der reelt løser samme opgave og ved at samle ens systemer i en fælles installation for alle brugere.

3. Fælles processer for nyanskaffelser
Der sættes fokus på, at alle nye anskaffelser, der omfatter it/ot teknologi, lever op til regionale standarder for sikkerhed, drift og økonomisk bæredygtighed.

Dette omfatter ensartede og effektive anskaffelsesprocedurer, som bør udarbejdes i tæt samarbejde mellem de tekniske afdelinger på enhederne, Regional IT og øvrige relevante afdelinger på baggrund af standardiserede udbudskrav og evalueringskriterier. Arbejdet skal medvirke til at skabe gennemsigtighed og sammenlignelighed i leverandørvalg med udgangspunkt i brugen af centrale opstillede krav og evalueringskriterier.

Dermed skabes mulighed for, at alle nyanskaffelser som udgangspunkt kan betragtes som regionale løsninger og bidrage aktivt til, at der kan indgås attraktive service- og driftsaftaler, som sikrer langtidsholdbarhed og stabil drift gennem hele systemets levetid.

Mål 1: Indsatsen skal sikre, at der i tæt samarbejde med alle interessenter etableres fælles processer for nyanskaffelser af it- og ot-løsninger, der omfatter standardiserede arbejdsgange og at dette sker i overensstemmelse med den vedtagne governancemodel samt regionale standarder for sikkerhed, drift og økonomisk bæredygtighed.

4. Samarbejdsfora og ansvarsplacering
På trods af et fælles ønske om tæt samarbejde er der generelt en opfattelse af, at afstanden mellem de tekniske områder (ot-delen) og it-området er for stor. Der er behov for at styrke den interne koordinering for at sikre effektiviseringsgevinster og mindste risikoen for at der investeres i samme løsninger flere steder.

Indsatsen skal derfor styrke samarbejdet mellem de lokale tekniske enheder, bygningsområdet og Regional IT, og bidrage til et løbende samarbejde hen over grænselandet mellem it og ot - både på det ledelses-mæssige plan (styregruppe) og på det mere operationelle plan (teknik- og driftsgrupper). Dette vil kræve, at der investeres i en generel opbygning af ot-kompetencer i Regional IT, og at der afsættes tid til samarbejdsaktiviteter hos de tekniske enheder.

Mål 1: Indsatsen skal bidrage til:

- at styrke samspillet mellem it og ot med fokus på sikkerhed, effektivitet og driftsstabilitet.
- at regionen holder sig ajour omkring ot-teknologier og udnytter potentialer ved bl.a. at opsætte standarder og retningslinjer inden for området.
- at der I forbindelse med bygge- og anlægsprojekter etableres et formelt samarbejde mellem byggeprojektet og it-området.

5. Bidrage til klimamålsætning
Teknik og Bygningsstyring spiller en central rolle i at fremme den grønne dagsorden på hospitalerne i Region Syddanmark. Området rummer et stort potentiale for optimering af ressourcer gennem avanceret måling og

intelligent styring af el, varme og vand. Ved at integrere maskinlæring og AI med strategisk planlægnings-information forventer vi, at der kan opnås betydelige besparelser i ressourceforbruget og reducering af miljø-påvirkningen.

Mål 1: Indsatsen skal bidrage til, at der bliver startet initiativer, der sigter mod avanceret ot ressourcestyring på tværs af enheder. Initiativerne vil blive gennemført i tæt samarbejde med de enkelte lokale enheder samt eventuelt i partnerskab med Digital Innovation og SDU.

Grønne gevinster fra små forbedringer: Da ot-området på hospitalerne er præget af et stort antal tekno-logiske komponenter, kan selv små forbedringer i effektivitet have en stor positiv effekt. De miljømæssige gevinster skal synliggøres, så der er grundlag for at vælge de mest miljørigtige komponenter til samme formål – både med fokus på energiforbrug og på øvrig miljøpåvirkning. Det vil inkludere principper om etiske produktionsvilkår og korrekt bortskaffelse af komponenter ved endt levetid. Det skal endvidere sikres, at kravene ikke kun gælder for primære leverandører, men også for deres underleverandører i henhold til principperne om udvidet leverandørstyring.

Mål 2: Indsatserne skal bidrage til, at der løbende indarbejdes principper, der aktivt bidrager til den grønne omstilling i det kommende udbudsbilag ”Kundens ot-miljø”.

6. Leverandørstyring

For at sikre en stabil og sikker drift af sygehusenes tekniske systemer er effektiv leverandørstyring afgørende. Regionens tekniske afdelinger skal i tæt samarbejde med Regional IT og øvrige relevante afdelinger styrke indsatsen omkring leverandørstyring for at sikre, at indkøb, implementering og drift af it- og ot-systemer sker i overensstemmelse med gældende sikkerheds- og kvalitetskrav.

En struktureret tilgang til leverandørstyring indebærer klare kravspecifikationer ved anskaffelser, løbende overvågning af leverandørernes ydelser samt klare aftaler om service, opdateringer og sikkerhed. Leverandører skal forpligtes til at følge regionens standarder for cybersikkerhed, databeskyttelse og systemintegration, så driften af kritisk infrastruktur ikke kompromitteres.

