



## Kartlegging av bruk av tingenes internett (IoT/ IIoT) i norsk kraftforsyning

---

*Marie Røyksund, Anne-Kari Valdal*

## Ekstern rapport nr. 2/2020

# Kartlegging av bruk av tingenes internett (IoT/IloT) i norsk kraftforsyning

**Utgitt av:** Norges vassdrags- og energidirektorat

**Forfatter:** Marie Røyksund, Anne-Kari Valdal

**Forsidefoto:** Foto av Louis Reed på Unsplash

**ISBN:** 978-82-410-2003-2

**ISSN:** 2535-8235

**Sammendrag:** Rapporten gir en overordnet introduksjon til bruken (og nær fremtids bruk) av tingenes internett (IoT) og industriens tingenes internett (IloT) i energiforsyningen. Dette inkluderer eksempler på løsninger som benyttes i industrien, hvilke leverandører som tilbyr slike produkter og tjenester, samt hvilke standarder og regelverk det eventuelt refereres til for produkter og tjenester.

**Emneord:** IoT, tingenes internett, energiforsyning, kraftforsyning, innovasjon

Norges vassdrags- og energidirektorat

Middelthunsgate 29

Postboks 5091 Majorstuen

0301 Oslo

Telefon: 22 95 95 95

E-post: [nve@nve.no](mailto:nve@nve.no)

Internett: [www.nve.no](http://www.nve.no)

februar, 2020

# Forord fra NVE

Digitalisering treffer energiforsyningen gjennom digitale sensorer i infrastrukturen, skytjenester og utsetting av IT-drift og gjennom avanserte måle- og styringssystemer (AMS) mv. Digitaliseringen gir mulighet for å utvikle løsninger for smarte energiøkonomiske hus og for mer effektiv drift hos selskapene. Bransjen gjennomgår en endring der en i økende grad benytter data fra sensorer til å lage sanntidsinformasjonsbilde på status i nettet. Data fra ulike kilder kan sammenstilles, korreleres eller kjøres gjennom algoritmer for å gi gode svar på konkrete spørsmål eller vise et sanntidsbilde. Men, digitalisering og tilknytning av stadig flere komponenter til internett eksponerer også de samme komponentene for en rekke cybertrusler og uønskede hendelser. Mye av dette har vi liten eller ingen erfaring med. Det er viktig for NVE å følge med på og også forstå denne utviklingen.

Forsyningssikkerhetsmessig er NVE i hovedsak opptatt av energisystemet frem til og med smartmåleren. Selve smartmåleren og det tilhørende AMS har NVE god oversikt over, men det tilbys i stadig større grad utstyr til industrielle kontrollsystemer og støttesystemer som kommuniserer med internett og faller inn under betegnelsen tingenes internett. Introduksjonene av denne type løsninger vil kunne påvirke energiforsyningen og NVE må ha en god oversikt for å kunne møte endringene disse kan ta med seg.

NVE trenger derfor en oversikt over bruk av internett av ting (IoT) og industrielle internett av ting (IIoT) i dagens energiforsyning. NVE trenger å vite hva som allerede brukes eller kan brukes i energiforsyningen i dag, og det som er forventet å bli tatt i bruk i de nærmeste årene (1-5) år. Det er også viktig å få innsikt i om det i hovedsak er hyllevare som tilbys og brukes, eller om det stort sett er skreddersydde løsninger. I tillegg er det viktige forskjeller mellom enkeltkomponenter og komplette løsninger som fulle skyplattformer og lignende.

Det er IoT og IIoT i kontrollsystemene og i støttesystemene kunnskapsbehovet til NVE er størst. Med kontrollsystemene mener vi systemene som brukes direkte til å styre og kontrollere produksjon og overføring av elektrisk energi. Med støttesystemer mener vi systemer som vedlikeholdssystemer og bygningstekniske systemer som ventilasjon, brann og adgangskontroll.

NVE bestilte derfor denne rapporten slik at vi kan få en oversikt over hva dagens status er for bruk av IoT og IIoT i energiforsyningen, og for å gi oss ett utgangspunkt for videre arbeid. Vi er godt fornøyd med rapporten og den gir oss nettopp utgangspunktet for å se på de faktiske løsningene som tilbys. Vurderingene fra rapporten er nyttige og noe vi vil ta med oss i vårt videre arbeid.



Ingunn Åsgård Bendiksen  
Avdelingsdirektør



Eldri Naadland Holo  
Seksjonssjef

## **RAPPORT**      **Norges vassdrags - og energidirektorat (NVE)**

### **Kartlegging av bruk av tingenes internett (IoT/IloT) i norsk kraftforsyning**



**Kunde:**

Norges vassdrags- og energidirektorat (NVE)

**Kontaktperson:**

Jon-Martin Pettersen Storm

**Oppsummering:**

Proactima har på oppdrag fra Norges vassdrags – og energidirektorat (NVE) gjennomført en innledende og overordnet kartlegging av bruken av tingenes internett (IoT) og det industrielle tingenes internett (IIoT) i energiforsyningen i dag og i nær fremtid (1-5 år).

Hovedformålet med prosjektet har vært å identifisere forhold av interesse for nærmere studier i fremtiden. Det skal også bidra til å heve kompetansen i NVE om forhold knyttet til digitalisering, til å gi grunnlag for fokus og løpende regelverksutvikling i NVE.

Følgende problemstillinger har lagt grunnlaget for undersøkelsen:

- Hva brukes av IoT/ IIoT -løsninger i industrielle kontrollsystemer (dvs. SCADA/DMS/ICS/PCS osv) og støttesystemer (dvs. vedlikeholdssystemer og byggetekniske systemer) i energiforsyningen?
- Hvilke tradisjonelle og nyetablerte leverandører tilbyr IoT / IIoT – produkter og løsninger, og hva tilbyr (herunder «hyllevarer vs. skreddersydde» tjenester) de?
- Hvilke standarder og regelverk benyttes eventuelt av leverandørene som tilbyr IoT / IIoT – løsninger til energiforsyningen?

Basert på kartleggingen gis det noen anbefalinger til videre oppfølging.

Nøkkelord	Kraftforsyning, IoT / IIoT, Standarder
Rapportnr.	1073611-RE-01
Forfatter(e)	Marie Røyksund / Anne-Kari Valdal
Konfidensialitet	Åpen
Revisjonsnr.	01
Revidert dato	29.01.2020
Antall sider	35

Rev.nr.	Dato	Årsak til revisjon
01	29.01.2020	Endelig rapport etter høring hos oppdragsgiver



**Utarbeidet av**  
Marie Røyksund



**Verifisert av**  
for Hermann Steen Wiencke



**For Proactima AS**  
Vibeke Langeland Pedersen

## Innholdsfortegnelse

<b>1</b>	<b>Sammendrag .....</b>	<b>4</b>
<b>2</b>	<b>Bakgrunn.....</b>	<b>5</b>
2.1	IoT og IIoT i energiforsyningen som del av smartgridutviklingen .....	5
2.2	Formål med kartleggingen .....	6
2.3	Arbeidsomfang og avgrensinger.....	7
2.4	Datagrunnlag.....	7
<b>3</b>	<b>Kartlegging og funn.....</b>	<b>8</b>
3.1	Dagens bruk av IoT / IIoT- løsninger i energiforsyningen.....	8
3.1.1	Eksempler på IoT-produkter som brukes i kontrollsystemer .....	8
3.1.2	IoT- produkter som brukes i støttesystemer.....	9
3.2	Utviklingen de neste årene.....	10
3.2.1	Trender og kommersialisering.....	10
3.2.2	Oversikt over relevante SmartGrid demoaktiviteter og piloter .....	12
3.3	Leverandører og løsninger som tilbys .....	15
3.3.1	Hyllevarer vs skreddersydde løsninger .....	15
3.3.2	Kjennskap til og bruk av standarder .....	16
<b>4</b>	<b>Vurdering og anbefalinger.....</b>	<b>18</b>
4.1	Forstå implikasjoner for forsynings sikkerheten ved innføring av IoT/IIoT- løsninger .....	18
4.2	Kartlegge kompetanse og holdninger, og behov for kunnskapsløft .....	19
4.3	Videreutvikle og forbedre veiledning og verktøy for risikostyring.....	20
4.4	Tilpasning av regelverk, tilsyn og kontroll.....	21
	<b>Referanser .....</b>	<b>23</b>
	<b>Vedlegg I Intervjuguide.....</b>	<b>24</b>
	<b>Vedlegg II Oversikt over Smartgrid-prosjekter .....</b>	<b>26</b>
	<b>Vedlegg III Eksempler på leverandører av IoT/IIoT-løsninger.....</b>	<b>32</b>

## 1 Sammendrag

Målet for denne kartleggingen har vært å gi en overordnet introduksjon til bruken (og nær fremtids bruk) av tingenes internett (IoT) og industriens tingenes internett (IIoT) i energiforsyningen. Dette inkluderer eksempler på løsninger som benyttes i industrien, hvilke leverandører som tilbyr slike produkter og tjenester, samt hvilke standarder og regelverk det eventuelt refereres til for produkter og tjenester.

Det er gjennomført totalt 8 intervjuer av nettselskaper, leverandører og bransjeorganisasjon, i tillegg til innledende litteratursøk og identifisering av relevante FoU-prosjekter og demoaktiviteter. Undersøkelsen viser at nettselskapene kun i begrenset grad benytter seg av IoT/IIoT i dag, og da hovedsakelig til innhenting av informasjon og til overvåking av nettet/anleggene. Dette bildet forventes imidlertid å endre seg drastisk innen bare få år. Det er flere produkter og løsninger som nå testes ut gjennom demoaktiviteter og/eller er i tidlig fase for kommersialisering. Videre ser man at leverandørene utvider tjenestene sine ved å tilby totalleveranser som inkluderer software, overføring, lagring i skyen og analyser, i tillegg til hardware. Implementeringen av IoT-teknologi, og endringer i tjeneste- og leverandørbildet, reiser flere aktuelle problemstillinger, som eksempelvis nye trusler og sårbarheter som oppstår ved økt systemkompleksitet, tette koplinger og nye grense -/ brukersnitt.

Inntrykket er at både selskapene og leverandørene generelt har et høyt fokus på IKT-sikkerhet. Samtidig har det kommet frem usikkerhet knyttet til både bruken av og implikasjonene for forsyningssikkerheten ved innføringen av IoT / IIoT løsninger. Gjennom denne kartleggingen er det enkelte temaer som har utpekt seg som særlig relevante for videre studier. Disse er å:

- Forstå implikasjoner for forsyningssikkerheten ved innføring av IoT/IIoT
- Kartlegge kompetanse, holdninger og behovet for et felles kunnskapsløft
- Videreutvikle og forbedre veiledning og verktøy for risikostyring
- Videreutvikle og tilpasse regelverk, tilsyn og kontroll

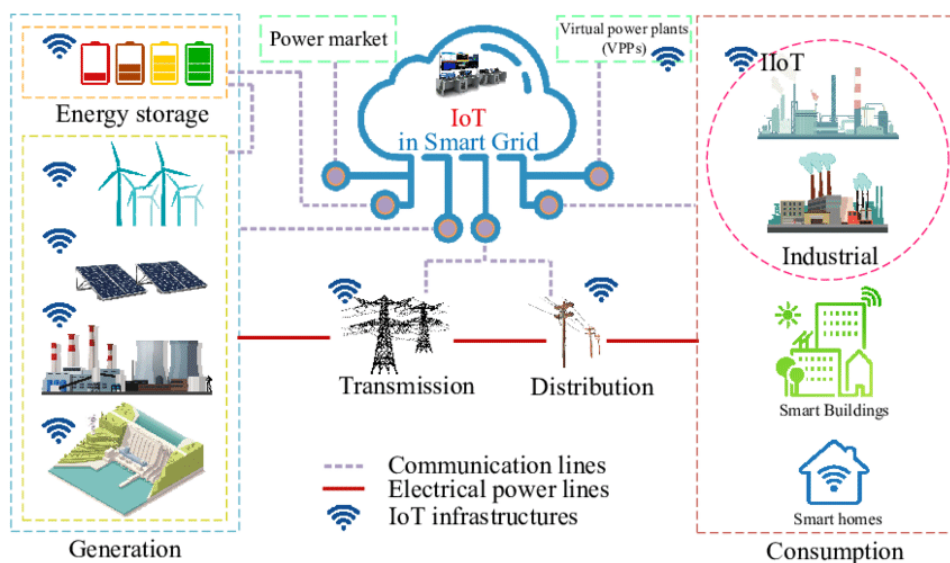
## 2 Bakgrunn

### 2.1 IoT og IIoT i energiforsyningen som del av smartgridutviklingen

NVE beskriver i sitt oppdragsnotat at «Digitalisering treffer energiforsyningen gjennom digitale sensorer i infrastrukturen, skytjenester og utsetting av IT-drift og gjennom avanserte måle- og styringssystemer (AMS) mv. Digitaliseringen gir mulighet for å utvikle løsninger for smarte energiokonomiske hus og for mer effektiv drift hos selskapene. Bransjen gjennomgår en digitalisering der en i økende grad benytter data fra sensorer til å lage sanntidsinformasjonsbilde på status i nettet. Data fra ulike kilder kan sammenstilles, korreleres eller kjøres gjennom algoritmer for å gi gode svar på konkrete spørsmål eller vise et sanntidsbilde. Men, digitalisering og tilknytning av stadig flere komponenter til internett eksponerer også de samme komponentene for en rekke cybertrusler og uønskede hendelser.»

