SINTEF

Rapport

Omarbeiding av veileder til sikkerhet for "Avanserte måle- og styringssystemer" (AMS) i avregningsforskriften

Forfattere:
Hanne Sæle, Maren Istad, Martin Gilje Jaatun

Rapportnummer: 2022:00400

Oppdragsgiver(e) :
NVE - RME

SINTEF Energi AS
Postadresse:
Postboks 4762 Torgarden
7465 Trondheim

Sentralbord: 45456000

energy.research@sintef.no

Foretaksregister:
NO 939 350 675 MVA

Rapport

Omarbeiding av veileder til sikkerhet for "Avanserte måle- og styringssystemer" (AMS) i avregningsforskriften

EMNEORD
AMS
Informasjonssikkerhet
Avregningsforskriften

VERSJON
1.0

DATO
2022-04-19

FORFATTER(E)
Hanne Sæle, Maren Istad, Martin Gilje Jaatun

OPPDRAGSGIVER(E)
NVE - RME

OPPDRAGSGIVERS REFERANSE
Catharina Hovin

PROSJEKTNUMMER
502003168

ANTALL SIDER
94

SAMMENDRAG
Denne rapporten er utarbeidet for RME i forbindelse med oppdraget "Omarbeidelse av veileder til sikkerhet for "Avanserte måle- og styringssystemer" (AMS) i avregningsforskriften. Oppdraget ble etablert etter en anbudsrunde høsten 2021.

Denne rapporten beskriver arbeidet fram mot en omarbeidet veileder til sikkerhet i AMS. Det er gjennomført en litteraturstudie basert på relevante dokumenter knyttet til utvikling av sikkerhet i AMS, og gjeldende regelverk knyttet til sikkerhet for AMS er presentert. I tillegg er det gjort en vurdering av hvordan NSMs grunnprinsipper for IKT-sikkerhet passer med gjeldende regelverk.

Teksten til ny veileder er presentert i Vedlegg B.

UTARBEIDET AV
Hanne Sæle

SIGNATUR
Hanne Sæle (May 2, 2022 09:19 GMT+2)

KONTROLLERT AV
Henning Taxt

SIGNATUR
Henning Taxt (May 6, 2022 14:04 GMT+2)

GODKJENT AV
Knut Samdal

SIGNATUR
Knut Samdal (May 6, 2022 14:11 GMT+2)

RAPPORT NR.
2022:00400

ISBN
978-82-14-07519-9

GRADERING
Åpen

GRADERING DENNE SIDE
Åpen

Innholdsfortegnelse

1 Innledning

Denne rapporten er utarbeidet for RME i forbindelse med oppdraget "Omarbeidelse av veileder til sikkerhet for "Avanserte måle- og styringssystemer" (AMS) i avregningsforskriften. Oppdraget ble etablert etter en anbudsrunde høsten 2021.

Hovedmålsettingen for oppdraget er å omarbeide veiledere til sikkerhet i AMS, som skal:

- innholdsmessig bygge på forrige veileder til sikkerhet i AMS samt rapport 44/2017 og 34/2019
- opplyse om overlappende regelverk (for eksempel personopplysningsloven og kraftberedskapsforskriften)
- kunne fungere som en interaktiv veileder på web

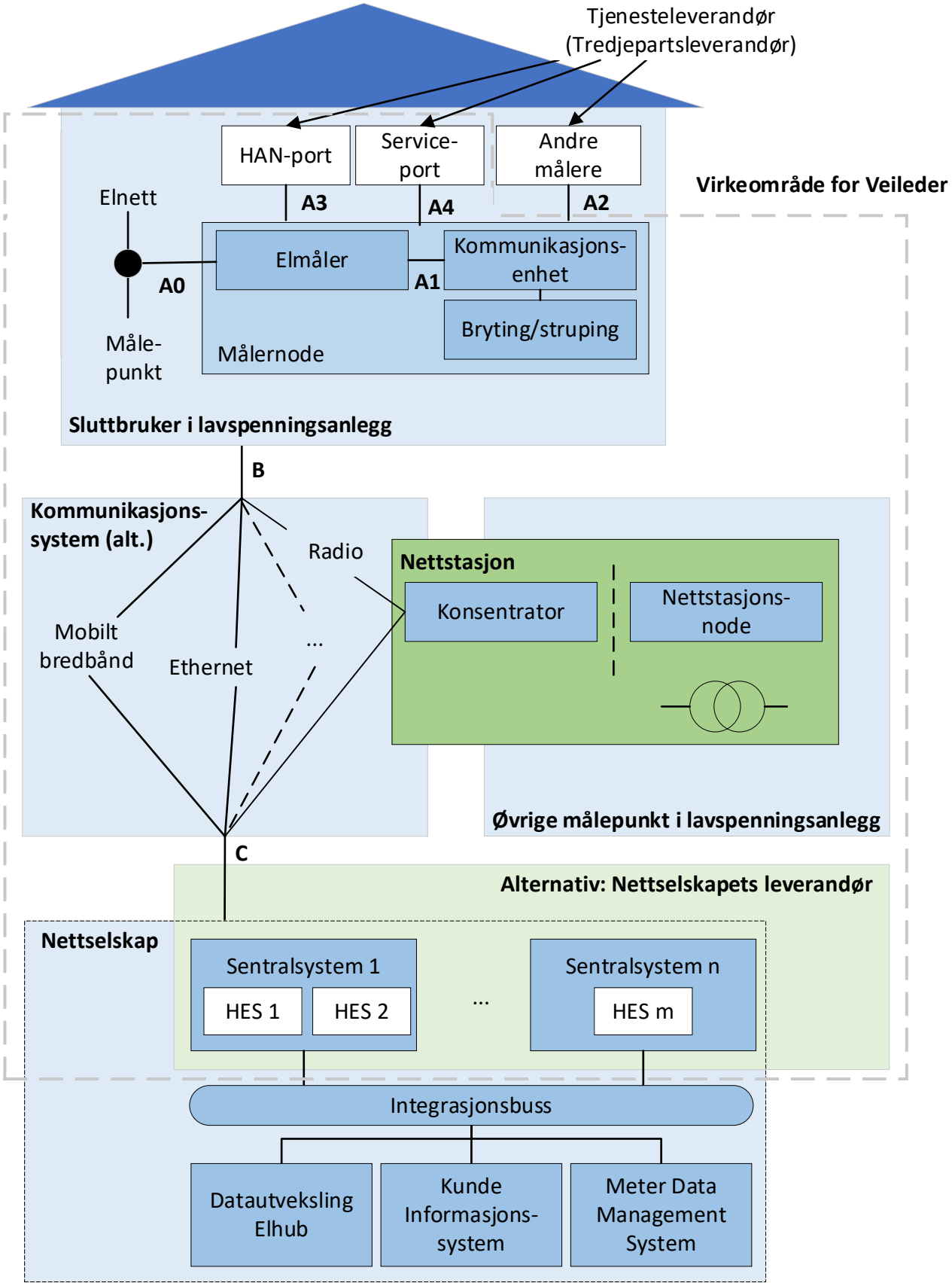
Denne rapporten beskriver arbeidet fram mot en omarbeidet veileder til sikkerhet i AMS. Det er gjennomført en litteraturstudie basert på relevante dokumenter knyttet til utvikling av sikkerhet i AMS, og gjeldende regelverk knyttet til sikkerhet for AMS er presentert. I tillegg er det gjort en vurdering av hvordan NSMs grunnprinsipper for IKT-sikkerhet passer med gjeldende regelverk.

Teksten til ny veileder er presentert i Vedlegg B. Strukturen på veilederen er basert på samme mal som veileder til kraftberedskapsforskriften [1].

Strukturen i veileder er basert på kravene (a-g) i avregningsforskriften § 4-6 Krav til sikkerhet for AMS [2].

Veileder har tatt utgangspunkt i at AMS er definert til å gjelde fra måler til sentralsystemet hos nettselskapet, inkl. kommunikasjonssystemet imellom. Systemer som evt. kobles til bak sentralsystemet, eller foran måler hos kunde, er ikke en del av AMS, men sikkerhetsnivået skal likevel opprettholdes. En illustrasjon av AMS og virkeområde for veileder, er vist i figur 1.1.

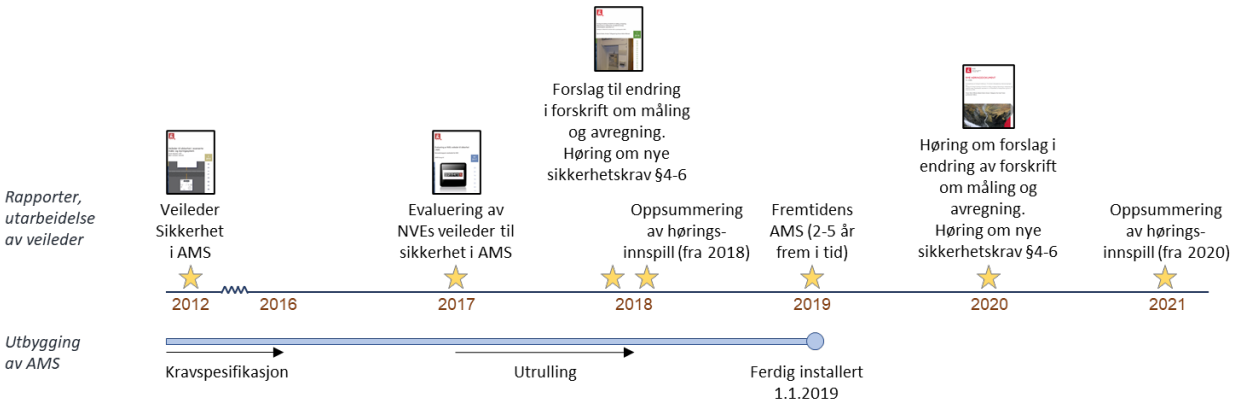
Figuren viser målepunkt i lavspenningsanlegg – både for sluttbruker og øvrige målepunkt, slik det er definert i Avregningsforskriften [2]. En mer detaljert beskrivelse av AMS-infrastruktur er gitt i Vedlegg B.



Figur 1.1 Illustrasjon av AMS-infrastruktur og virkeområde for veileder

2 Grunnlag for etablering av ny veileder – litteratur og regelverk

Det er gjennomført en litteraturstudie i forbindelse med utarbeidelse av ny veileder til sikkerhet i AMS, for å kunne basere oppdateringene på tidligere arbeid som er gjennomført siden forrige veileder ble ferdigstilt i 2012 [3] og forskriftsendringer som har skjedd i samme periode. Fokus i litteraturstudien har vært på temaer som er relevante for sikkerhet i AMS. Flere av dokumentene viser hvordan bl.a. krav og teknologier har utviklet seg, parallelt med økt erfaring med AMS. En oversikt over de viktigste dokumentene i litteraturstudien, og hvordan utgivelsen av disse er i forhold til utbygging av AMS, er vist i figur 2.1.



Figur 2.1 Tidslinje for dokumentene som inngår i litteraturstudien

2.1 Veileder til sikkerhet i avanserte måle- og styringssystem (Rapport 7/2012)

Ifølge forskriftskrav skulle utrullingen av AMS ferdigstilles innen 1. januar 2019. I avregningsforskriften som gjaldt da, var det kun kravet §4-2 g) som påla nettselskapene å sikre sine system, inkludert kommunikasjonsløsninger, mot uautorisert tilgang. Basert på dette forskriftsleddet, ble det i 2012 utarbeidet en egen veileder til sikkerhet i AMS [3], som beskriver hvordan nettselskapene kan oppfylle kravet i §4-2 g). Veilederen gjaldt for innsamlingssystemet – fra målepunktet hos kunden til sentral-systemet hos nettselskap, samt kommunikasjonssystemet. Dette er tilsvarende virkeområde som den nye veilederen, beskrevet i Vedlegg B.

Veilederen fra 2012 presiserer at nettselskapet er ansvarlig for informasjonssikkerheten for hele AMS-løsningen, også for de delene som eventuelt settes ut til tjenesteleverandør, og den gir også noen eksempler på sikkerhetstiltak som kan implementeres i AMS-løsninger for å kunne bidra til oppfyllelse av forskriftens krav §4-2 g). Kravene til sikkerhet er overordnet og gir ingen detaljerte føringer utover at nettselskapene har ansvaret for sikkerheten.

I veilederen fra 2012 er det tatt høyde for at man velger bryte - og strupefunksjonalitet med muligheter for masseutkoblinger. I ettertid er krav knyttet til bryterfunksjon overført til kraftberedskapsforskriften [4].

I veilederen er det beskrevet ulike sikkerhetsområder, og for hver av disse er det beskrevet kontrollmål og eksempler på hvordan kontrollmålene kan oppnås. For hvert kontrollmål er det gitt eksempler på tiltak, prosedyrer o.l. for å oppnå kontrollmålet, begrunnelse/hensikt med kontrollmål og supplerende veiledning (ved behov). En tilsvarende struktur er brukt i ny veileder (Vedlegg B). En oversikt over sikkerhetsområder og kontrollmål er gitt i tabell 2.1.

Tabell 2.1 Sikkerhetsområder og kontrollmål (Basert på [3])

Sikkerhetsområde	Kontrollmål
A. Krav til nettselskapet i henhold til forskrift	A.1 Robust sikkerhetsfunksjonalitet A.2 Sikkerhet i kommunikasjon i AMS-løsningen A.3 Utsetting av utrulling og/eller drift av AMS-løsningen til tredjepart
B. Overordnet sikkerhetsarbeid rundt AMS	B.1. Etablering og oppfølging av sikkerhetskrav B.2 Risiko- og sårbarhetsanalyse B.3 Oppdatert dokumentasjon av AMS-løsningen B.4 Sikkerhetsavtaler
C. Kontroll med tilgang til system og utstyr	C.1 Tilgangskontroll - system C.2 Identifisering og autorisasjon av enheter C.3 Identifisering og autorisering av eksternt utstyr C.4 Kontroll med integriteten til programvare C.5 Elektronisk beskyttelse mot ondsinnet programvare og inntrengning C.6 Oppbevaring av sikkerhetssertifikater og krypteringsnøkler
D. Overvåking og håndtering av hendelser	D.1 Kontroll med sårbarheter i programvare D.2 Logging og overvåking D.3 Avviks- og hendelseshåndtering D.4 Katastrofehåndtering og –øvelser D.5 Sikkerhetskopier og gjenoppretting
E. Endrings- og versjonskontroll	E.1 Kontroll med endringer i AMS E.2 Oversikt over versjoner i program- og maskinvare
F. Fjerntilgang til AMS-løsningen	F.1 Fjerntilgang til AMS fra tredjepart eller leverandør
G. Fysisk beskyttelse av AMS-løsningen	G.1 Beskyttelse mot fysisk uautorisert tilgang til AMS-utstyr
H. Bryte- og strupefunksjonalitet	H.1 Beskyttelse av bryte- og strupefunksjonalitet
I. Elektromagnetisk interferens (EMI)	I.1 Beskyttelse mot EMI

2.2 Evaluering av NVEs veileder til sikkerhet i AMS (Rapport 44/2017)

Mens utrulling av AMS pågikk, ble det i 2017 gjennomført en evaluering av veileder til sikkerhet i AMS [3]. Dette ble gjort i samarbeid med nettselskap og leverandører, for å hente inn erfaringer med bruk av veileder og å få innspill til forbedringer av innholdet. Denne evalueringen er beskrevet i NVE-rapport 44/2017 [5]. Anbefalingene som er gitt, er oppsummert i tabell 2.2, og disse er relevante for arbeidet med oppdatering av veileder til sikkerhet for AMS.

Tabell 2.2 Anbefalte endringer i veileder

Tema	Anbefaling
Generelt	▪ Veileder til sikkerhet i AMS må avstemmes mot andre veiledere, rundskriv og forskrifter som nettselskapene må forholde seg til. ▪ NVE må være tydelig på at de ønsker kontinuerlige tilbakemeldinger fra bransjen (nettselskap, leverandører, ...) om eventuelle gap mellom eksisterende teknologi, behov og gjeldende lover og krav.
Form/struktur	▪ Dagens veileder har en god, oversiktlig og logisk struktur, og det anbefales at denne videreføres. ▪ Sikkerhetsområdene bør beskrives med hensikten med sikkerhetsområdet først, før supplerende veiledning nevnes. ▪ Følgende flyttinger anbefales: • A.1 Robust sikkerhetsfunksjonalitet og A.3 Utsetting av utrulling og/eller drift av AMS-løsning til tredjepart flyttes til kapittel B ang. Overordnet sikkerhetsarbeid rundt AMS. • Sikkerhet i kommunikasjon i AMS-løsningen anbefales flyttet til kapittel C ang. Kontroll med tilgang til system og utstyr. Punktet bør plasseres før C.6, som også gjelder kryptering og krypteringsnøkler. • Dagens kap. A.3 bør endre navn til "Tjenesteutsetting", for å kunne inkludere allianser, skytjenester o.l..
Tema/sikkerhets-områder	▪ For å ytterligere tydeliggjøring av at veilederen gjelder AMS, bør forkortelsen "AMS" være med i navnet på veilederen.
Veilederens levetid	▪ Ved å korrigere på krav direkte knyttet til teknologi, kan tema/kontrollområder i denne veilederen også være dekkende etter at AMS er satt i drift.
Bruk av veileder	▪ Veilederen er et viktig dokument for å sikre et kontinuerlig forbedringsarbeid knyttet til sikkerhet i AMS.
Detaljnivå	▪ Temaene/kontrollmålene bør gjelde for alle nettselskap.
Tydeliggjøring av ansvar	▪ Nettselskapenes ansvar er tydelig beskrevet i dagens veileder, men det ønskes en mer utdypende beskrivelse, spesielt når det oppstår allianser som ivaretar en del av oppgavene som i utgangspunktet ligger hos nettselskapet.
Referanse til lovgivning/ forskrifter	▪ Veileder bør referere til relevante gjeldende lovverk (andre enn forskrift §4-2 g)), og det anbefales å avstemme veileder mot andre veiledere, rundskriv og forskrifter nettselskapet må forholde seg til. ▪ I risikoevalueringen som lå til grunn for veilederen ble det imidlertid påpekt at skadepotensialet ved utro tjenere er betydelig. Dette fremheves også i NOU 2016:19 Samhandling for sikkerhet. I [5] ble det ikke anbefalt at paragrafen om bakgrunnssjekk fjernes, men det kan være hensiktsmessig å nyansere kravet noe, for å gjøre det mer hensiktsmessig og harmonisert med andre deler av nettdrift og kraftsystem.
Tilgjengelighet AMS-data	▪ Ulike AMS-data (kWh/nettnytte) kan brukes til ulike oppgaver hos et nettselskap, og det øker også viktigheten at man får tilgang til disse data i de nødvendige arbeidsprosessene. Ingen av dagens tema/sikkerhetsområde omhandler tilgang på data. ▪ Tema C omhandler Kontroll med tilgang til system og utstyr. Ved å endre tittelen på temaet til Kontroll med tilgang til system, utstyr og informasjon kan det etableres et nytt kontrollområde C.7 Sikring av tilgjengelighet av informasjon med fokus på tilgjengelighet av AMS-data.

Tema	Anbefaling
Beskrivelse av kommunikasjons-teknologi	▪ Teknologien har utviklet seg etter at dagens veileder ble gitt ut, og teksten om kommunikasjonsteknologier bør derfor oppdateres. ▪ Beskrivelsen om at andre tjenesteleverandører skal kunne kommunisere over AMS er ikke lenger relevant.
Tilgangskontroll	▪ I veileder er det spesifisert tilgangskontroll for kritiske operasjoner i AMS-infrastruktur, bl.a. bryter i AMS-måler hos kunde. Det er bra at kritiske operasjoner ikke skal kunne utføres av én person alene. Det anbefales å videreføre dette, og videre presisere at den som gir tilgang til funksjonen ikke skal kunne utføre tilsvarende funksjon.
Aktører	▪ Det er ingen begrensninger med hensyn til tjenesteutsetting til under-leverandører. Beskrivelsen av driftsselskap i veilederen tar ikke høyde for alliansene som nå er inngått. I veilederen bør det være beskrivelse av hvordan slike allianser vil kunne påvirke sikkerheten, og hvordan nettselskapene bør håndtere dette. ▪ Det er ikke godt nok beskrevet hvordan leverandørkjeden skal følges opp. Behovet for en god prosjektorganisasjon og -gjennomføring for å ivareta sikkerhet i AMS bør tydeliggjøres.
Sikkerhet/Risiko-avtaleverk og testing	▪ Basert på diskusjoner om sikkerhet/risiko knyttet til avtaleverk og testing på arbeidsmøtene, er det gitt noen anbefalinger (Tabell 7.8 [5]).
Tilleggspunkter	▪ Nye versjon av veileder til sikkerhet i AMS bør omhandle tjenesteutsetting og komplekse leverandørmodeller i større grad enn i dag. Det må poengteres at tjenesteutsetting ikke endrer på nettselskapenes ansvar, og at det gir noen utfordringer sammenlignet med intern drift: samhandling, kommunikasjonsflyt, håndtering av avvik og uønskede hendelser. ▪ Med en rekke mulige tilleggstjenester og kobling mot Elhub og DMS/SCADA, er det behov for å skissere en tydeligere grense enn i dag for hva som dekkes av veileder til sikkerhet i AMS. ▪ Veilederen er utarbeidet for å sikre en myndighetspålagt AMS-infrastruktur planlagt for innsamling av kWh-verdier til bruk for avregning, men de siste årene har det blitt stadig mer fokus på nettnyttedata. Innsamling og utnyttelse av disse dataene forventes å være og/eller bli berørt av annen lovgivning, eksempelvis lover og forskrifter med bestemmelser om personvern. Det kan være hensiktsmessig å tydeliggjøre at bruk av veilederen ikke nødvendigvis sikrer overensstemmelse med denne typen lovgivning.

