NVE

EKSTERN RAPPORT NR. 17 / 2024

Gjensidige avhengigheter av IT og OT i kraftforsyningen

SKREVET AV Netsecurity

NVE Ekstern rapport nr. 17/2024
Gjensidige avhengigheter av IT og OT i kraftforsyningen

Utgitt av:	Norges vassdrags- og energidirektorat
Redaktør:	Jon-Martin Storm og Kristian Frafjord
Forfatter:	Netsecurity
Omslagsfoto:	Kontrollrom i Smestad transformatorstasjon. Foto: NVE

ISBN:	978-82-410-2389-7
ISSN:	2535-8235
Saksnummer:	202318531

Sammendrag: Rapporten drøfter risiko knyttet til økende integrering av informasjonsteknologi (IT) og operasjonell teknologi (OT). Den baserer seg på intervjuer med aktører fra kraftbransjen innen regulerbar vannkraft, vindkraft, og nettselskaper.

Rapporten understreker at økt digitalisering og integrasjon mellom IT og OT kan føre til en større angrepsflate mot kraftbransjen. Behovet for tydeligere definisjoner av kraftsensitiv informasjon og bedre regulering av IT-OT integrasjon vil derfor være viktig. Avslutningsvis gir rapporten anbefalinger for å forbedre eksisterende forskrifter for å styrke beskyttelsen av kraftforsyningen mot digitale trusler.

Emneord: IT-sikkerhet, OT-sikkerhet, driftskontroll, kraftberedskap

Norges vassdrags- og energidirektorat
Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 22 95 95 95
E-post: nve@nve.no
Internett: www.nve.no

Juni 2024

Forord

Kraftprodusenter og nettselskaper benytter en rekke ulike digitale systemer og tjenester. Kraftberedskapsforskriften stiller krav til sikring av digitale informasjonssystemer i kraftberedskapsforskriftens § 6-9. Kravene gjelder alle digitale IT-systemer og utgjør en grunnsikring. For driftskontrollsystemer setter kapittel 7 en rekke tilleggskrav. Med økende bruk av sensorer og analyseverktøy for å optimalisere styring av nett- og produksjonsanlegg kan dette skille bli mindre klart. Vi ønsket derfor innspill fra bransjen om hvordan dette burde reguleres.

NVE har observert at utviklingen ved nye digitaliserings- og innovasjonsprosjekter medfører en tettere kopling mellom IT og OT. Typiske IT-tjenester som sanntidsdata fra dataanalyse i skyen blir viktigere som input til fysiske prosesser som kjøres i OT. Den økte integrasjonen mellom IT og OT skaper flere gjensidige avhengigheter.

NVE ønsker mer innsikt i utviklingen av IT - OT integrasjon i kraftforsyningen og hvordan sammenkoblingen støtter forretningsprosesser, produksjon og nettdrift. Dette inkluderer å se på om krav til IT og OT er tilstrekkelige for å ivareta sikkerheten i mer integrerte systemer og om kravene er tilstrekkelig harmonisert.

Rapporten er utarbeidet av Netsecurity på oppdrag av NVE. Vi vil takke alle som stilte opp i intervjuer. De har bidratt til et bedre kunnskapsgrunnlag for vår regelverksutvikling for IT- og OT-systemer.

Oslo, juni 2024

Eldri Naadland Holo
seksjonssjef
Seksjon for beredskap
Tilsyns- og beredskapsavdelingen

Dokumentet sendes uten underskrift. Det er godkjent i henhold til interne rutiner.

Gjensidige avhengigheter av IT og OT i kraftforsyningen

Forord

På oppdrag for Norges vassdrags- og energidirektorat (NVE) har Netsecurity gjennomført et prosjekt tilknyttet belysningen av ulike problemstillinger relatert til integrasjonen av IT og OT i kraftforsyning. Prosjektet har inkludert en rekke fagressurser, og involvert flere deler av det norske kraftforsyningen innen regulerbar vannkraft, uregulerbar kraftproduksjon fra vind og i tillegg til distribusjonssystem-operatører (DSO).

Netsecurity vil takke alle ressurser som har bidratt med sin tid og kompetanse for å bistå i gjennomføringen av prosjektet. Deres kompetanse, erfaringer, refleksjoner og innspill har gjort det mulig å utforske området, og å utarbeide denne rapporten.

Respondentene i prosjektet tydeliggjør at NVE tilbyr og står seg som en svært behjelpelig og kompetent veileder.

På vegne av prosjektgruppen fra Netsecurity vil vi takke for tilliten og samarbeidet i forbindelsen med dette prosjektet. Vi føler oss privilegerte som får bistå i utviklingen informasjonssikkerhet innenfor Norsk kraftsektor sammen med så dyktige og kompetente mennesker.

Om Netsecurity

Netsecurity er et av Norges største IT-sikkerhetsselskaper. Vi hjelper private og offentlige virksomheter med tjenester og produkter som bidrar til økt trygghet i en digital verden. Som kunde av oss vil du få hjelp gjennom hele verdikjeden, før, under og etter et angrep. Netsecurity er godkjent av NSM for hendelseshåndtering, og partner av Nasjonalt Cybersikkerhetssenter (NCSC). Vi er blant landets fremste kompetansemiljø på Palo Alto Networks og Extreme Networks.

Sammendrag

Netsecurity har fått i oppdrag av Norges vassdrags- og energidirektorat, videre omtalt som NVE, å utarbeide en rapport tilknyttet gjensidige avhengigheter mellom informasjons-teknologi (IT) og operasjonell teknologi (OT). Hensikten med rapporten er å belyse ulike problemstillinger innenfor ulike caser, og for å danne beslutningsgrunnlag for ev. utarbeidelse eller justering av eksisterende krav.

Økt sammenkopling mellom IT og OT- miljøene som historisk sett har vært adskilt, øker angrepsflaten. I kontekst av den geopolitiske situasjonen verden i dag står ovenfor har Norge blitt en mer sentral energileverandør for Europa, noe som tydeliggjør viktigheten av å sikre kritisk infrastruktur.

I nyere tid har kritisk infrastruktur vært svært attraktive mål for flere trusselaktører [1], [2], [3] og flere nyere rapporter peker til at det forventes økt angrep mot kritisk infrastruktur også i Norge [2], [3] [4]. Dette understreker at det er viktigere enn noen gang å sikre kritisk infrastruktur mot angrep fra trusselaktører som i økende grad utnytter digitale sårbarheter for å oppnå sine mål. Gjensidige avhengigheter mellom IT og OT-miljøene innenfor kraftsektoren eksponerer i større grad miljøer som tidligere har vært adskilt.

Denne rapporten tar for seg hvilke fordeler og ulemper som blir introdusert ved en økt sammenkopling av IT og OT i kraftforsyningen på informasjonssikkerhet, innen tre ulike caser;

(1) regulerbar vannkraft

(2) uregulerbar kraftproduksjon fra vind

(3) distribusjonssystemoperatører (DSO).

Innhenting av informasjon har blitt basert på semistrukturerte intervjuer hvor deltakere innen de respektive casene har bidratt til informasjonsunderlaget. Utfordringer med dagens versjon av kraftberedskapsforskriften (videre omtalt som kbf) har blitt kartlagt gjennom intervjuprosessen.

Tolkbarheten til eksisterende kbf blir løftet fram som en utfordring. Forskriften stiller indirekte krav til at personell som leser kbf har informasjonssikkerhetskompetanse, og evnen til å forstå innholdet i forskriften. Det blir løftet frem at eksisterende veileder til kbf er et nyttig verktøy for å tolke kravene i denne prosessen. Tydelige krav i forskriften gjøre det enklere å få på plass effektive sikringstiltak. Dette vil også gi virksomheter en klar retning i hva som forventes fra myndighetene og kan dermed hjelpe virksomheter med å identifisere og prioritere nødvendige tiltak. Selv om tolkbarheten til forskriften kan være utfordrende, blir det også påpekt at dette gir rom for tilpasning. Virksomheter kan i større grad innrette seg uavhengig av deres størrelse og kompleksitet. Denne fleksibiliteten tillater virksomheter å implementere sikkerhetsmekanismer som er egnet for deres spesifikke behov.

