Statnetts strategi for cybersikkerhet, hvilke forskningsbehov avdekker den?

Lars Hansen
Senior Manager, KPMG

03.11.2021

Statnetts utfordringsbilde innen OT

Behov for økt bruk av sensor data

Økende bruk av ikke-regulerbar kraft fra sol og vind akselerer digitaliseringen i kraftsektoren, og fører til økt behov for bruk av sensorer og sensordata i Statnett.

Nye bruksområder, da spesielt tilknyttet Statnetts kjernesystemer innen OT, avhenger av strenge krav til cybersikkerheten i nye sensorløsninger.

Bedre datakvalitet

Digitalisering fører til økende bruk og avhengighet til data i automatiserte prosesser og beslutninger i sanntid eller nær sanntid i driftskontrollen.

Dette stiller strenge krav spesielt integritet og tilgjengelighet av dataene.

Økt evne til å stille sikkerhetskrav

Det har vært stor utvikling innen sensorteknologi de seneste årene, og også innen OT har nye tjenester og løsninger kommet til. I dette kappløpet mellom leverandører kan ofte funksjonalitet bli prioritert over cybersikkerheten i løsningene.

Dette innebærer at Statnett må være i posisjon til, samt ha kompetanse på, å stille krav til sikkerhetsnivået i løsningene.

Lang levetid

Ulik levetid på IT og OT-systemer er en utfordring når digitalisering fører til økt dataflyt og sammenkobling mellom IT og OT.

Statnett må balansere ny teknologi med teknisk gjeld, uten at det går på bekostning av sikkerheten.

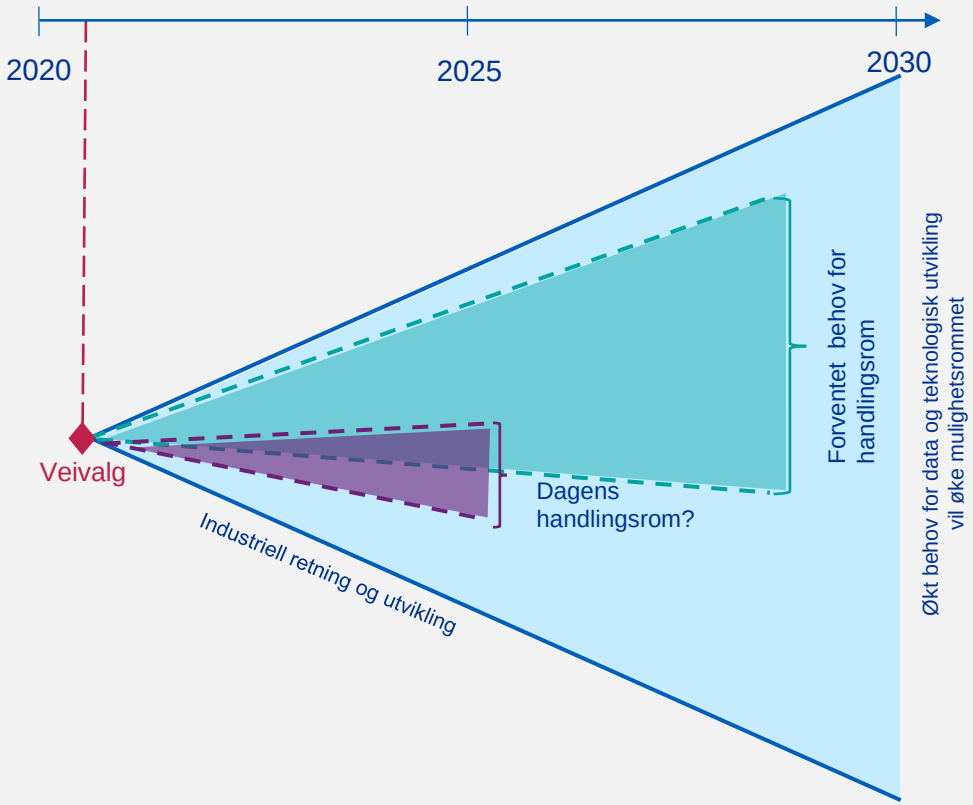
Behov for integrasjon

Nye integrasjoner fører til endringer i eksponering og angrepsflate, og dermed et nytt trusselbilde.

Dette gjør at fremtidig arkitekturmodell blir sentralt for å lykkes med integrasjoner som understøtter forretningsbehovet.

Hvordan velge en strategisk retning som gir størst handlingsrom

Strategi som sikrer handlingsrom



…samtidig som den ivaretar en helhet

En fremtidig strategi må se på alle de ulike komponenter for å sikre et helhetlig sikkerhetsregime.