2.3 Fremtidens Avanserte Måle- og Styringssystem (AMS) (Rapport 34/2019)

I 2019 ble det gjennomført en kartlegging av relevante patentsøknader og forskningsprosjekter, og sammen med representanter fra bransjen ble det kartlagt hvordan man ser for seg utviklingen av AMS i en tidshorisont på to til fem år. Dette er beskrevet i rapporten 34/2019 [6].

I følge [6], er sikkerhet, i alle betydninger av begrepet; informasjonssikkerhet, cybersikkerhet og person-vern, viktige områder i forskningen som en konsekvens av at kommunikasjon helt ned til sluttbrukere er noe nytt og kan åpne for andre typer sikkerhetshendelser enn nettselskapene er vant med. Sikkerhets-hendelser kan bli en "showstopper" for nytteverdi av AMS og er derfor viktig å ha kontroll på.

Videre skriver rapporten følgende om sikkerhet, knyttet til utviklingen i løpet av 2-5 år:
"Utviklingen kan også medføre at man må tenke annerledes på IT-sikkerhet. Tradisjonelt har sikkerhet vært realisert ved å lukke systemene inne, mens det i dag er diskusjoner om skyløsninger driftet av selskaper som har sikkerhet som sitt hovedområde. Ingen nettselskap ønsker spesialsystemer som låser data til et gitt format eller har utfordringer med å kommunisere/utveksle data med andre systemer. Her står bransjen overfor et paradigmeskifte fra ferdig leverte spesialsystemer til å leie inn leverandører for å løse spesifikke problemer/ funksjoner. Det bør legges til rette for at slike applikasjoner lett kan tas i bruk uten ressurs-krevende endringer i spesialsystemer."

Og

"Det er sannsynlig at IT-løsninger vil endre seg fra spesialsystemer/fagsystemer til enkeltapplikasjoner for å løse en funksjonalitet, det forventes at flere analyser/beregninger vil gjennomføres lokalt i AMS-måler, og at utviklingen i ny funksjonalitet fokuserer mer på å løse oppgaver etter behov i stedet for å følge den enkeltes leverandør sin utvikling av fagsystemer."

Den overnevnte utviklingen krevet et helt annet fokus på sikkerhet enn det tradisjonelt har vært i bransjen.

2.4 Forslag til endring i forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. (Rapport 1/2018)

NVE sendte i 2018 på høring et forslag til bestemmelser og endringer i forskrift av 11. mars 1999 nr. 301 om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester (avregningsforskriften) [2]. Formålet er å tydeliggjøre hvilke krav som stilles til sikkerhet i avanserte måle- og styringssystemer (AMS) [7].

I høringsdokumentet er det presisert at *AMS er et informasjonssystem som i likhet med andre informa-sjonssystemer må sikres mot uønskede hendelser. Informasjonssikkerhet handler om konfidensialitet, integritet og tilgjengelighet,*

hvor

- *Konfidensialitet* handler om å beskytte informasjon mot at uønskede får tilgang til den.
- *Integritet* handler om hvorvidt en kan stole på at informasjon er korrekt (at den ikke uønsket har blitt endret).
- *Tilgjengelighet* handler om i hvilken grad informasjon er tilgjengelig for rettmessige brukere når de trenger det.

NVE begrunnet forskriftsendringen i behovet for å stille tydeligere krav til hva plikten til å sikre AMS innebærer. I tillegg til krav til sikkerhet i AMS gitt gjennom forskrift for måling og avregning, er det også andre relevante regelverk, som dekker ytterligere behov. Det gjelder bl.a.:

- Kraftberedskapsforskriften
    - Stiller krav til et minimums sikkerhetsnivå gjennom grunnsikring av IKT-systemer, og inkluderer også AMS. Dette inkluderer nettselskapets informasjonssystem for overføring av måleverdier til Elhub, og det foreligger sikkerhetskrav ved overføring mellom nett-selskapets sentralsystem og Elhub som ivaretar konfidensialitet, integritet og tilgjengelighet. Dette ivaretar et tilstrekkelig sikkerhetsnivå for den resterende delen av måleverdikjeden som ikke er en del av AMS.
    - Det er foreslått krav som ivaretar konfidensialitet, integritet og tilgjengelighet.

- Beskyttelse av bryterfunksjonalitet i AMS er inkludert.

- Personvern/Personopplysningsloven
  - Måleverdier gir opplysninger om strømforbruket til personer som bor i boligen måleverdiene er knyttet til, og er dermed definert som personopplysninger. Datatilsynet har uttalt at personopplysningsloven stiller krav til hvordan slike data skal behandles og sikres.
  - Nettnyttedata som på tilsvarende vis kan si noe om hva enkeltpersoner gjør i hjemmet, vil også falle inn under definisjonen av personopplysninger.
  - NVE ønsker å sikre avregningen og måleverdikjeden, men regler om sikkerhet i AMS vil likevel dekke flere krav som stilles til sikring av personopplysninger. Ansvaret for å følge opp personregelverket, er det den enkelte virksomhet og Datatilsynet som har.
  - Nettselskapene må i henhold til personvernregelverket etablere tiltak for å sikre at disse måleverdiene kun er tilgjengelig for dem de er tiltenkt, at måleverdiene er riktige, og at de er tilgjengelig når det er behov for dem.
- Krav til elektrisitetsmålere (elmålerforskriften)
  - Elmålerforskriften stiller tilstrekkelige krav til beskyttelse mot manipulering av måleverdier i AMS i svindeløyemed, og stiller derfor ikke ytterligere krav til beskyttelse mot manipulering av måleverdier i AMS. Justervesenet er ansvarlig for å følge opp krav i forskriftene.

I høringsdokumentet ble det foreslått sju tilleggskrav, for å gi AMS et høyere sikkerhetsnivå enn grunnsikringsnivået. Begrunnelse for innføring av de ulike kravene er:

a) Alle enheter skal godkjennes før de gis tilgang til systemet, for å hindre at falske AMS-målere eller andre enheter kommuniserer til eller i AMS. En slik godkjenning kan gjennomføres i AMS eller i tilkoblede systemer. Kravet om godkjenning gjelder kun enheter som kommuniserer til eller i AMS, som elektrisitetsmålere og enheter benyttet av servicepersonell for tidsbegrenset tilkobling til AMS-måleren. Dette gjelder ikke sluttbrukerens private utstyr tilkobling HAN-grensesnitt, da det kun kommuniserer ut til kunden.

   Programvare skal godkjennes før den installeres i AMS, f.eks. ved at nettselskapet eller nettselskapets leverandør kontrollerer at et sammendrag av programkoden (sjekksum), samsvarer med tilsvarende sammendrag fra programvareleverandøren.

b) For å hindre at uvedkommende får innsyn i data, må kommunikasjonen i AMS sikres fra ende-til-ende, ved at sikkerheten skal opprettholdes i alle ledd i kommunikasjonsflyten i AMS.

   I tillegg skal konfidensialitet for informasjon om AMS-måler og programvare med betydning for måleverdikjeden sikres. Slik informasjon kan eksempelvis være oversendelse av programvare-oppdateringer eller krypterings- og tilgangsnøkler.

c) Programvare i AMS skal til enhver tid være oppdatert, for å motvirke at AMS-målere og andre enheter i AMS forblir sårbare dersom sikkerhetshull oppdages. Dette krever nødvendigvis at også AMS-målere og andre viktige enheter må kunne oppdateres.

d) Et sikkerhetsbrudd i AMS, som skjer andre steder enn i nettselskapets sentralsystem, skal ikke kunne få betydning for andre deler av, eller hele AMS. Dersom for eksempel krypteringsnøkler for en AMS-måler kommer på avveie, skal ikke dette medføre tilgang til andre AMS-målere eller sentralsystemet.

e) AMS skal for det første installeres med tilstrekkelig evne eller kapasitet for å til enhver tid kunne utføre tiltenkte oppgaver, f.eks. tilstrekkelig dimensjonert kommunikasjonsinfrastruktur for å kunne fjernoppdatere programvare eller at nettnyttedata kan oversendes uten at dette blokkerer for oversendelse av måleverdier.

   Enheter i AMS skal ikke ha funksjonalitet ut over det som er nødvendig for deres bruksoppgaver, siden sikkerhetsrisikoen vil øke dersom AMS leveres med økt funksjonalitet. Når sikkerhetsrisikoen øker samtidig som funksjonaliteten ikke gir noen nytteverdi, er det bedre om funksjonaliteten ikke er til stede.

f) Det stilles krav om logisk eller fysisk skille mellom AMS, og andre IKT-nettverk som nettselskapet eller nettselskapets leverandør benytter, for å hindre at IKT-nettverk blir attraktive angrepsmål for uvedkommende som ønsker tilgang til AMS. Kvaliteten på eventuelle logiske skiller må samsvare med risiko forbundet med tilgang til de adskilte nettverkene.

g) AMS-målere leveres med grensesnitt som display, HAN-port, blinkediode (S0-port) og M-Busport, og kan også i varierende grad leveres med andre grensesnitt, f.eks. et grensesnitt for servicepersonell (IR-port). Slike grensesnitt kan gi tilgang til enkeltkunders måleverdier, gjengitt med en hyppighet som kan si noe om aktiviteten i boligen. Datatilsynet har uttalt at personopplysningsloven stiller krav til hvordan slike data skal behandles, og at dataene derfor trenger en viss beskyttelse, enten fysisk eller ved kryptering.

   Nettselskapene skal innføre tiltak som begrenser tilgang til AMS-målerens grensesnitt. Nettselskapene kan selv vurdere hvilken løsning som er mest hensiktsmessig, basert på risiko og bedriftsøkonomiske vurderinger.

2.5 RME Høringsdokument (Rapport 2/2020)

Dette dokumentet er todelt, hvor første del er en konsepthøring om hvordan 15 minutters balanse-avregning kan innføres i Norge, og den andre delen er en høring om konkrete endringer i avregnings-forskriften om funksjonskrav og krav til sikkerhet for AMS [8].

I høringsdokumentet ble følgende definisjon av AMS gitt:
«Toveis informasjons- og kommunikasjonssystem fra og med elektrisitetsmålere benyttet til avregning for de enkelte målepunkt, til og med sentralsystemet hos nettselskap eller nettselskapets leverandør.»

Definisjonen inkluderer alle målepunkt benyttet for avregning i lav- og høyspenningsanlegg, inkludert alle målepunkt for uttak, innmating og utveksling mellom nettområder.

I tillegg til at [8] foreslår en ny definisjon av AMS, foreslås noen ytterligere presiseringer for AMS:

- For AMS i øvrige målepunkt enn de knyttet til sluttbrukere i lavspenningsanlegg, foreslår RME et nytt funksjonskrav om at AMS skal lagre måleverdier med en registreringsfrekvens på maksimalt 15 minutter.
- AMS skal registrere flyt av aktiv og reaktiv effekt i begge retninger.
- AMS i målepunkt for sluttbrukere i høyspenningsanlegg, skal ha et grensesnitt som legger til rette for kommunikasjon med eksternt utstyr basert på åpne standarder.
- Nye sikkerhetskrav for AMS i alle målepunkt.

Kravet om display på måleren er erstattet av HAN-porten – men det som kobles til HAN-porten er ikke en del av AMS.

I dette høringsdokumentet ble det foreslått nye krav til sikkerhet for AMS (Ny §4-6, beskrevet i kapittel 3.1), basert på følgende underlag:

I kraftberedskapsforskriften [4] stilles det krav om at:

- kommunikasjonen fra og med elektrisitetsmåleren til nettselskapets sentralsystem, enten krypteres eller foregår i et lukket nett som er stengt for uvedkommende
- nettselskapet bruker autentisering mellom elektrisitetsmåler og nettselskapets sentralsystem og
- det skal være mulig å legge inn passord som beskytter mot konfigurasjon av elektrisitetsmåleren via kommunikasjonskanalen mellom elektrisitetsmåleren og sentralsystemet.

I REN 4011[1] stilles det krav om at

- Elektrisitetsmåler og all dens kommunikasjon skal være «*godt sikret mot uautorisert tilgang*.»
- Autentisering og kryptering som benyttes i systemet, skal bygge på anerkjente og standardiserte sikkerhetsmekanismer.
- Det bør benyttes ende-til-ende kryptering av informasjon som kommuniseres.
- Leverandør skal dokumentere sikkerheten i elektrisitetsmåler, kommunikasjonssystem og nettselskapets innsamlingssystem.
- Elektrisitetsmåleren skal ha mulighet for passord som beskytter mot konfigurering av elektrisitetsmåleren via kommunikasjonssystemet.
- Enhver endring av elektrisitetsmålerens konfigurasjon skal være sporbar.

REN 4010[1] stiller krav om at

- Nettselskap skal ved enhver endring i måleinstallasjon i høyspenningsanlegg, sørge for at sikkerheten og kvaliteten i anlegget, eller i andre anlegg, ikke svekkes.

2.6 Oppsummering av høringsinnspill (Rapport 1/2021)

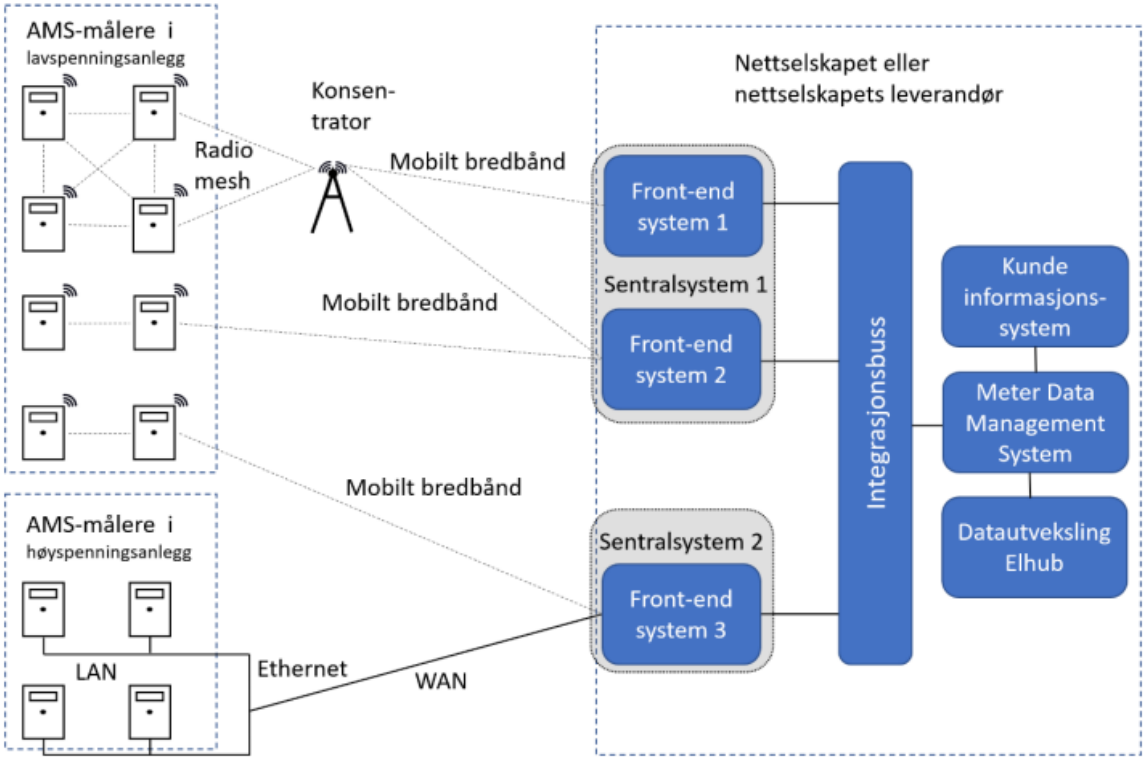
NVE-rapport 1/2021 [9] oppsummerer høringsinnspill og forslag knyttet til innføring av 15 minutters tidsoppløsning i balanseavregningen og endring i Avregningsforskriften (NVE-rapport nr. 2/2020, se kap. 2.5). Det er spesielt den delen om nye krav til sikkerhet i AMS i Avregningsforskriften som er relevant for ny veileder (Vedlegg B).

Med bakgrunn i høringen foreslås en ny definisjon av AMS:
«Avanserte måle- og styringssystem (AMS): Toveis informasjons- og kommunikasjonssystem fra og med elektrisitetsmålere som danner grunnlag for avregning av utveksling, innmating og uttak, til og med sentralsystemet hos nettselskapet eller nettselskapets leverandør.»

Denne definisjonen av AMS, angir at AMS er "til og med sentralsystemet hos nettselskapet eller nettselskapets leverandør". Med «sentralsystemet» mener RME front-end systemet eller systemene[2] som mottar data fra AMS-målere, enten direkte, eller via mastermålere eller konsentratorer. Alle målere som sender data til ett eller flere front-end system, er del av én enkelt AMS-løsning. Et nettselskap vil kunne ha

[1] https://www.ren.no/renbladserie/serie-4000-maling
[2] Uttrykket front-end benyttes her i nettverk-kontekst og henviser til maskinvaren som er plassert ytterst ut mot AMS-nettverket. SINTEF har laget en skisse til AMS infrastruktur som illustrerer plasseringen til sentralsystemet (side 7 [3])

forskjellige AMS-løsninger i drift samtidig, for eksempel fra gammel og ny AMS-leverandør. Figur 2.2 viser et eksempel på hvordan AMS og tilkoblede systemer kan se ut.



Figur 2.2 Eksempel på hvordan AMS og tilkoblede systemer kan se ut [9]

Integrasjonsbussen som gjør at de ulike systemene kan snakke sammen, og datasystemene som er koblet til front-end systemene via integrasjonsbussen, er i dette eksempelet å regne som nettselskapets back-end systemer[3] som er tilkoblet AMS. Slike back-end systemer er ikke en del av AMS. Likevel vil andre bestemmelser sikre at slike back-end systemer får et tilfredsstillende sikkerhetsnivå. I ny § 4-6 fjerde ledd foreslår RME at sikkerhetsnivået i AMS skal opprettholdes eller forbedres når andre systemer kobles til AMS. Nettselskapets back-end systemer som kommuniserer med AMS regnes som tilkoblet AMS, og må derfor etter forslag til ny § 4-6 fjerde ledd holde tilsvarende sikkerhetsnivå.

Gjeldende regelverk ivaretar også et tilstrekkelig sikkerhetsnivå for hele måleverdikjeden, inkludert de deler som ikke er definert som AMS eller tilkoblet AMS. Det følger av avregningsforskriften § 3-10 at nettselskapet skal kvalitetssikre måleverdier og håndteringen av disse gjennom hele måleverdikjeden i sitt nett. Måleverdikjeden omfatter hele den måletekniske installasjonen, samt all videre registrering, håndtering, og oversendelse av måleverdier til avregningsansvarlig. Samtidig må avregningsansvarlig sørge for at nettselskapets utgående kommunikasjon er sikret, ved at meldinger de mottar i Elhub er kryptert, jf. avregningsforskriften § 6-21. Til slutt stiller kraftberedskapsforskriften § 6-9 krav til sikkerhet i digitale informasjonssystemer, hvilket inkluderer overnevnte back-end systemer og andre deler av måleverdikjeden som nettselskapet har ansvaret for.

I tillegg til at systemer tilknyttet AMS skal være sikre, beskriver rapporten også oppdaterte forskriftskrav (ny § 4-6 i avregningsforskriften, se kap 3.1) knyttet til sikkerhet for AMS.

[3] Uttrykket «back-end» viser til den delen av IKT-systemet som er nærmest der lagring og kalkulering skjer. Det er vanlig at én eller flere servere er del av back-end miljøet

I forbindelse med krav §4-6 c) om ende-til-endre kryptering, er det noen høringsinstanser som mener kravet er utfordrende å oppfylle for AMS i andre målepunkt enn de knyttet til sluttbrukere i lavspennings-anlegg. Derfor har RME foreslått at kravet kan fravikes der nettselskapet bruker en separat kommunika-sjonskanal stengt for uvedkommende. For eksempel kan AMS-målere i høyspenningsanlegg være montert i nettstasjoner som har et eget Ethernet mot nettselskapet. I tilfeller hvor én del av kommunikasjonskanalen mellom AMS-måler og sentralsystemet er beskyttet med kryptering, og en annen del foregår i et eget datanettverk som er stengt for uvedkommende på en annen måte enn kryptering, oppfyller beskyttelsen fortsatt forskriftskravet.

I forbindelse med krav §4-6 g) om å begrense tilgang til AMS-målerens grensesnitt, så skal ikke dette kravet føre til at nettselskap må reise rundt og fysisk kontrollere at alle AMS-målere står i låste skap. Et eksempel på et grensesnitt som kan medføre sikkerhetsrisiko er HAN-porten, i tilfeller der kunder kontakter nettselskapet for å få denne aktivert. For å begrense tilgang til grensesnittet for uvedkommende i tråd med det foreslåtte forskriftskravet, kan nettselskapet be kunden bekrefte at AMS-måleren står inne i bolig eller i et låst skap før porten åpnes.

Norsk Elektroteknisk Komite (NEK) har beskrevet hvordan nettselskapet kan gå frem når de spør kunden om å bekrefte fysisk sikring og krypterer informasjonen fra HAN-porten [10].

2.7 Veiledning til kraftberedskapsforskriften (kbf)

Veiledning til kraftberedskapsforskriften [1] beskriver hvem forskriften gjelder for og har med eksempler på hvordan krav kan etterleves [11]. Veileder har samme kapittelinndeling som forskriften den gjelder for. Hvert kapittel viser først forskriftskravet, deretter fulgt av ordforklaring og anonymiserte eksempler. Veilederen gir også informasjon om aktuelle kilder (standarder, maler, temaveiledninger fra NVE og andre, og krysskoblinger til andre paragrafer og regelverk).