Kbf blir i dag brukt som et hjelpemiddel for å få gjennomslag til å gjennomføre ulike informasjonssikkerhetstiltak. Det blir påpekt av respondentene at standardisering er positivt for kraftbransjen og at tydelige krav i forskriften kan spille en avgjørende rolle for å få gjennomslag for forskjellige sikringstiltak.

Definisjonen av kraftsensitiv informasjon oppleves som utfordrende, og mer konkrete eksempler er ønskelig i en revidert veileder i fremtiden. Respondentene understreker også at det bør vurderes om ulike kategorier av kraftsensitiv informasjon vil gjøre prosessen med

å identifisere og sikre informasjonen enklere. Videre kan komplekse eierstrukturer skape utfordringer når det gjelder ansvarsfordeling, og hvem som gjør hva under eksempelvis en informasjonssikkerhetshendelse.

Rapporten utforsker hvordan IT og OT støtter eksisterende forretningsprosesser, produksjon og nettdrift. Ulike sikkerhetsutfordringer tilknyttet økt sammenkopling blir lagt frem i hver enkelt case.

Vi har også utforsket om kravene som blir stilt i dagens kbf., innenfor § 6-9 og kapittel 7, er tilstrekkelig regulert og om dette støtter eller setter begrensninger for økt sammenkopling av IT og OT-miljøer.

Avslutningsvis inkluderer rapporten forslag til hvordan eksisterende kbf kan bli bedre for sluttbrukere, samt anbefalinger for å sikre IT-OT-avhengigheter. Rapporten er utarbeidet av et tverrfaglig team bestående av strategiske rådgivere, tekniske konsulenter og etiske hackere fra Netsecurity.

Innhold

1. Innledning

Økt sammenkopling mellom IT og OT skaper unike muligheter, for en rekke industrivirksomheter, til å forbedre operasjonell effektivitet og beslutningsstøtte. Det kan bidra med optimalisering gjennom økt automatisering av både operasjonelle prosesser og produksjonsplanlegging. Automatisering av operasjonelle oppgaver kan resultere i enklere og en mer sømløs kopling mellom IT og OT-systemer.

Ved å innhente informasjon fra OT, i kombinasjon med IT, vil dette kunne skape mer helhetlig datagrunnlag. Denne informasjonen kan brukes i analyser av store datasett, som kan skape økt innsikt og prediktive analyser. Innenfor kraftbransjen kan dette bety et bedre grunnlag for å estimere levetid på komponenter i strømnettet, med kontinuerlig overvåkning av komponentenes faktiske slitasje, fremfor å ha en definert utskiftningshyppighet. Nye sensorer og smartmålere gir en bedre oversikt over strømforbruk og tilstanden til strømnettet i sanntid.

Ved en økt sammenkopling vil det åpnes for en større grad av fleksibilitet og skalerbarhet. Virksomheter kan i høyere grad tilpasse seg endringer i krav og behov. Fleksibiliteten kan forenkle tilpasningsprosessen av nye teknologier og endringer i forretningskrav.

Økt sammenkopling mellom IT- og OT-systemer medfører økt risiko. Disse risikoene må håndteres for å møte virksomhetens risikoakseptanse. Det er viktig å ha god oversikt over arkitektur, informasjon, dataklassifisering og informasjonsflyt i vurderingen av risikoene.

IT- og OT-miljøene har tradisjonelt hatt noe ulikt fokus og prioriteringer. Disse miljøene må i høyere grad forstå de forskjellige faglige utfordringene og samarbeide for å skape motstandsdyktighet og hensiktsmessige løsninger. Økt opplæring og samhandling vil være viktige bidragsytere for å ta bort skillelinjene. Innføringen av nye systemer og høyere grad av sammenkoplede miljøer krever at de ansatte får nødvendig opplæring for å kunne operere, drifte og vedlikeholde nye systemer og teknologi som innføres. Innføringen av en mer sammenkopling av IT og OT vil kreve interne ressurser, og tilstrekkelig redundans, til å være med på utviklingen, implementeringen, utbygging av infrastruktur, samt drift, vedlikehold og utvikling av allerede eksisterende systemer.

Transport av data inn og ut av driftskontrollsystemet må risikovurderes nøye. Ved å sende data ut, må det gjøres vurderinger om hvor sensitive dataene er opp mot kbf. Ønsker man å få data inn, så må det vurderes om de kan hentes inn, eller om det er et eksternt system som skal sende inn data. Eksterne systemer som kan sende inn informasjon åpner for utfordringer. Ved å åpne for eksterne tjenester tillates kommunikasjon med aktører utenfor virksomheten. Dette øker risikoen for uønskede handlinger. Utnyttelse av sårbarheter i tjenesten gjør at aktører utenfor virksomheten kan få tilgang til kritisk infrastruktur. Uønsket endring av informasjonen som transporteres inn, kan påvirke blant annet produksjon.

1.1 Bakgrunn

På oppdrag for Norges vassdrags- og energidirektorat (NVE) har Netsecurity utarbeidet en rapport tilknyttet gjensidige avhengigheter mellom informasjonsteknologi (IT) og operasjonell teknologi (OT). Hensikten med rapporten er å belyse ulike problemstillinger innenfor ulike caser, og for å danne beslutningsgrunnlag for ev. utarbeidelse av krav til uregulerbar produksjon, samt innspill til revisjon av eksisterende forskrift og tilhørende veileder. Rapporten har også som formål å øke NVEs kunnskap, status og situasjonsforståelse for IT-OT integrasjon i den norske kraftforsyningen, hvilket mulighetsrom og risikoer som eksisterer med slike integrasjoner.

Rapporten adresserer utfordringer som IT-OT integrasjonen medfører og ev. begrensninger som kbf. § 6-9 og kap. 7 setter for kraftbransjen for å utnytte kommunikasjonslinjer som går mellom IT- og OT-miljø.

Prosjektet ser på tre ulike caser innen norsk kraftsektor. Casene som blir presentert for å belyse problemstillingen fra ulike perspektiver har blitt utarbeidet i samspill med NVE og godkjent før prosjektet ble påbegynt. Denne rapporten utforsker følgende tre caser:

1. Regulerbar vannkraft
2. Uregulerbar kraftproduksjon fra vind
3. Distribusjonssystemoperatør (DSO)

Disse tre casene ble vurdert som de mest hensiktsmessige å utforske for å begrense omfanget av rapporten, tilpasset prosjektets retningslinjer og tidsramme. Ved å ha definert tre ulike caser danner dette en bredde i evalueringsgrunnlaget slik at det blir dekkende for kraftbransjen.

Sensordata fra linjeovervåkning blir brukt som beslutningsgrunnlag for justeringer av kraft. Hvordan kan det sikres at disse dataene er korrekte (sikring av integritet) når sensorene har et annet sikkerhetsnivå enn andre deler av informasjonskjeden.

Et eksempel kan være i hvor stor grad kan vi ha tillit til data som sendes til sky og som skal brukes videre i OT-miljøet, og hvordan vi trygt og sikkert kan tilrettelegge for dette.

Det er avgjørende å ha forståelse for IT-OT avhengighetene, hvilken kritikalitet disse integrasjonene utgjør og hvor lenge en kan være uten slike koplinger (kontinuitetsbrudd). Hvor lenge kan vi klare oss uten disse tilkoblingene? Én uke, én dag, én time, eller er vi helt avhengig av denne tilkoblingen til enhver tid? Uavklarte avhengigheter kan føre til situasjoner slik som *Colonial Pipeline* som NVE belyser [5]. Kort oppsummert vil en avklart oversikt over avhengigheter resultere i en effektiv beredskap.