Denne utviklingen er ikke unik for kraftbransjen, men preger samfunnsutviklingen generelt. Virksomheter og samfunn ser et betydelig potensial i å samle, analysere og trekke beslutningsstøtte ut av store informasjonsmengder – som tidligere ikke var håndterbare. Trenden fremmes ved at bedre og billigere løsninger for å samle, kommunisere og analysere data utvikles. Digitaliseringen gjør at ulike funksjoner, og ikke minst kritiske samfunnsfunksjoner, i stadig større grad henger sammen i komplekse systemer med store avhengigheter av hverandre. Kraftbransjen er en av de sentrale bransjene i en slik utvikling. Stadig flere interessenter og funksjoner er avhengige av stabile, trygge og fleksible kraftleveranser. Utvikling knyttet til bærekraft og det grønne skiftet, herunder elektrifisering av stadig større del av eksempelvis transport og logistikkjeder, understreker behovet for å tilrettelegge for en effektiv, fleksibel og sikker strømforsyning.

Fremtidens «smarte» kraftsystem kjennetegnes av at det blir mer produksjon fra fornybare energikilder og forbrukerfleksibiliteten øker<sup>1</sup>. Overvåking og drifting av nettet vil i økende grad skje gjennom digitalisering og automatiserte prosesser. For kraftbransjen er mye av teknologiutviklingen knyttet til ny og endret bruk av sensorer og informasjon fra disse. Dette omtales gjerne som tingenes internett (Internet of things – IoT) og industriens tingenes internett (Industrial internet of things - IIoT). Som vist i figuren under, er bruken av IoT en uunnværlig del av implementeringen av fremtidens smarte nett (smartgrid) og smarte byer / smarte bygg.



Figur 1 Prinsippkisse for IoT i smartgrid (hentet fra Shahinzadeh et al., 2019)

<sup>1</sup> Smartgrids <https://www.sintef.no/smartgrids1/>

Tingenes internett (IoT) er en samlebetegnelse for et nettverk av fysiske enheter som kobles sammen, og samler informasjon som deles med hverandre via internett. Med andre ord inkluderer det hardware (sensorene), overførings- og kommunikasjonsløsning (EDGE, 4G o.l.), og lagring av informasjonen (skyløsning). I tillegg inkluderes ofte også analysene og tolkningen av informasjonen (Big data) i begrepet. Her benyttes algoritmer og maskinlæring som igjen kan mates inn i drift og optimalisering, og kommuniseres til virksomheten. Enhetene er typisk batteridrevet og utstyrt med ulike sensorer for å måle eksempelvis temperatur og trykk i systemer, i tillegg til å inneholde komponenter for trådløs kommunikasjon. Når det snakkes om industriens tingenes internett (IIoT) knyttes denne typen teknologiske løsning til bruk i industrisammenheng og i applikasjoner.

Noe av motivasjonen som fremmer bruken og utviklingen av IoT i kraftbransjen knyttes til:

- Behovet for bedre utnyttelse og mer fleksibel bruk av kapasiteten i nettet (knyttet til elektrifisering, døgn- og sesongvariasjoner i kraftbehov mm.)
- Behovet for å håndtere en mer fleksibel produksjon av kraft i nettet; eksempelvis til et endret produksjonsmønster med mikronett og elementer i nettet som varierer mellom å forbruke og produsere strøm (som vindmøller)
- Krav og forventning om en mer miljøvennlig produksjon og distribusjon av kraft, og til å bidra i en mer bærekraftig utvikling av samfunnet
- Ønske om optimalisering og effektivisering av drift
- Forventning om mer sømløs interaksjon og kommunikasjon med kunder
- Ønske om innhenting av mer informasjon
- Krav og forventning til en stabil leveringspålitelighet og fokus på forsyningssikkerhet
- Klimaendringer og økt forekomst av ekstremvær
- Økonomiske hensyn (investering / utbygging) og bedre utnyttelse av det eksisterende nettet
- Reduksjon av risiko knyttet til sikkerheten for ansatte og andre (bruk av teknologi til å utføre risikofylte operasjoner uten menneskelig tilstedeværelse)

Samtidig vil utviklingen, kompleksiteten og ikke minst avhengighetene kunne åpne for nye trusler, sårbarheter og risiko som bransjen må forholde seg til, og håndtere.

## 2.2 Formål med kartleggingen

Proactima har på oppdrag fra Norges vassdrags – og energidirektorat (NVE) gjennomført en innledende og overordnet kartlegging av bruken av tingenes internett (IoT) og det industrielle tingenes internett (IIoT) i energiforsyningen i dag og i nær fremtid (1-5 år).

Hovedformålet med kartleggingen er å identifisere forhold av interesse for nærmere studier i fremtiden. Det skal også bidra til å heve kompetansen i NVE om forhold knyttet til digitalisering, til å gi grunnlag for fokus og løpende regelverksutvikling i NVE.

Følgende problemstillinger har lagt grunnlaget for undersøkelsen:

- Hva brukes av IoT/ IIoT -løsninger i industrielle kontrollsystemer (dvs. SCADA/DMS/ICS/PCS osv) og støttesystemer (dvs. vedlikeholdssystemer og byggetekniske systemer) i energiforsyningen?
- Hvilke tradisjonelle og nyetablerte leverandører tilbyr IoT / IIoT – produkter og løsninger, og hva tilbyr (herunder «hyllevarer vs. skreddersydde» tjenester) de?
- Hvilke standarder og regelverk benyttes eventuelt av leverandørene som tilbyr IoT / IIoT – løsninger til energiforsyningen?

I tillegg gir rapporten en kortfattet beskrivelse av enkelte løsninger som er brukt i de første smartgrid-pilotene.

## 2.3 Arbeidsomfang og avgrensinger

Problemstillingen som belyses i denne kartleggingen er i utgangspunktet omfattende og bred. Studien er imidlertid begrenset i tid og omfang. Det er derfor gjort følgende avgrensinger i samråd med NVE:

- Kartleggingen er innledende og overordnet, og skal først og fremst være en basis for valg av grundigere utredninger på senere tidspunkter
- Kartleggingen fokuserer kun på bruken av IoT / IloT løsninger i energioverføringen. Det innebærer at informasjon som gjelder kraftproduksjon og fjernvarme ikke er innhentet eller adressert i rapporten
- NVE har god oversikt og kunnskap om bruken av avanserte målersystemer (AMS). Denne teknologien har derfor ikke vært fokus i kartleggingen såfremt det ikke fremkommer ny informasjon som vil være av særlig interesse for noen av problemstillingene nevnt i kap 2.2.
- Oppdraget har ikke vært rettet mot vurderinger av risiko
- Informasjon og betraktninger rundt etableringen av mikronett / øysamfunn er ikke særlig omtalt i rapporten, med unntak av det som presenteres i SmartGrid Demoaktiviteter i kap 3.2.2.

## 2.4 Datagrunnlag

Per i dag er det flere enn 120 selskaper som driver med nettvirksomhet (helt eller delvis eiet av en eller flere kommuner), i tillegg til de mange aktørene som leverer tjenester til kraftbransjen. Med den raske utviklingen av nye og digitale teknologiske løsninger, ser man også en økning i antall nye leverandører som tilbyr tjenester eller produkter til denne sektoren. I en innledende kartlegging som dette er det ikke mulig å innhente informasjon som er dekkende for hele nedslagsfeltet. Det er derimot valgt å gjøre et utvalg av enkelte informanter som antas vil kunne belyse flest mulig av elementene som undersøkes – på et overordnet nivå.

I et oppstartsmøte med NVE ble det bestemt å gjennomføre intervjuer av et lite utvalg av nettselskaper, leverandører og bransjeorganisasjoner. Fem nettselskaper ble valgt ut og kontaktet, hvorav fire gav tilbakemelding på at de hadde mulighet til å bidra. Samtlige har deltatt i pilotprosjekter relatert til Smartgrid eller IoT/IloT og har dermed høstet erfaringer om denne tematikken. Utvalget forventes ikke å være representativt for hele bransjen. De mindre nettselskapene har trolig ikke kommet like langt i innføringen av denne typen teknologi. Kompetansebakgrunnen og rollene informantene innehar i sine respektive selskapene inkluderer både IKT sikkerhetskoordinator, prosjektleder for FoU prosjekter og driftspersonell.

På leverandørsiden bidro en tradisjonell leverandør av kontrollsystemer, og tre mer nyetablerte leverandører av IoT / IloT-løsninger med informasjon. En bransjeorganisasjon (Forum for informasjonssikkerhet i kraftforsyningen) deltok i undersøkelsen for å ivareta spørsmål knyttet til mulige trender på et mer overordnet nivå. Ulike intervjuguider ble utarbeidet for henholdsvis nettselskap, leverandør og bransjeorganisasjon (se Vedlegg I). Disse ble hovedsakelig benyttet som sjekklister under intervjuene for å sikre at alle problemstillingene ble ivaretatt.

For å få en forståelse av og økt kunnskap om dagens bruk og nær fremtidsbruk av IoT / IloT -løsninger i energiforsyningen, har det også vært nyttig å kartlegge gjennomførte og pågående pilotprosjekter og FoU prosjekter. Det forteller mye om hvilke utfordringer bransjen forventer må ivaretas i fremtidens nett. Oversikten over pågående demoaktiviteter og prosjekter som er utarbeidet av Smartgridsenteret<sup>2</sup> gav et godt utgangspunkt, i tillegg til øvrig internetsøk på aktuelle tidsskrifter (f.eks. Teknisk ukeblad og EnerWe). Videre har relevante offentlige utredninger inngått i datagrunnlaget (se referanseliste).

---

<sup>2</sup> <https://smartgrids.no/>

### 3 Kartlegging og funn

I de følgende delkapitlene gis korte beskrivelser av resultatet fra den innledende kartleggingen av IoT / IloT løsninger i energiforsyningen. Hensikten har vært å gi noen innledende betraktninger over hvilke IoT-løsninger og produkter som benyttes og tilbys i dag, og som er aktuelle de neste årene.

#### 3.1 Dagens bruk av IoT / IloT- løsninger i energiforsyningen

##### 3.1.1 Eksempler på IoT-produkter som brukes i kontrollsystemer

Historisk sett har kraftforsyningen lenge benyttet sensorteknologi kun til drift, vedlikehold og overvåking av nettet. Et eksempel er fjernstyring av kraftverk, hvor sensorteknologi ble benyttet til å starte og stoppe anlegget. Et annet eksempel er overvåking av oljenivå og temperatur på transformatorene som den gang gav nyttig, men begrenset, informasjon om tilstanden på komponentene. Dagens internettbasert sensorteknologi ivaretar mange av de samme funksjonene, men gir mer nøyaktig informasjon og på flere områder, i tillegg til at dataene innhentes og kommuniseres via internett. Ved å bruke IoT-teknologi kan mengde informasjon bidra til å bedre prosessene gjennom f.eks. automatisering. Eksempler på IoT-produkter og typiske løsninger som er implementert i energiforsyningen i dag er:

- Jordfeilovervåking
- Overvåking av temperatur / oljenivå / gassnivå
- Tilstandsmåling (f.eks. viklingstemperatur)
- Data fra vernsystemet

Sensordataene har frem til nå ikke blitt overført direkte til SCADA-systemet, men blitt lagret og prosessert i stasjonsdatamaskiner / sidesystem, og derfra overført via krypterte kanaler til driftskontrollsystemet.

Internettbasert sensorteknologi som skal bidra til å utnytte linjenettet bedre og / eller øke ytelsen på kabelsettene er også tatt i bruk i energiforsyningen, men da gjerne kun på deler av nettet (linjene / kablene / stasjonene). Et eksempel er sensorkuler som måler tilstanden på høyspentledningen gjennom sanntidsmålinger av f.eks. temperatur, vibrasjon og linjesig. Innspill fra bransjen er at det vil være for kostbart å implementere IoT teknologi på alle anlegg og linjer. Informasjonen fra «testområdene» kan imidlertid brukes til å kalibrere beregningene og til dimensjonering, drifting og til vedlikehold av nettet for øvrig.

#### **Datainnsamling i målere som del av beslutningsgrunnlaget.**

Nettselskapene er pålagt å måle og overvåke jordfeil i distribusjonsnettet. De ordinære målerne («indirekte målere») plassert i nettstasjonene har ivaretatt dette kravet, i tillegg til å måle strøm og spenning ut til kundene. De senere årene har det imidlertid skjedd en utvikling i type målere som tilbys i markedet, hvor måleinstrumenter (f.eks. av typen Nemo D4-Le) gir mer detaljert og presis informasjon, bl.a. om spesifiserte lastegenskaper, avbruddsinformasjon, spenningsdropp og jordfeil. Nettselskapene kan selv bestemme intervallet på datainnsamlingen og filtreringen av informasjon. Alarmer genereres til spesifiserte mottakere (for eksempel vedlikehold). Dataene samles inn og kommuniseres. Informasjonen / verdikjeden eies av nettselskapet, mens kommunikasjonsløsninger og datalagring driftes av eksterne eKom og IT-leverandører (f.eks. Telenor, Basefarm, Microsoft Azure etc.). Multiinstrumentene og tilhørende kommunikasjonsløsning kan kategoriseres som IoT-produkter. Som det fremkom under intervjuene, benyttes dataene som innhentes hovedsakelig til beslutningsstøtte opp imot de eksisterende arbeidsprosessene i virksomheten(e). Samtidig muliggjør teknologien og systemene potensielle automatiserte prosesser, som f.eks. å autogenerere et informasjonsskriv til kunder som er rammet av jordfeil. Det brukes også målere på regionalnettsnivå. I tillegg til å oversikt på spenning og strøm, brukes informasjonen til avregning og til å gi en balanseoversikt, herunder estimere tap i nettet.