Figur 2.3 viser en forklaring på symbolbruk som brukes i veileder.

Figur 2.3 Forklaring til symbolbruk i veileder

Ny veileder til sikkerhet for AMS skal ha samme oppbygging og bruk av symbol, som den veilederen til kraftberedskapsforskriften.

3 Gjeldende regelverk relevant for sikkerhet i AMS

I dette kapitlet presenteres gjeldende regelverk som er relevant for sikkerhet i AMS. Det har vært flere høringsrunder knyttet til oppdatering av forskriftskrav, men det er kun siste (og gjeldende) versjon som er presentert i dette kapitlet.

Fokus er på regelverk som er relevant for sikkerhet i AMS. Dette er ikke en total oversikt over regelverk relatert til AMS.

3.1 Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv

Avregningsforskriften [2] stiller både krav til funksjonalitet og sikkerhet i AMS. Begge deler er presentert nedenfor, da funksjonskrav til AMS er relevant for virkeområdet til den nye veilederen (målere som inngår i skisse til AMS-infrastruktur, Figur B.1) og krav til sikkerhet for AMS er utgangspunktet for ny veileder.

3.1.1 Forskriftstekst

§ 4-2.Funksjonskrav for AMS i målepunkt for sluttbrukere i lavspenningsanlegg[4]
I målepunkt for sluttbrukere i lavspenningsanlegg skal AMS:

a) lagre måleverdier med en registreringsfrekvens på maksimalt 60 minutter, og kunne stilles om til en registreringsfrekvens på minimum 15 minutter,
b) ha et standardisert grensesnitt som legger til rette for kommunikasjon med eksternt utstyr basert på åpne standarder,
c) kunne tilknyttes og kommunisere med andre typer målere,
d) kunne bryte og begrense effektuttaket i det enkelte målepunkt, unntatt trafomålte anlegg,
e) kunne sende og motta informasjon om kraftpriser og tariffer, samt kunne overføre styrings- og jordfeilsignal og
f) registrere flyt av aktiv og reaktiv effekt i begge retninger.

§ 4-3.Funksjonskrav for AMS i øvrige målepunkt enn de knyttet til sluttbrukere i lavspenningsanlegg
For andre målepunkt enn de knyttet til sluttbrukere i lavspenningsanlegg, skal AMS:

a) lagre måleverdier med en registreringsfrekvens på maksimalt 15 minutter,
b) registrere flyt av aktiv effekt i begge retninger og
c) registrere flyt av reaktiv effekt i begge retninger.

I målepunkt for sluttbrukere i høyspenningsanlegg, skal AMS ha et grensesnitt som legger til rette for kommunikasjon med eksternt utstyr basert på åpne standarder.

Dersom AMS lagrer måleverdier med en finere tidsoppløsning enn 15 minutter, skal måleverdiene kunne summeres opp til 15 minutter.

[4] I Avregningsforskriften er sluttbruker definert som *kjøper av elektrisk energi som ikke selges denne videre* [2].

§ 4-6.Krav til sikkerhet for AMS
Nettselskapet er ansvarlig for å sikre AMS. Nettselskapet er ansvarlig for at sikkerhet vurderes ved oppstart og gjennomføring av endringsprosesser tilknyttet AMS. Nettselskapet skal velge løsninger som gir høyest sikkerhetsnivå i AMS så lenge kostnaden er forsvarlig etter en kost/nytte-vurdering.

Sikkerhetsløsninger i AMS skal oppfylle kravene til digitale informasjonssystemer i kraftberedskaps-forskriften.

I tillegg skal følgende krav være oppfylt:

a) Enheter og brukere som skal kommunisere til eller i AMS, må godkjennes i AMS av nettselskapet eller nettselskapets leverandør før de får tilgang.
b) Enhver endring av programvare og konfigurasjon av dataprogram i AMS skal kunne spores tilbake til bruker, tidspunkt og endringen som ble gjort.
c) Kommunikasjon i nettverket mellom AMS-måler og sentralsystem skal være beskyttet med ende-til-ende-kryptering. Ved bruk av et eget datanettverk, stengt for uvedkommende, kan kravet om ende-til-ende-kryptering fravikes.
d) Programvare i AMS skal være oppdatert. Før ny programvare installeres i AMS, skal nettselskapet eller nettselskapets leverandør kontrollere at programvaren er autentisk.
e) Hendelser som kompromitterer sikkerheten i en AMS-måler, eller dens kommunikasjon med sentralsystemet, skal ikke kompromittere sikkerheten i andre AMS-målere, deres kommunikasjon med sentralsystemet, eller sentralsystemet i seg selv.
f) AMS skal til enhver tid kunne utføre de oppgaver systemet er designet for. Nettselskapet eller nettselskapets leverandør skal deaktivere funksjonalitet i AMS som ikke skal benyttes.
g) I målepunkt for sluttbrukere i lavspenningsanlegg skal tilgang til AMS-målerens grensesnitt begrenses for andre enn sluttbruker, nettselskapet og andre aktører med legitimt behov. I øvrige målepunkt skal kun nettselskapet og andre aktører med legitimt behov ha tilgang til AMS-måleren.

Dersom nettselskapet eller nettselskapets leverandør kobler andre enheter eller systemer til AMS, skal sikkerhetsnivået i AMS opprettholdes eller forbedres. Tilsvarende gjelder dersom sluttbruker eller tredjepart kobler seg til AMS.

Nettselskapet skal dokumentere oppfyllelse av krav i første til fjerde ledd i et internkontrollsystem.

3.2 Kraftberedskapsforskriften

Kraftberedskapsforskriften (kbf) [4] skal sikre at kraftforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene. I denne forskriften blir informasjonssikkerhet og krav til digitale informasjonssystemer omhandlet i kapittel 6.

3.2.1 Forskriftstekst

Kapittel 6. Informasjonssikkerhet
§ 6-1.Identifisering av kraftsensitiv informasjon og rettmessige brukere
KBO-enheter skal etter energiloven § 9-3 første ledd identifisere hva som er kraftsensitiv informasjon, hvor denne befinner seg og hvem som har tilgang til den.

Identifiseringen av hva som er kraftsensitiv informasjon og hvor denne befinner seg, skal omfatte oppbevaring på papir, lagring i elektronisk form eller lagring på annen måte.

Med rettmessig bruker menes fysiske eller juridiske personer som har tjenstlig behov for kraftsensitiv informasjon. Den enkelte KBO-enhet skal selv avgjøre hvem som har tjenstlig behov for kraftsensitiv informasjon innenfor sin virksomhet.

Den enkelte KBO-enhet kan avgjøre om det er tjenstlig behov for å videreformidle kraftsensitiv informasjon til andre utenfor egen virksomhet. Den som har fått tilgang til kraftsensitiv informasjon av en KBO-enhet kan ikke videreformidle den kraftsensitive informasjonen til andre. Beredskapsmyndigheten kan i tvilstilfeller avgjøre hvem som er rettmessig bruker.

§ 6-2.Kraftsensitiv informasjon
Kraftsensitiv informasjon er underlagt taushetsplikt etter § 9-3 i energiloven.

Med kraftsensitiv informasjon menes spesifikk og inngående opplysninger om kraftforsyningen som kan brukes til å skade anlegg, system eller annet eller påvirke funksjoner som har betydning for kraftforsyningen, herunder:

a) Alle system som ivaretar viktige driftskontrollfunksjoner, herunder også nødvendig hjelpeutstyr som samband.
b) Detaljert informasjon om energisystemet, herunder enlinjeskjema, med unntak av enlinjeskjema for mindre viktige produksjonsanlegg.
c) Detaljert informasjon om klassifiserte transformatorstasjoner med tilhørende koblingsanlegg, herunder anleggets oppbygning og drift.
d) Oversikt over fordelingsnett til samfunnsviktige funksjoner. Oversikt over rørnett for fjernvarme til samfunnsviktige funksjoner.
e) Nøyaktig kartfesting av jordkabler. Nøyaktig kartfesting av rørnett i fjernvarmeanlegg med varmesentraler i klasse 2.
f) Forebyggende sikkerhetstiltak mot bevisst skadeverk.
g) Lokalisering av reserve driftssentraler og andre særskilte beredskapsanlegg for ledelse og drift.
h) Detaljerte analyser av sårbarhet som kan brukes til bevisst skadeverk.
i) Beredskapsplaner for å håndtere bevisst skadeverk.
j) Samlet oversikt over reservemateriell, reserveløsninger eller reparasjonsberedskap av betydning for håndtering av bevisst skadeverk.

§ 6-3.Beskyttelse, avskjerming og tilgangskontroll
Virksomheter som har eller behandler kraftsensitiv informasjon skal etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for kraftsensitiv informasjon. Beskyttelse skal omfatte tiltak mot avlytting og manipulering fra uvedkommende.

System og rutiner skal omfatte merking, oppbevaring, bruk og distribusjon, tilintetgjøring og tiltak for intern og ekstern rapportering av hendelser av betydning for informasjonssikkerheten.

Særskilte regler og sikkerhetstiltak skal utarbeides ved bruk av mobile enheter som kan motta, sende og lese kraftsensitiv informasjon.

§ 6-4.Sikkerhetsinstruks
Virksomheter som har eller behandler kraftsensitiv informasjon skal utarbeide og praktisere en sikkerhetsinstruks som sikrer at kravene til informasjonssikkerhet ivaretas. Sikkerhetsinstruksen skal

beskrive hvilke system, rutiner og tiltak som er iverksatt for å etterleve kravene til informasjonssikkerhet, herunder krav til beskyttelse, avskjerming og tilgangskontroll.

Sikkerhetsinstruksen skal omfatte informasjon til ansatte og andre rettmessige brukere om taushetsplikten etter energilovens § 9-3 annet ledd og stille krav til undertegning av taushetserklæring. Sikkerhets-instruksen skal også omfatte informasjon om at taushetsplikten medfører at kraftsensitiv informasjon ikke skal offentliggjøres.

§ 6-5.Anskaffelser
KBO-enheter har ansvaret for at bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon ivaretas i anskaffelser. KBO-enheter skal i anskaffelser påse at leverandører er forpliktet til å etterleve bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon.

Det skal i avtale sikres at KBO-enheter gis rett til å kontrollere, herunder revidere, leverandørens etterlevelse av disse bestemmelsene.

Plikten til å påse innebærer at det skal iverksettes system og rutiner for å undersøke, og om nødvendig, følge opp at reglene om informasjonssikkerhet og taushetsplikt etterleves.

Bestemmelsene i første og annet ledd gjelder tilsvarende når KBO-enheter setter ut oppdrag for prosjektering, installering, vedlikehold og feilretting av driftskontrollsystemet.

§ 6-6.Begrenset anbudsinnbydelse
Anbudsinnbydelser og lignende skal begrenses når det er nødvendig for å hindre at sikkerhetsgradert eller kraftsensitiv informasjon blir offentlig tilgjengelig gjennom anbudsdokumentene.

Forståelsen av begrenset anbudsinnbydelse bygger på anskaffelsesregelverket.

§ 6-7.Personkontroll
KBO-enheter skal gjennomføre en bakgrunnssjekk av personer før ansettelse.

KBO-enheter kan kreve at personer som skal få tilgang til anlegg, system eller annet i klasse 2 og 3 skal fremlegge kredittsjekk.

KBO-enheter skal før de fremsetter krav etter annet ledd foreta en risikovurdering. Kredittsjekk skal ikke anvendes dersom det kan iverksettes andre egnede sikkerhetstiltak.

Bakgrunnssjekken etter første og annet ledd skal brukes som grunnlag for å vurdere en persons egnethet til å få tilgang til klassifiserte anlegg, system eller annet. Kredittsjekk skal slettes når egnethetsvurderingen er gjennomført.

Krav om personkontroll etter første til fjerde ledd gjelder ikke personer som er sikkerhetsklarert og autorisert etter den til enhver tid gjeldende lov om nasjonal sikkerhet (sikkerhetsloven).

Beredskapsmyndigheten kan etter søknad gi unntak fra kravene i første til fjerde ledd i denne bestemmelsen. Beredskapsmyndigheten kan ved vedtak fastsette krav om bakgrunnssjekk etter første til fjerde ledd for bestemte anlegg, system og annet.

§ 6-8.Sikkerhetskopier
Virksomheter skal ha oppdaterte sikkerhetskopier av nødvendig informasjon, programvare og konfigurasjoner av driftskontrollsystemet som er av betydning for drift, sikkerhet og gjenoppretting av kraftforsyningen. Sikkerhetskopiene skal fjernlagres på et sikkert sted, som er lett tilgjengelig for virksomheten.

Nødvendig dokumentasjon om energisystemet og som lagres på datamedia, skal også foreligge som papirutskrifter. Disse skal oppdateres årlig og oppbevares på et sikkert sted som er lett tilgjengelig for virksomheten.

§ 6-9.Digitale informasjonssystemer
Virksomheter skal sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas.

Det er den enkelte virksomhets ansvar å planlegge, gjennomføre og vedlikeholde sikringstiltak etter det digitale informasjonssystemets type, oppbygging og funksjon.

Virksomheter skal ha en grunnsikring for digitale informasjonssystemer i henhold til anerkjente standarder og normer, herunder:

a) Identifisere og dokumentere
   Virksomheter skal identifisere og dokumentere verdier, leveranser, tjenester, systemer og brukere i sine digitale informasjonssystemer. Dokumentasjonen skal holdes oppdatert.

b) Risikovurdering
   Virksomheter skal gjennomføre risikovurdering ved systemendringer. Risikovurderingen skal holdes oppdatert.

c) Sikre og oppdage
   Virksomheter skal sikre sine digitale informasjonssystemer for å motstå eller begrense skade fra uønskede hendelser. Virksomheter skal overvåke sine digitale informasjonssystemer slik at uønskede hendelser oppdages og registreres. Virksomheten skal varsle uønskede hendelser i sine digitale informasjonssystemer til den beredskapsmyndigheten bestemmer.

d) Håndtere og gjenopprette
   Virksomheter skal håndtere uønskede hendelser i sine digitale informasjonssystemer og gjenopprette normaltilstand uten ugrunnet opphold.

e) Tjenesteutsetting
   Virksomheter skal sørge for at sikkerhetsnivået opprettholdes eller forbedres ved utsetting av tjenester.

f) Sikkerhetsrevisjon
   Virksomheter skal jevnlig gjennomføre revisjoner av iverksatte sikringstiltak for digitale informasjonssystemer. Revisjoner skal påse at tiltakene faktisk er etablert og fungerer etter sin hensikt. Hver revisjon kan ta for seg deler av sikringstiltakene.

§ 6-10.Brytefunksjonalitet i avanserte måle- og styringssystem (AMS)
Nettselskap som har avanserte måle- og styringssystem (AMS) med brytefunksjonalitet, skal sikre dette mot uønsket tilgang. Brytefunksjonalitet som definert i forskrift om måling, avregning, fakturering av

nettjenester og elektrisk energi, nettselskapets nøytralitet mv. § 1-3, inkluderer i denne bestemmelsen begrensning av energi- og effektuttaket i det enkelte målepunkt. Nettselskap skal etablere og opprettholde egne sikkerhetstiltak for brytefunksjonaliteten, herunder:

a) Det er kun nettselskap som har tillatelse til å utføre fjernstyring av brytefunksjonaliteten. Fjernstyring av brytefunksjonaliteten skal utføres fra en adgangskontrollert sone.

b) Leverandør med fjerntilgang til brytefunksjonaliteten, skal være lokalisert i et land som er medlem i EFTA, EU eller NATO. Leverandør lokalisert i andre land kan få tidsavgrenset fjerntilgang til brytefunksjonalitet under løpende oppsyn av kvalifisert personell fra nettselskapet eller kvalifisert personell fra leverandør lokalisert i land som er medlem i EFTA, EU eller NATO.
Før leverandør lokalisert i land utenfor EFTA, EU eller NATO får fjerntilgang til brytefunksjonaliteten, skal nettselskapet foreta en risikovurdering som inneholder en vurdering av landrisiko.

c) Nettselskap har ansvar for at det etableres kontrollordninger for bruk av bryte- og oppdateringsfunksjonaliteten som hindrer at en enkelt person eller enkelt bruker kan koble ut flere målepunkt samtidig.

d) Fjernoppdatering av programvaren i AMS skal utføres fra en adgangskontrollert sone hos nettselskap eller leverandør. Ved bruk av leverandør skal vilkårene i bokstav b være oppfylt.

e) Hver enkelt måler skal ha en individuell sikkerhetsløsning for bryte-, og oppdateringsfunksjonen, som forhindrer at hendelser som kompromitterer sikkerheten i en måler, kompromitterer sikkerheten i en annen måler.

3.2.2 Momenter som er relevante for sikkerhet i AMS

§6-1 - §6-7 omhandler kraftsensitiv informasjon, og er i utgangspunktet mindre relevante for AMS. Forbruksinformasjon i AMS er å regne som personopplysninger, men ikke sensitive personopplysninger, og trenger derfor "noe" beskyttelse[5].

§6-8 omhandler sikkerhetskopi, og er relevant for AMS i den grad det dreier seg om å sikre drift av AMS.

Det er i første omgang §6-9 som er relevant for sikkerhet i AMS. Denne ligger tett opp til anbefalingene i NSMs grunnprinsipper for IKT-sikkerhet [12] [13]:

§6-9 a) Dekkes av hele kategori 1
§6-9 b) 1.1.3, 2.1.9, 2.2.7, 2.3.10
§6-9 c) En rekke tiltak i kategori 2 og 3, 4.2.3
§6-9 d) Dekkes av hele kategori 4
§6-9 e) 2.1.9, 2.1.10, 2.2.7, pluss temarapport om tjenesteutsetting [14].
§6-9 f) 1.1.3, 2.3.5, 2.6.2, 3.4.1, 3.4.3, 3.4.4

§6-10 omhandler bryterfunksjon, og er også relevant for AMS.

§6-10 a) Fjernstyring av bryter kun av nettselskap fra kontrollert sone
§6-10 b) Fjernstyring av bryter fra leverandør i EU/EFTA/NATO
§6-10 c) Hindre masseutkobling
§6-10 d) Fjernoppdatering av programvare kun fra kontrollert sone
§6-10 e) Individuell sikkerhet

[5] Regelverk for personopplysninger behandles i Personopplysningsloven, som er beskrevet i kapittel .3.

3.3 Personopplysningsloven

Lov om behandling av personopplysninger (personopplysningsloven) [15] eksisterer for å verne fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger. Dette lovverket er også kalt generell personvernforordning (PVF) eller GDPR (General Data Protection Regulation). Datatilsynet følger opp personopplysningsloven.

Personopplysning er definert som: "enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliserings-opplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet".

Et viktig prinsipp når det gjelder personopplysninger er samtykke fra den fysiske personen opplysningen omhandler. I loven er det angitt unntak fra prinsippet om samtykke i kapittel 3 §9: dersom behandlingen er nødvendig for arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål og samfunnets interesse i at behandlingen finner sted, klart overstiger ulempene for den enkelte. Før det foretas behandling det rådføres med personvernombudet eller en annen som oppfyller vilkårene i personvernforordningen artikkel 37 nr. 5 og 6 og artikkel 38 nr. 3 første og annet punktum. Ved rådføringen skal det vurderes om behandlingen vil oppfylle kravene i personvern-forordningen og øvrige bestemmelser fastsatt i eller med hjemmel i loven her. Rådføringsplikten gjelder likevel ikke dersom det er utført en vurdering av personvernkonsekvenser etter personvernforordningen artikkel 35 (Vurdering av personvernkonsekvenser).

AMS-data er opplysninger om blant annet strømforbruk til husholdninger (en eller flere fysiske personer). Ifølge Datatilsynet er opplysninger om strømforbruk er å anse som en personopplysning og må behandles som slike [16]. Bruk av måledata som registreres av AMS er blant annet underlagt personopplysningsloven. Dette innebærer at nettselskap og kraftleverandør kun kan bruke de personopplysninger som er nødvendig for å fakturere kunden. Hvilken informasjon som skal registreres og hva måleren skal gjøre er regulert i funksjonskravene. Utover det ovenstående har kunden råderett over og kan bestemme hvem som får tilgang til egne data. Nettselskapet kan ikke lagre data om kunden lenger enn 3 år. Forskning på AMS-data må meldes inn til NSD (Norsk senter for forskningsdata), som er personvernombud for forskningen.

Informasjonssikkerhet er viktig for å sørge for at personopplysninger, som strømforbruk, ikke kommer på avveie eller benyttes til annet enn formålet det er gitt tillatelse til.

Artikkel 32 spesifiserer sikkerhet ved behandling av personopplysninger: "Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,

a) pseudonymisering og kryptering av personopplysninger,
b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,
c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,

d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

Det er Datatilsynet som utfører kontroller for å sikre at personvernlovgivningen etterleves. Datatilsynet er både tilsyn og ombud. Datatilsynets oppgave er å føre kontroll med personvernregelverket og medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem [17].