Industrielle miljøer har historisk sett ikke vært designet for å være påkoblet og eksponert mot IT eller internett, og kan som en konsekvens av dette anses som *insecure-by-design*, noe som vil si at sikkerhet, i form av *information security*, ikke har vært en del av løsningens design. Kontrollsystemer har vært designet med mål om å øke produksjonseffektivitet og sikkerhet (safety) gjennom å automatisere fysiske prosesser. Prosessene er ofte tidskritiske og må håndteres umiddelbart eller innenfor et svært kort tidsvindu, for å forhindre feil, avbrudd eller mulige katastrofer. Kontrollsystemer er typisk designet for å ha en levetid på +/- 25år, og levetiden blir stadig forlenget som følge av oppgraderinger og optimaliseringer.

Bransjen bør ha en risikobasert tilnærming til IT-OT integrasjon, i tillegg til å ha fokus på sikker design (*security-by-design*) og sikker konfigurasjon (*security-by-default*) ved anskaffelser. Dette forutsetter at bransjen jobber tett sammen og øker den kollektive sikkerhetskompetansen.

For at prinsippene for sikker design og –konfigurasjon blir implementert iht. forventinger kreves det at den enkelte aktør definerer hvilket rammeverk eller standard som skal brukes, slik at bestiller og leverandør kan kommunisere via et felles språk. For at sikker design og –konfigurasjon blir ivaretatt gjennom livssyklusen for systemer må nødvendige sikkerhetsressurser være tilgjengelige. Dette gjelder fra konseptfase for å kunne spesifisere krav enten de er risikobaserte, funksjonelle, tekniske, compliance-baserte eller basert på sikkerhetsmål (eks: integriteten til RTU skal ivaretas, SCADA-systemet skal være tilgjengelig etc.).

Et felles språk mellom bestiller og leverandør kan etableres ved å definere hvilke(t) rammeverk eller standard som skal brukes under prosjektets livssyklus. Dette vil bidra til å skape rammer for arbeidet og forutsigbarhet mellom partene mht. hva som kan forventes.

Målet for prosjektet er at NVE skal ha et godt underlag for beslutningsstøtte til å vurdere hvilke muligheter og begrensninger det er p.t. slik kbf. § 6-9 og kap. 7 er definert, dette for å gjøre NVE i stand til å forstå og prioritere anbefalinger og tiltak.

1.2 Mål og hensikt

Oppdraget har følgende mål og hensikt:

1. Beskrive eksempler (caser) på IT-OT integrasjon i kraftforsyningen og hvordan den styrkede sammenkoplingen støtter forretningsprosesser, produksjon og nettdrift.

    a) Identifisere og beskrive 3-5 caser (eksempler) på økt integrasjon mellom IT og OT. Disse casene skal dekke produksjon og nett.

    b) Minst ett case skal handle om uregulerbar kraftproduksjon fra sol eller vind.

2. Drøfte sikkerhetsutfordringer knyttet til punkt 1, vurdere kravene i kraftberedskaps-forskriften (kbf.) § 6-9 og kapittel 7 opp mot sikkerhetsutfordringene og påpek områder i dagens regulering der dagens krav er lite.

3. Vurdere sikkerhetsutfordringer ved økt informasjonsflyt mellom produksjons-planlegging og driftskontrollsystem, inkluder bruk av eksterne produksjons-planleggingstjenester. Undersøk muligheter for å heve sikkerhetsnivået på produksjonsplanleggingsverktøy.

4. Vurdere om kravene i kbf. § 6-9 og kapittel 7 er til hinder for tettere sammenkopling. Dette inkluderer også å se på der kravene nå setter utilsiktede barrierer for utviklingen og implementasjon av nødvendige digitale systemer for å drifte fremtidens kraftsystem.

1.3 Omfang og avgrensning

Prosjektets tidsperiode strekker seg fra november 2023 til mars 2024. Rapporten har følgende avgrensninger:

- Ekskluderer uklassifiserte regulerbare aktører (Klasse 0).
- Ekskluderer fjernvarme.

Relevante intervjuobjekter har blitt fremlagt i samarbeid med NVE. Respons og aktiv deltakelse fra intervju deltakere er en faktor som har hatt påvirkning på datagrunnlaget.

1.4 Metode

Arbeidsmetodikken som ligger til grunn for rapporten er basert på semistrukturerte intervjuer. Prosjektet er utarbeidet i et tverrfaglig team med spiss kompetanse innenfor informasjonssikkerhet, IT og OT. Intervjuene som har blitt gjennomført har inkludert en rekke ulike selskaper, av varierende størrelse.

Prosjektgruppen av valgt å ta i bruk semistrukturerte intervjuer for å kunne besvare oppgaven. Hensikten med å ta i bruk semistrukturerte intervjuer er for å utforske intervjudeltakernes antakelser og meninger. Denne intervjuteknikken åpner for muligheten til å stille oppfølgingsspørsmål for å sikre tydelige, forståelige og brukbare svar rettet mot de ulike problemområdene. Intervjuobjektene som har blitt brukt som kilder til informasjon har blitt anonymisert. Nedenfor presenteres en liste over de ulike respondentene.

Aktørene som har bistått i prosjektet er fra regulerbar vannkraft, uregulerbar kraftproduksjon fra vind og distribusjonssystemoperatører.

1.5 Rapportstruktur

Rapporten er strukturert som følger:

- **Kapittel 1** - Gir en introduksjon til problemstillingen, bakgrunn, mål og hensikt, omfang og avgrensninger samt hvilke metoder som er brukt. Det gir også en oversikt over prosjekttilnærming og respondenter.

- **Kapittel 2** – Omhandler gjensidige avhengigheter innenfor IT og OT i kraftforsyningen. Kapittelet tar for seg fordeler med sammenkopling, utfordringer og trusler som kan utnytte seg av økt sammenkoplede miljøer.

- **Kapittel 3** - Adresserer viktige funn tilknyttet gjensidige avhengigheter IT og OT i kraftforsyning gjennom tre ulike caser: Regulerbar vannkraft, uregulerbar kraftproduksjon fra vindkraft og DSO. Gjennom disse tre casene blir det sett på utfordringer, områder som er for lite regulert og hvordan eksisterende kbf kan bli bedre for sluttbruker.

- **Kapittel 4** - Foreslår anbefalinger som bør vurderes i prosessen tilknyttet økt IT og OT-integrasjon. Anbefalingene har tilknytning til hver enkelt case, med referanse til kbf og den relaterte utfordringen.

- **Kapittel 5** - Viser til referanser som har blitt brukt i prosjektet.

2. Gjensidige avhengigheter IT og OT i kraftforsyningen

Dette kapittelet gir en innføring i gjensidige avhengigheter mellom IT og OT i kraftforsyningen, fordeler og utfordringer som introduseres, og hvilke trusler som kan utnytte nye sårbarheter som følge av økt sammenkopling.

2.1 Hvorfor økt sammenkopling?

En av hensiktene med økt grad av sammenkopling mellom IT og OT er at informasjon hentet ut fra OT-miljøet kan distribueres til beslutningstakere innenfor OT, og videre på tvers av virksomheten, for å ta informative beslutninger. Fordeler som introduseres av sammenkoplingen inkluderer blant annet sanntidsmonitorering og kontroll, effektivisering og strømlinjeformede prosesser, reduserte operasjonelle kostnader som følge av høyere systemeffektivitet og planlagte serviceintervaller som kan reduseres.