…morgendagens utnyttelse av teknologi

Morgendagens OT kjennetegnes ved:

- Større datamengder
- AI og Automatisering
- Sammensmelting av OT og IT
- Integrasjon mot skyløsninger
- Økt trussel eksponering
- Økt grad av tjenestekjøp
- Ulike leveransemodeller

Tjenester, funksjoner og prosesser

- Informasjon som grunnlag for styring av OT antas i økende grad å eies og leveres av andre aktører (kraftprodusenter og nettselskaper)
- De digitale prosessene som skal understøtte fremtidige forretningsbehov vil inkludere mange eksterne, både andre aktører i kraft bransjen og leverandørindustrien

Teknologi

- OT og IT teknologi sammensmeltet i vesentlig grad i nye løsninger
- Fortsatt eldre OT teknologi i bruk
- Økt avhengighet til automatiske prosesser i driftskontrollsystem medfører sammenkobling av OT og markedssystemer
- Økt behov for sensorer på linjenett og i anlegg for å bedre utnyttelsesgraden
- Leverandører tar i bruk nye kommunikasjons- og prosesseringsløsninger for sensorer og sensordata (5G, satellitt, sky)
- Økt bruk av standard programvare og programvarebiblioteker i OT systemer og som deler av driftskontroll øker leverandørkjederisiko

Utviklingsbehov

- Økt viktighet av kvalitet, integritet og tilgjengelighet av data gir behov for nye kontroll- og revisjonstiltak
- Tydelige prosesser og retningslinjer for dataforvaltning og dataeierskap
- Arkitektur og arkitekturstyring som understøtter både sikker bruk av eldre teknologier og nye løsninger samt nye leverandører og endrede leveranseformer innen IT og OT
- Styrket kompetanse på nye kommunikasjons og prosesseringsløsninger (også for myndighetspåvirkning)
- Styrket verdi og leverandørkjede forståelse og risikovurderingsevne

Leverandør- og sourcingstrategi

- De klassiske el-kraft leverandørene vil fortsatt levere, men med følgende endringer:
  - i større grad ta i bruk IT-teknologi, men i første omgang med lav modenhet
  - Ønske om å levere større del av verdikjeden (prosessering og nye tjenester som status)
  - I større grad levere software og tjenester
- Nye leverandører med mer disruptive løsninger og leveransemodeller, vil ta markedsandeler i kraftbransjen
- Verdikjeder spres over flere leverandører og sikkerhet må sees på tvers i disse

Ytelse og etterlevelse

- Økt bruk av standard IT i OT-systemer trigger behovet for bedre kompetanse, rutiner og prosesser for oppfølging av ytelser og etterlevelse av sikkerhetskrav i OT-systemer
- Økt bruk av tjenesteleveranser innen OT vil kreve bedre evne til kravsetting og kontroll av kvaliteten i slike leveranser
- Økt bruk av underleverandører i produkt og tjenesteleveranser spesielt økter behovet for evne til kontroll med lange leveransekjeder
- Mer komplekst leveransebilde for produkter og tjenester kreves styrket evne til vurdering og forståelse av risiko. Risikovurderingene bør i økende grad være datadrevet

Utviklingsbehov

- Nye metoder for rapportering og kontroll for å skape nødvendige tillit til forsvarlig cybersikkerhet i nye teknologier og leveranseformer
- Håndtering av underleverandører og lange verdikjeder i tjenesteleveranser må styrkes
- Risikostyring i det nye leveransebildet må styrkes med fokus på risikomodeller og risikovurderinger basert på kvantitative data

Ressurser og kompetanse

- Økt behov for tverrfaglig kompetanse i grensesnittet mellom elkraftteknologi, kontrollsystemer, IT og cybersikkerhet
- Juridisk kompetanse ved anskaffelse blir sentralt for å sikre nødvendig innsyn hos leverandører
- Økende grad av tjenestekjøp vil forsterke behovet for kompetanse på eierskapsforhold i leverandører og underleverandører
- Styrket trusselaktørforståelse vil bli viktig for å håndtere dynamiske sikkerhetstiltak i tillegg til grunnsikringstiltak.

Organisasjon og styring

- Økende digitalisering, sammensmelting av OT og IT, endrede leveranseformer og endring i trusselbildet stiller nye krav til styring og organisering
- Verdikjedene endres og krever en annen samhandling en tidligere med tydelig definerte ansvarsområder
- Stor sannsynlighet av behov for tilpasning av organisasjon og styringsmodell.

Utviklingsbehov

- Forsterket evne til å forstå risiko og sårbarheter i mer komplekse løsninger.
- Endring i operasjons- og leveransemåte samt teknologi krever mer tverrfaglig kompetanse i skjæringspunktet mellom IT og OT både teknologisk og prosessuelt
- Risikoforståelse og juridisk kompetanse med betydelig IT forståelse må utvikles for å understøtte økt grad av tjenestekjøp og lange leverandørkjeder
- Styrket trusselaktørforståelse

Prioriterte FoU prosjekter

Arkitektur og teknologi

Utforske og utvikle prinsipper for arkitekturstyring av tjenestesammenkoblinger

Utforske og standardisere teknologi som kan operasjonalisere arkitekturen og understøtte oppnåelsen av forsvarlig sikkerhet når ulike løsninger og teknologier sammenkobles for oppnå ønsket digitalisering.