3.4 Elmålerforskriften

Forskrift om krav til elektrisitetsmålere (elmålerforskriften) [18] inneholder krav til elektrisitetsmålere og det er Justervesenet som fører tilsyn med denne forskriften. Justervesenet er et direktorat for måleteknikk underlagt Nærings- og Fiskeridepartementet. Justervesenet har ansvaret for at Norge har en måleteknisk infrastruktur som både har nasjonal og internasjonal tillit. Etaten yter bistand innen kvalitetssikring og måleteknikk, og er et kompetansesenter for næringsliv og myndigheter [19]. Justervesenet utfører tilsyn med måling med elektrisitetsmålere hos et utvalg av nettselskaper [20]. Justervesenet stiller bare måletekniske krav til elmålere, altså at målerne skal vise riktig verdier. Det er krav til nye elmålere og elmålere i bruk: "I Norge er det også krav til kontroll med elmålere etter at de er tatt i bruk. En elmåler som er tatt i bruk skal kontrolleres av nettselskapet 3 år etter produksjonsår, og deretter hvert 8. år. I og med at målerne er plassert ute i private hjem er dette en kostbar kontroll, og derfor blir den oftest gjennomført som en stikkprøve. Det innebærer at nettselskapene bare kontrollerer en liten andel av en gruppe målere av samme type. Hvis for mange av disse ikke overholder kravene, skal hele partiet byttes ut. [21]"

I elmålerforskriften *§ 19 Beskyttelse mot manipulering* sier dette:
Dersom elektrisitetsmåleren koples til en annen anordning direkte eller ved fjerntilkopling, skal dets måletekniske egenskaper ikke påvirkes av anordningen på en feilaktig måte. Komponenter som har avgjørende betydning for de måletekniske egenskapene, skal være konstruert slik at de kan sikres. De anvendte sikkerhetstiltak skal gjøre det mulig å påvise om inngrep har funnet sted.

Programvare som har avgjørende betydning for de måletekniske egenskapene, skal være merket tilsvarende, og skal være sikret. Identifikasjon av slik programvare skal lett framskaffes fra elektrisitetsmåleren. Eventuell informasjon eller indikasjon på at det har funnet sted et inngrep skal være tilgjengelig i et rimelig tidsrom.

Måledata, programvare som er av avgjørende betydning for måleegenskapene, og måleteknisk viktige parametere som lagres eller overføres, skal være beskyttet på hensiktsmessig vis mot tilsiktede eller utilsiktede endringer.

Visningen av samlet mengde eller visningene som samlet mengde kan utledes fra, og som helt eller delvis danner grunnlaget for betaling, skal ikke kunne tilbakestilles under bruk.

Justervesenet stiller måletekniske krav til elmålere for å sikre at riktig verdier vises, men tilkoblede anordninger og programvare som har betydning for måletekniske egenskaper skal sikres mot feil og tilsiktede endringer.

4 NSMs grunnprinsipper for IKT-sikkerhet

NSMs grunnprinsipper for IKT-sikkerhet [12] (Gjengitt i Tabell 4.1) anbefales for alle norske virksomheter, og bl.a. kraftberedskapsforskriftens krav til informasjonssikkerhet er i stor grad basert på grunnprinsippene (se kapittel 3.2). Grunnprinsippene er i stor grad anvendbare på industrielle systemer som smart grid [13].

Tabell 4.1: NSMs grunnprinsipper for IKT-sikkerhet

Identifisere og kartlegge		Beskytte og opprettholde		Oppdage		Håndtere og gjenopprette	
1.1	Kartlegg styrings-strukturer, leveranser og understøttende systemer	2.1	Ivareta sikkerhet i anskaffelses- og utviklings-prosesser	3.1	Oppdag og fjern kjente sårbarheter og trusler	4.1	Forbered virksomheten på håndtering av hendelser
1.2	Kartlegg enheter og programvare	2.2	Etabler en sikker IKT-arkitektur	3.2	Etabler sikkerhetsover-våkning	4.2	Vurder og klassifiser hendelser
1.3	Kartlegg brukere og behov for tilgang	2.3	Ivareta en sikker konfigurasjon	3.3	Analyser data fra sikkerhetsovervåkning	4.3	Kontroller og håndter hendelser
		2.4	Beskytt virksomhetens nettverk	3.4	Gjennomfør inntrengnings-tester	4.4	Evaluer og lær av hendelser
		2.5	Kontroller dataflyt				
		2.6	Ha kontroll på identiteter og tilganger				
		2.7	Beskytt data i ro og i transitt				
		2.8	Beskytt e-post og nettleser				
		2.9	Etabler evne til gjenoppretting av data				
		2.10	Integrer sikkerhet i prosess for endringshåndtering				

Grunnprinsippene er delt i 4 kategorier (Identifisere og kartlegge; Beskytte og opprettholde; Oppdage; Håndtere og gjenopprette), og hvert prinsipp er detaljert i et antall tiltak. Tabell 4.2 viser kobling mellom sikkerhetskrav i avregningsforskriften og relevante tiltak fra NSMs grunnprinsipper.

Tabell 4.2: Kobling mellom sikkerhetskrav i avregningsforskriften og tiltak i NSMs grunnprinsipper

Forskriftskrav	Kort beskrivelse	Tiltak i NSMs grunnprinsipper	I hvilken grad dekker tiltakene forskriftskravet?
§4-6 a)	Godkjennelse av enheter og brukere som skal kommunisere til eller i AMS	1.2.1 1.2.2 1.2.3 1.3.1 1.3.2 2.6.2 2.6.3 2.6.6	Dekkes fullt ut
§4-6 b)	Loggføring av endringer av programvare og konfigurasjon av dataprogram i AMS	1.2.4 2.2.1 d) 2.10.1	Dekkes i stor grad, men sier ikke eksplisitt at endringer skal spores tilbake til enkeltbruker
§4-6 c)	Ende-til-ende kryptering i kommunikasjonen mellom AMS-måler og sentralsystem	2.4.2 2.7.1 2.7.2 2.7.4	Dekkes i stor grad, selv om ende-til-ende-kryptering ikke angis eksplisitt. Imidlertid vil ikke ende-til-ende-kryptering være et krav dersom nettselskapet kontrollerer (og kan forhindre uvedkommendes tilgang til) alle steder informasjonen er ukryptert
§4-6 d)	Oppdatering av programvare i AMS	2.1.2 2.10.4 3.1.3 2.3.1	Dekkes fullt ut
§4-6 e)	Sikkerhet i AMS-målere skal ikke påvirkes av hverandre	2.2.5 2.3.4 2.5.3 2.7.1	Dekkes i stor grad, men sier ikke eksplisitt at alle målerne skal ha forskjellige symmetriske nøkler
§4-6 f)	Funksjonalitet i AMS skal fungere til enhver tid. Funksjoner som ikke brukes, skal deaktiveres	2.3.3 2.9.1	Andre del av kravet dekkes fullt ut
§4-6 g)	Kontroll på tilgang til AMS-målerens grensesnitt		Dekkes ikke (for spesifikt til å dekkes av grunnprinsipper)

5 Intervjuer

5.1 Beskrivelse av plan og guide for gjennomførte intervjuer

I november og desember 2021 (ett intervju ble gjennomført i januar 2022) ble det gjennomført 14 1-timersintervjuer via Teams med tre ulike grupper; sju nettselskaper, tre myndighetsorgan og fire systemleverandører. Dette er de mest relevante aktørene med tanke på å få innspill til en veileder for sikkerhet i AMS. Intervjuguiden som ble brukt i intervjuene er presentert i Vedlegg A.

Intervjuguiden er tredelt, med en del for nettselskapene (Vedlegg A.1), en del for systemleverandører (Vedlegg A.2) og en del for myndighetsorgan (Vedlegg A.3). I tillegg benyttet vi i intervjuene en oversikt over sikkerhetsområdene som er brukt i dagens veileder for sikkerhet i AMS (Vedlegg A.4). Hovedtemaene for intervjuene er gjengitt under. Intervjuguidene for de tre ulike gruppene er litt forskjellige. Hoved-temaene er like for nettselskaper og systemleverandører, men underpunktene er litt ulike, da disse to gruppene har ulike roller med tanke på sikkerhet i AMS.

For myndighetsorganene er grensnitt med annet lovverk et viktig punkt i intervjuene. Det ble brukt mest tid på evaluering av dagens veileder (punkt 4) og forskriftskrav til sikkerhet i AMS (punkt 5).

Vi opplevde at det stort sett var relevante personer som stilte i intervjuene, det vil si at de hadde en rolle/stilling knyttet til sikkerhet i AMS. Noen intervjuobjekter hadde hatt en rolle/stilling knyttet til innkjøp/installasjon av AMS, men hadde ikke helt oversikt over dagens situasjon. Dette gjaldt imidlertid et mindretall av intervjuobjektene.

Vedlegg A.1/A.2: Intervjuguide for nettselskaper og systemleverandører

1. Innledning
    - Generell informasjon om prosjektet, og databehandling.
    - Spørsmål knyttet til informanten og selskap (relevant for sikkerhet i AMS)
2. Status i dag ang. AMS
    - Antall målere, antall åpnede HAN-porter, bruk av serviceport, nøkkeladministrasjon og drift av AMS
3. Status i dag ang. bruk av veileder til sikkerhet for AMS
    - Bruk av veileder i dag, avtaler om sikkerhet i AMS med eventuelle leverandører
4. Evaluering med dagens veileder
    - Noe som mangler/er overflødig i dagens veileder, innspill til nye punkter
5. Forskriftskrav til sikkerhet i AMS
    - Nye forskriftskrav til sikkerhet i AMS (§4-6 i forskrift for måling og avregning)
6. Annet lovverk/forskrifter som er relevant for sikkerhet i AMS
    - Kraftberedskapsforskriften, personopplysningsloven, elmålerforskriften og eventuelt annet relevant lovverk.

Vedlegg A.3: Intervjuguide for myndighetsorgan

1. Innledning
    - Generell informasjon om prosjektet, og databehandling.
    - Spørsmål knyttet til informanten og selskap (relevant for sikkerhet i AMS)
2. Status i dag ang. AMS
    - Hvilket lovverk forvaltet av myndighetsorganet er relevant for sikkerhet i AMS?
3. Status i dag ang. bruk av veileder til sikkerhet for AMS og utvikling av regelverk

- Bruk av veileder i utvikling av veileder og aktuelle grensesnitt med andre lovverk

4. Evaluering av dagens veileder
    - Noe som mangler/er overflødig i dagens veileder, innspill til nye punkter
5. Forskriftskrav til sikkerhet i AMS
    - Nye forskriftskrav til sikkerhet i AMS (§4-6 i forskrift for måling og avregning) og relevans til lovverk som forvaltes av myndighetsorganet som intervjues.

5.2 Oppsummering av intervjuer

En viktig observasjon fra intervjuene er at dagens veileder til sikkerhet i AMS var flittig i bruk ved spesifikasjon og innkjøp av AMS-målene, **men at den i liten grad er i bruk nå**, altså i driftsfasen av AMS. Dette har selvfølgelig bakgrunn i at nå er AMS-systemene kjøpt inn og i drift og sikkerhetsrelaterte arbeidsprosesser er på plass. Hovedfokus når det gjelder sikkerhet er dermed daglig drift med blant annet avvikshåndtering og software-oppgraderinger. Situasjoner hvor veilederen kan bli brukt er ved tilsyn fra myndighetsorgan og ved behov for endringer (oppsett av software eller lignende), og som det ble påpekt i et intervju vil det skje nye spesifikasjoner/innkjøp av AMS framover, så behovet for en veileder er til stede. Tabellen under gir en oppsummering av svar på de viktigste spørsmålene fra intervjuene.

Tabell 5.1 Oppsummering av intervjuer

Intervjuspørsmål fra Vedlegg A	Oppsummering av svar
Nettselskap, intervjuguide Vedlegg A.1	
Spørsmål 6 HAN-porten	Alle de intervjuede nettselskapene har gode rutiner for HAN-porten. Sluttbrukerne kan logge inn i en selvbetjeningsløsning eller ringe kundeservice for å åpne HAN-porten og porten lukkes når nettselskapet mottar flyttemelding. Hele 5 av 7 nettselskaper som ble intervjuet har automatisert både åpning og lukking av HAN-port, mens to nettselskap fremdeles har manuelle løsninger, men jobber med automatisering. HAN-port er enveiskommunikasjon, så det er ingen frykt for at inntrengere skal komme seg "inn" via HAN-porten. Men, hvis rutiner for åpning/ lukking ikke fungerer kan uvedkomne få tilgang til informasjon om strømforbruket til sluttkunder. Strømforbruk er personinformasjon, så dette er problematisk fra et personvernperspektiv. Fokus er dermed på å lage gode rutiner for korrekt identifisering av hvem som kan åpne HAN-port og rutiner for lukking ved flytting. Dataene fra HAN-porten er kundens eiendom og nettselskapet har ingen oversikt over hva dataene brukes til hos sluttbrukerne. Data fra HAN-porten er ukryptert. Det virker å være en økning i antallet sluttkunder som vil åpne HAN-porten.
Spørsmål 7 og 8 serviceporten	To av de intervjuede nettselskapene bruker ikke (eller sjelden) serviceporten og sier at det ikke er mye som kan gjøres via denne. Et nettselskap skifter heller måler hvis det oppstår problemer enn å forsøke å reparere problemet. Ett av de intervjuede nettselskapene bruker serviceporten og sier at hver bruker (f.eks. ansatt i nettselskap som er autorisert for å få tilgang) må ha et personlig sertifikat med utgangsdato og at det er forskjellige tilganger avhengig av hva som skal gjøres. Slike sertifikater kan fås fra den som drifter AMS, enten leverandør eller nettselskapet selv. Flertallet (4 nettselskaper) forteller at den som skal bruke serviceporten må ha en krypteringsnøkkel/kode for å få tilgang. Målerleverandørene leverer typisk målere hvor serviceporten er deaktivert fra fabrikk.

Spørsmål 9 Administrasjon av krypteringsnøkler	AMS-målere leveres fra fabrikk ferdig konfigurert med unike symmetriske nøkler som brukes til autentisering og etablering av sesjonsnøkler. Leverandøren overfører lister med måler-ID og korresponderende nøkkel til nettselskap (eller den som drifter HES på vegne av nettselskapet), og sletter listen etter at den er bekreftet mottatt. I varierende grad brukes også asymmetriske nøkler for punkt-til-punkt autentisering, for eksempel for etablering av VPN-tunell fra konsentrator til HES, eller for kryptering av trådløs trafikk i MESH-nett.
Spørsmål 10 drift av AMS-system	Det er ulike modeller for drift av AMS. Tre av de intervjuede nettselskapene har egne selskap som drifter AMS (dvs. utfører firmwareoppdateringer, tester, kjører nye versjoner, patching, etc.), mens de selv ordner det som eventuelt ikke fungerer (kommunikasjon, skifte målere, etc.). To nettselskaper gjør all drift selv, men er i tett kontakt med leverandør av AMS for oppdateringer, etc., eventuelt gjør leverandøren visse oppgaver på oppdrag fra nettselskapet. Ett nettselskap har vedlikeholdsavtaler med leverandøren av AMS-løsningen, men drifter AMS selv. Et nettselskap har avtale om drift av servere og databaser fra ekstern leverandør, men drifter målerinfrastrukturen selv.
Spørsmål 11 bruk av dagens veileder internt	Dagens veileder er lite i bruk etter at AMS-systemet var ferdig spesifisert og innkjøpt. Nå inngår AMS-systemet i rutiner knyttet til generell IT-sikkerhet. 3 av 7 nettselskaper nevner at andre forskrifter/veiledere er oppdatert etter 2012 og at disse dermed er mer i bruk. 6 av 7 nettselskaper nevner av veilederen var flittig i bruk i spesifikasjon/innkjøpsfasen for AMS. NSM, GDPR og kraftberedskaps-forskriften ble nevnt spesifikt som eksempler på andre kilder som er mer i bruk knyttet til sikkerhet i AMS.
Spørsmål 12 og 13 bruk av dagens veileder mot eksterne	To nettselskaper nevner spesifikt at de har hatt dialog om dagens veileder med bedriften som drifter AMS-systemet om sikkerhet generelt, og da bryterfunk-sjonen spesielt. Det som har vært tema for diskusjoner, er tilgang til bryter-funksjon fra leverandør som drifter AMS. Det er lagt (software og rutinestyrte) begrensinger på hvem som kan bryte strøm og hvor mange som kan brytes innen gitte tidsrom. Det er i praksis vanskelig å sikre fullstendig at leverandør ikke har tilgang til å kunne bryte strømmen, da de sitter på tilgang til det meste, men logger vil avsløre om dette skjer. Ett nettselskap nevner også at veilederen ble tatt fram igjen i forbindelse med revisjon/ tilsyn fra NVE.
Spørsmål 14 sikkerhetsavtaler	Databehandleravtaler ble nevnt under dette punktet. De som har eksterne bedrifter som drifter AMS har sikkerhet som en del av avtalen med disse (eksempelvis varsling ved hendelser, etc.).
Spørsmål 15 og 16 sikkerhets-områder som mangler/ overflødige/ uklare	På dette punktet ble bryterfunksjonen nevnt av alle de intervjuede. Nedenfor er det oppsummert kommentarer for ulike punkt i dagens veileder *H1 – Beskyttelse av bryte- og strupefunksjonalitet* oppsummert ("Eksempler for å oppnå kontrollmål"). Selv om dette er gitt om eksempler i veilederen er det tydelig at alle nett-selskapene har lagt mye arbeid i å studere eksemplene og prøve å oppfylle dem: - Kun særskilt autoriserte personer skal kunne få tilgang til- og adgang til å utøve strupe- og bryterfunksjonalitet Kommentar: OK, men om AMS-systemet driftes av andre vil disse i praksis ha tilgang til å kunne bryte strøm fordi de eksempelvis administrerer gruppetilganger for nettselskapet.

	- Det skal ikke være mulig for én person alene å autorisere samt utføre bryte- eller strupefunksjonen Kommentar: Dette er i dag etablert hos alle de intervjuede nettselskapene. Det er ingen krav i dag om at flere enn én person må godkjenne bryting av strømmen. Det har vært en lang prosess før man kommer til at strømmen skal brytes og dette skal sikre at det er nødvendig å bryte strømmen hos enkeltkunder. - Det skal etableres automatiske kontroller som vil redusere mulighet for å bryte eller strupe et stort antall punkter som følge av feil eller målrettede angrep Kommentar: OK. Alle som ble intervjuet, har et maks antall som kan brytes innenfor et gitt tidsintervall. - Den fysiske lokasjonen til systemene for strupe- og bryterfunksjonalitet skal være en egen adgangskontrollert sone Kommentar: Bryting har blitt gjort fra hjemmekontor via VPN pga. COVID-19, selv om det ikke er en fysisk adgangskontrollert sone, men en digitalt adgangskontrollert sone, inkludert en logg over hvem som har utført strømbrytingen. Punktet om tilgangskontroll burde oppdateres ut ifra et "hjemmekontorperspektiv". Dette med bryting er spesielt med AMS, og også inkludert i kraftberedskaps-forskriften, gjennom kravteksten i paragraf 6-9. Det kom også spørsmål om hva ende-til-ende kryptering egentlig innebærer og hvor strengt dette kravet skal tolkes. Det kom ønske om mer tydelig veileder på dette området. Det ble kommentert under intervjuene at skyløsninger bør nevnes i ny veileder. Et annet forslag var å fokusere på kraftberedskapsforskriften, og dens tilknytning til NSMs grunnprinsipper. Disse prinsippene skal følges generelt, både for AMS og andre systemer. Av samme grunn ble det kommentert at punktet "overordnet sikkerhetsarbeid" er overflødig og at det heller bør refereres til NSM sine grunnprinsipper. Overvåking av hendelser er viktig, og dette inngår også i kraftberedskapsforskriften. En av de intervjuede nevnte at det mangler noe om andre tjenester som bruker samme infrastruktur, som vannmåling, nettstasjonsovervåking, osv. Fysisk beskyttelse av AMS-løsningen: hvordan håndtere dette kravet for HAN-port? Det er kundens "port" og data er ukryptert ut fra denne porten. Struping er en bra mulighet for rasjonering, at alle får noe – men det er mange forskjellige kunder. Dette er en potensiell sikkerhetsutfordring, men det er ingen av de intervjuede som har tatt i bruk struping ennå. Under hvert punkt i ny veileder bør det refereres til hvilke andre forskrifter som er relevante.