Økt bruk av *Industrial Internet of Things (IIoT)* som eksempelvis sensorer som overvåker strømnett for å få tilgang til sanntidsdata eller overvåkningskameraer, brukes blant annet til monitorering eller i beslutningsprosesser. IIoT-utstyr er ofte internettilkoblet eller har en viss form for skytilkobling, noe som kan utfordre eksisterende sikkerhetsoppsett og arkitekturvalg. Dette øker IT-OT-avhengighet. Kontroll på dataintegritet og -kvalitet under slik datautveksling blir vesentlig [6]. Bruken av denne type teknologi åpner muligheter for å få mer korrekt datagrunnlag blant annet fra belastning og slitasje. Dette kan resultere i bedre utskiftningsgrunnlag, i tillegg til å være mer bærekraftig og økonomisk. Et utbedret utskiftningsgrunnlag kan også gi sikkerhets- og tidsmessige fordeler.

Innhentingen av data over tid kan være med å bygge store datasett som kan anvendes i prediktive analyser. Resultatene fra disse type analyser kan intensjonelt redusere nedetid, og driftsstans. Disse dataene vil kunne åpne for muligheter til å ta mer informative og strategiske beslutninger.

2.2 Utfordringer med økt sammenkopling

Selv om det introduseres en rekke fordeler med en høyere grad av sammenkopling mellom IT og OT, kommer ikke disse uten utfordringer. Cybersikkerhet er en sentral utfordring som er uunngåelig i prosessen med økt sammenkopling. Siden tradisjonelle OT-miljøer vanligvis ikke har vært tilkoblet internett, var sannsynligheten for å oppleve digitale angrep redusert. Når vi snakker om en økt sammenkopling mellom disse miljøene er det ofte assosiert med tilgang via samme nettverk, IT-nettverket, som har tilgang til internett. Det er flere grunner til at dette er hensiktsmessig. Noen av disse grunnene kan være blant annet å kunne få tilgang til sanntidsdata, fjernsupport eller fjernovervåkning. Smart vedlikehold og produksjonsoptimalisering blir introdusert som følge av økt tilgjengelighet gjennom fjerntilgang til industrielle kontrollsystemer. Det er avgjørende å sikre disse fjerntilgangene for å hindre at trusselaktører får tilgang til kritisk infrastruktur gjennom OT [3].

Økt bruk av fjerntilgang og tilgjengeliggjøring av sanntidsdata fra operasjonelle miljøer medfører økt risiko [3]. Kritisk infrastruktur som eksponeres mot internett er avgjørende å sikre, da dette utvider angrepsflatene betydelig.

Den økte sammenkoplingen effektiviserer forretningsprosesser og kraftproduksjon, og kan gjøre nettet smartere. Dette øker sannsynligheten for lengre levetid og mindre nedetid på en rekke ulikt nettutstyr. Selv om sammenkopling muliggjør effektivisering, kostnadsreduksjon og økt levetid på komponenter er det også flere sårbarheter og innganger til kritisk infrastruktur.

Sårbarheter kan introduseres gjennom tilgangsstyring på tvers av IT- og OT-miljøene. Dette kan resultere i en kompromittering av IT-enheter med mulighet for at en angriper kan traversere inn til OT på grunn av tilgang og rettigheter. En annen utfordring er bruk av felles nettverksutstyr, der OT- og IT-utstyr bruker en felles svitsj, gjør det mulig å hoppe mellom virtuelle nettverk (VLAN). Denne koplingen krever høyere grad av beskyttelse enn de tradisjonelt separate miljøene, da kritisk infrastruktur i større grad blir eksponert mot internett og digitale trusler.

2.3 Økt angrepsflate

Utdrag fra *Risiko 2024*, *Nasjonal trusselvurdering 2024*, *Fokus 2024* viser at det er flere ulike stater som utgjør en betydelig etterretningstrussel mot Norge, også i 2024. Noen av metodene som forventes anvendt mot norske mål i 2024 er blant annet cyberoperasjoner og rekruttering av kilder. Nyere trender viser at rekruttering av kilder kan finne sted via digitale virkemidler som eksempelvis chatteapplikasjoner. Som følge av den geopolitiske situasjonen i verden i dag har Norge blitt en mer sentral energileverandør for Europa.

Både offentlig og private virksomheter er utsatt for fremmede staters etterretnings-aktivitet. Eksempler på typer etterretningsaktivitet er blant annet e-poster med lenker som en ikke må trykke på, personer som stiller detaljerte spørsmål om jobben din, eller et selskap som ønsker å kjøpe varer virksomheten din produserer.

I den nasjonale trusselvurderingen kommer det frem at flere europeiske borgere er pågrepet og tiltalt for å ha utført etterretningsvirksomhet på vegne av andre stater. Oppdraget de har fått har blant annet vært å tilegne seg informasjon om eget lands forsvarsevne og kritisk infrastruktur. I enkelte av disse tilfellene var utpressing årsaken til at dette ble utført, men de fleste tilfellene var økonomisk motivert.

Trusselen i cyberdomenet blir fremmet som dynamisk og i kontinuerlig utvikling, og statlige aktører vil mest sannsynlig utføre cyberoperasjoner mot norske virksomheter, organisasjoner og privatpersoner i 2024. Formålet med disse cyberoperasjonene er hovedsakelig informasjonsinnhenting. Det vurderes at fremmede stater kan utføre destruktive operasjoner mot norske mål. Blant de statlige aktørenes hovedmål er energisektoren nevnt. Gjennom virksomheters verdikjede kan eksempelvis underleverandører utgjøre en betydelig sårbarhet dersom ikke sikkerhetstiltak er implementert tilsvarende de virksomheten selv har på plass [7].

Vurderinger gjennomført av Etterretningstjenesten belyser sikkerhets-utfordringer som blant annet viser at andre stater har tidligere vist vilje og evne til å ramme kritisk infrastruktur i en konfliktsituasjon. Dette har blant annet skjedd via industrielle kontrollsystemer utført gjennom cyberoperasjoner [4]. På samme tid blir det også vurdert at nye tjenestenektangrep mot Norge på vegne av eller til støtte for disse statene er sannsynlig i det kommende året. Etter militærdoktrine kan disse statene ramme sivile mål, som blant annet samfunnskritisk infrastruktur og mål av stor økonomisk verdi, gjennom cyberoperasjoner [4].

Kritisk infrastruktur og -verdier må beskyttes, da cyberoperasjoner kan gjøre betydelig skade [3]. Ved å ha en helhetlig tilnærming til sikring av kritisk infrastruktur, reduseres sannsynligheten for at sårbarheter blir utnyttet av en trusselaktør.

Konsekvensene som kan inntreffe vil kunne ha påvirkning på befolkningen, og Forsvarets evne til å forsvare norsk territorium [3]. I ytterste konsekvens vil cyberoperasjoner kunne resultere i konsekvenser som alvorlige fysiske skader på kritisk infrastruktur og personell [3].

3. Viktige funn

Gjennom intervjuer av et utvalg respondenter har vi sett nærmere på problemstillingen rundt gjensidige avhengigheter mellom IT og OT i norsk kraftsektor. Funnene blir fremstilt nedenfor med inndeling i tre ulike caser. Innenfor hver enkelt case sees det på hvordan økt sammenkopling støtter forretningsprosesser, produksjon og nettdrift. Videre utforskes utfordringer, hvor eksisterende kbf stiller for lite krav og forslag til hvordan eksisterende kbf kan bli bedre for sluttbrukerne.

3.1 Case 1: Regulerbar vannkraft

I Norge kommer 90 % av all kraftproduksjon fra vannkraft, og på verdensbasis utgjør vannkraft en sjettedel av den totale kraftproduksjonen [8]. Innenfor denne seksjonen vil vi legge frem funn som blir løftet frem sett fra regulerbar vannkraft sitt perspektiv.