### Avanserte målesystem (AMS) – 3. parts tilgang via Home Area Network (HAN-porten)

Utrulling av avanserte målesystem (AMS) i norske husstander / hos sluttbrukere skal eksempelvis gi bedre overvåking og styring på distribusjonsnettnivå. I utgangspunktet innhentes måledata fra forbrukerne ved gitte tidsintervall som sendes via en kommunikasjonskanal til nettselskapets kundesystem og til den nasjonale databasen (Elhub). Med de smarte målerne er det også mulig for nettselskapene å oppdage jordfeil, i tillegg til å overvåke spenning både i eget nett og hos sluttbruker, noe som gir økt personsikkerhet<sup>3</sup>. Det stilles krav til at AMS skal inneha en bryterfunksjon. Dersom denne benyttes av nettselskapet, er AMS å anse som del av driftskontrollsystemet.

Videre legger AMS til rette for tredjeparttilgang, dvs. at nye aktører kan bidra med produkter og løsninger som skal drifte forbrukerens energibruk på en mer rasjonell, kostnadseffektiv og energioptimal måte gjennom HAN-porten. HAN-porten er et grensesnitt som kan gi strømkunder tilgang til informasjon om eget forbruk. Informasjonen skal i utgangspunktet kun være tilgjengelig for kunden, og nettselskapet gis tilgang til dataene etter avtale med kunden (NVE, 2017). Forbrukerne må selv kjøpe utstyr til å koble seg til HAN-porten, og det forventes at andre aktører vil tilby tjenester basert på informasjon fra denne.

Problemstillinger knyttet til AMS-målerne var i utgangspunktet ikke prioritert i denne kartleggingen, da NVE og bransjen har god oversikt over dette området. Grunnen til at det likevel nevnes i denne rapporten er at undersøkelsen avdekket informasjon om pågående pilotprosjekter som omhandler testing av HAN-utstyr til varmestyring / hjemmestyring. Formålet med prosjektet er å undersøke hvordan slike produkter kan bidra til unngå effekttopper / overlast i nettet og for sluttbruker å få lavere nettleie og/ eller strømregning. Ulike leverandører av hjemmestyring testes ut. Felles for løsningene er at informasjonen fra HAN-porten kan sende informasjon til hjemmestyringssystemet, som via automatiserte prosesser kan slå av og på energikrevende produkter etter behov (f.eks. slå av varmtvannsbereder eller lade el-bil for å tilpasse strømforbruket). På sikt kan det komme forskjellige tilbud som tilbyr tjenester basert på informasjon fra HAN-porten. Dette kan gi positive effekter, men det er samtidig viktig å være bevisst på potensielle sikkerhetsutfordringer, f.eks. muligheten for manipulering av data og tilgang til forbruker.

#### 3.1.2 IoT- produkter som brukes i støttesystemer

Kraftberedskapsforskriften stiller krav til at nettselskapene skal ha kontroll på hvem som gis adgang til anleggene, i tillegg til at det er etablert gode systemer for branndeteksjon og - slukking. Basert på denne overordnede kartleggingen, er det tilsynelatende forskjeller blant nettselskapene hvorvidt sensortechnologi brukes til styring. Et nettselskap oppgav at de brukte sensorer kun til å innhente informasjon om temperatur, fuktnivå og dørstilling i transformatorstasjonene, mens andre benyttet sensortechnologi også til styring fra driftssentralen. Et eksempel er bruken av digitale sikkerhetskort og adgangsstyring til å kontrollere og styre adgangen til stasjonene via en IT-løsning (APP). Fysiske adgangskort erstattes med digitale sikkerhetskort og det benyttes autentisering (AIF) gjennom en app hvor personellet melder seg inn og ut av anleggene. Dette gir driftssentralen en oversikt over hvem som befinner seg i stasjonen til enhver tid. Videre kan alarmsystemene (brann og innbrudd) tilknyttes et sideordnet system med binær kontakt (åpen/lukket) til SCADA-systemet, noe som gjør det mulig å aktivere / deaktivere alarmsystemet via SCADA-systemet fra driftssentralen. Implementering av IoT-teknologi endrer dermed måten aktørene overvåker og styrer disse prosessene, og introduserer samtidig noen potensielle nye sårbarheter.

Når det gjelder bruken av IoT – løsninger for vedlikeholdssystemer kom det frem av kartleggingen at enkelte nettselskaper fremdeles foretrekker tidsbasert og planlagt vedlikehold. Det viktigste er å forebygge at noe skjer. Dersom en sensor gir beskjed om at eksempelvis en pakning er defekt, er det allerede for sent. Det ble fremhevet at ny teknologi må ha en nytteverdi og/ eller gi økt gevinst dersom den skal implementeres. I det ligger det at en må vurdere fordelene ved å ta i bruk nye IoT-produkter opp mot ulempene. For

<sup>3</sup> Regulering av IKT-sikkerhet (NVE, 2017:26) [http://publikasjoner.nve.no/rapport/2017/rapport2017\\_26.pdf](http://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf)

eksempel trenger sensorene strømforsyning hvor batteripakkene må byttes ved jevne mellomrom, noe som kan gi økte operasjonelle kostnader. I andre tilfeller finnes tilleggsfunksjoner i systemløsningen som ikke tas i bruk fordi det ikke vurderes som hensiktsmessig. Et eksempel er et vedlikeholdssystem som kan autogenerere ordre. Inntrykket er at denne funksjonaliteten i liten grad er tatt i bruk per i dag. Dette skyldes blant annet at det må vurderes / kvalitetssjekkes om ordren må eller bør prioriteres med hensyn også til andre styringsfaktorer.

Bransjen har også til en viss grad begynt å ta i bruk andre type tjenester gjennom software-løsninger som inkluderer analyse og tolkning av innsamlet data, hvor resultatene synliggjøres eksempelvis via Power BI. Endringer i hvilke tjenester som tilbys blir ytterligere omtalt i neste kapittel.

### 3.2 Utviklingen de neste årene

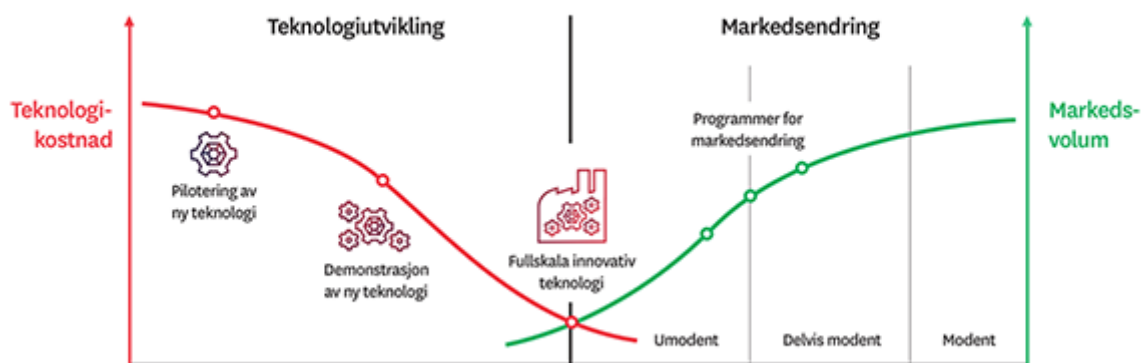
Under følger en kort introduksjon av aktuelle trender som har kommet frem av kartleggingen, inkludert hvilke IoT/IloT - løsninger og produkter som testes gjennom ulike FoU-prosjekter og Smartgrid piloter, samt hvilke produkter og tjenester som befinner seg i en tidlig fase i kommersialiseringen.

#### 3.2.1 Trender og kommersialisering

På generelt grunnlag, bidrar ny teknologi (IoT/IloT-produkter) med ny type informasjon om nettet og svarer på noen av problemstillingene bransjen står overfor i dag. Følgende tre kjennetegn ble av en av informantene omtalt som de viktigste driverne for utvikling og innføring av ny teknologi:

- Ekstremvær som følge av klimautfordringer
- Elektrifiseringen av samfunnet (transportsektoren, båter, fly)
- Vindkraftutbygging – behov for mer fleksible nett

For å møte disse utfordringene må også energibransjen tenke innovativt, noe som åpner opp for nye produkter, løsninger og aktører. Det kan imidlertid ofte ta lang tid før ny teknologi får gjennomslag og sprer seg i markedet. Figuren under viser sammenhengen mellom teknologiutvikling og markedsending. For å utvikle ny teknologi er det ofte nødvendig å få hjelp til å bære den økonomiske byrden, dvs. investeringsrisikoen (f.eks. gjennom samarbeid bransje og leverandør eller gjennom ulike støtteordninger som eksempelvis Enova).



Figur 2 Teknologiutvikling og markedsending (Kilde: <https://energifaktanorge.no/et-baerekraftig-og-sikkert-energisystem/enova/>)

Etter hvert som teknologien er tilstrekkelig utprøvd og moden for kommersialisering, er det fremdeles noen barrierer som skal forseres for å bidra til reell markedsendring. Selv om det er igangsatt flere spennende initiativer og prosesser for å teste ut ny teknologi i energiforsyningen i dag, er det altså fremdeles en vei å gå før mange av produktene og tjenestene er fullt ut kommersialisert. Det er imidlertid grunn til å tro at denne utviklingen skjer stadig raskere. Gjennom denne kartleggingen fant vi tre bruksområder hvor nye smarte løsninger antas å kunne implementeres i storskala i relativt nær fremtid.

### **Sensorteknologi som overvåker og gir beslutningsstøtte**

En generell trend er at nettselskapene ønsker å benytte sensorteknologi for å innhente mest mulig informasjon om tilstanden på anleggene. Tilgangen på ulike typer sensorer er drastisk økende, samtidig som kostnadene ved å produsere produktene (hardware) blir lavere. Dette er en medvirkende årsak til at det blir introdusert sensorteknologi som kan brukes på flere anvendelsesområder enn tidligere. I tillegg kan denne typen sanntidsinformasjon gi bedre beslutningsstøtte, gjennom at nettselskapene får økt kunnskap og dermed redusert usikkerhet. Eksempler på innovasjoner som i senere år er testet gjennom ulike prosjekter og som antas å bli implementert av flere nettselskaper er:

- Sensorkuler til overvåking av kraftlinjer
- Smarte, trådløse sensorer (temperatur +++)
- Informasjon om leveringskvalitet
- Sekundærdata (f.eks. måle vibrasjon)

Tradisjonelt har leverandørene levert moduler, hardware og løsninger for innhenting av data, og nettselskapene har eid og behandlet dataene på egenhånd. Gjennom utviklingen av IoT / IloT- løsninger ser man en økende trend hvor leverandørene tilbyr totalleveranser, dvs. sensorteknologi (hardware) i kombinasjon med software / skylagring, analyser og support (service and support). I stedet for å kjøpe og eie data, forventes det at kundene i større grad vil betale for bruken av produktene.

### **Droneteknologi til linjeinspeksjoner og beredskap<sup>4</sup>**

Tradisjonelt har nettselskapene benyttet helikopter til å gjennomføre linjeinspeksjoner, men flere uønskede hendelser i forbindelse med denne aktiviteten (f.eks. kollisjoner, skade på linjer) har bidratt til en økt interesse for å erstatte helikopter med droner. I tillegg til at autonome droneinspeksjoner har en risikoreduserende effekt med hensyn til personsikkerhet og materielle skader på linjer, gir digitaliseringen og sensorteknologien merverdi til selskapene gjennom effektivisering av driften og økt kunnskap om tilstanden på master / linjer som igjen kan gi bedre styring. Dronene som brukes har tre primære funksjoner:

1. Bidra med høyoppløste bilder av mastepunkt og linjer (bildearkiv)
2. Termografering (identifikasjon av hot spots)
3. Vegetasjonskontroll (innmåling av masten som sees opp imot kartgrunnet).

Det finnes eksempler på aktører som har utviklet programvarer / algoritmer som gjør det mulig for droner å styre seg selv basert på sanntidsinformasjon som analyseres ved hjelp av maskinlæring (se Vedlegg III). Bruk av droneteknologi kan blant annet bidra til:

- Mer effektive arbeidsprosesser / autonome inspeksjoner
- Redusere gjenopprettelsestiden og kortere avbruddstider i en feilsituasjon / beredskapssituasjon
- På sikt – gjennomføre operasjoner på mer ufremkommelige steder

<sup>4</sup> <https://www.cw.no/artikkel/drone/ny-norsk-proffdrone>  
<https://www.tu.no/artikler/dette-proveprosjektet-kan-bety-enormt-mye-for-dyr-inspeksjon-av-kraftlinjer/433135>  
<https://enerwe.no/droner-har-kommet-for-a-bli-i-nettbransjen/165556>  
<https://www.uasnorway.no/halogaland-kraft-inspisere-5000-km-droner/>

## Norges vassdrags - og energidirektorat (NVE)

Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning,

- Kostnadseffektive prosesser
- Bedre personsikkerhet

Enkelte dronetjenester er allerede kommersialisert, som f.eks. linjeinspeksjon, men det er fremdeles flere prosjekter som befinner seg i en tidlig fase. Et eksemplet er det nylig oppstartede FoU prosjektet til Hafslund<sup>5</sup> i samarbeid med KVS Technologies som handler om å supplere og optimalisere beredskapsarbeidet med bruk av en autonom droneflåte. Regulatoriske krav, f.eks. gjennom luftfartsregulativer, setter imidlertid enkelte begrensninger for hvor fort utviklingen med droner kan gå.