Utforske 5G teknologi for gi kompetanse til å utnytte denne for bedre effektivitet og sikkerhet i løsninger

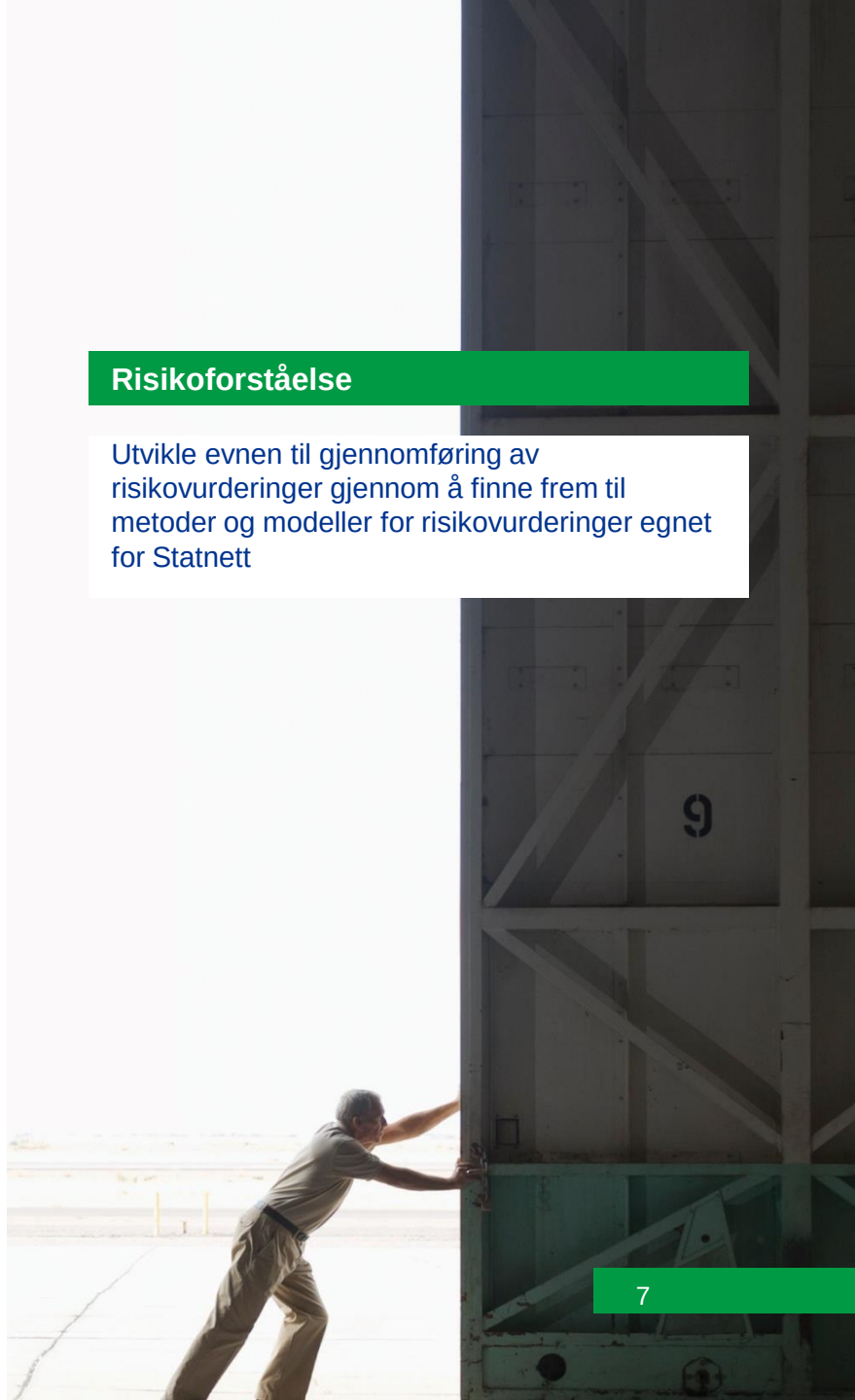
Kontrolltiltak og revisjon

Utvikle kontrolltiltak for og revisjonsevne til komplekse verdikjeder og tjenesteleveranser ved:

- Vurdere forhold relevant for sikkerhet i verdikjedene
- Utvikle egnede kontrolltiltak og fokusområder for revisjon

Risikoforståelse

Utvikle evnen til gjennomføring av risikovurderinger gjennom å finne frem til metoder og modeller for risikovurderinger egnet for Statnett



home.kpmg/socialmedia