3.1.1 Hvordan kan den styrkede sammenkoplingen mellom IT og OT støtte forretningsprosesser og produksjon?

Styrket sammenkopling innenfor IT og OT-miljø under regulerbar vannkraft understøtter en rekke prosesser. Økt sammenkopling gir innsikt som tidligere ikke har vært mulig hvor prediktiv data kan effektivisere blant annet produksjon, drift og vedlikehold.

Økt bruk av en rekke sensorer åpner muligheten for nøyaktige målinger og predikering av vedlikehold. Dette kan eksempelvis være børstesensorer i kraftgeneratorer som gir bedre innsikt i faktisk slitasje. Denne typen sensorer åpner for muligheten av en riktigere utskiftningshyppighet på komponenter fremfor å ha tidsbestemt utskiftningsrytme. Bruk av kameraovervåkning kan bli brukt som informasjonsgrunnlag i beslutningstaking knyttet til både IT og OT-miljøer.

En del av dagens skytjenester ønsker tilgang til relativt store mengder data eller tilgang til utstyr for å kunne få innsikt, og fungere etter intensjon. Det blir adressert at flere av dagens skyløsning tilbyr oversikt og datafremstilling på en visuelt pen måte, men at funksjonalitetene ellers er relativt begrenset. Den initielle investeringen har en betydelig kostnad, og per i dag blir det adressert at funksjonalitetene i varierende grad rettferdiggjør denne investeringen.

Produksjonsplanleggingstjenester som blir benyttet i dag er ofte en kombinasjon av systemer levert av tredjeparter, men i tillegg benyttes egenutviklet programvare. På tross av dette er det alltid menneskelige vurderinger i bildet. Innenfor produksjonsplanlegging oppleves det som et begrenset ønske om å dele informasjon utover dette.

3.1.2 Hvilke sikkerhetsutfordringer er tilknyttet økt sammenkopling innen IT- og OT-integrasjonen?

Økt sammenkopling mellom IT- og OT-miljøet blir utfordret når det kommer til bruk av flere sensorer, som også kan gå under betegnelsen IIoT (Industrial Internet of Things). Tilgjengelighet og integritet blir ofte prioritert fremfor konfidensialitet i OT-miljøer. Dersom integriteten blir brutt, eller data blir manipulert, vil dette kunne få store konsekvenser. Ved å anvende flere typer sensorer er det avgjørende å ha kontroll på disse enhetene for å sikre integriteten.

Informasjon fra overvåkningskameraer kan bli brukt i beslutningstaking som påvirker IT og OT-miljøet. Integriteten til datastrøm fra overvåkningskameraer kan være avgjørende for å sikre rett beslutningsgrunnlag.

Økt sammenkopling mellom IT og OT kan resultere i økt systemkompleksitet. Når kompleksiteten øker vil det være avgjørende å ha en helhetlig oversikt av de ulike avhengighetene, for å sikre redundans og beredskap på nødvendige områder. Dette inkluderer menneskelig redundans som besitter relevant kompetanse og en helhetlig forståelse for hvordan systemene henger sammen. Økt kompleksitet og sammenkopling vil kunne utgjøre en betydelig utfordring når det kommer til å kunne drifte og operere kraftverk manuelt (øy-modus). Det er avgjørende å ha tilstrekkelig personell som besitter helhetsforståelsen av systemene, og evner å drifte disse systemene manuelt ved behov.

En annen sikkerhetsutfordring som blir løftet frem gjennom respondentene er at leverandører ikke forstår kravene i kbf, og har i varierende grad arbeidet mot disse reguleringene. En påstand fra flere respondenter er at endring i lov og forskrift henger ofte langt bak både markedsbehov og samfunnsbehov.

Hva er egentlig styring? er et gjentakende spørsmål som kommer frem. Flere respondenter opplever dette som utydelig. Videre ytrer flere respondenter at kbf kan oppleves som et hinder ift. skytjenester, særlig mot klasse 3 anlegg. Dette peker mot § 7-15 c som ikke tillater styring gjennom eksterne forbindelser.

3.1.3 Hvilke krav stilles i kbf. § 6-9 og kap. 7, og finnes det områder som er for lite regulert?

Respondentene innen regulerbar vannkraft trekker frem at eksisterende kbf fremdeles i stor grad er tolkbar. Det blir dratt frem enkelte fordeler med at denne tolkningen muliggjør å tilpasse seg forskriften uavhengig størrelse og kompleksitet på virksomheten. Tolkingen introduserer en grad av fleksibilitet.

§ 6-9 fungerer relativt bra, men innenfor kapittel 7 er det fremdeles enkelte utfordringer. To av områdene som blir løftet frem som utfordrende i dag er § 7-14 og § 7-15. Disse kan være utfordrende å forstå seg på, og det blir etterspurt mer konkret rettede tiltak mot kapittel 7. Det blir identifisert at det kunne i større grad vært et tydeligere skille mellom § 6-9 og kapittel 7. Refleksjoner blir dratt frem av respondenter at tydeligere og konkrete punkter i kbf kan resultere til enkelte restriksjoner. Veilederen blir brukt som et viktig hjelpemiddel for å forstå dagens forskrift. Det oppleves som at virksomheter i stor grad er selv ansvarlig for å velge en definisjon på hva som er *godt nok* og *sikkert nok* for virksomheten. Dette skaper en frykt for å komme i en situasjon knyttet til at en har tolket forskriften feil. *Standardisering er bra for bransjen* er utsagn som kommer frem intervjuprosessen, samtidig som det reflekteres mye rundt hva det egentlig vil si å ha kontroll.

Kbf oppleves av respondentene som et viktig verktøy og hjelpemiddel de kan anvende som beslutningsgrunnlag for investering tilknyttet sikkerhetsløsninger. Ved å ha tydelige krav vil det være enklere å kunne få gjennomslag for implementasjonen av sikkerhetstiltak.

Respondenter ytrer at bruk av sky og skytjenester har vært tvetydig, og enkelte tolker at det har blitt lagt ned forbud på bruk av sky. Det bør stille krav til at skytjenesteleverandører må dokumentere et visst sikkerhetsnivå basert på internasjonale standarder. Dette kan være ISO 27001, IEC 62443, SOC2 Type 2, resultater fra gjennomførte penetrasjonstester eller tilsvarende.

Flere respondenter har valgt å anvende internasjonale standarder som ISO 27001, NIST CSF, CIS Controls for å supplere kravene i § 6-9 og kapittel 7. Det ytres at dette muligens kan være retningen kraftbransjen vil bevege seg mot på sikt. Dette gjelder hovedsakelig aktører som arbeider internasjonalt, og kan regnes som større aktører innenfor kraftbransjen. Amerikanske rammeverk oppleves som mer direkte og tydeligere knyttet til *å beskrive tiltak man kan iverksette*.

3.1.4 Hvordan kan forskriften bli bedre?

Kbf har enkelte områder som må i varierende grad tolkes. For å kunne gjøre forskriften bedre kan det være hensiktsmessig å arbeide mot å redusere muligheten for tolkning der det lar jeg gjøre. *Tilstrekkelig sikkerhet*, g*odt nok* og *sikkert nok* er eksempler på ordlyd som er utfordrende for brukerne å ta stilling til. Hva betyr det egentlig å ha *kontroll*? Disse spørsmålene kan knyttes til en frykt for å tolke kbf og/eller veilederen feil. Konkrete eksempler tilpasset størrelsesorden på ulike kraftvirksomheter vil kunne være nyttig i forhold til hva som er *godt nok* og *sikkert nok* for liknende virksomheter.

De enkelte virksomhetene må i dag i stor grad ta stilling til disse definisjonen selv. En utfordring som adresseres er at mindre virksomheter ofte har begrenset antall ressurser tilgjengelig med relevant kompetanse. Det vil være fordelaktig å fortsette arbeidet med å forbedre eksisterende veileder til kbf, og etterstrebe konkrete løsningsforslag og metoder.