### Effektivisere arbeidsprosesser gjennom digitalisering

Som allerede nevnt, har bransjen begynt å digitalisere prosesser som tradisjonelt har vært håndtert manuelt, enten det dreier seg om adgangskontroll eller drift- og vedlikeholdsstyring. En av informantene påpekte at økning av antall leverandører til kraftbransjen er en tydelig trend, noe som også inkluderer tilbydere av ulike softwareprogram og tjenester. Inntrykket er at bransjen ønsker mest mulig informasjon, men at selskapene ikke helt har definert hvilke behov og prosesser all informasjonen skal ivareta eller erstatte. Flere av informantene fremhevet viktigheten av å forstå nytteverdien av IT-løsningene som blir implementert, samt utvise forsiktighet med tanke på risiko.

Gjennom kartleggingen har det kommet frem at bransjen har et stort og økende fokus på innsamling av informasjon. Det har ikke fremkommet tydelige planer og tanker for hvordan informasjonen kan brukes til å effektivisere arbeidsprosessene i fremtiden. En av leverandørene bekreftet at de opplevde at kraftbransjen etterspør mer data, men uten nødvendigvis å være opptatt av kvaliteten på dataene og at det til dels mangler en forståelse av hva informasjonen kan og skal brukes til.

### 3.2.2 Oversikt over relevante SmartGrid demoaktiviteter og piloter

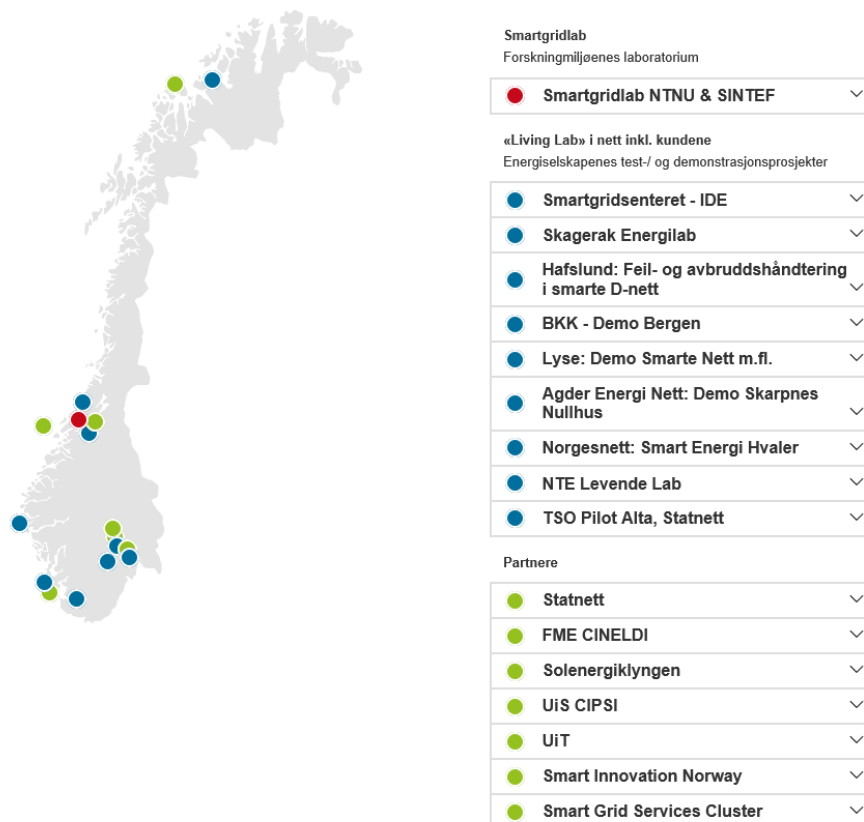
En stor del av forskningen og utviklingen relatert til fremtidens energiforsyning finansieres og støttes av Norges Forskningsråd gjennom bl.a. Energix-programmet, tilskudd fra Enova og NVEs finansieringsordning for FoU-prosjekter. De fleste av de aktive prosjektene er assosiert med Smartgridsenteret, et nasjonalt kompetansesenter og samhandlingsplattform for aktører innen smartgrid i Norge. Per i dag har de knyttet til seg 45 medlemmer fra energi-/nettselskapene, forskningsinstitusjoner og fra industrien. Smartgridsenteret driver også en nasjonal demokomiteé, Demo Norge, som støtter og bidrar til etableringen av demonstrasjonsaktiviteter innenfor smartgrids hos flere energi-/ nettselskaper. Per i dag er det 10 prosjekter tilknyttet Demo Norge fordelt som vist i figuren på neste side. Enkelte av disse demonstrasjonsaktivitetene er rettet mot utvikling og testing av ny teknologi, mens andre omfatter mer læring av bruken av ny teknologi for drift og planlegging innenfor nett.

---

<sup>5</sup> <https://enerwe.no/drone-hafslund-nett-nettselskap/hafslund-nett-skal-bruke-droner-til-a-finne-feil-pa-stromkabler/345438>

## Norges vassdrags - og energidirektorat (NVE)

Kartlegging av bruk av tingenes internett (IoT/IloT) i norsk kraftforsyning,



Figur 3 Oversikt over deltakere i Demo Norge (hentet fra Smartgrids.no)

Å gi en detaljert beskrivelse av samtlige aktive og avsluttende prosjekter har ikke vært en del av denne kartleggingen<sup>6</sup>. I det følgende omtales likevel noen av demoaktivitetene som eksempler på IoT/IloT-løsninger som kan implementeres i bransjen i fremtiden (se Vedlegg II for omtaler av flere prosjekter).

**Demo Smarte Nett Stavanger**<sup>7</sup> er et Enova støttet prosjekt som Lyse Elnett iverksatte i 2016. Totalt har 31 nettstasjoner i Stavanger og omegn blitt oppgradert med ny teknologi slik at de kan fjernstyres og overvåkes. Nettstasjonene ble gjort fullautomatiske og tilkoblet mange ulike sensorer, bl.a. som overvåker temperatur og om dører er låst. I prosjektet testet Lyse Elnett ut nytteverdien av smartgrid-teknologi kombinert med nye automatiske strømmålere hos kundene i et større område. Det er mulig å ta ut sanntidsdata som viser forbruk, effekttopper og ledig kapasitet i strømmettet. Ved feil i området kan teknologien i deler av nettstasjonen kobles om automatisk. Formålet med prosjektprogrammet var å demonstrere tekniske og praktiske behov ved bygging og oppgradering av nettstasjoner, se på hvordan ulike teknologiske løsninger virker/samvirker, og vurdere kostnader og nytte av ny teknologi. Prosjektperioden er avsluttet, men noen av nettstasjonene blir videreført som egne prosjekter og skal driftes over en toårs-periode for å demonstrere og dokumentere positive effekter av løsningen.

**Feil- og avbruddshåndtering i smarte distribusjonsnett (FASAD)**<sup>8</sup> er et prosjekt hvor målet var å kartlegge hvordan ny smartgrid-teknologi kan utnyttes i det elektriske distribusjonsnettet til å redusere avbrudd i strømforsyningen, og samfunnsøkonomiske kostnader ved avbrudd. Et viktig element i smarte distribusjonsnett er å ta i bruk ulike sensorer som kan oppdage når det inntreffer feil i nettet. Utnyttelse av

<sup>6</sup> Se <https://smartgrids.no/> for nærmere informasjon om de enkelte prosjektene som er tilknyttet Smartgridsenteret.

<sup>7</sup> For mer informasjon om Demo Smarte Nett Stavanger vises til <https://www.lysenett.no/smartnett/#articleTab1>.

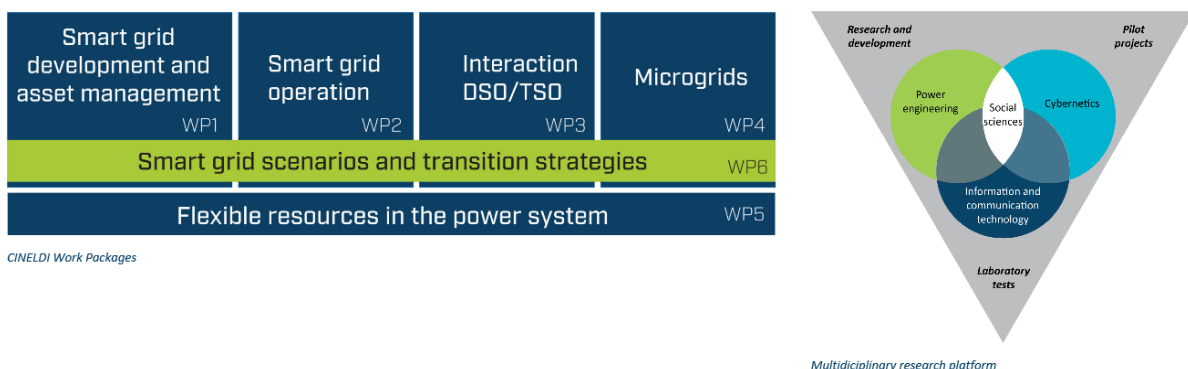
<sup>8</sup> For mer informasjon om FASAD-prosjektet se <https://www.sintef.no/prosjekter/feil-og-avbruddshandtering-i-smarte-distribusjonsn/>

denne informasjonen gir potensialer for reduksjon i både antall og varighet av avbrudd i strømforsyningen. Sensorene kan dermed utnyttes for smartere feil- og avbruddshåndtering gjennom at feil i nettet raskere detekteres, lokaliseres og isoleres. Dette gir en raskere gjenoppretting av strømforsyningen for de sluttbrukerne som har opplevd avbrudd. Sensorenes evne til å oppdage feil i nettet kan også bidra til å redusere antallet koblinger under driftsforstyrrelser, og dermed resultere i færre kortvarige avbrudd og spenningsfall. Informasjonen om feil i nettet kan samles inn ved å knytte sensorene til driftskontrollsystemet. Videre kan denne informasjonen kombineres med ulike målinger i nettet til å beregne avstanden til feilstedet. Dette vil redusere tid til feilsøking og gi beslutningsstøtte for driftsoperatørene til å foreta raskere koblinger for å gjenopprette strømforsyningen.

Demo- og uttesting av ulike feilindikatorer har vært gjennomført hos Hafslund Nett og Skagerak Nett i totalt 7 ulike nettområder, både luftnett og kabelnett. Ulike typer kortslutnings- og retningsbestemte jordslutningsindikatorer, kombinert med fjernstyring og bruk av målinger til estimering av avstand til feilsted ble testet. I tillegg har prosjektet også testet og dokumentert automatiserte koblingsprogram (selvreparerende nett).

«Pilot Flexibilitet» (Engene transformatorstasjon)<sup>9</sup> var et samarbeid mellom Agder Energi og Microsoft for å møte den økte etterspørselen etter strøm for et spesifikt område hvor de hadde utfordringer med overbelastninger på vinteren. Engene transformatorstasjon ble et testobjekt for bruk av skybasert teknologi. Prosjektet gikk ut på å utnytte fleksibiliteten i nettet på en bedre måte, ved å utvikle nye forretningsmodeller. Tradisjonelt har produksjon av strøm blitt justert etter hvor stor etterspørselen er, men i dette prosjektet ble denne tankegangen snudd. I stedet tok man utgangspunkt i å bruke så mye strøm som faktisk var tilgjengelig, noe som krevde informasjon i sanntid, prediksjoner og ulike analyser av værdata, historiske data og produksjonsdata. Ved bruk av maskinlæring og algoritmer åpnes nye muligheter hvor alle elementer snakker med hverandre for å løse utfordringene og helst før de inntreffer. Resultatet av prosjektet var at transformatoren på Engene transformatorstasjon ikke ble overbelastet i testperioden (vinteren 2017) der eksempelvis varmekabler hos storforbrukerne (bedriftene) ble koblet ut etter behov. Prosjektet demonstrerte hvordan endring og øking i fleksibiliteten er et godt verktøy for å drifte fornybar energi. Prosjektet er videreført gjennom NORFLEX<sup>10</sup> og NODES<sup>11</sup>.

**CINELDI (Centre for Intelligent Electricity Distribution)** er et forskningssenter med tilknytning til SINTEF. Prosjektperioden varer fra 2016-2024 og har som formål å tilrettelegge for en kostnads-effektiv realisering av fremtidens fleksible og robuste distribusjonsnett. Det inngår flere arbeidspakker i prosjektet som vist i figuren under.



Figur 4 CINELDI-prosjektet. Kilde: <https://www.sintef.no/projectweb/cineldi/research/>

<sup>9</sup> <https://www.ae.no/aktuelt/nyheter/slik-ble-engene-transformatorstasjon-verdensberomt/>

<sup>10</sup> NORFLEX-prosjektet: <https://www.energinorge.no/fagomrader/stromnett/nyheter/2019/losninger-for-fremtidens-stromnett2/>

<sup>11</sup> NODES: <https://nodesmarket.com/>

### 3.3 Leverandører og løsninger som tilbys

Det finnes i dag en rekke leverandører som tilbyr tjenester relatert til IoT/IloT mot kraftbransjen. Omfang og type tjenester varierer i stor grad, og det er ikke her gjort en helhetlig kartlegging av alle leverandører som har produkter eller tjenester i dette segmentet. Det kan imidlertid være hensiktsmessig å sortere leverandørene i 2 hovedtyper leverandører, som indikert i tabellen under.