Spørsmål 17 bruk av sjekkliste	Ingen bruker sjekklista i dag, men sier at den ble brukt ved oppsett av systemer i den perioden AMS ble etablert. Sjekklista er tatt inn i den daglige driften og i prosesser, men brukes ikke aktivt som en separat sjekkliste. ROS-analyser utføres, og en av nettselskapene sier at dagens sjekkliste er dekket av ROS-analyser. Et annet nettselskap mener at det er behov for en helt annen type sjekkliste som kan brukes om det er noen problemer i AMS, f.eks. ved mistanke om hacking – hva gjør man da?
Spørsmål 18 innspill til oppdatering av veileder	Det var 2 av 7 nettselskaper som nevnte at det hadde vært nyttig med en veileder som samler flere tråder og gir en totaloversikt over krav til sikkerhet i AMS, da det er mange forskrifter man må forholde seg til. En slik veileder kan beskrive hva de ulike forskrifter inneholder av sikkerhetskrav – som er relevant for nettselskap. I dag er det mange ting som går over i hverandre og det er vanskelig å holde oversikt over gjeldende regelverk. En ny veileder kan inneholde forslag til måter å sikre head-end systemer på (overvåkninger eller lignende), i tillegg til praktiske eksempler. Utfordring for AMS: All trafikk ut fra head-end er kryptert, dermed er det vanskelig å overvåke trafikk. I drift av AMS er det viktig med testing, verifisering og overvåking. Det må stilles krav til leverandør til hva som er testet, dokumentert og levert. Hva gjør vi nå for å utnytte AMS bedre? Hva med det andre enn kun måleverdier? Hittil har det vært fokus på måleverdier knyttet til sikkerhet i AMS: Hvordan ivareta sikkerhet i AMS ved bruk av nye typer data? Ved innsamling av verdier med høyere og høyere oppløsning blir det mer og mer utfordrende mtp. personvern.
Spørsmål 19 og 20 § 4.6 i avregnings-forskriften	Avregningsforskriften § 4.6 i følges. 6 av 7 nettselskaper mener det ikke medfører store endringer og at den største endringen var utvidelsen av hva som dekkes av AMS og direkte henvisning til kraftberedskapsforskriften. Ett av nettselskapene sier de jobber med å lage en godkjenningsgruppe for hvert system for å godkjenne oppdateringer fra leverandører. Sikkerhet i AMS er en kontinuerlig prosess og nettselskapene følger med på endringer i forskrifter. Det ble kommentert at ende-til-ende-kryptering ikke er nødvendig, hvis man har kontroll på trafikken og detekterer uønsket aktivitet. Dette gjelder om man bruker eget datanettverk. Et nettselskap kommenterte at ansatte er observante på sikkerhet i AMS og at selskapet kjører egne kurs om generell IT-sikkerhet. Det er viktig at alle er oppmerksomme på sikkerhet fordi det daglig mottas phishing-mailer. Et nettselskap forteller at de har sikkerhetstester på ulike nivå i selskapet og at de har dobbelt opp av systemer, for å håndtere en full stopp av IT-systemer. Et nettselskap forteller at de har drift av AMS er på forskjellige lokasjoner av sikkerhetsgrunner.
Spørsmål 21 Elmålerforskriften	Elmålerforskriften krever beskyttelse mot manipulering av måleverdier. Et nettselskap forteller at de detekterer unormaliteter i forbruket, men at strøm-

	tyveri ikke er noe stort problem. Det kommer også varsler hvis deksel på måler tas av og ved sterke magnetfelt i nærheten av måleren. Det gjøres stikkprøve-kontroller av målere for å sjekke målenøyaktigheten. Det ble også gjort stikkprøver under produksjon av målerne. Justervesenet har vært på tilsyn hos en av de intervjuede nettselskapene for å sjekke internkontrollrutiner knyttet til elektrisitetsmålere.
Spørsmål 22 Person-opplysningsloven	Hendelser relevant for personvern rapporteres til Datatilsynet ifølge en av de intervjuede som hadde opplevd en hendelse. Datatilsynet har vært på tilsyn hos et av de intervjuede nettselskapene, men da knyttet til kundedata, og ikke AMS spesifikt. Nettselskapene arbeider mye med interne rutiner knyttet til kundedata (personopplysninger) for å sikre at disse ikke kommer på avveie.
Spørsmål 23 Kraftberedskaps-forskriften	Alle de intervjuede nettselskapene har hatt NVE på tilsyn. Kun et nettselskap skulle snart ha tilsyn med sikkerhet i AMS som tema. De andre tilsynene fra NVE var knyttet til kraftberedskapsforskriften, og disse tilsynene dekket mye (sentralsystem og punkter i sjekkliste), men ikke alt ut til måler hos kunde.
Systemleverandør, intervjuguide Vedlegg A.2	
Spørsmål 7 drift av AMS-system	Det er flere ulike modeller for drift av AMS-systemer. Noen nettselskaper står for all drift selv, med noe samarbeid med målerleverandør om oppdateringer osv. Andre har leverandører til å drifte Head-end-system (HES), eventuelt hele måleverdikjeden. Noen nettselskaper har leverandør som "host" for dataene sine og får tilgang til data gjennom dashboard. Skydrift av HES har blitt mer etterspurt og to leverandører nevner at de leverer dette som en tjeneste til nettselskapene. Ifølge de intervjuede systemleverandørene administrerer de krypteringsnøkler for noen nettselskaper. Men de fleste nettselskaper håndterer nøkler selv ved å oppdatere de symmetriske nøklene som leveres med måleren, samt at kortvarige sesjonsnøkler genereres for hver tilkobling. Avhengig av avtaleverk kan leverandører ha ansvar overfor nettselskapet for at sikkerhet leveres (ihht. avtale/kravspesifikasjon/angitte standarder) og fungerer som det skal,i tillegg til å oppdatere ved nye krav/utvikling (selv om det er nettselskapet som er ansvarlig for sikkerhet i AMS).
Spørsmål 8 og 9 bruk av dagens veileder internt	Veilederen er ikke i aktiv bruk av systemleverandørene i dag. Nettselskapene stilte i sin tid krav for målere ut fra veilederen, så den var aktuell i innkjøpsfasen. Noen systemleverandører lagde løsningene sine strengere enn lover og forskrifter for å være sikker på å tilfredsstille krav fra 2012. Det kan bli diskusjoner om veilederen dersom nettselskapene har ønsker som er i strid med veilederen. Nettselskapene tenker mest på funksjonalitet, så det er en avveiing mellom sikkerhet og "brukervennlighet". Sikkerhet kan medføre lengre tid til eksempelvis innlogging og annet som er "støy" for en vanlig bruker.
Spørsmål 10 sikkerhetsavtaler	Systemleverandørene inngår databehandleravtaler med alle kunder. Slike avtaler regulerer hva leverandøren kan og ikke kan gjøre. Det får konsekvenser om krav som kunden setter til leverandør blir brutt (bøter, medansvar) ved avvik knyttet til personvern/sikkerhet. Kunden har ofte rett til å revidere leverandør. Revisjon gjelder det som står i kontrakt med kunden, ikke revisjon av hele leverandør-bedriften. Noen leverandører er sertifisert, ISO 27001 ble nevnt. SSA-D (Statens standardavtale type D[6]) er nevnt som en brukt avtale.
Spørsmål 11, 12 og 13 sikkerhets-	Brytere har vært i fokus, og da risiko for å legge ut mange brytere samtidig. Beredskapsplaner er laget for hva som må gjøres hvis dette skjer. Det er lagt til

[6] https://anskaffelser.no/verktoy/maler-ogsa-kontrakt-og-avtalemaler/driftsavtalen-ssa-d

områder som mangler/ overflødige/ uklare	begrensinger i bryterstyring i form av begrensing på antall brytere som kan brytes samtidig innenfor et visst tidsrom. Egne krypteringsnøkler trengs for å få tilgang til bryterfunksjonen. Det er ulike krav, og enkelte nettselskap har både krav om riktig sertifikat og API-nøkkel for å kunne bryte strømmen. Noen nettselskaper har lagt til noe på toppen av dette, et styringsregime, hvor det er lagt styringsrettigheter til et eget miljø. Følgende er en problemstilling knyttet til systemleverandører og tilgang til bryterstyring: En leverandør av et system vil typisk måtte ha tilgang til systemet for oppgradering/feilretting, men skal selvfølgelig ikke operere brytere. Er alle krav i forskriften oppfylt selv om leverandørene har tilgang til funksjonen? Det er viktig at ny veileder spesifiserer hva som er eksempler og ikke krav (eneste løsning) som må overholdes. Det kan være ulike måter å oppfylle kravene på. Grensesnittene i AMS-infrastruktur A1/A2/A3 (Se figur 1.1) er gjennomarbeidet og testet, og det er bra. Bransjen er åpen for cloudbaserte løsninger og det er den veien det går. Dette vil medføre at ansvaret til leverandørene øker og det er viktig med gode avtaler med underleverandører. I dag er trolig de fleste angreps-punktene knyttet til cloud-/ skyløsninger. Det er ifølge de intervjuede system-leverandørene etablert akseptable løsninger for cloud/skyteknologi. Det er etablerte regimer for testing både av releaser og testing ende-til-ende hos nett-selskaper før nye versjoner slippes (i testmiljøer hos store nettselskaper). System-leverandørene melder revisjoner i selve målerne til Justervesenet og MID (måle-instrumentdirektivet) -godkjenning må fornyes ved store endringer. System-leverandørene har ikke vært invitert til sikkerhetsøvelser hos nettselskapene ennå, men forventer mer fokus på øvelser fremover. Det kom innspill om at det meste er med i veilederen slik den foreligger nå, men at fokus hos nettselskapene vil endre seg.
Spørsmål 14 bruk av sjekkliste	Sjekklisten brukes ikke aktivt i dag, men som en del av anskaffelsen ble den brukt.
Spørsmål 15 innspill til oppdatering av veileder	Systemleverandørene er mest opptatt av NSM og kraftberedskapsforskriften og at en veileder innen sikkerhet i AMS må stemme overens med generell IKT-sikkerhet. NSM sine grunnprinsipper er viktige for flere aktører, eksempel: hvordan oppbevare nøkkelmateriell (flere referer til FIPS-godkjente lagringsmekanismer, dvs. FIPS 140-3, som nå henviser til ISO/IEC 19790:2012(E)). Ny veileder for bruk av skytjenester ble også nevnt som et dokument som benyttes i dag av systemleverandørene. Sikkerhetshendelser er viktig og bør være med i ny veileder. Angående "fysisk beskyttelse" må det som står i kraftberedskapsforskriften oppfylles. I lys av digitalisering er det viktig å sette kontekst for hva punktene i veilederen egentlig innebærer. Veilederen må ha krav som er realistiske å tilfredsstille på eksisterende målerpark, mener en av de som ble intervjuet. Fremover er det også viktig at veileder fokuserer mer på sikkerhet i forhold til programvare-håndtering, versjoner, oppgradering, fjernoppgradering, kryptering, osv. Det er mer behov for veiledning på IT-sikkerhet enn på fysisk sikkerhet, eksempelvis hvordan gjøre sikring – mekanisk eller virtuelt skille? Det er strenge krav i dag til fysisk skille, men det kunne blitt bedre tjenester hvis det var virtuelle skiller, som er trygt (selv om det er remote).

	Veilederen burde konkretisere operasjonelle driftsaspekter, f.eks. hvordan håndtere måler via fjernstyring? Veilederen må ta hensyn til at det svinger mer mot bruk av offentlig telekom, eksemplifisert ved at 60% av det svenske markedet benytter offentlig telekom. Veileder må ikke stille så strenge krav at man ikke kan bruke offentlig telecom. Ende-til-ende-kryptering var med i det gamle systemet, men er nå innebygd i kommunikasjonsløsningen. Det bør ikke være forskjellige krav til eksisterende og nytt utstyr. Kritiske punkter (som gjelder både nye og gamle målere) er: • Programvareoppdateringer • Hacking av brytere • Styring av brytere Det bør også avklares om det er ok at leverandører har kontroll på nøkler. Bør det stilles krav til hvor nøkler lagres, eller dekkes det av andre krav? Kommunikasjonskrav må være oppdatert ut fra hva målerleverandører har av tilgjengelige kommunikasjonsløsninger i dag. Man bør også ta hensyn til kryperingsmuligheter i public cloud, samt under kryptering av transport. Det er viktig å sikre data også under lagring Det er også behov for gode krav knyttet til identifisering og autentisering. Det er viktig å sikre at det er riktig måler som kobler seg til riktig system. Krav knyttet til integritet i programvare oppleves av noen som litt gammeldagse. Det finnes noe testopplegg i målere som sjekker at det ikke har skjedd endringer i programvaren. Ved firmware-oppdatering av målere er det viktig at nettselskapet har kontroll på hva som skjer ute i målerne. EMI-beskyttelse dekkes av annet lovverk som MID – Metering Infrastructure Directive.
Spørsmål 16 og 17 § 4.6 i avregnings-forskriften	a) Enheter – ok b) Endring programvare – vanlig med sporbarhet. c) Ende-til-ende-kryptering – diskusjon om "mellomdata" lagres i konsentratorer? Nå har nettstasjonsovervåking erstattet dette? a. Fra måler og inn til head-end. d) Oppdatert programvare – litt for "micro management"? Hva betyr "oppdatert"? Forrige versjon, eller enda eldre versjon. a. Autentisk programvare – Sikkerhetsdiskusjon mellom kunde og leverandør. b. Egen elektronisk signatur/signaturnøkkel – for at måler skal kunne kjenne igjen en autentisk programvare. e) Hendelser – Spørsmål til måler-/komm.leverandør f) Design – kundens ansvar om det kjøpte systemet dekker det som er bestilt. a. Aktivere/deaktivere funksjonalitet – gjøres fra HES b. Brukerstyring – tofaktorstyring av tilgang.

	g) Tilgang a. Har ingen begrensning. Sikre at rett kunde ber om at HAN-port åpnes. Automatisk lukking av HAN-port når kunden flytter. Nye forskrifter har ikke endret hvordan sikkerhet til AMS håndteres. Endringen i loven førte ikke til noen protokollendringer eller lignende.
Spørsmål 18 Elmålerforskriften	Målerprodusentene er i kontakt med Justervesenet om produktene sine, men ikke tjenesteleverandører. Det er nå overvåkning på deksel og magnetmanipulasjon etc., så nettselskapet har aldri hatt bedre kontroll.
Spørsmål 19 Person-opplysningsloven	Databehandleravtale er viktig. Datatilsynet har vært aktive på temaet personvern og AMS, og opptatt av at oppløsningen av data ikke skal være høyere enn nødvendig og at formålet med datainnsamlingen skal være godt dokumentert. Det er også viktig at kundedata til strømkundene er godt håndtert og at leverandørene vet minst mulig om strømkundene. Brudd på personopplysningsloven varsles til Datatilsynet.
Spørsmål 20 Kraftberedskaps-forskriften	Kraftberedskapsforskriften er viktig, men systemleverandørene er ikke KBO-er og har derfor ikke NVE på tilsyn. Grensesnitt kraftberedskapsforskrift og avregningsforskrift er ifølge en av de intervjuede som følger: • AMS er (i dag) ikke en del av nettdrift. • 10% av datainnsamlingen gjelder måling og avregning. Analyse og nettnyttedata utgjør de resterende 90% av datamengden.
Myndighetsorganer, Intervjuguide Vedlegg A.2	
Spørsmål 5 og 6 deres regelverk omhandler sikkerhet i AMS	Det er en klar link til sikring av digitale informasjonssystemer (paragraf 6.9) og bryterfunksjonalitet i AMS (paragraf 6.10) i kraftberedskapsforskriften. NVE skal sikre at alle har strøm, mens RME skal sørge for at aktørene overholder regelverket som sikrer like konkurransevilkår i kraftmarkedet og et effektivt drevet strømnett. HAN-porten og det som kobles på HAN-porten er utenfor NVE sitt område. Unntatt om tredjepartsaktører blir så store at de påvirker stabiliteten i nettet – da vil NVE blande seg inn. Leverandører av AMS er innenfor NVE sitt ansvarsområde da de har tilgang til målere og kan bryte strømmen. Tilsyn med 6.10 innebærer tilsyn med AMS - noe ble installert før kravene, må kanskje omgjøres? Tilsyn er opptatt av forsyningssikkerhet og bryter. Hvis ikke var bryter i AMS, så hadde det ikke vært krav fra NVE. Men så ble det mulig å koble ut kunder som ikke betaler: nettselskap skal ha egne sikkerhetstiltak for bryterfunksjonalitet. Ingen krav til "separation of duty" i forskrift, men spør om det på tilsyn. En måte å sikre at det ikke blir masseutkobling er at det er to stykker som må bryte. Nesten ingen har dette, men begrensninger på antall målere som kan kobles ut innen et tidsrom og avgrense antall personer som kan bryte. Kan være riktig å koble ut raskt (rasjonering - har ikke skjedd). Det er få kunder samtidig i dag. Rasjoneringsforskriften er også gyldig – det kan være et gode i anstrengte situasjoner å kunne koble ut mange. For Datatilsynet er det personopplysningsloven (GDPR) som er relevant mht sikkerhet i AMS. Det er sluttbrukers personopplysninger som Datatilsynet er

	opptatt av og reguleringer av behandlingsansvar. Databehandleravtaler er viktig. Datatilsynet er bekymret for at det blir for mange aktører som skal behandle AMS-data og at ansvaret blir uklart. Justervesenet er opptatt av korrekt måling. Det er Elmålerforskriften som er mest relevant med tekniske krav til måler og målefunksjon. Justervesenet skal godkjenne også kommunikasjonsenhet som oversender måledata for å sikre at måledata er riktig. Justervesenet kommer til å inkludere krav til sikring ved oversendelse av data og gjennom hele måleverdikjeden. Datastrøm fra måler til fakturering. Mest relevant knyttet til kvalitetssikring §3.10. Sikre at de målte verdiene som brukes som grunnlag for økonomisk oppgjør er korrekte. HAN-porten er ikke interessant for Justervesenet.
Spørsmål 7 vurdert veileder til sikkerhet for AMS i utvikling av regelverket	Det er ingen link fra kraftberedskapsforskriften til veileder for sikkerhet i AMS.
Spørsmål 8 viktige grensesnitt	Infrastruktur med forbrukere og produsenter er felles for RME og NVE. Forbrukere er RME sitt bord. Det er KBOenhetene som reguleres av NVE. Nettselskap er KBOer, alle sammen. Kraftmarkedet er litt i grenseland mellom RME og NVE. NVE har ikke lagt strømsalg til KBO.
Spørsmål 12 og 13 sikkerhetsområder som mangler/ overflødige/ uklare	Hovedmangelen er HAN-porten i veileder. Det er viktig at HAN kun åpnes når sluttbruker vil. Når HAN er åpnet - hva da? Hvordan ivaretas personvern da? De som får tilgang til HAN-data skal forholde seg til personvernlovgivning og blir behandlingsansvarlig og regulert av Datatilsynet. HAN-data er kontinuerlige og dermed mer alvorlige personvernmessig enn timesverdier for sluttbrukere. Veilederen er relevant. Ende -til -ende kryptering er avgjørende. Noen mener at dette er utdatert fordi det er kommet bedre løsninger. Datatilsynet er IKKE enig i dette. Det må en veldig god risikovurdering for å komme fra dette kravet. NVE sin veileder: henvist til litteratur og ikke så detaljert som AMS sikkerhetsveilederen. Behov for sikkerhetsveileder for AMS? Det som går på markedet og måleverdi er ikke dekket av KBF. Fokusere på dette! F) Fjerntilgang (skjedd ting de siste 10 årene) - like relevant i dag? Brytefunksjonalitet - leverandør kan ikke koble ut og inn kunder. Bygger inn sikkerhet. Ikke nødvendigvis feil med hjemmekontor (pålogging via flere nivå). NSM grunnprinsipper og 6.9 i KBF - bygger på internasjonale standarder. Tilleggskrav til grunnprinsipper: papirkopier (skisse av nettet som utgangspunkt ved restart). Skille RME/NVE har skjedd siden 2012. §4-6d) Programvare skal være oppdatert… Dersom den delen av måleren som kommuniserer måleverdier er inkludert i samsvarsvurdering, vil det være evt. hinder mot oppdatering. Låses inn, kan ikke

	oppgraderes. I Norge inkluderes denne kommunikasjonsmodul vanligvis ikke i samsvarsvurdering. En leverandør kan få samsvarsgodkjenning i andre land i Europa, og bruke den i Norge.
Spørsmål 14 og 15 paragraf 4.6 i avregnings-forskriften	Paragraf 4.6 supplerer og henviser til kraftberedskapsforskriften. 4.6 er ikke noe nytt sammenlignet med kraftberedskapsforskriften, men det kan være at virkeområdet er ulikt? Utfordring at nettselskapene har så mange forskjellige system og kan ikke bare kaste ut det som er gammelt. Det blir viktig å spore/detektere og oppdage om det skjer noe uregelmessig. Ende-til-endre kryptering beskytte personvern/forretningssensitive opplysninger og gjøre skadeverk. Oppdatert programvare er et godt sikkerhetsprinsipp - problem å ha i forskrift: noen har gammelt AMS-system som ikke kan oppdateres, fungerer ikke sammen hvis har noe gammelt og noe nytt. Punkt F) er et funksjonskrav - det er likt kap 7 med driftskontrollsystem, opp til selskapet de skal ha for å oppfylle dette (tilgjengelighet, kvalitet og integritet).

6 Referanser

[1] NVE, «Veiledning til kraftberedskapsforskriften,» NVE, 07 12 2020. [Internett]. Available: https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap/veiledning-til-kraftberedskapsforskriften/. [Funnet 20 12 2021].

[2] www.lovdata.no, «FOR-2021-06-25-2308 Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv,» 01 07 2021. [Internett]. Available: https://lovdata.no/dokument/SF/forskrift/1999-03-11-301.

[3] F. S. (NVE) og B. J. (Deloitte), «NVE-rapport 7/2012 - Veileder til sikkerhet i avanserte måle- og styringssystem,» https://www.nve.no/Media/5525/veiledertil-sikkerhet-i-ams.pdf, 2012.

[4] www.lovdata.no, «FOR-2018-11-01-1641 Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften),» 01 01 2019. [Internett]. Available: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157. [Funnet 19 10 2021].

[5] H. Sæle, M. Bartnes, B. A. Høverstad og M. G. Jaatun, «NVE-rapport 44/2017 - Evaluering av NVEs veileder til sikkerhet i AMS,» https://publikasjoner.nve.no/rapport/2017/rapport2017_44.pdf, 2017.

[6] H. Sæle, K. Ingebrigtsen og M. Istad, «NVE-rapport 34/2019 Fremtidens Avanserte Måle- og Styringssystem (AMS). Forventet utvikling 2-5 år frem i tid,» http://publikasjoner.nve.no/rapport/2019/rapport2019_34.pdf.

[7] Ø. A. A. Toftegaard og H. A. Hillestad, «NVE-rapport 1/2018 Forslag til endring i forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv.,» https://publikasjoner.nve.no/hoeringsdokument/2018/hoeringsdokument2018_01.pdf, 2018.

[8] H. A. Hillestad, Ø. A. A. Toftegaard, Å. G. Tveten og A. Kellerer, «RME Høringsdokument Nr. 2/2020 Konsepthøring om forslag til innføring av 15 minutters tidsoppløsning i balanseavregningen og Høring om forslag til endring av Avregningsforskriften,» http://publikasjoner.nve.no/rme_hoeringsdokument/2020/rme_hoeringsdokument2020_02.pdf.