Skillet mellom kbf. § 6-9 og kapittel 7 blir belyst som et område som kan bli tydeligere. Kapittel 7 burde være mer konkret rettet mot tiltak, gjerne gjennom veilederen. Kbf § 7-14 og § 7-15 kan, slikt den står i dag, være utfordrende å forstå seg på. Samtidig opplever flere respondenter at omfanget av kbf blir stadig mer omfattende, og tar for seg mer enn bare det som er kjernevirksomhet.

Det kommer frem at det fremdeles er utfordringer knyttet til hva som egentlig er kraftsensitiv informasjon, som har vært mye diskutert i de ulike intervjuene. Å samle folk rundt definisjonen av hva som er og ikke er kraftsensitiv informasjon er per dags dato enda en utfordring. Vedlikehold og utvikling av kompetanse, samt å videreutvikle felles situasjonsforståelse blir løftet som utviklingsområder.

3.2 Case 2: Uregulerbar kraftproduksjon fra vind

Kraftproduksjon fra vind er i kontinuerlig utvikling, men i Norge er dette en relativt ny teknologi innenfor energiutvinning. Fra Norges første kjente vindkraftverk med strømproduksjon bygd i 1910 ved Elverum [9] sammenlignet med det første kommunale elektrisitetsverket basert på vannkraft som ble satt i drift på Hammerfest i 1891 [10]. Denne seksjonen ser på de ulike fordelene og problemstillingene som økt sammenkopling introduserer, sett fra respondenter innen uregulerbar kraftproduksjon fra vind.

3.2.1 Hvordan kan den styrkede sammenkoplingen mellom IT og OT støtte: Forretningsprosesser og produksjon?

Uregulerbar kraftproduksjon fra vind og vindturbiner har økende interesse globalt, men også nasjonalt. I dag er ikke uregulerbar kraftproduksjon fra vind underlagt kbf, men det kan på sikt være til vurdering om dette området skal underlegges forskriften. Økt sammenkopling mellom IT- og OT-miljøet innenfor vindkraft gir turbinoperatører enklere fjerntilgang til vindturbinene for feilsøking og løpende vedlikehold. Denne fjerntilgangen og styringen er driftet av de ulike turbinleverandørene. Turbinleverandørene har mulighet til å overstyre turbinene gjennom fjerntilgang ved behov.

Batteriteknologi kan tilrettelegge for mellomlagring av strøm og til dels regulering i perioder med lav kraftproduksjon. En av fordelene ved å ha tilgang til batterier og mellomlagring av kraft er å kunne brukes i støttemarkedet til kraftbransjen. Dette kan utløses ved behov for økt kraftbehov under eksempelvis akutt kraftmangel.

3.2.2 Hvilke sikkerhetsutfordringer er tilknyttet økt sammenkopling innen IT- og OT-integrasjonen?

Som andre aktører innen norsk kraftbransje har også vindkraft vært vant til mer lukkede miljøer mellom IT og OT. En økende etterspørsel på sanntidsdata utfordrer den etablerte tanken om et skille mellom disse miljøene. Utfordringen med denne utviklingen er å gjøre denne dataen tilgjengelig og samtidig sikre at utviklingen gjøres på en sikker måte.

Vindturbiner er utviklet for å ha en lang holdbarhet, med en estimert levetid fra 25-30 år, men det er en rekke variabler som kan påvirke turbinens reelle levetid som blant annet plassering og klima.

Eierstruktur innen kraftproduksjon fra vind er kompleks, noe som utgjør en utfordring tilknyttet å ha en helhetlig forståelse av ansvarsfordeling, eksempelvis dersom en informasjonssikkerhetshendelse skulle inntreffe.

3.2.3 Hvilke krav stilles i kbf. § 6-9 og kap. 7, og finnes det områder som er for lite regulert?

Dersom uregulerbar kraftproduksjon fra vind skulle blitt underlagt kbf bør det vurderes utdyping og regulering knyttet til ansvarsfordeling i eierstrukturen. Dagens eierstruktur er kompleks, og drift av eksisterende turbiner prioriteres utfra oppetid. Vindturbiner kan bli stående for seg selv over lengre perioder uten nødvendigvis å måtte gjennomføre regelmessig tekniske oppdateringer. Serviceintervaller blir gjennomført, men disse er i dag i liten grad *informasjons-teknisk* prioritert.

3.2.4 Hvordan kan forskriften bli bedre?

Ettersom at uregulerbar kraft fra vind i dag ikke er underlagt kbf kan det være aktuelt å vurdere om det er hensiktsmessig å underlegge denne sektoren forskriften. Hensikten vil være å i større grad standardisere med intensjon om å gjøre det enklere og tenke sikkerhet i alle ledd. Utsagnene *standardisering er bra for bransjen* ble nevnt under intervjuprosessen som understøtter argumentet for underleggelse av forskriften.

Det kan være hensiktsmessig å tydeliggjøre hvem som er overordnet ansvarlig for informasjonssikkerhet og beredskap innen uregulerbar kraftproduksjon fra vind. Det bør stilles tydelige krav til leverandører og underleverandører for å få klarhet i leverandørstyring og avhengighet, samt regelmessig sikkerhetsrevisjon. Samtidig er det viktig at det stilles konkrete krav til informasjonssikkerhet i leverandøravtaler og anskaffelsesprosesser.

3.3 Case 3: Distribusjonssystemoperatør (DSO)

DSO`ene drifter strømnettet i de forskjellige regionene i landet. Disse spiller en nøkkelrolle i å sikre at distribusjonsnettet er pålitelig, effektivt og sikkert. I denne seksjonen av rapporten blir DSO`enes perspektiver mot økt sammenkopling presentert.

3.3.1 Hvordan kan den styrkede sammenkoplingen mellom IT og OT støtte: Forretningsprosesser og nettdrift?

Økt sammenkopling kan resultere i moderne IT- og OT-miljøer. Ved å i større grad utvikle IT som skal plasseres og anvendes i miljøer som historisk sett har vært adskilte, utfordres etablerte tankesett på hvordan dette skal sikres. Forretningsprosesser og nettdrift kan bli mer kostnadseffektivt ved hjelp av OT-løsninger som i større grad gir fra seg informasjon som kan bli anvendt i beslutningsprosesser. Økt sammenkopling kan også resultere i høyere effektivitet. Eksempelvis sensorer som måler belastning på strømnettet så det kan reguleres ved behov. Utskiftning av komponenter blir også dratt frem som et område som økt sammenkopling kan bidra med å løse på en bedre måte fremfor mer satte utskiftningsintervaller.

Enkelte respondenter sier at de ikke opplever nye utfordringer som følge av mer sammenkoplede miljøer. Informasjonsutveksling mellom systemer er noe som i stor grad har blitt gjort over lang tid. Det som kan være forskjellen er størrelse og datavolum eller at de har gått fra en manuell til en automatisert prosess. Ved å anvende flere sensorer innenfor nettdrift skapes det også en større mengde data. Dersom sensorer som har et lavere sikkerhetsnivå får tilgang til kritisk infrastruktur kan dette øke angrepsflaten. Enkelte respondenter mener det fremdeles er ønskelig å ha fysisk adskilte miljøer, ikke bare logisk. En av respondentene har policy på å ha et fysisk skille mellom de to miljøene.