Den ene typen leverandører kan sies å være godt etablerte, og har levert ulike produkter og tjenester til kraftbransjen i over 10 år. Dette dreier seg typisk om klassiske kontrollsystemleverandører. Den andre typen leverandører vi har sett på er relativt nye i markedet (<10 år). Disse retter seg i mindre grad direkte mot kontrollsystemene, men tilbyr gjerne sensorteknologi og droneteknologi, tillegg til softwareløsninger, skyløsninger og i enkelte ganger også analyse av dataene.

En oppfatning som kom frem i intervjuene var at når de etablerte aktørene kommer med et produkt, så er det langt på vei ferdig «testet» - og må være kompatibelt med andre produkter de har i sortimentet sitt. Nyetablerte innovatører / leverandører er imidlertid mer avhengige av å gjennomføre utviklingsaktiviteter i samarbeid med bransjeaktørene før produktene / tjenestene kan tilbys kommersielt. Tabellen under viser en del av de relevante leverandørene som finnes på markedet per i dag. Se Vedlegg III for ytterligere beskrivelser av hva de enkelte aktørene tilbyr.

**Tabell 1 Eksempler på etablerte (>10 år) og nye (< 10 år) leverandører av IoT-løsninger**

> 10 år	<ul style="list-style-type: none"><li>• ABB</li><li>• Aidon</li><li>• Enfo</li><li>• Kamstrup</li><li>• Powel</li></ul>	<ul style="list-style-type: none"><li>• Rejlers</li><li>• Siemens</li><li>• Valider</li><li>• Verico</li></ul>
< 10 år	<ul style="list-style-type: none"><li>• Broentech Solutions AS</li><li>• Disruptive Technologies</li><li>• eSmart Systems</li><li>• Greenbird</li><li>• Heimdall Power</li></ul>	<ul style="list-style-type: none"><li>• KVS Technologies</li><li>• Nordic Unmanned</li><li>• SafeBase</li><li>• Syseco</li><li>• Versor</li></ul>

#### 3.3.1 Hyllevarer vs skreddersydde løsninger

Svaret på hvorvidt leverandørene hovedsakelig tilbyr såkalte hyllevarer eller skreddersydde løsninger er todelt. Hovedinntrykket er at selve produktene (hardware / modulene / sensorteknologien) som regel produseres og leveres som hyllevarer, men at tjenestene kan (og må) utvikles og tilpasses i samarbeid med bransjen og etter den enkelte kundens behov og systemer. Når det er sagt, tilbyr leverandørene i økende grad komplette tjenester, bestående av både hardware, kommunikasjon (gateway, Edge), skyløsninger (f.eks. Microsoft Azure) og analyser av dataene ved bruk av algoritmer. Dette krever ofte individuelle tilpasninger eller skreddersøm med tanke på kundens eksisterende IT-arkitektur (f.eks. drifts- og vedlikeholdssystem). Som tidligere nevnt, er det forventet at det etter hvert blir langt billigere å produsere hardware / sensorteknologi enn dagens nivå, og at forretningspotensialet følger av de ulike tilleggstjenestene. Flere av informantene nevnte at det i fremtiden i større grad vil tilbys ulike abonnementsordninger (Software and Service) i tillegg til sensorteknologien (hardware).

På spørsmål om hvem som er de største pådriverne for utviklingen av IoT-løsninger, er det en generell oppfatning blant både leverandørene og nettselskapene om at dette går begge veier. En av informantene oppgav at de i enkelte tilfeller var «lite imponert» over hvor lite fremtidsrettet noen av leverandørene var, og at det var bransjen selv som måtte utfordre leverandørene til å utvikle nye løsninger. Motsatt var det også eksempler hvor leverandørene tar initiativ og ønsker å teste ut og utvikle produktene sine innenfor pågående prosjekter. I slike tilfeller kan det være utfordrende for nettselskapet å forstå implikasjoner og risiko knyttet til innføring av nye varer, tjenester eller endret bruk av disse.

Det kan også virke som det er noen forskjeller mellom de etablerte leverandørene til kraftforsyningen, og de mer nyetablerte aktørene. I samtale med en av de tradisjonelle kontrollsystemleverandørene kom det frem at de, med tanke på IoT-teknologi, først og fremst justerte og utvidet eksisterende produkter. De tar i bruk og tilrettelegger for nye/flere sensorer (måling av data), men nyvinningene er hovedsakelig relatert til kommunikasjonsløsninger og ny bruk av dataene (innsamling og lagring). Produktene som tilbys må også i stor grad være kompatible med den øvrige produktporteføljen. Videre ble det nevnt at markedsføringen i større grad retter seg mot abonnementstjenester (Software og Service) sammenlignet med tidligere.

De nye aktørene, derimot, er gjerne i større grad pådriverne og utviklere av nye produkter og tjenester, som f.eks. sensorkulene til Heimdal Powell, autonome droner (f.eks. KVS Technologies, eSmart Systems) og trådløse sensorer (levert av f.eks. Disruptive technologies og SafeBase).

### 3.3.2 Kjennskap til og bruk av standarder

Kraftberedskapsforskriften (Kbf) § 6-9 stiller krav til at «virksomheter skal sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas», gjennom planlegging, gjennomføring og vedlikehold av hensiktsmessige sikringstiltak. Ifølge tilleggsveilederen til Kbf<sup>12</sup> følger kravene grunnprinsippene for IKT-sikkerhet formulert av NSM, som igjen bygger på internasjonale anerkjente standarder og veiledere som f.eks. ISO/IEC 27002. Når det gjelder risikovurderinger vises det bl.a. til *Risikovurdering for sikring (NSM)*<sup>13</sup>, *Veiledning for risiko- og sårbarhetsanalyser for kraftforsyningen (NVE)*<sup>14</sup> og nasjonale (NS 5814:2008 / NS 5832:2014) samt internasjonale standarder (ISO 27000-serien). I veilederen gis det i tillegg en rekke beskrivelser og anbefalinger til hvordan forskriftens (funksjonelle) krav kan ivaretas.

I kartleggingen av dagens bruk av IoT / IloT løsninger i energiforsyningen, har det vært særlig fokus på leverandørenes oppfølging og bruk av IKT-standarder. Nettselskapene som svarte på undersøkelsen gav i liten grad konkret informasjon på dette temaet, men påpekte at «de fleste følger en eller annen standard». Det var også i varierende grad informasjon tilgjengelig på de aktuelle leverandørenes hjemmesider. Noen oppgav at de var ISO sertifisert etter f.eks. ISO 27000 – standarden, andre viste til ulike RENblad (f.eks. REN6025 – krav til nettstasjoner) og generelle krav til sikkerhetsløsninger for kommunikasjon i driftskontrollsystemene gjennom IEC61850. Vi fant også eksempler på leverandører som har beskrevet om egen informasjonssikkerhetspolicy i et såkalt «White Paper»<sup>15</sup>.

Samtlige leverandører gav uttrykk for at IKT - sikkerhet har et høyt fokus. Flere nevnte at kraftberedskapsforskriften var styrende for deres IKT-sikkerhetsarbeid. Felles for informantene i denne kartleggingen var kravet om at dataene skulle lagres i godkjente land / områder. Et selskap oppgav at de stilte krav om at dataene skulle lagres nasjonalt. Det ble også vist til interne rutiner for adgangskontroll til kontorlokaler (to-faktor autorisering). Når det gjelder bruk av standarder, var det noe varierende

<sup>12</sup> Foreløpig tilleggsveileder til kraftberedskapsforskriften (NVE, 2018).

<sup>13</sup> Håndbok: Risikovurdering for sikring, Publisert: 04.02.2016 | Sist endret: 16.03.2016,

<https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/risikovurdering-handbok/>

<sup>14</sup> Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen, NVE 2010,

[http://publikasjoner.nve.no/veileder/2010/veileder2010\\_02.pdf](http://publikasjoner.nve.no/veileder/2010/veileder2010_02.pdf)

<sup>15</sup> <https://www.disruptive-technologies.com/wp-content/uploads/2018/11/Disruptive-Technologies-Security-White-Paper.pdf>

tilbakemeldinger på graden av implementering. Enkelte oppgav at de ikke har blitt ISO-sertifisert enda på grunn av at organisasjonen er for ung og/eller at produktene fremdeles er i en utprøvningsfase og enda ikke blitt tatt i kommersielt bruk. Et annet poeng som ble fremhevet var at underleverandørene har kvalitetssystem (f.eks. ISO 9001, ISO 27000-serien eller ISO 21000). Samtidig ble det problematisert at det ikke nødvendigvis er utarbeidet egnede IKT- standarder for de produktene og tjenestene som ble levert, med tanke på grensesnittet mellom krav som retter seg mot IKT/ kommunikasjonsløsninger (f.eks. EDGE og skyløsning) og krav som gjelder driftskontrollsystemene<sup>16</sup>.

En generell oppfatning blant informantene er at kraftforsyningen / nettselskapene har fokus på leverandørens policy rundt informasjonssikkerhet, men at kunnskapen rundt dette ikke nødvendigvis er tilstrekkelig hos alle. En informant beskrev hvordan de enkelte ganger opplever at det stilles omfattende krav, hvor kunden benytter seg av standardiserte sikkerhetskrav som ikke nødvendigvis er relevant for produktet eller tjenesten som skal leveres. Dette medfører enkelte ganger mye ekstraarbeid for leverandør(e), og at kravene ikke nødvendigvis ansees som gjennomførbare.

Gjennom kartleggingen kom det også frem at nettselskapene i liten grad fører tilsyn / følger opp om leverandørene etterlever IKT-sikkerhetsarbeidet. Et tilfelle er nevnt hvor et nettselskap har vært i dialog med en leverandør om å utarbeide en kravspesifikasjon i fellesskap, som deretter kan brukes i tilsynsøyemed.

---

<sup>16</sup> En tilsvarende problemstilling ble omtalt i Teknisk Ukeblad 28.07.16. <https://www.tu.no/artikler/sikkerhetsplattformer-for-innvevd-utstyr-i-industriell-iot/349076>

## 4 Vurdering og anbefalinger

I det følgende vil vi trekke frem noen temaer som gjennom denne kartleggingen har utpekt seg som relevante for videre studier på ulike områder (teknologi og sikkerhet) og nivåer (forvaltning, industri og aktører). Disse er å:

- Forstå implikasjoner for forsynings sikkerheten ved innføring av IoT/IloT- løsninger
- Kartlegge kompetanse og holdninger, og behov for kunnskapsløft
- Videreutvikle og forbedre veiledning og verktøy for risikostyring
- Tilpasning av regelverk, tilsyn og kontroll

Delkapitlene følger samme struktur. Først gis en kort begrunnelse av hvorfor problemstillingen vurderes som aktuell, etterfulgt av anbefalinger om mulige aktiviteter for videre oppfølging.

### 4.1 Forstå implikasjoner for forsynings sikkerheten ved innføring av IoT/IloT- løsninger

Denne kartleggingen har identifisert noen konkrete produkter og tjenester som man vil se mer av i tiden fremover. Det gjelder eksempelvis bruken av droner til inspeksjoner og beredskap, digitalisering av adgangskontroll og mer utstrakt bruk av internettbasert sensorteknologi. Bruken av nye teknologiske løsninger, f.eks. sensorer som leverer sanntidsdata, har mange oppsider. Selskapene får mer nøyaktig informasjon om tilstanden, noe som blant annet tilrettelegger for bedre overvåking, styring og vedlikehold av anleggene. Innføringen av AMS - teknologi er slik sett et godt eksempel på hvordan innovasjoner fører til økt kvalitet på informasjon (målerdata) og forvaltningen av denne (Elhub), og samtidig åpner opp for andre måter å drifte nettet på gjennom bryterfunksjonaliteten (smarte nett). Sistnevnte funksjonalitet er ikke tatt i bruk enda, men antas å bli en sentral del av hvordan energiselskapene drifter fremtidens nett. Gjennom demoaktivitetene ser vi også konturene av hvordan ny og smart teknologi kan møte og ivareta utfordringene energiforsyningen står overfor som følge av den drastiske økningen av forbruk og behov for fleksibilitet (f.eks. elektrifisering av transportsektoren og petroleumsvirksomheten), gjennom effektivisering, nye forretningsmodeller og bedre utnyttelse av nettet.

Inntrykket er at det er en erkjennelse i bransjen at innføringen av ny teknologi potensielt også gir flere angrepsflater, feilkilder og nye sårbarheter/trusler. Selv om bruken av IoT-løsninger er økende er det stort fokus på å beskytte driftskontrollsystemet (dvs. holde det mest mulig «lukket»). Et eksempel er sensordata som går via en stasjons-PC (sidesystem) og videre i krypterte tunneler til SCADA-systemet. Brannmurer og filtreringsteknikker (såkalt logisk skille) brukes for å beskytte kommunikasjonskanalen, noe som reduserer risikoen for inntrenging. Men logiske skiller gir ikke 100 % beskyttelse. Gjennom intervjuene ble sårbarhetene eksemplifisert ved at underleverandørene har tilgang eller mulighet for oppkobling ut i stasjonene gjennom servicelinjer dersom det er behov for fjerndiagnose og programoppdateringer (systemendringer). Vanlig praksis er at tilgangen tidsbegrenses og sikres ved bruk av nøkler. Likevel er det svært viktig å ha kontroll på grensesnittene, bakdørene og på sikkerhet, ytelse og pålitelighet.