[9] H. A. Hillestad, Ø. A. A. Toftegaard, C. Hovind og A. Kellerer, «RME Rapport Nr. 1/2021 Oppsummering av høringsinnspill og forslag til innføring av 15 minutters tidsoppløsning i balanseavregningen og høringsinnspill og forslag til endring av Avregningsforskriften,» https://publikasjoner.nve.no/rme_rapport/2021/rme_rapport2021_01.pdf.

[10] Norsk Elektroteknisk Komite, «Vedlegg 1 – HAN Personvern – et tillegg til utredningen "AMS + HAN – om å gjøre sanntids måledata tilgjengelig for forbruker",» https://www.nek.no/wp-content/uploads/2018/02/AMS-HAN-Vedlegg-1-Personvern-NEK-rapport-20180215.pdf, Lilleaker 15. februar 2018.

[11] NEK - Norsk Elektroteknisk Komite, «AMS + HAN. Om å gjøre sanntid måledata tilgjengelig for forbruker. Hoveddokument. Versjon 2.0.,» https://www.nek.no/wp-content/uploads/2017/01/AMS-HAN-utredning-NEK-20150122.pdf, 2015.

[12] Nasjonal sikkerhetsmyndighet, «NSMs Grunnprisipper for IKT-sikkerhet, versjon 2.0,» https://nsm.no/getfile.php/133735-1592917067/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf.

[13] M. G. Jaatun, E. Wille, K. Bernsmed og S. S. Kilskar, «Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer,» https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/id4-grunnprinsipper-for-ikt-sikkerhet_sintef-rapportnr-2021-00055-feb---signert.pdf, 2021.

[14] Nasjonal Sikkerhetsmyndighet, «Sikkerhetsfaglige anbefalinger ved tjenesteutsetting,» https://nsm.no/getfile.php/133666-1592829282/Filer/Dokumenter/tjenesteutsetting2018v1.1_enkelstsider.pdf, 2018.

[15] www.lovdata.no, «LOV-2018-12-20-116 Lov om behandling av personopplysninger (personopplysningsloven),» www.lovdata.no, 20 07 2018. [Internett]. Available: https://lovdata.no/dokument/NL/lov/2018-06-15-38.

[16] Datatilsynet, «Automatisk strømmåling,» 21 06 2018. [Internett]. Available: https://www.datatilsynet.no/personvern-pa-ulike-omrader/overvaking-og-sporing/strommaling/. [Funnet 20 12 2021].

[17] Datatilsynet, «Datatilsynets oppgaver,» [Internett]. Available: https://www.datatilsynet.no/om-datatilsynet/oppgaver/. [Funnet 20 12 2021].

[18] www.lovdata.no, «FOR-2018-12-10-1883 Forskrift om krav til elektrisitetsmålere,» 01 01 2019. [Internett]. Available: https://lovdata.no/dokument/SF/forskrift/2007-12-28-1753. [Funnet 05 01 2022].

[19] Justervesenet, «Om Justervesenet,» [Internett]. Available: https://www.justervesenet.no/aktuelt/om-justervesenet/. [Funnet 20 12 2021].

[20] Justervesenet, «Elektrisitetsmålere - Regelverk,» 17 10 2019. [Internett]. Available: https://www.justervesenet.no/regelverk/justervesenets-arsavgift-og-gebyrer/elektrisitetsmalere/. [Funnet 20 12 2021].

[21] Justervesenet, «Elektrisitetsmålere - Tilsyn,» 16 12 2021. [Internett]. Available: https://www.justervesenet.no/tilsyn/elektrisitetsmalere/. [Funnet 20 12 2021].

[22] M. Bartnes, G. I. Johansen og H. Sæle, «SINTEF-rapport A22318 "Risikovurdering AMS",» https://infosec.sintef.no/informasjonssikkerhet/2012/02/risikovurdering-av-ams/, 2012.

A Intervjuguider

A.1 Intervjuguide for nettselskap

Hovedmålsettingen for oppdraget er å omarbeide veiledere til sikkerhet i AMS, som skal

- innholdsmessig bygge på forrige veileder til sikkerhet i AMS samt rapport 44/2017 og 34/2019
- opplyse om overlappende regelverk (for eksempel personopplysningsloven og kraftberedskapsforskriften)
- kunne fungere som en interaktiv veileder på web

Mål med intervjuene:

- Innhente oppdatert informasjon om status for bruk av AMS og sikkerhet i AMS

Målgruppe/type informanter: 1-2 ressurspersoner hos 10-15 nettselskap av ulik størrelse (små – mellomstore – store).

Metode: ca. 1 timers dybdeintervju (semi-strukturerte) høsten 2021.

1. Innledning

Generell informasjon om prosjektet, og databehandling.

1. kort informasjon rundt prosjektet og håndtering av data.

Spørsmål knyttet til informanten og selskap

2. Be informanten fortelle litt om seg selv og stilling/rolle i organisasjonen/arbeidsplass
3. Be informanten fortelle om organisasjon/arbeidsplass/rolle knyttet til sikkerhet i AMS

2. Status i dag ang. AMS

4. Hvilken AMS-løsning har dere installert?
5. Hvor mange kunder er det i nettområdet, og hvor mange AMS-målere er installert?
6. Hvor mange kunder har åpnet HAN-port? Hva skjer med HAN-port ved f.eks. ved at kunden flytter?
7. Hvem kan bruke serviceporten? Hvordan følges tilganger opp?
8. Hvem har tilgang til serviceporten på AMS-målene og hvordan følges tilgangen opp?
9. Hvordan administreres krypteringsnøkler i AMS?
10. Drifter dere hele AMS-systemet selv, er det deler som driftes av andre selskaper, evt. hvilke deler og av hvem?

3. Status i dag ang. bruk av veileder til sikkerhet for AMS

11. Er veileder til sikkerhet for AMS i bruk i selskapet i dag, og hvordan (f.eks. til hvilket formål/oppgave, hvem, hvor ofte, …) brukes denne i dag? Hvilke deler av selskapet er involvert i arbeidet med sikkerhet for AMS? Kom gjerne med eksempler på bruk av veileder.
12. Hvis deler av AMS-systemet driftes av andre: Hvordan brukes veileder til sikkerhet for AMS i dialog med driftsselskap?
13. Hvordan brukes veileder i dialog med AMS-/systemleverandør? (Angi type leverandør)
14. Er det etablert egne avtaler knyttet til håndtering av sikkerhet i AMS, når andre selskaper drifter deler av AMS-systemet på vegne av nettselskapet? Hvordan er ansvar for sikkerhet spesifisert/ dokumentert?

4. Evaluering av dagens veileder

Dagens veileder til sikkerhet i AMS inneholder de sikkerhetsområder som er presentert i tabell A1 (kap. A.4).

15. Er det noen sikkerhetsområder som mangler, eller er overflødig i dagens veileder?
16. Er det noe som er uklart/tvetydig/utdatert i dagens veileder og sikkerhetsområder?
17. Brukes sjekklista som er med i veileder, og evt. hvordan (f.eks. til hvilket formål/oppgave, hvor ofte, …)?
18. Veileder til sikkerhet i AMS ble utarbeidet mens utrullingen av AMS pågikk. Har du/dere innspill til om noe som bør endres/oppdateres som følg av at AMS nå er ferdig installert og har kommet over i driftsfasen?

5. Forskriftskrav til sikkerhet i AMS

19. I hvilken grad og hvordan er nye forskriftskrav til sikkerhet i AMS (§4-6 i forskrift for måling og avregning), tatt hensyn til? Kom gjerne med eksempler?
20. Har nye forskrifter medført at dere har endret på hvordan dere håndterer sikkerhet til AMS? Kom gjerne med eksempler?

6. Annet lovverk/forskrifter som er relevant for sikkerhet i AMS

21. Elmålerforskriften krever beskyttelse mot manipulering av måleverdier. Hvordan fungerer grensesnittet mellom elmålerforskriften og forskriftskrav om sikkerhet i AMS i dag?
22. Datatilsynet fører tilsyn med personopplysningsloven. Har dere hatt tilsyn fra Datatilsynet?
    a) Datatilsynet har bestemt at strømforbruk er personopplysninger. Hvordan fungerer grensesnittet mellom personopplysningsloven og forskriftskrav om sikkerhet i AMS i dag? Er det behov for endringer?
23. NVE fører tilsyn med kraftberedskapsforskriften. Har dere hatt tilsyn fra NVE?
    a) Hvordan fungerer grensesnittet mellom kraftberedskapsforskriften og forskriftskrav om sikkerhet i AMS i dag?
    b) Er det behov for endringer?

A.2 Intervjuguide for systemleverandører

Hovedmålsettingen for oppdraget er å omarbeide veiledere til sikkerhet i AMS, som skal

- innholdsmessig bygge på forrige veileder til sikkerhet i AMS samt rapport 44/2017 og 34/2019
- opplyse om overlappende regelverk (for eksempel personopplysningsloven og kraftberedskapsforskriften)
- kunne fungere som en interaktiv veileder på web

Mål med intervjuene:

- Innhente oppdatert informasjon om status for bruk av AMS og sikkerhet i AMS

Målgruppe/type informanter: 1-2 ressurspersoner hos relevante systemleverandører.

Metode: ca. 1 timers dybdeintervju (semi-strukturerte) høsten 2021.

1. Innledning

Generell informasjon om prosjektet, og databehandling.

1. kort informasjon rundt prosjektet og håndtering av data.

Spørsmål knyttet til informanten og selskap

2. Be informanten fortelle litt om seg selv og stilling/rolle i organisasjonen/arbeidsplass

3. Be informanten fortelle om organisasjon/arbeidsplass/rolle knyttet til sikkerhet i AMS
4. Hvor mange nettselskap leverer dere systemer til?
5. Hvor mange AMS-målere har dere levert

2. Status i dag ang. AMS

6. Hvilken AMS-løsning har dere levert?
7. Drifter dere deler av AMS-systemet på vegne av nettselskap? Beskriv hvordan?

3. Status i dag ang. bruk av veileder til sikkerhet for AMS

8. Er veileder til sikkerhet for AMS i bruk i selskapet i dag, og hvordan (f.eks. til hvilket formål/oppgave, hvem, hvor ofte, …) brukes denne i dag? Hvilke deler av selskapet er involvert i arbeidet med sikkerhet for AMS? Kom gjerne med eksempler på bruk av veileder.
9. Hvordan brukes veileder til sikkerhet for AMS i dialog med nettselskap?
10. Er det etablert egne avtaler knyttet til håndtering av sikkerhet i AMS, når andre selskaper drifter deler av AMS-systemet på vegne av nettselskapet? Hvordan er ansvar for sikkerhet spesifisert/ dokumentert?

4. Evaluering av dagens veileder

Dagens veileder til sikkerhet i AMS inneholder de sikkerhetsområder som er presentert i tabell A1 (kap. A.4).

11. Er det noen sikkerhetsområder som mangler, eller er overflødig i dagens veileder sett fra dere som leverandør?
12. Er det spesielle temaer/områder som nettselskapene er opptatt av som mangler i dagens veileder?
13. Er det noe som er uklart/tvetydig/utdatert i dagens veileder og sikkerhetsområder?
14. Brukes sjekklista som er med i veileder, og evt. hvordan (f.eks. til hvilket formål/oppgave, hvor ofte, …)?
15. Veileder til sikkerhet i AMS ble utarbeidet mens utrullingen av AMS pågikk. Er det noe som bør endres/oppdateres som følg av at AMS nå er ferdig installert og har kommet over i driftsfasen?

5. Forskriftskrav til sikkerhet i AMS

16. I hvilken grad og hvordan er nye forskriftskrav til sikkerhet i AMS (§4-6 i forskrift for måling og avregning), tatt hensyn til? Kom gjerne med eksempler?
17. Har nye forskrifter medført at dere har endret på hvordan dere håndterer sikkerhet til AMS? Kom gjerne med eksempler?

6. Annet lovverk/forskrifter som er relevant for sikkerhet i AMS

18. Justervesenet fører tilsyn med elmålerforskriften. Elmålerforskriften krever beskyttelse mot manipulering av måleverdier. Hvordan fungerer grensesnittet mellom elmålerforskriften og forskriftskrav om sikkerhet i AMS i dag?
    a. Er det behov for endringer?
19. Datatilsynet fører tilsyn med personopplysningsloven. Datatilsynet har bestemt at strømforbruk er personopplysninger. Hvordan fungerer grensesnittet mellom personopplysningsloven og forskriftskrav om sikkerhet i AMS i dag?
    a. Er det behov for endringer?
20. NVE fører tilsyn med kraftberedskapsforskriften. Hvordan fungerer grensesnittet mellom kraftberedskapsforskriften og forskriftskrav om sikkerhet i AMS i dag?
    a. Er det behov for endringer?

A.3 Intervjuguide for myndighetsorganer

Hovedmålsettingen for oppdraget er å omarbeide veiledere til sikkerhet i AMS, som skal

- innholdsmessig bygge på forrige veileder til sikkerhet i AMS samt rapport 44/2017 og 34/2019
- opplyse om overlappende regelverk (for eksempel personopplysningsloven og kraftberedskapsforskriften)
- kunne fungere som en interaktiv veileder på web

Mål med intervjuene:

- Innhente oppdatert informasjon om gjeldende lover og forskrifter knyttet til sikkerhet i AMS

Målgruppe/type informanter: 1-2 ressurspersoner hos relevante myndighetsorganer.

Metode: ca. 1 timers dybdeintervju (semi-strukturerte) høsten 2021.

1. Innledning

Generell informasjon om prosjektet, og databehandling.

1. kort informasjon rundt prosjektet og håndtering av data.
2. intensjon om å hjelpe bransjen med å få oversikt over tilgrensende regelverk og henvise til regelverk som er relevant.

Spørsmål knyttet til informanten og selskap

3. Be informanten fortelle litt om seg selv og stilling/rolle i organisasjonen/arbeidsplass
4. Be informanten fortelle om organisasjon/arbeidsplass/rolle knyttet til sikkerhet i AMS

2. Status i dag ang. AMS

5. Hvilke(t) av deres regelverk omhandler AMS? Hvilke deler av AMS er behandlet? (Måler hos kunde, grensesnitt på måler, kommunikasjonssystem, sentralsystem hos nettselskap, data)
6. Hvilke punkter i deres regelverk er relevante for sikkerhet i AMS?

    a. Justervesenet: Elmålerforskriften?
    b. Datatilsynet: Personopplysningsloven?
    c. NVE: Kraftberedskapsforskriften?
    d. Annet?

3. Status i dag ang. bruk av veileder til sikkerhet for AMS og utvikling av regelverk

7. Har dere vurdert veileder til sikkerhet for AMS i utvikling av det regelverket som dere har ansvar for?
8. Ser dere noen viktige grensesnitt, evt. overlappende tematikk, mellom deres regelverk og forskrift om måling og avregning, knyttet til sikkerhet i AMS?
9. Datatilsynet: Hvilken type AMS-data berøres av deres regelverk?
10. Datatilsynet: Dere har godkjent NEK sitt forslag til løsning på hvordan personvern blir tilfredsstillende for AMS-HAN[7]. Virker dette å fungere godt? Har dere planer om mer regulering på dette området?
11. Datatilsynet: Vil det være andre krav for personvern når AMS-date blir 15 minuttersmålinger i 2023?

4. Evaluering av dagens veileder

Dagens veileder til sikkerhet i AMS inneholder de sikkerhetsområder som er presentert i tabell A1 (kap. A.4).

[7] https://www.nek.no/wp-content/uploads/2018/02/AMS-HAN-Vedlegg-1-Personvern-NEK-rapport-20180215.pdf

12. Er det noen sikkerhetsområder som mangler, eller er overflødig i dagens veileder? F.eks. at de dekkes av andre regelverk en forskrift om måling og avregning?
13. Er det noe som er uklart/tvetydig/utdatert i dagens veileder og sikkerhetsområder, ref. andre regelverk?

5. Forskriftskrav til sikkerhet i AMS

14. I hvilken grad og hvordan er nye forskriftskrav til sikkerhet i AMS (§4-6 i forskrift for måling og avregning), tatt hensyn til i andre regelverk? Kom gjerne med eksempler?
15. Har nye forskrifter medført at dere har endret på hvordan dere ser på sikkerhet til AMS, evt. behov for presiseringer i eget regelverk? Kom gjerne med eksempler?

A.4 Vedlegg til intervjuguidene

Tabell A1 Sikkerhetsområder i dagens veileder til sikkerhet i AMS

Sikkerhetsområde	Kontrollmål
A. Krav til nettselskapet i henhold til forskrift	A.1 Robust sikkerhetsfunksjonalitet A.2 Sikkerhet i kommunikasjon i AMS-løsningen A.3 Utsetting av utrulling og/eller drift av AMS-løsningen til tredjepart
B. Overordnet sikkerhetsarbeid rundt AMS	B.1. Etablering og oppfølging av sikkerhetskrav B.2 Risiko- og sårbarhetsanalyse B.3 Oppdatert dokumentasjon av AMS-løsningen B.4 Sikkerhetsavtaler
C. Kontroll med tilgang til system og utstyr	C.1 Tilgangskontroll - system C.2 Identifisering og autorisasjon av enheter C.3 Identifisering og autorisering av eksternt utstyr C.4 Kontroll med integriteten til programvare C.5 Elektronisk beskyttelse mot ondsinnet programvare og inntrengning C.6 Oppbevaring av sikkerhetssertifikater og krypteringsnøkler
D. Overvåking og håndtering av hendelser	D.1 Kontroll med sårbarheter i programvare D.2 Logging og overvåking D.3 Avviks- og hendelseshåndtering D.4 Katastrofehåndtering og –øvelser D.5 Sikkerhetskopier og gjenoppretting
E. Endrings- og versjonskontroll	E.1 Kontroll med endringer i AMS E.2 Oversikt over versjoner i program- og maskinvare
F. Fjerntilgang til AMS-løsningen	F.1 Fjerntilgang til AMS fra tredjepart eller leverandør
G. Fysisk beskyttelse av AMS-løsningen	G.1 Beskyttelse mot fysisk uautorisert tilgang til AMS-utstyr
H. Bryte- og strupefunksjonalitet	H.1 Beskyttelse av bryte- og strupefunksjonalitet
I. Elektromagnetisk interferens (EMI)	I.1 Beskyttelse mot EMI

B Veileder til sikkerhet for "Avanserte måle- og styringssystemer" (AMS) i avregningsforskriften

Innholdsfortegnelse

B.1 Innledning

Reglene om avanserte måle- og styringssystemer (AMS) skal bidra til korrekt avregning, nødvendig informasjon til styring av eget strømforbruk og økt mulighet for nettselskapet til å effektivisere driften av nettet. Disse er gitt i forskrift 11. mars 1999 nr. 301 om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. (avregningsforskriften) [2].

Innføringen AMS gir en rekke fordeler, hvor en av de tydeligste er å opprette direkte kommunikasjon mellom kundenes strømmålere og nettselskapet for oversendelse av målerdata ved automatisk avlesning av målerne[8]. Nettselskapene skal sørge for at AMS er installert i hvert målepunkt, dvs. at det er nettselskapene som har ansvaret for å innføre og drifte AMS-systemet i sitt forsyningsområde.

Denne veilederen er utarbeidet for å vise hvordan et nettselskap kan tilfredsstille kravene gitt i avregningsforskriften § 4-6 om krav til sikkerhet for AMS [2]. Veilederen er inndelt tilsvarende som kravene i § 4-6 bokstav a til g.

Veilederen gir noen eksempler på sikkerhetstiltak som kan implementeres i AMS-løsninger for å kunne bidra til oppfyllelse av forskriftens krav.

B.2 Veilederens virkeområde og omfang

Virkeområde
Veilederens virkeområde er sikkerhet i AMS for nettselskap, som definert i avregningsforskriften § 1-3.

Omfang
Veiledningen omfatter innsamlingssystemet – fra målepunktet hos kunden til sentralsystemet hos nettselskap, samt tilhørende kommunikasjonssystem mellom disse. Veilederen følger definisjon av AMS, som definert i avregningsforskriften § 1-3:

Avanserte måle- og styringssystemer (AMS): Toveis informasjons- og kommunikasjonssystem fra og med elektrisitetsmålere som danner grunnlag for avregning av utveksling, innmating og uttak, til og med sentralsystemet hos nettselskapet eller nettselskapets leverandør.