3.3.2 Hvilke sikkerhetsutfordringer er tilknyttet økt sammenkopling innen IT- og OT-integrasjonen?

Respondentene ytrer bekymring for at den økende sammenkopling innen IT- og OT-integrasjon kan føre til økt angrepsflate. Klarer en angriper å kompromittere en IT-enhet, kan de bruke det som en vei inn for å angripe OT-systemene. Dette scenarioet kan være spesielt risikabelt hvis OT-systemene mangler tilstrekkelig sikkerhet (insecure-by-design), da de tradisjonelt har vært isolert fra IT-nettverket. Dette forsterker risikoen for sikkerhetsbrudd, og dersom et angrep lykkes, kan konsekvensene bli alvorlige, gitt at OT-systemene ofte styrer kritiske infrastrukturer.

Videre utrykker respondentene bekymring knyttet til at de har flere leverandører å måtte forholde seg til, som kan gjøre det mer utfordrende å ha oversikt over blant annet ansvarsfordeling. Med et økende antall leverandører kan det være vanskelig å fastslå hvem som er ansvarlig for hva. Dette kan skape usikkerhet og konflikter. Angriperne kan utnytte denne usikkerheten for å få tilgang til verdifull informasjon eller forstyrre tjenester.

Sensorer blir løftet som en utfordring tilknyttet økt sammenkopling innen IT og OT. Særlig implementering av sensorer i det fysiske OT-nettverket, spesielt med tanke på sikkerhet. Respondenter ytrer at for å møte dagens krav og drive effektivt har en egentlig ikke noe valg, og en kommer ikke utenom en større sammenkopling mellom IT og OT.

3.3.3 Hvilke krav stilles i kbf. § 6-9 og kap. 7, og finnes det områder som er for lite regulert?

Det kommer også frem fra DSOer at eksisterende kbf er tolkbar. Fordelen med at den er tolkbar er at forskriften i større grad kan tilpasses hver enkelt virksomhet, uavhengig av størrelse og kompleksitet. Denne fleksibiliteten kan være svært fordelaktig, men det introduserer på samme tid enkelte utfordringer. En av utfordringene er knyttet til individers evne til å tolke kbf som kan ha betydning for hva som er *godt nok* og *sikkert nok*. Dette stiller indirekte krav til hver enkelt sin kompetanse innenfor informasjonssikkerhet, samt forståelse av oppbygning og ordlyd i kbf.

Det er flere likhetstrekk med kravene som stilles i kbf. § 6-9 og NSM Grunnprinsipper for IKT-sikkerhet. Enkelte av DSOene har bygd opp styringssystemer som samsvarer med NSMs Grunnprinsipper. Noen av argumentene som blir brukt for å gjøre nettopp dette er at det er tydeligere definerte tiltak, med tilhørende forklaringer og støttedokumenter. Det kommer frem at veilederen til kbf er et nyttig verktøy, som blir brukt blant annet for å finne eksempler på hvordan en skal implementere enkelte sikkerhetsmekanismer.

Enkelte av respondentene ytrer at de gjerne kunne hatt strengere og tydeligere krav til hva virksomheten skal ha på plass. Krav i forskriften er et betydelig verktøy for å få gjennomslag til å implementere sikkerhetstiltak, og blir i enkelte samtaler omtalt som en *brekkstang for å få gjennomslag*. Det kan trekkes paralleller mot om strengere og tydeligere krav vil kunne resultere i høyere sikkerhet. For mindre virksomheter kan det være utfordrende å ha tilstrekkelig ressurser i menneskelig og økonomisk forstand, til å etterleve for omfattende krav. Videre er det flere respondenter som setter søkelys på begrensninger på tilgang til ressurser som kan brukes på sikkerhet og IT-løsninger generelt.

Det oppleves uklart hvor grensen går for hva driftskontrollsystemer omfatter. Nyere teknologi blir gjerne stående på utsiden av byggene. Dette utfordrer grensene for hva som regnes som driftskontrollsystemer. I følge kbf blir det regnet som driftskontrollsystem og må derved følge gjeldene krav til EMI/EMP sikring ref. § 7-13. Når utstyr blir plassert utenfor kontrollrom, *hvordan skal alt dette flyttes ut? Når kabler flyttes fra datarommet med effektbrytere og utstyr ute på lokasjon, hvilke krav gjelder da og hvordan skal dette EMP sikres?* Disse spørsmålene blir løftet som utfordrende å ta stilling til iht. § 7-13.

3.3.4 Hvordan kan forskriften bli bedre?

Det kommer frem fra respondentene at det i varierende grad er en felles forståelse for hva som ansees å være kraftsensitiv informasjon. Det kan være hensiktsmessig å videreutvikle kbf eller inkludere flere konkrete eksempler på kraftsensitiv informasjon. Gjennom intervjuprosessen blir det løftet forslag om å ha en form for gradering av den kraftsensitive informasjonen.

«Hvorfor ikke vise til mer anerkjente standarder fremfor å finne opp kruttet på nytt?».

3.4 Utfordringer

Gjennom respondentene innenfor de respektive casene har det blitt identifisert en rekke utfordringer. Tabellen nedenfor gir en oversikt over utfordringene sammen med en beskrivelse.

#	Utfordring	Beskrivelse
1	Oversikt over systemavhengigheter.	Det økte behovet for sammenkobling av IT og OT systemer, fører til blant annet større grad av automasjon og utveksling av sanntidsdata. Det er krevende å holde oversikt og kontroll over hvor data kommer fra og hvor data flyter. I tillegg blir det mer utfordrende å ha oversikt over kritikaliteten til hver enkelt avhengighet.
2	Varierende og ulik forståelse for risiko.	Historisk sett har IT- og OT-miljøene operert separat. Som følge av økt sammenkopling mellom disse to miljøene vil det stilles andre krav til fremtidige samarbeid, blant annet med risikovurderinger.
3	Kompetanse- og ressursmangel.	Økt kompleksitet skaper behov for å ha interne ressurser som har en helhetlig forståelse for hvordan systemer (IT og OT) henger sammen. Dersom en eller flere av koplingene faller ut vil det være avgjørende å ha personell tilgjengelig med rett kompetanse for å kunne sikre drift i situasjoner som krever manuell drift.
4	Ekstern kommunikasjon/styring av produksjon.	Ekstern styring av anlegg i klasse 3 sentraler er ikke tillatt av kbf. Dette oppleves som en utfordring med økt og automatisert justering av produksjon. Økt sammenkobling av IT/OT med behov for kommunikasjon/styring inn og ut av driftskontrollsystem fører til flere angrepsflater mot virksomheter.
5	Kbf er tolkbar.	Respondenter ytrer at dagenes kbf i stor grad er tolkbar. Dette inkluderer områder som: - Hva er *godt nok*? - Hva er *sikkert nok*? - Hva er *styring*? - Hvor går grensen for hva et driftskontrollsystem er? - Hva er kraftsensitiv informasjon? Enkelte respondenter syntes det er positivt at kbf har en viss grad av tolkbarhet, da det gir mulighet for fleksibilitet. Det er høyt fokus på lønnsomhet i virksomhetene. Utydelige krav i kbf kan derfor bli nedprioritert i en vurdering av kost/nytte, til tross for at disse er viktige.
6	Kravstilling og oppfølging av leverandører.	Leverandører har i varierende grad kjennskap og erfaring med kbf, og flere forstår ikke kravene som stilles i forskriften. I en verden som er i stadig endring oppleves det utfordrende å stille både fleksible nok, men samtidig gode krav i avtaler med leverandører, og underleverandører

		For få virksomheter har en systematisk tilnærming og regelmessig oppfølging av leverandører. Komplekse eierstrukturer og leverandørkjeder skaper utfordringer knyttet til ansvarsfordeling. I tillegg øktes mulighetene for å bli rammet av leverandørkjedeangrep.
7	Kbf oppleves som utdatert.	Flere respondenter opplever kbf som utdatert, og forskriften henger ikke med i utviklingen. I dag dekkes skytjenester eller sensorbruk i liten grad i kbf.
8	Grensen for hva som er driftskontrollsystem utvides, som kan resultere i en mer omfattende kbf.	Avgrensningen av hva et driftskontrollsystem er ikke tilstrekkelig. Det oppleves at grensen stadig utvides med nye teknologier og ønsker om å flytte komponenter som tradisjonelt har vært i driftskontrollsentralen ut fra EMP/EMI-sikker sone.