Det ble under intervjuene også stilt spørsmål til datakvaliteten når IoT brukes til innhenting av data, og hvem som skal eie informasjonen. Tradisjonelt har selskapene «eid» og hatt kontroll på dataene, men dette kan endre seg gjennom at leverandørene tilbyr totalløsninger som inkluderer også lagring og analyse av data. Hvor sikre er man på at informasjonen som kommer ut er riktig, eksempelvis ved bruk av AI til analyser? Kan man stole «blindt» på at informasjonen stemmer, og hvilken betydning har det om det er en feil i algoritmene som benyttes eller i dataene som mates ut? På sikt forventes det at denne typen analyser og databehandling benyttes som input til automatisert prosesser (og profesjonalisering). Et eksempel er å autogenerere et informasjonsskriv til strømkundene om jordfeil. Hvordan skal denne informasjonen kvalitetssikres, og hvilke følgefeil kan feilinformasjon gi? Videre er det usikkerhet knyttet til hvorvidt det er mulig å tilsiktet eller utilsiktet endre data slik at det oppstår overlast og dermed strømutfall.

Det er et tydelig behov for mer kunnskap om og forståelse av hvordan systemene og elementene kan påvirke hverandre. Noe arbeid er allerede igangsatt gjennom de ulike demoaktivitetene og utviklingsprosjektene (leverandør/bransje). Det fremkommer imidlertid også behov for kartlegginger som tar for seg konkrete teknologiske løsninger og mulige implikasjoner for forsyningssikkerheten. Som det ble nevnt under intervjuene, er det viktig å kartlegge og forstå nytteverdien av å implementere nye løsninger tilpasset de prosessene de skal ivareta. Det er en fare for at bransjen tar i bruk teknologi fordi det er innovativt og tilsynelatende nyttig, uten tilstrekkelig erkjennelse av at implementeringen også åpner opp for nye mulige feilkilder og/ eller fører til operasjonelle merkostnader.

**Med bakgrunn i dette anbefales det at det initieres studier som tar sikte på å systematisk kartlegge og vurdere muligheter (nyttien) og utfordringer knyttet til utvalgte teknologiske løsninger og tjenester. Det er også naturlig at disse har et fokus på forsyningssikkerheten.**

#### Eksempler på aktuelle studier er:

- Muligheter og utfordringer ved bruk av utvalgte teknologiske løsninger:
  - Autonome droner
  - Potensielle feilkilder ved bruk av sensorteknologi
  - Nye og flere angrepsflater ved bruk av ny teknologi
- Utforske problemstillinger knyttet til datakvalitet med bruk av IoT til datainnsamling
  - Bruk av maskinlæring, AI og analyse – hvor sikre er vi på at informasjonen stemmer
- Vurdering av kostnader (økte og reduserte) ved innføring av utvalgte teknologiske nyvinninger/-løsninger

#### 4.2 Kartlegge kompetanse og holdninger, og behov for kunnskapsløft

Datainnsamlingen avdekket at det hersker en usikkerhet knyttet til informasjonssikkerhet i bransjen, også relatert til innføring av IoT, og at det er for få dedikerte IKT-ressurser i nettselskapene til å følge opp alle digitaliseringsprosjektene. Som et eksempel er ikke ansatte med IT-forståelse/kunnskap (f.eks. IKT-sikkerhetskoordinator) nødvendigvis involvert når drift beslutter å teste og/eller implementerer ny sensorteknologi (IoT). IT-avdelingene oppleves ofte som underbemannet. Energisektoren er i en radikal endring, hvor IT-kompetanse og systemforståelse blir stadig viktigere. Tiden hvor nettselskapene kun drev på med elkraft er over, noe som på sikt kan tvinge frem en endring i hvordan virksomhetene organiseres og bemannes. Ifølge en av informantene kan et scenario være at det etableres nye, mer fremtidsretta driftsplattformer hvor virksomhetene i større grad benytter en partnerstrategi som inkluderer ekstern rådgivning innen IT. Dette fordi nettselskapene ikke vil kunne opprettholde spisskompetansen som er nødvendig for å drifte fremtidens smarte nett (inkl. IoT/IIoT-løsninger). En slik strategi forutsetter likevel at selskapene har nok kompetanse internt til å utforme kvalifiserte bestillinger.

**Det anbefales å kartlegge og vurdere hvilken kompetanse som er nødvendig for å drifte og vedlikeholde nettet og anleggene når energibransjen digitaliseres.**

#### Tema som foreslås dekket er:

- Behov for bedre bestillerkompetanse
- Se på grensesnittet mellom elkraft og IT i fremtidens kraftforsyning og organisering
- Behov for økt kunnskap og forståelse for de prosessene ny teknologi skal ivareta – sett opp i mot IKT-sikkerhet

### 4.3 Videreutvikle og forbedre veiledning og verktøy for risikostyring

I NOU 2018:14 «IKT-sikkerhet i alle ledd» legger utvalget tre overordnede prinsipper til grunn for sine anbefalinger, hvorav det første er et «arbeidet med IKT-sikkerhet må ha en risikobasert tilnærming som innebærer at vesentlig risiko prioriteres»<sup>17</sup>. Energiloven og Kraftberedskapsforskriften med veileder og tilleggsveileder har den samme innretningen. Når det gjelder digitale informasjonssystemer ihht. Kbf § 6-9 plikter KBO enhetene å gjennomføre risikovurderinger ved systemendringer og holde disse oppdatert. De digitale informasjonssystemene skal også overvåkes for å identifisere, håndtere (og varsle om) eventuelle uønskede hendelser. Tilleggsveilederen gir føringer i forhold til gjennomføringen av risikovurderinger med hensyn til konfidensialitet, integritet og tilgjengelighet (s 27-28), og inkluderer betraktninger rundt risiko, usikkerhet, kunnskapsstyrke, metoder, tilsiktede hendelser mm. Videre anbefales det at større virksomheter med klassifiserte systemer bruker anerkjente standarder og metoder for risikovurdering, som f.eks. NSM NSMs *Risikovurdering for sikring*<sup>18</sup> og nasjonale (NS 5814:2008 og NS 5832:2014<sup>19</sup>) og internasjonale standarder (spesielt ISO 27000-serien).

Mange av virksomhetene i kraftbransjen bruker NVEs *Veiledning for risiko- og sårbarhetsanalyser for kraftforsyningen*<sup>20</sup> fra 2010, som basis i arbeidet med å kartlegge og vurdere risiko. Bransjen har, som beskrevet også i denne kartleggingen gjennomgått (og gjennomgår) en rivende teknologisk utvikling siden 2010. Kompetansesammensetningen i virksomhetene endres, med stadig større vekt på IKT-kompetanse. Språk og begreper endres. Endret teknologi gjør at kritikalitet flytter seg, og at stadig nye trusler og sårbarheter må forstås og håndteres. Til sammen skaper dette behov for annen type veiledning og andre verktøy for å kartlegge og vurdere risiko i dag og i fremtiden.

**Det anbefales å gjennomføre en evaluering av eksisterende veiledning for risiko- og sårbarhetsanalyser, for å vurdere behov for endringer.**

**Videre anbefales studier av behov – og eventuell utvikling av verktøy som understøtter effektiv vurdering og håndtering av risiko ved innføring av IoT og IloT-løsninger i fremtidens kraftnett.**

<sup>17</sup> <https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/>

<sup>18</sup> Håndbok: Risikovurdering for sikring, Publisert: 04.02.2016 | Sist endret: 16.03.2016, <https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/risikovurdering-handbok/>

<sup>19</sup> NVE fraråder den særegne varianten i NS 5832:2014 hvor (sikrings)- risikoanalyse omfatter (sikrings)risikovurdering (s.28).

<sup>20</sup> Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen, NVE 2010, [http://publikasjoner.nve.no/veileder/2010/veileder2010\\_02.pdf](http://publikasjoner.nve.no/veileder/2010/veileder2010_02.pdf)

#### 4.4 Tilpasning av regelverk, tilsyn og kontroll

Kartleggingen understreker betydningen av å ha regelverk og kontroll/oppfølging som både bidrar til å ivareta forsyningsikkerheten i kraftbransjen, men som også gir rom og legger til rette for innovasjon og utvikling. Som for resten av samfunnet utfordres lov- og regelverk i sin form ved behovet for mer dynamikk og funksjonell tilnærming. Kravene må beholde relevans ved en stadig raskere teknologisk utvikling og digitalisering, i et samfunn der funksjoner henger stadig mer sammen i komplekse systemer. På dette området foregår en rekke studier og arbeider på ulike samfunnsområder i dag, herunder NVEs egen rapport «Regulering av IKT-sikkerhet» fra 2017. En fellesnevner for mange av områdene er at det synliggjøres et behov for stadig mer veiledning, utvikling og læring i grensesnittet mellom myndigheter og bransje.

NVE har også gjennomført et internt forskningsprosjekt hvor målet var å utvikle et verktøy (spørreskjema og analytisk fremgangsmåte) for å følge utviklingen i sikkerhetstilstanden i energisektoren over tid<sup>21</sup>. Rapporten viser at 8 av 10 selskaper trenger hjelp fra leverandørene til håndtering og gjenoppretting når det skjer en IT-relatert feil, samtidig som det tilsynelatende ikke er god nok leverandørkontroll og mangler i sikkerhetsoppdateringene av operativsystemer og programvarer. Det ble blant annet konkludert med at det er et behov for økt kompetanse i bransjen når det gjelder outsourcing av IT-tjenester, i tillegg til at nivået for grunnsikringen for digitale systemer generelt må heves.

Undersøkelsen av bruken av IoT / IloT -løsninger i energiforsyningen bekrefter langt på vei funnene i NVE-prosjektet (NVE, 2017). Basert på intervjuene, tyder det på at selskapene i ingen eller liten grad gjennomfører tilsyn / revisjoner av leverandørenes informasjonssikkerhet, selv om det er indikasjoner på at oppmerksomheten knyttet til IKT – sikkerhet generelt øker i bransjen. Leverandørinformantene oppgav bl.a. at kundene i større grad stiller krav til sikkerheten i forkant av at avtaler blir inngått, men at de opplever enkelte ganger at virksomhetene ikke nødvendigvis selv forstår (omfanget av) hva de etterspør, noe som kan skyldes både bestillerkompetanse og et ønske om å «være på den sikre siden». Det kom også frem av intervjuene at det nok stilles mer krav til de mindre og nyetablerte leverandørene sammenlignet med de større leverandøren som virksomhetene er godt kjent med.

Erfaringsdeling og samarbeid mellom nettselskapene, samt mellom myndighetene og bransjen, er én måte å få til et felles kunnskapsløft om bruken av IoT / IloT – løsninger og spørsmål rundt informasjonssikkerhet. Som nevnt er det flere FoU-prosjekter og demoaktiviteter som kan bidra til dette, men mange av disse ser på problemstillinger som er aktuelle litt lenger frem i tid (smartgrid, forretningsmodeller, utnyttelse av fleksibilitet etc.). Når det gjelder spesifikt leverandør oppfølging (herunder oppfølging av informasjonssikkerhet) og det som allerede brukes av ny, smart sensorteknologi, er inntrykket at det i mindre grad samarbeides på tvers av selskaper for å utvikle kravspesifikasjoner og felles retningslinjer. Et slikt initiativ ble etterlyst i et av intervjuene. Når det er sagt, er utrulling av AMS et hederlig unntak, hvor en rekke initiativ og kartlegginger ble gjennomført av både myndigheter, sektor, forskningsinstitusjoner og bransjeorganisasjoner for å få best mulig kunnskap om denne endringen både i forkant, under og etter at målerne var utplassert.

---

<sup>21</sup> [http://publikasjoner.nve.no/rapport/2017/rapport2017\\_90.pdf](http://publikasjoner.nve.no/rapport/2017/rapport2017_90.pdf)

**Basert på ovenstående anbefales det å vurdere å videreføre og konkretisere studier/utredninger av regelverksutforming som tilrettelegger for ivaretagelse av forsyningsikkerheten og understøtter teknologisk utvikling i bransjen.**

**Videre gis det en anbefaling om at det tilrettelegges for at bransjen samarbeider om å utvikle felles retningslinjer for oppfølging av leverandørenes håndtering av informasjonssikkerhet. Herunder felles rammer for kravstilling til leverandører og gjennomføring av leverandørtilsyn/-revisjoner. Samtidig at det jobbes målrettet for å legge til rette for erfaringsdeling i eksisterende arenaer/forum.**

Norges vassdrags - og energidirektorat (NVE)  
Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning,

## Referanser

NOU 2015:13 Digital sårbarhet – sikkert samfunn.

NOU 2018:14 IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet.

NVE 2015:118 Teknologiskrifte i energiforsyningen. Studie om muligheter og sårbarheter.

NVE 2017:26 Regulering av IKT-sikkerhet. Et helhetlig og fremtidsrettet sikkerhetsregime for forsyningsikkerhet i en digitalisert energisektor.

NVE 2017:90 Informasjonssikkerhetstilstanden i energiforsyningen

Shahinzadeh et al (2019) IoT Architecture for Smart Grids.

Teknisk Ukeblad (2016). Sikkerhetsplattformer for innvevd utstyr i industriell IoT.