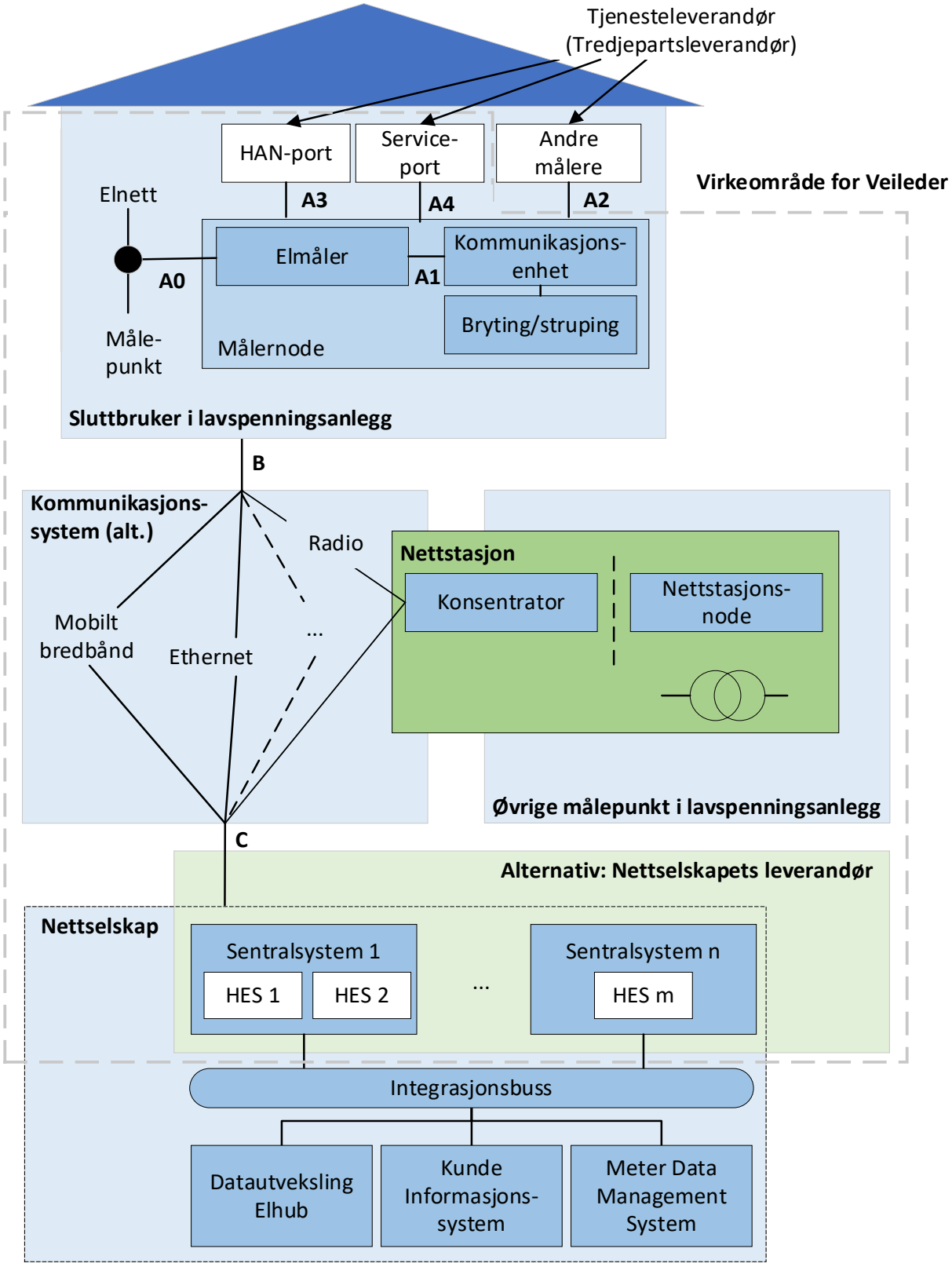
Definisjonen inkluderer alle målepunkt benyttet for avregning i lav- og høyspenningsanlegg, inkludert alle målepunkt for uttak, innmating og utveksling mellom nettområder. Der ikke annet er spesifisert, er det denne definisjonen av AMS som gjelder. Hvis det er spesielle forhold knyttet til AMS lokalisert hos sluttbruker eller i det øvrige strømnettet, er dette særskilt beskrevet.

Figur B.1 er en illustrasjon av hvilke systemer som overfører AMS-data i forbindelse med driften av AMS, og ikke en detaljert beskrivelse av IT-strukturen for AMS. Fokus i illustrasjonen er på AMS tilknyttet målepunkt i lavspenningsanlegg. Grensesnitt A-C er basert på tidligere skisser av AMS-infrastruktur [22]. Figuren viser målepunkt i lavspenningsanlegg – både for sluttbruker og øvrige målepunkt, slik det der definert i avregningsforskriften [2].

Målerne som er inkludert i AMS-figuren, er direktekoblede målere i lavspenningsanlegg. For måler hos sluttbruker er det angitt hvilke interne deler som inngår, og ulike grensesnitt A0-A3 er vist. Målere med

[8] I denne sammenhengen er automatisk avlesning synonymt med fjernavlesing.

måletrafo (for kunder i lavspenningsanlegg, men uten brytefunksjonalitet) og presisjonsmålere med målertrafo for høyspenningsanlegg er ikke inkludert i figuren selv om disse målertypene også kan levere verdier over samme infrastruktur.



Figur B.1 Illustrasjon av AMS-infrastruktur

I forbindelse med kommunikasjon fra kunde til nettstasjon (Mellom grensesnitt B og C), benyttes noen ganger en master/ konsentrator i nettstasjon. Denne enheten samler inn data fra alle underliggende målere og overfører dette samlet inn til sentralsystemet hos nettselskapet. Ulike kommunikasjonsløsninger kan brukes, og dette er illustrert ved å ta med flere alternativer i figuren. Det er ikke gjort forsøk på å lage en uttømmende oversikt, og derfor er det også inkludert en stiplet linje. Noen løsninger bruker konsentrator f.eks. plassert i en nettstasjon, for å samle opp måledata fra AMS-målere, for deretter å sende disse videre inn til sentralsystemet hos nettselskap. Ved f.eks. bruk av radio-mesh, kan en måler installert hos sluttbruker fungere som en konsentrator.

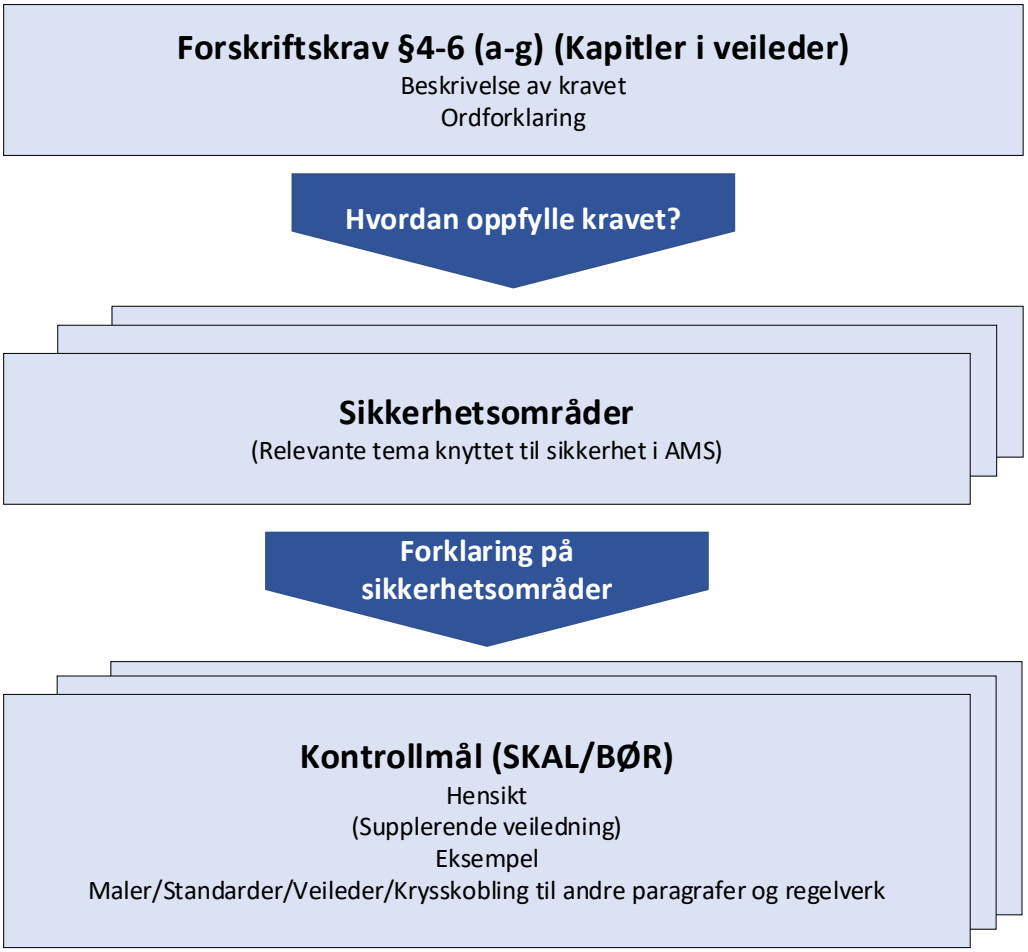
Måledata samles inn til innsamlingssystemet hos nettselskapet. Dette er vist som HeadEnd System (HES) i figuren. Et sentralsystem kan bestå av ett eller flere innsamlingssystemer, og et nettselskap kan ha ett eller flere sentralsystem. Sentralsystemet kan driftes av/outsources til en ekstern leverandør, og med en slik løsning vil nettselskapet motta/hente ut måleverdiene og bruke disse videre i egne systemer. Dette er vist i figuren som en alternativ boks.

Veilederen er utarbeidet for å ivareta sikkerhet knyttet til myndighetspålagt AMS-infrastruktur for innsamling av kWh-verdier til bruk for avregning, og de andre funksjonskravene gitt i avregningsforskriften § 4-2 og § 4-3. AMS-infrastruktur kan også benyttes til å samle inn nettnyttedata, men dette er ikke regulert gjennom avregningsforskriften, og dermed er det i liten grad vurdert i forbindelse med utarbeidelse av veileder.

B.3 Struktur på veileder

Veileder tar utgangspunkt i definisjonen av AMS gjengitt i veilederens virkeområde og omfang (kapittel B.2). Systemer som evt. kobles til bak sentralsystemet, eller foran elektrisitetsmåler, er ikke en del av AMS, men sikkerhetsnivået skal likevel opprettholdes.

Oppbyggingen av veileder er presentert i figur B.2. De ulike delene er beskrevet i teksten etter figuren.



Figur B.2 Oppbygging av veileder

Kapitler

Kapittelinndelingen i veilederen er gjort med utgangspunkt i kravene (a-g) i § 4-6 Krav til sikkerhet for AMS i forskrift for måling og avregning (avregningsforskriften) [2].

Forskriftskrav §4-6 a-g

Veiledningen gjengir forskriftsteksten til hvert krav (a-g), etterfulgt av en kort beskrivelse av kravet, ordforklaringer der dette er vurdert som nødvendig, og råd om hvordan kravene kan oppfylles i praksis. Disse er organisert etter tematiske sikkerhetsområder som beskrevet under.

For noen forskriftskrav er det gitt oversikt over relevante maler, standarder, veiledere og eventuelle krysskoblinger til andre paragrafer og regelverk, og der det er spesielle behov for presiseringer, benyttes gule Obs-bokser. Det gjelder spesielt der det er viktig å presisere om kravene gjelder måler hos sluttbruker eller måler lokalisert andre steder i strømnettet.

Sikkerhetsområde og kontrollmål

For hvert forskriftskrav er det beskrevet sikkerhetsområder, som er en oversikt over hvilke temaer som er relevante knyttet til etablering av sikkerhet i AMS.

Videre i veilederen er det for hvert sikkerhetsområde utarbeidet egne kontrollmål som er målbare krav/ anbefalinger til sikkerhet. Kontrollmålene er beskrevet som SKAL- eller BØR-krav, hvor "SKAL-krav" må gjennomføres for å tilfredsstille forskriftskrav, mens "BØR-krav" er anbefalinger som kan gjøres for å øke sikkerheten i AMS, samt øke sannsynligheten for at forskriftskravene er oppfylt.

For hvert kontrollmål er det gitt en begrunnelse, eller hensikt, og også en supplerende veiledning der det er funnet hensiktsmessig.

Til kontrollmålene er det gitt eksempler på tiltak, prosedyrer og lignende for å oppnå det enkelte kontrollmål. Disse er **kun** ment som eksempler og skal gi en pekepinn på hvilke tiltak som kan iverksettes for å bidra til å oppnå kontrollmålet. Nettselskapet står fritt til å velge andre tiltak.

En oversikt over sammenhengen mellom forskriftskrav, sikkerhetsområde og kontrollmål er gitt i sjekklisten i vedlegg B.14.

Nettselskapet må selv vurdere hvilke kontrollmål som skal prioriteres, gitt AMS-løsningens størrelse (f.eks. antall kunder), kompleksitet, teknologiske valg, og andre relevante forhold, forutsatt at forskriftskrav tilfredsstilles.

Veilederen har tilsvarende struktur som veileder til kraftberedskapsforskriften [1], med tilsvarende bruk av følgende symboler:

Krav	Eksempel	Sjekkliste	Obs!	Mer info
				

Nettselskapet må kunne begrunne om enkelte obligatoriske kontrollmål (SKAL-krav) utelates. Det er derfor lagt ved (vedlegg 1) en tabellarisk fremstilling av kontrollmålene med eksemplene, der selskapet selv kan begrunne hvorfor/ hvorfor ikke et kontrollmål er valgt. Nettselskapene er hele tiden ansvarlige for at forskriftskrav tilfredsstilles.

I denne veilederen henviser RME videre til andre dokumenter, for eksempel kraftberedskapsforskriften [4], avregningsforskriften [2], NSMs veiledere på sikkerhet, temarapporter utarbeidet av NVE eller andre myndigheter og organisasjoner, maler og skjema fra NVE, og nasjonale og internasjonale standarder. RME anbefaler at brukere av denne veilederen innhenter mer kunnskap og råd i disse refererte dokumentene når virksomheten mener det er relevant. Merk at RME fører tilsyn med etterlevelsen av forskriftskravene, ikke med etterlevelse av veilederen, standarder og andre temadokumenter det er henvist til i denne veilederen.

B.4 Krav til nettselskapet i henhold til forskrift (§4-6 første og andre ledd)

§

§4-6. *Krav til sikkerhet for AMS*
Nettselskapet er ansvarlig for å sikre AMS. Nettselskapet er ansvarlig for at sikkerhet vurderes ved oppstart og gjennomføring av endringsprosesser tilknyttet AMS. Nettselskapet skal velge løsninger som gir høyest sikkerhetsnivå i AMS så lenge kostnaden er forsvarlig etter en kost/nytte-vurdering.

Sikkerhetsløsninger i AMS skal oppfylle kravene til digitale informasjonssystemer i kraftberedskapsforskriften.

Beskrivelse av kravet
Dette kravet presiserer at det er nettselskapet som er ansvarlig for sikkerhet i hele AMS-løsningen, også for de delene som eventuelt settes ut til tjenesteleverandør. Tjenesteutsetting endrer ikke på nettselskapet sitt ansvar for sikkerhet i AMS. Alle former for tjenesteutsetting må reguleres gjennom gode avtaler som inkluderer forhold som er relevante for sikkerhet. Med utgangspunkt i en kost-/nyttevurdering, skal det velges løsninger som gir høyeste praktisk mulig sikkerhetsnivå i AMS. Dette betyr at dersom den beste sikkerhetsløsningen medfører kostnader som ikke er økonomisk forsvarlige, må en annen løsning velges. Etter den store utrullingen av AMS rundt 2019, har AMS gått over i driftsfasen for nettselskapene, men det vil bli utskiftninger av målere i årene framover. Det forventes derfor at kost/nytte vurderinger knyttet til sikkerhetsnivå må utføres på nytt.

Sikkerhet i AMS omfatter beskyttelse mot alle typer uautorisert tilgang for å hindre misbruk, tyveri av data, spredning av ondsinnet programvare, utførelse av uautoriserte kommandoer og liknende.

Kravet presiserer også at de sikkerhetsløsningene som velges i AMS skal oppfylle krav til digitale informasjonssystemer i kraftberedskapsforskriften, gitt gjennom §6 Informasjonssikkerhet og §7 Beskyttelse av driftskontrollsystem.

Ordforklaring

Vurdere sikkerhet	Gjennomføre risiko- og sårbarhetsanalyse (ROS) eller på annen hensiktsmessig måte vurdere sikkerhet for AMS
Oppstart	Igangsettelse av AMS
Endringsprosesser	Betydelige endringer i en eller flere deler av AMS-systemet (fra måler hos kunde, via kommunikasjonssystemet og inn til innsamlingssystemet. For AMS-struktur, se figur B.1)
Sikkerhetsnivå	En indikasjon på grad av motstandsdyktighet mot angrep. Høyere sikkerhetsnivå medfører vanligvis flere eller mer omfattende sikkerhetstiltak, f.eks.: Krav til autentisering: Fra enkelt passord (lavt nivå) til to eller flere faktorer (høyt nivå)

Standarder
ISO/IEC 27002:2017
Veileder
Veiledning til kraftberedskapsforskriften Kapittel 6: Informasjonssikkerhet
Veiledning til kraftberedskapsforskriften Kapittel 7: Beskyttelse av driftskontrollsystem
NSMs Grunnprinsipper for IKT-sikkerhet
Informasjonssikkerhet og personvern: Støtte til risikoanalyse av AMS og tilgrensende systemer
Krysskobling til andre paragrafer og regelverk
Kraftberedskapsforskriften §6 Informasjonssikkerhet
Kraftberedskapsforskriften §7 Beskyttelse av driftskontrollsystem

Hvordan oppfylle kravet?
Bestemmelsen plasserer ansvaret for å sikre AMS, hos nettselskapet. I tillegg til krav til sikkerhet gitt gjennom avregningsforskriften § 4-6, bør sikkerhetsløsninger som velges for AMS, også tilfredsstille kravene gitt gjennom følgende sikkerhetsområder:

1. Etablering og oppfølging av sikkerhetskrav (B.4.1)
2. Risiko- og sårbarhetsanalyse (B.4.2)
3. Sikkerhetsavtaler (B.4.3)
4. Utsetting av utrulling og/eller drift av AMS-løsningen til tredjepart (B.4.4)
5. Elektronisk beskyttelse mot ondsinnet programvare og inntrengning (B.4.5)
6. Beskyttelse mot uautorisert fysisk tilgang til AMS-utstyr (B.4.6)

Hvert sikkerhetsområde er forklart med kontrollmål, hensikt, evt. supplerende veiledning, med påfølgende eksempler.

B.4.1 Etablering og oppfølging av sikkerhetskrav

Kontrollmål:	Vurdering av krav
a. Nettselskapets ledelse skal utarbeide og godkjenne interne krav for det overordnede sikkerhetsnivået til AMS-løsningen. Disse skal dekke alle prosesser og systemer relevant for AMS. Kravene skal være målbare og dokumenteres.	SKAL
b. Nettselskapet ledelse bør etablere et system for å følge opp og forbedre sikkerhetskravene for AMS.	BØR

Hensikt
Hensikten med kravet er at ledelsen i nettselskapet skal gi retning og støtte for sikkerhetsarbeidet, samt sørge for at man gjennom organiseringen av nettselskapet følger opp arbeid med sikkerhet i AMS. Oppfølgingen er ment å skulle bidra til utvikling og forbedring av de interne sikkerhetskravene.

Supplerende veiledning
Disse kontrollmålene ligger tett opptil kravet om overordnede sikkerhetskrav i henhold til kraftberedskapsforskriften og organiseringen knyttet til beskyttelse av driftskontrollsystem.

I mindre virksomheter kan det være fornuftig å samle flere utøvende sikkerhetsoppgaver hos én person, f.eks. å vurdere om ledelse av sikkerhetsarbeidet i AMS også skal ligge under funksjonen til IKT-sikkerhetsleder/-koordinator, som er en funksjon det er krav om i henhold til kraftberedskapsforskriften. I tillegg kan det være nødvendig å gi utøvende ansvar for sikkerhetsoppgaver til personell som hovedsakelig har andre gjøremål. I slike situasjoner er det særlig viktig å påse at dette personellet gis nok tid og kompetanse til å utføre sikkerhetsoppgavene, og at ingen settes til å kontrollere eget arbeid.

Eksempel: Etablering og oppfølging av sikkerhetskrav
Nettselskapet skal utarbeide og godkjenne overordnede nivå til sikkerhet i sin AMS-løsning. For å få til dette, peker ledelsen ut en person som er ansvarlig for sikkerhet i AMS. Denne personen må ha/få tilstrekkelig kompetanse for å ivareta denne oppgaven, samtidig som det er viktig at personen gis nødvendig myndighet og ansvar, samt får avsatt tilstrekkelig med tid og ressurser slik at funksjonen kan ivaretas på en tilfredsstillende måte. Nettselskapet er lite, så dette ansvaret er allokert til en person. For å ivareta sikkerhet i AMS, er det viktig at alle Nettselskapets egne og innleide ressurser får tilstrekkelig opplæring på informasjonssikkerhet.

Når nettselskapet har ervervet seg tilstrekkelig kompetanse knyttet til informasjonssikkerhet, gjennomføres det en risiko- og sårbarhetsanalyse for å sette sikkerhetskravene på et akseptabelt nivå. Minst en gang i året gjennomgås sikkerhetskravene, for å sikre at Nettselskapet har hensiktsmessige sikkerhetskrav i forhold til nettselskapets behov, etterlevelse av forskriftskrav og om kravene er tilstrekkelige.

B.4.2 Risiko- og sårbarhetsanalyse

Kontrollmål:	Vurdering av krav
a. Det skal gjennomføres risiko- og sårbarhetsanalyse eller annen hensiktsmessig sikkerhetsvurdering av AMS med den hensikt å identifisere risiko forbundet med drift og sikkerhet av AMS. Vurderingen skal gjentas med jevne mellomrom, og i hvert fall når det skjer vesentlige endringer i AMS-systemet og/eller omgivelser.	SKAL
b. Konfigurasjon og oppsett for kritiske kommandoer, målerdata og annen informasjon i AMS løsningen bør være basert på risiko.	BØR

Hensikt
Sikkerhetsvurderingene skal gi nettselskapet styringsgrunnlag for å etablere hensiktsmessige sikkerhetstiltak og for å verifisere at risikoen er akseptabel. Dette gjennomføres gjerne som en risiko- og sårbarhetsanalyse (ROS-analyse).

ROS-analysen har som hensikt å identifisere årsaker til uønskede hendelser i AMS-løsningen, samt sannsynligheten for at de ulike hendelsene inntreffer og hvilke konsekvenser hendelsene kan utløse. Videre vil en slik analyse vurdere sannsynlighets- og /eller konsekvensreduserende tiltak. Avhengigheter mellom ulike deler av systemet bør også inkluderes i ROS-analyser.