Med et stigende trusselsbillede, herunder NIS2-lovgivningen, er det nødvendigt at integrere forebyggende sikkerhedstiltag i alle leverandøraftaler. Der skal stilles krav om løbende sikkerhedsopdateringer, adgangskontrol og compliance med nationale og europæiske regulativer. Samtidig skal der sikres en beredskabsplan, der hurtigt kan aktiveres i tilfælde af sikkerhedsbrud eller systemnedbrud inden for kritiske områder.

De eksisterende kontraktforhold skal således genbesøges og vurderes i forhold til, om de vedtagne krav til serviceklasser kan overholdes. Der skal også lægges vægt på vurdering i forhold til udvidet leverandøransvar.

Mål 1: Indsatsen skal sikre, at regionen kommer i god kontrol med alle væsentlige leverandører, og således sikre høj driftsstabilitet af it- og ot-systemer, økonomiske besparelser og en fremtidssikret infrastruktur, der understøtter en effektiv og sikker sygehusdrift i overensstemmelse med regionens sikkerheds- og kvalitetskrav.

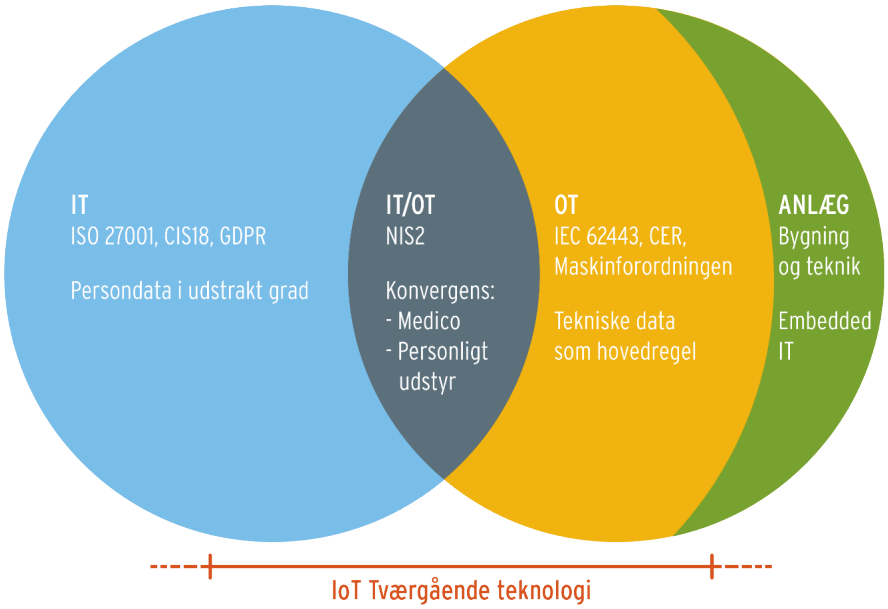
7. Fra underforvaltning til tilstrækkelig forvaltning

En kortlægning af systemlandskabet har påvist en væsentlig underforvaltning af de it-systemer, der hører til området for teknik og bygningsstyring sammenlignet med øvrige systemområder. Der er således behov for at få opbygget en solid forvaltningsfunktion, der skal sikre, at porteføljen lever op til gældende principper og retningslinjer, at der sker en reduktion og forenkling af systemlandskabet, og at der arbejdes på en bedre udnyttelse af den blivende portefølje.

Indsatsen skal således både have fokus på udviklingen i it systemporteføljen og på opbygningen af en tilstrækkelig forvaltningsfunktion. I forbindelse med gennemgangen af systemporteføljen skal det vurderes, om det er muligt at konsolidere nogle af de it-systemer, der løser samme opgave, om der skal ske en bedre udnyttelse af det enkelte system og om der foreligger en korrekt vurdering af det enkelte systems kritikalitet.

Etableringen af en tilstrækkelig og velfungerende forvaltningsfunktion kræver tildeling af ressourcer til området, men også en ekstra indsats til at løfte det nuværende basisniveau for systemforvaltning, især inden for områderne compliance (sikkerhed), leverandørhåndtering og forandringsledelse.

Mål 1: Indsatsen skal bidrage til, at der kan etableres en forvaltning af it- ot-løsningerne på området, som aktivt bidrager til den ønskede sikkerhed og udvikling inden for teknik og bygningsområdet.



Figur 1

Begreberne it (InformationsTeknologi) og ot (Operationel Teknologi) beskriver to hovedområder inden for teknologi i en organisation. Et OT-system suppleres ofte af en IT-del, der administrerer OT-delen.

- IT (Informationsteknologi) fokuserer på data- og informationshåndtering i digitale systemer, f.eks. netværk, servere og software, for at optimere forretningsprocesser. IT dækker over systemer, der håndterer data, netværk, og kommunikation, og har især fokus på datasikkerhed i forhold til personfølsomme data.
- OT (Operationel Teknologi) handler om kontrol og styring af fysiske processer og udstyr, som bruges i industrien til f.eks. produktion og energi, for at sikre sikker og stabil drift.