## Vedlegg I Intervjuguide

### Nettselskap

1. Hva legger dere i IoT / IloT – løsninger?
2. Hva har dere oppkopleet til nett i dag (på områdene som nevnes i a-e), og hva ser dere for dere kan koples opp de neste årene?
  - a. Kontrollsystemer
  - b. Hjelpesystemer
  - c. Vedlikeholdssystemer
  - d. Optimalisering / fleksibilitet
  - e. Hyllevarer vs spesialiserte løsninger?
3. Bruker underleverandørene deres noen oppkoplinger? Og til hva?
4. Hva er hensikten med oppkoplingen – og hva kan det gi tilgang til?
5. Hva har produsentene tilbudt dere?
6. Hva har dere foreslått for leverandørene?
7. Hva kommer dere til å etterspørre?
8. Hvilke leverandører ser dere som langt fremme på dette området? Hvem tilbyr hva?
9. Har dere noe inntrykk av hvilke standarder leverandørene jobber etter eventuelt
10. Hvilke muligheter og utfordringer gir digitalisering (IoT/IloT) i kraftforsyningen?

### Leverandør

1. Hva legger dere i IoT / IloT – løsninger?
2. Er dette et område dere har fokus på? Satsning/potensiale?
3. Hvilke produkter eller tilpasninger tilbyr og/eller leverer dere til nettselskapene i dag? Hvordan har IoT / IloT-løsninger blitt inkludert i produktene?
4. Hva brukes i dag i bransjen?
5. Hva tilbys «mest» (hyllevarer vs spesialtilpassede produkter?) – hva ønsker nettselskapene og hva ønsker dere å tilby?
6. Etterspørres det noen spesielle fremtidige løsninger, eller er det noen løsninger dere ønsker å utvikle/selge? Hvilke?
7. Hvilke muligheter og utfordringer ser dere ved økt digitalisering (IoT/IloT) i kraftforsyningen?
8. Finnes det noen standarder som stiller krav til produktene og leveransene på dette området? Hvilke standarder / regelverk følger dere eventuelt?

### Bransjeorganisasjon

1. Hva legger dere i IoT / IloT – løsninger?
2. Hvilket inntrykk har dere av bruk av IoT / IloT -løsninger i bransjen i dag og fremover?
  - a. Hva er i bruk?

- b. Mange som bruker løsningene?
  - c. Hva er strømningene i bransjen i dag – og hva ser dere som mest aktuelt de neste 5 årene?
3. Hva slags og hvilke prosjekter og initiativer kjenner dere til på området? Hva handler de om?
4. Er dette et område dere som miljø har fokus på? Hvorfor/hvorfor ikke?
5. Hvilke muligheter og utfordringer gir økt digitalisering (IoT/IIoT) i kraftforsyningen?
  - a. Hva oppfatter dere at bransjen tenker og fokuserer på?
  - b. Hva oppfatter dere at leverandører til bransjen er opptatt av og tilbyr?
  - c. Hvilke leverandører har fokus på dette?
  - d. Hva tenker dere - og hvorfor?

## Vedlegg II Oversikt over Smartgrid-prosjekter

Tabellen under beskriver noen relevante Smartgrid -prosjekter og piloter i norsk kraftforsyning. Informasjonen er hentet fra de aktuelle aktørenes og forskningssentrenes/prosjektenes hjemmesider i tillegg til henvisninger og omtaler på [www.smartgrids.no](http://www.smartgrids.no) (Smartgridsenteret). Denne listen er ikke fullstendig, og det forventes at det finnes andre pågående eller avsluttede initiativ og prosjekt som kunne inngått i en slik oversikt.

Prosjekt	Beskrivelse	Aktør	Pågående	Avsluttet
CINELDI	Senteret skal bidra til å digitalisere og modernisere distribusjonsnettet på en kostnadseffektiv, fleksibel og robust måte. Målet er at nettet skal håndtere samspill med smarte nettkunder, elektrisk transport, solcelleanlegg og annen fornybar kraft. Senteret er ett av åtte sentre som i 2016 ble tildelt statusen «Forskningssenter for Miljøvennlig Energi», og ledes av SINTEF Energi.	SINTEF Energi	X  (2016-2024)	
Coast Center Base (CCB) – Fleksibilitet hos stor industriell kunde	Formålet med fleksibilitetsundersøkelsen er å kartlegge kundefleksibilitet som alternativ til tradisjonell forsterkning av nettet. De lastene som normalt er mest fleksible (ikke er merkbar for brukerne) er den energien som er lagret termisk. Men på et stort industrielt anlegg som CCB foregår det også tester av pumper og motorer som kan gi store effekttopper, og det kan medføre kostnader ved å flytte disse utenfor morgen- og ettermiddagstoppene.	BKK Nett AS	X	
Demo Statnett FoU Pilotprosjekt Nord-Norge	I Demo Statnett FoU Pilotprosjekt Nord-Norge utvikles og testes løsninger som skal bidra til planlegging og drift av kraftsystemet i tråd med systemoperatøransvarets oppgaver (FOS).  Nye distribuerte systemer for måling og styring baner veien for smart drift og planlegging når systemoperatørene skal sikre effektiv og pålitelig leveranse av elektrisk energi. Nettbasert overvåking gir nye muligheter til effektiv distribusjon og utnyttelse av styresignaler.  I Statnett FoU Pilotprosjekt Nord-Norge har Statnett samlet flere av delprosjektene i foretakets Smart Grid-program. Enkeltvis og samlet skal delprosjektene utvikle nye modeller og verktøy som kan bli testet «live» i driftsmiljøet ved Regionsentralen i Alta.	Statnett	X	

## Norges vassdrags - og energidirektorat (NVE)

Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning.

Prosjekt	Beskrivelse	Aktør	Pågående	Avsluttet
EarlyWarn	<p>EarlyWarn prosjektet utvikler metoder basert på maskinlæring for å detektere og identifisere reelle og potensielle feilhendelser i transmisjons og distribusjons nettet. Prosjektets mål er å detektere hendelser under utvikling før det oppstår feil som kan påvirke sluttbruker, og dermed være i stand til å iverksette forebyggende tiltak for å unngå uønskede situasjoner.</p> <p>Det norske nettet er utstyrt med en rekke sensorer, og utviklingen går mot stadig større grad av instrumentering på alle spenningsnivå. Flere av disse sensorene registrerer spennings- og strøm-verdier kontinuerlig og med høy oppløsning. Noen instrumenter måler med opp mot 50 kHz oppløsning. Det er et premiss i prosjektet at målinger med så høy oppløsninger kan detektere mønstre eller signaturer som kommer i forkant av historiske uønskede hendelser slik at disse kan detekteres i forkant av fremtidige uønskede hendelser.</p>	SINTEF Energi	X  (2017-2021)	
Elnett21	<p>Formålet er å utvikle og demonstrere løsninger som kan takle et fremtidig økt effektbehov. Løsningene skal bidra til optimal bruk av eksisterende nett gjennom lokal produksjon (mikronett), lagring og styring av energi. Ved å ta i bruk en styringsplattform utviklet av Smartly ønsker man å få de ulike elementene til å fungere sammen på tvers av bygg og områder. Styringen gjøres ved hjelp av analyser og prognoser for både energiproduksjon og energiforbruk. Kunstig intelligens automatiserer denne styringen, både mot tradisjonelle behov i bygg og ikke minst mot de nye elementene som er stasjonære batterier, lokal sol- og vindenergiproduksjon samt lading av fly, busser, skip og biler.</p>	Avinor Forus næringspark Lyse Elnett Smartly Stavanger Havn	X  (2019-2024)	
ENERGYTICS	<p>Prosjektet skal demonstrere hvordan maskinlæring og kunstig intelligens kan øke nytteverdien av de nye smarte strømmålerene (AMS) som nettselskap har installert hos sluttbrukerne. AMS legger til rette for andre nytteverdier gjennom utnyttelse av sanntidsdata, og muligheten til å bygge opp gode databaser for historiske nøkkeldata fra distribusjonsnettet. Slike data vil kunne gi et bedre beslutningsgrunnlag for drift og investeringer. Dette er avgjørende for utviklingen av et smartere, mer fleksibelt og mer miljøvennlig energisystem, og at investeringene i nettet blir gjennomført så effektivt og optimalt for samfunnet som mulig. Prosjektet er finansiert av Forskningsrådet.</p>	Hafslund Nett SINTEF	X  (2017-2021)	
FASAD Feil - og	<p>Prosjektet har undersøkt hvordan ny smartgrid-teknologi kan utnyttes i det elektriske distribusjonsnettet til å redusere avbrudd i strømforsyningen og samfunnsøkonomiske kostnader ved avbrudd, bl.a. ved å ta i bruk ulike sensorer som kan oppdage når feil oppstår.</p>	Hafslund  SINTEF		X

## Norges vassdrags - og energidirektorat (NVE)

Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning,

Prosjekt	Beskrivelse	Aktør	Pågående	Avsluttet
avbruddshåndtering i smarte distibusjonsnett	Sensorene kan utnyttes for smartere feil- og avbruddshåndtering gjennom at feil i nettet raskere detekteres, lokaliseres og isoleres. Prosjektet inngikk i Demo Norge under Smartgridsenteret.			
IDE (Intelligent distribusjon av elektrisitet)	Hovedmålet er å demonstrere nye teknologier og digitale løsninger i stor skala, verifisere hvordan de fungerer, og estimere nytteverdi ved full skalering til distribusjonsnettet i hele Norge. Følgende løsninger skal demonstreres: 1) Demonstrasjon av automatisk spenningsregulering for fordelingstransformatorer 2) Demonstrasjon av nett-batterier, fjernstyrte effektbrytere og styringssystem 3) Demonstrasjon av nett-batterier og bilaterale avtaler for forbrukerfleksibilitet 4) Demonstrasjon av avansert løsning for selvhelende nett	Hafslund Nett Eidsiva Nett BKK Nett Tensio TN Norgesnett Skagerak Nett Agder Energi Nett Epos Consulting NTNU Smartgridsenteret	X	
Intersecure	Prosjektet har til hensikt å styrke rammeverk og metoder for risikostyring for smarte nett og interaksjonen med digitale systemer. Det inkluderer å identifisere og vurdere trusler og sårbarheter når SCADA-systemet integreres med andre IT-systemer. Systeminteraksjoner og avhengigheter, samt menneskelige og organisatoriske faktorer vil bli adressert i prosjektet. I tillegg skal prosjektet søke å identifisere, analysere og vurdere mulige risikoreducerende tiltak og barrierer.	Lyse Elnett Agder Energi Nett Hafslund Nett NVE NKOM SINTEF Digital SINTEF Energi NTNU	X  (2019-2022)	
IoTSec	Initiativet IoTSec - Sikkerhet i Tingenes Internett for Smarte Nett ble etablert i 2015 for å støtte opp under et smart elektrisitetsnett som er tilstrekkelig sikkert og respekterer personvern.  Prosjektet har to aspekter: etablere en kunnskapsklynge rundt sikkerhet for tingenes internett, og relatere forskningen til utfordringer som industrien og samfunnet har når det gjelder styring og kontroll av smarte nett.	UiO NTNU  Glitre Energi NU Fredrikstad Nett eSmart systems	X	

## Norges vassdrags - og energidirektorat (NVE)

Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning,

Prosjekt	Beskrivelse	Aktør	Pågående	Avsluttet
		NCE smart Movation		
NORFLEX	Prosjektet består av et overordnet demonstrasjonsprosjekt og tre piloter. Bruk av fleksibilitet skal bidra til reduserte nettinvesteringer og sikrere nettdrift. Hensikten er å se på nytten av å bruke fleksibilitet ved dimensjonering og drift av både transmisjonsnett og distribusjonsnett, hvordan fleksibilitet kan benyttes ved anstrengte situasjoner i kraftnett og hvordan fleksibilitet kan brukes til å levere systemtjenester. Husholdninger og bedrifter kan tjene penger på være fleksible med strømforbruket sitt, og selskaper kan samle opp og selge fleksibiliteten i markedet. Ved å kjøpe denne fleksibiliteten kan nettselskapene lette belastningen på strømmettet og spare penger ved at behovet for nettførsterkning blir mindre. Prosjektet har mottatt ENOVA-støtte	Agder Energi Glitre Energi Mørenett NODES Statnett	X  (Ut 2021)	
Pilot Flexibilitet	Prosjektet gikk ut på å utnytte fleksibiliteten i nettet på en bedre måte, ved å utvikle nye forretningsmodeller. Ved bruk av maskinlæring og algoritmer åpnes nye muligheter hvor alle elementer snakker med hverandre for å løse utfordringene og helst før de inntreffer. Resultatet av prosjektet var at transformatoren på Engene transformatorstasjon ikke ble overbelastet i testperioden (vinteren 2017) ved eksempelvis varmekabler hos storforbrukerne (bedriftene) ble koblet ut etter behov. Prosjektet demonstrerte hvordan endring og øking i fleksibiliteten er et godt verktøy for å drifte fornybar energi. Prosjektet er videreført gjennom NORFLEX.	Agder Energi Microsoft		X
PROsmart	ProSmart er et Kompetanseprosjekt (KPN-prosjekt) ved NTNU med start i 2015 og som ble delfinansiert av Energix-programmet. Med økende grad av kompleksitet og integrering av distribuert energiproduksjon stiller fremtidens kraftnett nye og store krav til håndtering av feil. Prosjektet søker å forbedre klassisk relevern i kraftnettet gjennom bruk av kommunikasjonsteknologi. Hensikten er økt pålitelighet, bedre feilhåndtering og høyere utnyttelse av kraftnettet, med redusert fare for store utfall. Den nyeste generasjon med releer er i stand til å kommunisere i sanntid og dra nytte av informasjon fra andre deler av kraftnettet.	NTNU		X