4. Anbefalinger

Dette kapittelet sammenstiller de ulike anbefalingene og endringsforslagene som har blitt kartlagt og utarbeidet gjennom prosjektet. Å etterstrebe en forskrift som omfatter alle unike behov vil være umulig. Hver virksomhet har et ulikt forhold til risikoakseptanse, og det vil være forskjellige behov basert på virksomheters størrelse og kompleksitet. Anbefalingene blir knyttet til de forskjellige utfordringene som har blitt identifisert, og prioritert i tabellen nedenfor.

Utfordring	Anbefaling/endringsforslag
Oversikt over systemavhengigheter.	Virksomheter må ha en oppdatert oversikt over de mest kritiske driftssystemene. Oversikten må inneholde eksisterende avhengigheter og type informasjon som utveksles mellom systemer. I tillegg må det identifiseres om informasjonen er kraftsensitiv.
Varierende og ulik forståelse for risiko.	Det anbefales at det arbeides systematisk med å få en felles situasjons-forståelse mellom IT og OT miljøet, slik at det kan gjennomføres risikovurderinger som tar opp aspekter fra begge miljøer. Det anbefales at det utarbeides tiltakskort for å håndtere hendelser i grensesnittet mellom IT og OT, som må øves regelmessig.
Kompetanse- og ressursmangel.	Det anbefales å kartlegge, vurdere og dokumentere kritikalitet til eksisterende avhengigheter mellom IT- og OT- miljøene for å sikre drift og redundans på kritiske systemavhengigheter. Det er avgjørende å ha tilstrekkelig intern kompetanse som har en helhetlig forståelse for de sammenkoplede miljøene. I tillegg er det viktig at personellet evner å drifte disse systemene manuelt dersom en eller flere kritiske koplinger blir utilgjengelig. Det anbefales at det stilles krav til å ha menneskelig redundans for å sikre kontinuitet og redusere avhengighet til enkeltpersoner. Det er også viktig å ha på plass sentrale styringsdokumenter som både kan sikre sporbarhet og i tillegg enhetlige- og helhetlige prosesser. IKT-sikkerhetskoordinator er i flere tilfeller plassert langt nede i organisasjonen hos ulike virksomheter. Dette kan skape begrensninger da de har liten innvirkning mot resten av organisasjonen. Det er viktig at myndighet til vedkommende blir spesifisert i større grad enn i dag.

Ekstern kommunikasjon/styring av produksjon.	Kbf må endres dersom ekstern sentral styring av produksjon skal kunne tillates. Det anbefales at det gjøres en utredning av ekstern kommunikasjon/styring av produksjon. Resultatet fra utredningen kan benyttes i fremtidige revisjoner av kbf. Verifisering og validering av sikkerhetsmekanismer/-systemer er essensielt for å evaluere om disse har blitt implementert riktig og oppnår ønsket effekt. Et verktøy for å evaluere slike mekanismer er penetrasjonstesting. Det kan være ifm. commissioning av anlegg (rett før idriftsettelse), f.eks. Site Acceptance Test (SAT). Gjennomfør regelmessig penetrasjonstester/inntrengningstester for å sikre effektive sikkerhetstiltak, og identifisere områder som krever lukking av kartlagte sårbarheter. Dette kan kobles mot kbf revisjon av § 6-9 f. Penetrasjonstesting bør minimum gjennomføres årlig og ved større endringer. Nye løsninger bør bli utsatt for penetrasjonstest innenfor et testmiljø før implementasjon.
Kbf er tolkbar.	Det anbefales å beholde noe tolkbarhet i kbf, da dette gir virksomheter fleksibilitet og mulighetsrom for å tilpasse informasjonssikkerhets-arbeidet mot virksomhetens risikoakseptanse. Samtidig er det avgjørende for små- og mellomstore virksomheter å ha tydelige krav i kbf for å få gjennomslag for sikringstiltak. Fokus på lønnsomhet i virksomhetene gjør at viktige krav kan bli nedprioritert i en kost/nytte vurdering dersom kravene ikke er tydelige nok. Lag en veileder med flere konkrete eksempler, spesielt tilpasset små og mellomstore virksomheter. Veilederen bør inneholde figurer for visualisering, i tillegg til tekst. Still tydeligere krav i kbf om overvåkning av systemer gjennom et Security Operations Center (SOC). Dette er et uttalt ønske etterspurt fra respondenter.
Kravstilling og oppfølging av leverandører.	Det anbefales å stille tydeligere krav tilknyttet informasjonssikkerhet til leverandører i anskaffelse, leveranse og oppfølgingsprosesser. I forbindelse med anskaffelsesprosessen er det viktig at ansvarfordeling blir tydeliggjort med leverandører i avtaler. Dette bør vurderes mot kritikaliteten anskaffede leverandører utgjør for virksomheten. Det bør være mulig å endre leverandøravtaler ved behov, som eksempelvis ved lovendringer, endringer hos leverandør, trusselbildet eller liknende. Det anbefales å ha en regelmessig og systematisk tilnærming til oppfølging av leverandører og leverandørkjeder.
Kbf oppleves som utdatert.	Det bør vurderes om det i større grad kan henvises direkte mot internasjonalt anerkjente standarder som: ISO 27001, ICA 62443, NIST CSF, CIS Controls, Network Codes eller liknende, i fremtidige revisjoner av kbf. Respondentene ønsker at Kapittel 7 blir prioritert først. Ved en revisjon bør kbf harmoniseres med andre norske lover som Lov om digital sikkerhet.

Grensen for hva som er driftskontrollsystem utvides, som kan resultere i en mer omfattende kbf.	Det anbefales at det gjøres en justering av hva som er avgrensningen av et driftskontrollsystem. Grensen utvides stadig med nye teknologier og ønsker om å flytte komponenter ut fra sikker og EMP-sikret sone, nærmere eller på stasjonene. Det bør vurderes om omfanget av kbf kan fokusere på kjerne-virksomhet. En definisjon på hva som ansees å være kjernevirksomhet bør i tilfelle utarbeides.

5. Bibliografi

[1] Dragos, «2023 ICS/OT Cybersecurity Year in Review,» 2024.

[2] Telenor, «Digital Sikkerhet 2023 - Det blir alvor,» 2023.

[3] Nasjonal sikkerhetsmyndighet, «Risiko,» 2024.

[4] Etterretningstjenesten, «Fokus,» 2024.

[5] K. Haver, A.-K. Valdal, T. Vernholt og H. S. Wiencke, «Veikart for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden,» Norges vassdrags- og energidirektorat (NVE), 2021.

[6] Petroleumstilsynet, «Beskyttelse av data i ro og transit,» 2021.

[7] Politiets sikkerhetstjeneste, «Nasjonal trusselvurdering,» 2024.

[8] Statkraft, «Vannkraft,» [Internett]. Available: https://www.statkraft.no/var-virksomhet/vannkraft/. [Funnet 23 02 2024].

[9] S. B. Dybesland, «Vindkraft i Norge,» NVE, 2008.

[10] Regjeringen, «Norsk vannkrafthistorie på 5 minutter,» 20 Mars 2019. [Internett]. Available: https://www.regjeringen.no/no/tema/energi/fornybar-energi/norsk-vannkrafthistorie-pa-fem-minutter/id2346106/. [Funnet 21 Februar 2024].

[11] K. Hofstad, «Regulerbarhet (energiproduksjon),» 2021.

NVE

Norges vassdrags- og energidirektorat

Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo
Telefon: (+47) 22 95 95 95