## Norges vassdrags - og energidirektorat (NVE)

Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning,

Prosjekt	Beskrivelse	Aktør	Pågående	Avsluttet
Sensorkuler	Lyse Elnett har testet ut sensorkuler, utviklet av Heimdall Power, som samler inn informasjon om tilstanden på kraftlinjen gjennom målinger av temperatur, vibrasjon og linjesig. Informasjonen brukes til å vedlikeholde og håndtere situasjoner før feil oppstår. Sensorkulene gir også informasjon om ledig kapasitet i strømmettet, som er viktig når det skal tas beslutning om å investere i nytt strømmnett eller om kostbare investeringer kan utsettes.	Lyse Elnett Heimdall Power	X	
Smartgridsenteret	Smartgridsenteret driver en nasjonal demokomiteé som har som mandat å bidra til etablering av komplementære demonstrasjonsaktiviteter hos energi-/nettselskapene innenfor smartgrids.		X	
Skagerak Energilab	Skagerak Energi og samarbeidspartnere har etablert et pilotanlegg for lokal produksjon og lagring av elektrisk energi ved Skagerak Arena i Skien. Prosjekt har tre hovedmålsettinger: <ol style="list-style-type: none"> <li>1. Demonstrere og verifisere utfordringer og muligheter knyttet til store solcelleanlegg</li> <li>2. Pilottesting og kompetansebygging på energilagring/batteriteknologi</li> <li>3. Skaffe erfaring knyttet til utveksling, tjenester, rammevilkår for lokal distribusjon av kraft/effekt</li> </ol> <p>I tillegg vil det være en arena for testing av teknologi, driftsmodus og forretningsmodeller.</p>	Skagerak Energi	X	
Smarte nettstasjoner	Totalt har 31 nettstasjoner i Stavanger sentrum og omegn blitt oppgradert med ny teknologi slik at de kan fjernstyres og overvåkes. Alle nettstasjonene ble fullautomatisert og ulike sensorer implementert. <p>Formålet var å verifisere:</p> <ul style="list-style-type: none"> <li>– Viktige behov ved ombygging og oppgradering av nettstasjoner</li> <li>– Teknologi og funksjonalitet</li> <li>– Kost/nytte-verdier</li> <li>– Fullskalaeffekter og verdipotensial ved utrulling i full skala</li> <li>– Dele opp og vurdere på hvilke områder, deler av nettet, kundegrupper og arbeidsprosesser</li> </ul>	Lyse Elnett ABB		X

## Norges vassdrags - og energidirektorat (NVE)

Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning,

Prosjekt	Beskrivelse	Aktør	Pågående	Avsluttet
	<p>Løsningene vil være kostnadseffektive og hvordan lønnsomhetsgraden fordeles innenfor ulike segmenter</p> <p>ABB leverte anleggene som er testet, som bestod av nye luftisolerte koblingsanlegg. Prosjektet mottok ENOVA støtte.</p>			

### Vedlegg III Eksempler på leverandører av IoT/IIoT-løsninger

Tabellen under gir eksempler på leverandører som tilbyr IoT/IIoT-produkter og løsninger. Beskrivelsene er hentet fra leverandørenes markedsplattformer, og er ikke kvalitetssikret med den enkelte aktør. Listen er heller ikke uttømmende, og det forventes at det finnes langt flere tilbydere i kraftforsyningen enn det som kommer frem av denne oversikten.

Aktør	Beskrivelse	Etablert
ABB	ABB er et teknologiselskap som leverer produkter til produksjon, overføring og distribusjon av kraft.	1988
Aidon	<p><b>Aidon@your service</b> leverer skeddersydde pakker med tjenester som er designet for å møte kundens behov, og inkluderer AMS service, Prosjektledelse, Power Grid Management, Service desk (tilgjengelige eksperter).</p> <p><b>Head-end system (HES)</b> inkluderer alle elementer i et komplett AMS-system, som kan integreres med nettselskapenes informasjonssystemer</p> <p><b>Energy Service Devices (ESD)</b> kombinere måler, kommunikasjon, allsidige sensorer og grensesnitt med effektiv prosesseringskraft.</p> <p><b>Effektiv kommunikasjon</b></p>	2004
Broentech Solutions AS	Broentech Solutions AS provides IoT (Internet of Things) technological infrastructures. This includes everything needed for an IoT application : • “Fog devices”, consisting of sensor-integration hardware with wireless radio antennas, • Gateway software to connect the “Fog” to the internet, • Cloud backend to connect to all gateways and users using REST API, • server-clusters to handle BigData storage and analysis, and finally, • End user controller and monitoring applications. These individual modules can be interchanged with other similar 3rd party modules, the customer simply chooses which modules are needed for their specific applications.	2012
Disruptive Technologies	Disruptive Technologies is a rapidly growing innovator in the IoT market and developer of the world's smallest commercial-grade wireless sensors. Our sensing solution based on these mini-sensors simplifies data collection and delivers the data securely to our partners' analytics programs in the cloud. Leading-edge companies build radically different smart solutions on our platform for Industry 4.0, commercial real estate, retail, food service and safety, and connected living applications. Together we enable facility managers to maximize space and keep	2013

## Norges vassdrags - og energidirektorat (NVE)

Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning.

Aktør	Beskrivelse	Etablert
	tenants happy, pharmacists to ensure drugs don't spoil, and engineers to protect critical assets. From predictive maintenance to proper refrigeration, we're connecting people and information to deliver Connected Change.	
Enfo	Enfo provides the right technology to the flexibility provider, so that they are able to forecast available flexibility from consumption, place bids with available flexibility to the grid company and remotely manage and dispatch flexible loads. Software – Microsoft.	2004
eSmart Systems	<p>eSmart Systems builds and delivers the next generation software solutions for inspections of powerlines, grid maintenance planning and energy flexibility optimization. We target utilities worldwide and offer reduced costs and prolonged asset life with the use of our AI-powered solutions.</p> <p><b>Connected Prosumer</b> provides the end user with the possibility to optimize the energy consumption, production and storage according to their energy contracts, all through a simple and visually soothing dashboard or app interface. <b>Connected Grid</b> collects internal and external data, performs real-time analytics and visualizes data in an intelligent top system that provides decision support for optimal operation, maintenance and planning of your grid. Cloud native, Connected Grid is built with the latest tools and technology. Connected Grid is scalable and robust, and designed to meet the challenges and opportunities a digital future brings. <b>Drones</b> for inspection.</p>	2012
Greenbird Integration Technology	There is a revolution going on in the energy business. Utilities depending on yesterday's business models will be outsmarted by digital utilities that will serve a society in need of smarter energy solutions. With <b>Utilihive</b> we empower utilities to be ready for the future in months instead of years, enabling them to optimize grid operations, embrace the data economy, and to become a platform operator for smart city applications infrastructure. Utilihive is a unique digital integration hub and iPaaS built for utilities. Greenbird believes that utilities powered by Utilihive can transform from traditional grid operators to platform operators that will create more innovative services in the new digital energy markets.	2010
Heimdall Power	Utvikler og leverandør av sensorkuler som overvåker strømmettet og varsler om feil før de skjer. Kulen inneholder sensorer som sender sanntidsdata tilbake til nettselskapet. Sensorkulene sender informasjon om tilstanden på kraftlinjene gjennom målinger av temperatur, vibrasjon og linjesig. Dette kan for eksempel varsle nettselskapet om snø og is på linjene. Selskapet kan sende ut mannskap for å gjøre vedlikehold før strømlinjen faller ned og gir strøbrudd. Sensorkulene kan settes på linjene under spenning.	2016

## Norges vassdrags - og energidirektorat (NVE)

Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning.

Aktør	Beskrivelse	Etablert
Kamstrup	Power Intelligence: Varsler og gir en oversikt over jordfeil i nettstasjonen på kart eller i en liste. AMS strømmålerne er optimalisert for smarte målesystemer, og tilbyr sømløs integrering i en lang rekke forskjellige systemer for innhenting av data via standardisert DLMS/COSEM-grensesnitt.	1946
KVS Technologies	Our mission is to provide the world with a safer and smarter way to continuously monitor the condition of transmission and distribution power grid, our most important infrastructure. KVS is developing the most complete end-to-end AI driven solution for autonomous drones to serve the mission of helping power grid companies work safer and smarter. Long distance remote control, Cyber-physical systems, Embedded computing, Robotics, Industry 4.0, Human Robot Interaction, Disaster Response Readiness , Artificial Intelligence, Drones, autonomous, fleet management, UAV, AI, machine learning	2015
Nordic Unmanned	Bruk av droner til inspeksjon av kraftlinjer og kartlegging av vegetasjon	2014
Powel	<p>Powel tilbyr verktøy som gir nettselskap mulighet til å prosjektere, vedlikeholde, kontrollere, analysere og overvåke strømnettet i sanntid. De leverer både kunnskapen og teknologien som skal til for å effektivisere arbeidsprosessene med enkle- og skybaserte løsninger.</p> <p><b>Powel Sensor Connect</b> samler og behandler ulike datakilder i strømnettet innenfor en og samme plattform. Dette gir nettselskapene innsikt i den faktiske tilstanden i strømnettet, helt ned på komponentnivå. Powel Sensor Connect registrerer feil og mangler på strømnettet, og datainnsamlingen er kontinuerlig og i sanntid.</p>	1996
Rejlers	<b>Quant Insight</b> representerer en portefølje av tjenester som gir helt nye muligheter i proaktiv drift og analyse av distribusjonsnettverket. Dette inkluderer moduler for jordfeilanalyse, rapportering av utfall, kapasitetsberegninger, spenningskvalitet. For eksempel kan Insight Storm vise virkningen av værforholdene på distribusjonsnettverket.	1998 (Norge)
Rutrinok	Tysk selskap, med kontor i Norge (Oslo). Tilbyr både komponenter og helhetlige løsninger for IoT og IIoT inn mot energiforsyningen.	1973
SafeBase	SafeBase tilbyr kundene å samle inn, tolke, lagre og visualisere data. Med <b>SensorHub</b> kan nettselskapene enkelt overvåke kvaliteten på strømmen de leverer og gjøre feilrettinger før det oppstår skader. SensorHuben kan kobles på transformatorkioskene for å ta ut informasjon fra strømnettet. Nettleverandørene kan da overvåke nettet og rette feil direkte fra driftssentralene.	2013

## Norges vassdrags - og energidirektorat (NVE)

Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning.

Aktør	Beskrivelse	Etablert
	Teknologiplattformen <b>SafeMon</b> kan brukes som et toppsystem for andre programvarer eller som et dashboard for data som vises utelukkende i SafeMon. Det kan bety alt fra å robotisere registrering av hendelser og tiltakene som kreves for å respondere og automatiske varslinger og alarmer, til visualisering av kompliserte og sammensatte datasett.	
Sensero	Sensero er en start-up med bakgrunn fra Entreprenørskolen ved NTNU som jobber med software-løsninger for nettselskaper. De har som mål å redusere nettselskapenes kostnader ved å utvikle løsninger for å innhente og analysere de store mengdene med sensordata nettselskapene får i dag.	ukjent
Siemens	Leverer bl.a. produkter for fordelingsnettene som omfatter nettstasjoner, fordelingstransformatorer, bryteranlegg, lavspenningstavler, friluftsbrytere, utstyr for automatisk seksjonering, sikringer og avledere.	1898 (Norge)
Sysco	Sysco leverer IT-tjenester med energinæringen som hovedområde. Syscos tilstandsmøll bygger på automatisk innlasting av data, kombinert med maskinlæring, slik at modellenes presisjon øker med mengden av tilgjengelig datagrunnlag. Modellen trenes på kjente feil, og ferdig modell brukes deretter for å gi en prediksjon på risiko for feil på eksisterende kabelnett. MVP analyseapplikasjon som gir nettselskaper mulighet til å bygge avanserte modeller for prediksjon av levetid på jord- og sjøkabler i distribusjonsnettene. Systemet henter informasjon om avbrudd og topologi fra proprietære systemer, og genererer prediksjoner på sannsynlighet for feil på den enkelte komponent.	2004
Validér	Validér bearbeider og analyserer innsamlede data fra nettselskapenes AMS-infrastruktur og visualiserer all informasjon i en oversiktlig og digital dashbord-løsning hos nettselskapene.	2013
Verico	Verico tilbyr software til digitalt sikkerhetskort og adgangsstyring.  <b>Permitto</b> - adgangskontroll gir full styring på hvem som til enhver tid er bemyndiget og gitt tilgang til hvilke anlegg samt hvem som til enhver tid oppholder seg i disse anleggene – både av internt og eksternt personell. Gjennom Permitto-appen på telefonen, kan personell melde seg inn og ut av anlegg. Løsningen er utvidet med støtte for prosjekter og HMS-kort (byggekort), nøkkelhåndtering, HMS-meldinger tilknyttet anlegg/prosjekter, samt en rekke mindre utvidelser.	1999



NVE

## Norges vassdrags- og energidirektorat

---

MIDDELTHUNSGATE 29  
POSTBOKS 5091 MAJORSTUEN  
0301 OSLO  
TELEFON: (+47) 22 95 95 95

[www.nve.no](http://www.nve.no)