Eksempel: Gjennomføring av risiko- og sårbarhetsanalyse

Nettselskapet gjennomfører sin årlige risiko- og sårbarhetsanalyse (ROS-analyse) for å identifisere risiko forbundet med drift av AMS. I denne analysen vurderer de alle forhold som for eksempel kan hindre korrekt avregning, hindre tilfredsstillende funksjonalitet, sette informasjonssikkerheten i fare eller hindre funksjonalitet i kraftforsyningen. Når alle forhold er vurdert, fastsettes det hva som er akseptabelt risikonivå som de ulike risikoene i ROS-analysen vurderes opp mot. Avhengigheter mellom ulike deler av systemet er med i ROS-analysen. Et eksempel på avhengighet kan være at selv om nettselskapet har sitt eget maskenettverk, er de likevel avhengig av Telenors 4G-nettverk.

Hvis nettselskaper finner tilfeller hvor risikonivå er høyere enn hva som er akseptabel risiko, etablerer de tiltak slik at de kan oppnå akseptabelt risikonivå. Til enhver tid skal nivå på sikkerhetstiltak være tilpasset risiko. Hvis Nettselskapet må gjøre større tiltak for å oppnå akseptabelt risikonivå, iverksettes tilstrekkelige midlertidige kompenserende tiltak inntil permanente tiltak er på plass.

I tillegg til å gjøre en slik ROS-analyse årlig, gjennomfører nettselskapet også ROS-analyser hvis det gjøres noen endringer i løsninger eller hvis en trusselsituasjon påvirker drift og sikkerhet i AMS.

Maler

Mal for risikovurdering av IKT-systemer – Nasjonal Sikkerhetsmyndighet

Veileder

Risikovurdering av IKT-systemer – Nasjonal Sikkerhetsmyndighet

Risikovurdering - Datatilsynet

Om risiko og risikovurdering - Digdir

Informasjonssikkerhet og personvern: Støtte til risikoanalyse av AMS og tilgrensende systemer

B.4.3 Sikkerhetsavtaler

Kontrollmål:	Vurdering av krav
a. Nettselskapet skal inngå sikkerhetsavtaler med alle leverandører eller enkeltpersoner som ikke er ansatt i nettselskapet dersom de skal utføre arbeid på sentrale løsninger eller komponenter i AMS-løsningen.	SKAL

Hensikt

Hensikten er å sørge for at leverandørene og enkeltpersonene gjennom avtalen behandler informasjonen og kunnskapen de får om nettselskapets AMS-løsning i henhold til nettselskapets egen policy på området.

Eksempel: Etablering av sikkerhetsavtaler med ekstern leverandør
Nettselskapet planlegger å gjennomføre en endring på AMS-løsningen, dvs. at de skal bytte kommunikasjonsløsning for målerne fra mobilt bredbånd til egen fiberløsning. De har bestemt seg for å sette ut deler av dette arbeidet til en ekstern leverandør. Før den eksterne leverandøren kan starte på jobben, inngår Nettselskapet en egen sikkerhetsavtale med leverandøren og de personene som skal utføre arbeidet.

Maler
Driftsavtale (SSA-D) – Direktoratet for forvaltning og økonomistyring
NVEs sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen
Veileder
Avtale om håndtering og beskyttelse av kraftsensitiv informasjon

B.4.4 Tjenesteutsetting av utrulling og/eller drift av AMS-løsningen til tredjepart

Kontrollmål:	Vurdering av krav
a. Sikkerheten i AMS skal ikke påvirkes ved at utrulling eller drift av AMS settes ut til ekstern tjenesteleverandør.	SKAL

Hensikt
Utsettelse av utrulling eller drift av AMS til en ekstern tjenesteleverandør skal ikke påvirke sikkerheten i AMS.

Supplerende veiledning
Hvis enkelte deler av løsningen driftes eller på annen måte håndteres av en tjenesteleverandør, bør nettselskapet avtalefeste krav om rett til revisjon av leverandøren.

Nettselskapet bør også kunne gis mulighet til, i sin avtale med leverandøren, å angi at den overnevnte retten til revisjon skal kunne benyttes av RME. Revisjon av leverandøren bør kunne gjennomføres uten hinder.

Eksempel: Tjenesteutsetting av utrulling og/eller drift av AMS-løsningen til tredjepart
Nettselskapet har bestemt seg for å sette ut utrulling og drift av AMS-løsningen til en tredjepart. For å kunne gjøre dette, og samtidig ivareta sitt ansvar for sikkerhet i AMS, må Nettselskapet ha tilstrekkelig kompetanse til at de kan lage en kravspesifikasjon hvor krav til sikkerhet i AMS er beskrevet. Nettselskapet må også kunne kontrollere at tredjepart klarer å etterleve disse kravene i en driftssituasjon. For å kunne gjennomføre slike kontroller, har Nettselskapet satt målbare krav til leverandøren sin, som Nettselskapet følger opp regelmessig.

For at Nettselskapet skal kunne følge opp dette regelmessig, må de få innsyn i og ha en forståelse av de sikkerhetstiltakene som etableres og risikoen en slik tjenesteutsetting medfører. Hvis Nettselskapet ser

at tredjepart ikke overholder avtalen, må de ha en realistisk mulighet til å trekke tilbake avtalen ved et slikt avtalebrudd, uakseptabel risiko eller endringer i regulering.

Gjennom utarbeidelse av en god kravspesifikasjon som følges opp regelmessig, sikrer nettselskapet at tjenesteutsettingen ikke påvirker risiko for kraftforsyningen negativt.

Nettselskapet inngår Databehandleravtale med leverandøren.

Veileder
Nasjonal sikkerhetsmyndighet - Sikkerhetsfaglige anbefalinger ved tjenesteutsetting
Datatilsynet – Databehandleravtale
Krysskobling til andre paragrafer og regelverk
Energilovforskriften §3-6
Avregningsforskriftens §4-6 første ledd første setning og fjerde ledd

B.4.5 Elektronisk beskyttelse mot ondsinnet programvare og inntrengning

Kontrollmål:	Vurdering av krav
a. Det skal etableres et system for overvåking og beskyttelse av programvaren i AMS med hensikten å oppdage og stanse ondsinnet programvare.	SKAL

Hensikt
Forhindre at ondsinnet programvare eller inntrengning forstyrrer eller ødelegger AMS i den grad at informasjonssikkerheten blir kompromittert.

Eksempel: Elektronisk beskyttelse mot ondsinnet programvare og inntrengning
For å oppdage og stanse ondsinnet programvare, har Nettselskapet etablert et eget system for overvåking og beskyttelse av programvaren i AMS. I sentralsystemet har de et anti-skadevare og intrengningsdeteksjonssystem for å oppdage skadevare og andre angrep. Firmware i den enkelte AMS-måler er signert av leverandør, og ved oppstart vil AMS-måleren verifisere signaturen samt at firmwaren ikke har blitt endret.

B.4.6 Beskyttelse mot uautorisert fysisk tilgang til AMS-utstyr

Kontrollmål:	Vurdering av krav
a. Alle rom som inneholder utstyr som er kritisk for AMS skal være i en egen adgangskontrollert sone.	SKAL
b. Komponenter i AMS utenfor adgangskontrollerte soner skal beskyttes mot uautorisert fysisk tilgang.	SKAL
c. Alle forsøk på å få uautorisert tilgang til utstyr i AMS-løsningen eller rom med kritisk AMS-utstyr skal registreres og varsles så snart som mulig.	SKAL

Hensikt

Forhindre fysisk tilgang til komponentene i AMS, spesielt de som er plassert utenfor nettselskapets kontrollerte område. Slik tilgang kan gi elektronisk tilgang til AMS og systemene som inngår i AMS-infrastruktur.

Eksempel:
Nettselskapet bruker AMS-målere som er plombert i tillegg til elektronisk pirkesikring. Dersom noen del av måleren forsøkes åpnet, genereres det et alarmsignal som medfører en alarm til nettselskapet/leverandør i sentralsystemet.

Eksempel:
Nettselskapet har plassert sentralsystemet i tilknytning til driftssentralen. Lokalene er fysisk sikret, og adgang forutsetter bruk av adgangskort og kode. Lokalene er ytterligere beskyttet av alarmsystem knyttet til vekterselskap med utrykning.

Eksempel:
Med utgangspunkt i kravet om at sikkerhetsløsninger i AMS skal oppfyllet kravene til digitale informasjonssystemer i kraftberedskapsforskriften, utfører nettselskapet i utgangspunktet alle sikkerhetskritiske oppgaver fra adgangskontrollert sone. I de tilfeller det er nødvendig med fjerntilgang til AMS-systemet fra hjemmekontor eller lignende, skal dette godkjennes i hvert enkelt tilfelle, og det skal dokumenteres at løsningene som brukt, er sikkerhetsmessig tilfredsstillende, f.eks. at det brukes en VPN-løsning med tilstrekkelig sikkerhet, at det kun er datautstyr administrert av Nettselskapet som tillates brukt, og at brukergrensesnittet låses med passord når det ikke er i bruk.

Bruk av hjemmekontor

Husk at kraftberedskapsforskriften §6-10 fortsatt krever at bryterfunksjonen utføres fra adgangskontrollert sone.

B.5 Godkjenning av enheter og brukere som skal kommunisere til eller i AMS (§4-6 a)

a. Enheter og brukere som skal kommunisere til eller i AMS, må godkjennes i AMS av nettselskapet eller nettselskapets leverandør før de får tilgang.

Beskrivelse av kravet
Dette kravet omfatter godkjennelse av enheter og brukere som skal kommunisere til eller i AMS. Godkjennelsen gjøres innen AMS, og det er nettselskapet eller nettselskapets leverandør som gjør dette før den enkelte enhet og/eller bruker gis tilgang.

Ordforklaring

Enheter	Elektronisk utstyr som skal kobles til AMS
Brukere	Kunde (åpning av HAN-port) Ansatte i nettselskap Ansatte hos tredjepart

Hvordan oppfylle kravet?
Godkjenning av enheter og brukere som skal kommunisere til eller i AMS (§4-6 a) inkluderer følgende sikkerhetsområder:

- Tilgangskontroll for system (B.5.1)
- Identifisering og autorisasjon av enheter (B.5.2)
- Identifisering og autorisering av eksternt utstyr (B.5.3)
- Fjerntilgang til AMS fra tredjepart eller leverandør (B.5.4)

Hvert sikkerhetsområde er forklart med kontrollmål, hensikt, med påfølgende eksempler.

B.5.1 Tilgangskontroll for system

Kontrollmål:	Vurdering av krav
a. Nettselskapet skal ha prosedyrer og kriterier for tildeling, endring, sletting og verifikasjon av korrekt tilgang til kundedata samt AMS-funksjonalitet	SKAL

Hensikt
Nettselskapet har kontroll på hvem som har tilgang til kundedata og AMS-funksjonalitet, og hva de har tilgang til. Dette gjør det lettere for nettselskapet å avdekke eventuell uautorisert tilgang.

Eksempel: Etablering av rutine for tilgangskontroll til system
Nettselskapet har laget en egen rutine som sikrer at det kun er personer med rett autorisasjon som kan få tilgang til, endre, slette eller utlevere måledata eller annen sensitiv kundeinformasjon. Prosedyrene som er utarbeidet gjelder både for intern og ekstern tilgang.

Prosedyren inneholder også krav om bakgrunnssjekk av personell som skal ha tilgang til å håndtere sensitive systemer og informasjon. Bakgrunnssjekken skal som et minimum være vandelsattest (hvis mulig) og referansesjekk.

Når personer er godkjent, skal tilgang administreres på basis av forhåndsdefinerte roller og tilgangsnivåer, og det skal være tjenstlig behov som gir grunnlag for at tilganger skal tildeles, endres, fjernes og revideres.

Eksempel: Rutine for å avdekke endring i målerdata eller annen kundeinformasjon
For å ivareta kontroll på tilgang til systemet og på data i systemet, har Nettselskapet laget tekniske løsninger for både å oppdage uautorisert endring i måler- eller kundedata og for å forhindre uautorisert utlevering av måler- eller kundedata. For å ha kontroll på datakvaliteten, har Nettselskapet også laget tekniske løsninger for å loggføre dersom det utføres endringer i allerede registrerte målerdata og dersom målerdata eller annen kundeinformasjon utleveres til autorisert tredjepart.

Eksempel: Tilgang fra underleverandører
Nettselskapet har bruk for assistanse fra en leverandør som ikke er involvert i daglig drift av AMS-løsningen. Leverandøren får tilgang via en VPN-forbindelse som åpnes via sentralsystemet for en tidsbegrenset periode.

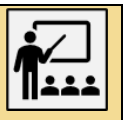
Krysskobling til andre paragrafer og regelverk
Kraftberedskapsforskriften §6-1 Rettmessig bruker
Kraftberedskapsforskriften §6-7 Personkontroll

B.5.2 Identifisering og autorisasjon av enheter

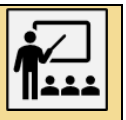
Kontrollmål:	Vurdering av krav
a. Det skal implementeres mekanismer for å autentisere og autorisere enheter i AMS før det opprettes forbindelse mellom enheten og resten av AMS.	SKAL
b. Ved bruk av nettverk som nettselskapet ikke kontrollerer, f.eks. Mobilt Bredbånd (MBB), bør ekstra sterk autentisering foretas.	BØR

Hensikt
Implementere en mekanisme for sikker identifisering av hver enkelt enhet som tilkoples AMS. Svært mange av enhetene i AMS vil måtte fysisk plasseres på steder der nettselskapet har begrenset kontroll med utstyret.

Dette gjelder i særdeleshet måleren og annet utstyr som blir plassert nær kundene (f.eks. vannmålere). Derfor bør enhetene underlegges strenge sikkerhetskontroller før de kommer i kontakt med AMS-løsningen.



Eksempel: Identifisering og autorisasjon av enheter
Hver enhet i AMS er tildelt et unikt sikkerhetssertifikat som kontrolleres før det sendes/mottas data fra enheten. Hvis man ikke får til å kontrollere enheten, eller den ikke kan verifiseres, skal enheten nektes tilgang til nettverket. Sikkerhetssertifikatet skal benyttes for å autorisere enheter i AMS.

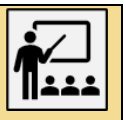


Eksempel: Identifisering av nye målere
Nettselskapet har rullet ut smarte målere fra leverandøren. Målerne kommer ferdig konfigurert med en symmetrisk krypteringsnøkkel, og Nettselskapet har en database med krypteringsnøklene til de forskjellige målerne i sitt nett. Ved hver kommunikasjon mot måleren gjennomføres det autentisering mot måleren, og kommunikasjonen mellom måler og sentralsystem krypteres ende-til-ende.

B.5.3 Identifisering og autorisering av eksternt utstyr

Kontrollmål:	Vurdering av krav
a. Håndholdte enheter (feltutstyr) må være autorisert og skal autentiseres av AMS-løsningen. Bruker skal være autorisert og autentisert.	SKAL

Hensikt
Implementere streng autorisasjons- og brukskontroll for påkobling av eksternt utstyr til AMS-løsningen for å forhindre misbruk.



Eksempel: Identifisering og autorisering av eksternt utstyr
Nettselskapet har utarbeidet en prosedyre for autoriseringsprosessen av eksternt utstyr som tilkobles AMS. I forbindelse med at prosedyren ble laget, har de gått gjennom at det er ingen portal/grensesnitt hvor man kan koble til eksternt utstyr uten at disse er autoriserte og autentiserte. Sikkerhetssertifikatet skal benyttes for å autorisere enheter i AMS. Hver enhet i AMS er tildelt et unikt sikkerhetssertifikat som kontrolleres ved oppkobling mot enheter i AMS. Hvis det er enheter ute i nett som skal tilkobles, gjøres godkjennelsen ved at nummeret på enhet kontrolleres mot liste over godkjente enheter. Den eksterne enheten som kobles til, skal ikke benyttes til annet enn oppgave mot AMS.

Hvis man ikke får til å kontrollere enheten, eller den ikke kan verifiseres, skal enheten nektes tilgang til nettverket. Det skal være mulig å fjerne/endre autorisering av håndholdte enheter sentralt.

B.5.4 Fjerntilgang til AMS fra tredjepart eller leverandør

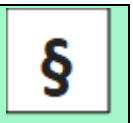
Kontrollmål:	Vurdering av krav
a. Det skal etableres prosedyrer for godkjenning, administrering og overvåking av eksterne tilkoblinger for vedlikehold og diagnostiske aktiviteter på alle komponenter i AMS-systemet.	SKAL

Hensikt
Beskytte komponenter i AMS-systemet mot uautorisert tilgang slik at AMS-løsningen ikke utsettes for store sårbarheter og trusler i de tilfeller nettselskap ønsker å benytte en tredjepart eller leverandør til å bistå med systemvedlikehold, oppgradering av programvare, feilretting eller liknende.

Eksempel: Fjerntilgang til AMS fra tredjepart eller leverandør
For å ivareta sikkerhet i AMS ved fjerntilgang til AMS fra tredjepart eller leverandør, har nettselskapet satt som krav at det ikke skal opprettes tilkobling til tredjepart eller leverandør uten eksplisitt avtale med selskapet. Gjennom denne avtalen må tredjepart forplikte seg til å etterleve relevante sikkerhetskrav, som bl.a. inkluderer krav om å benytte en sikker løsning for fjerntilgang. En slik fjerntilgang skal kun tillates fra sikre lokasjoner som ikke medfører økt risiko.

I kravspesifikasjonen fra Nettselskapet er det også tatt med at når eksternt vedlikehold er fullført, skal det fra Nettselskapet eller fra AMS-komponenten avslutte alle økter og eksterne tilkoblinger som er opprettet.

B.6 Sporbarhet av endringer av programvare og konfigurasjon av dataprogram (§4-6 b)



b. Enhver endring av programvare og konfigurasjon av dataprogram i AMS skal kunne spores tilbake til bruker, tidspunkt og endringen som ble gjort.

Beskrivelse av kravet
Dette kravet omfatter sporing av enhver endring av programvare og konfigurasjon av dataprogram i AMS: Det skal være mulig å spore tilbake til bruker, tidspunkt for endring og hvilken endring som ble utført.

Hvordan oppfylle kravet?
Sporbarhet av endringer av programvare og konfigurasjon av dataprogram omfatter følgende sikkerhetsområder:

- Kontroll med og sporing av endringer (B.6.1)
- Oppdatert dokumentasjon av AMS-løsningen (B.6.2)
- Kontroll med integriteten til programvare (B.6.3)

Hvert sikkerhetsområde er forklart med kontrollmål, hensikt, med påfølgende eksempler.

B.6.1 Kontroll med og sporing av endringer

Kontrollmål:	Vurdering av krav
a. Nettselskapet skal dokumentere prosedyrer for å planlegge og utføre endringer i AMS-miljøet.	SKAL
b. Sentralsystemet skal logge alle endringer i programvare og konfigurasjon i AMS	SKAL

Hensikt
Kontroll med endringer i AMS-løsningen er avgjørende for å ivareta krav om robust sikkerhets-funksjonalitet og at AMS-løsningen fungerer etter sin hensikt også etter endringer.

Eksempel:
Nettselskapet har dokumentert en prosedyre for IT-avdelingen som angir at alle planlagte endringer i AMS-løsningen registreres i et eget konfigurasjonsstyringsverktøy, og at både planlagte og ikke-planlagte endringer registreres her når de er utført. Prosedyren angir at IT-leder er ansvarlig for å overvåke når leverandør publiserer endringer i AMS-systemets programvare eller firmware, og sørge for at endringer blir risikovurdert og planlagt utført i konfigurasjonsstyringsverktøyet.

Eksempel:
Nettselskapet har et sentralsystem som krever innlogging med personlig brukernavn og tofaktor autentisering. Sentralsystemet logger automatisk alle endringer i konfigurasjon og programvare-oppdateringer med brukernavn og tidspunkt, og i tillegg registreres endringene manuelt i konfigurasjonsstyringssystemet. Større endringer som medfører utskifting av hele sentralsystemet logges manuelt i konfigurasjonsstyringsverktøyet. Sentralsystemet vil også logge konfigurasjons-endringer og installasjon av oppdatert firmware på AMS-målere (måler-ID, brukernavn, tidspunkt, og endring).

B.6.2 Oppdatert dokumentasjon av AMS-løsningen

Kontrollmål:	Vurdering av krav
a. Det skal til enhver tid foreligge fullstendig og oppdatert dokumentasjon av AMS-løsningens komponenter og konfigurasjoner.	SKAL

Hensikt
Fullstendig og oppdatert dokumentasjon er viktig for å vurdere risiko, planlegge sikkerhetstiltak, plan-legging av nye funksjoner, samt vedlikehold. Ved feil eller større hendelser hvor man må gjenoppbygge deler av systemet, vil dokumentasjonen være helt avgjørende i forhold til hvor lang tid gjenoppretting vil ta.

Oppdatert systembeskrivelse er også viktig for hvordan man vurderer for eksempel tilgang på reserve-materiell, mulige reserveløsninger og andre beredskapstiltak. Det er derfor viktig at dokumentasjonen også utformes med tanke på slik bruk.

Eksempel:
Nettselskapet har implementert et konfigurasjonsstyringsverktøy som inneholder dokumentasjon av alle komponentene i AMS-systemet, samt kopi av alle konfigurasjonsfiler.

B.6.3 Kontroll med integriteten til programvare

Kontrollmål:	Vurdering av krav
a. Det bør etableres et system for overvåking av endringer for å kunne oppdage uautoriserte endringer av programvare og informasjon.	BØR

Hensikt
Systemkomponenter som har gjennomgått uventede eller uautoriserte endringer har trolig blitt kompromittert eller korrupte. Slike hendelser må oppdages, rapporteres, vurderes og eventuelt korrigeres av kompetent personell.
Man må påse at bruken av automatiske verktøy for integritetskontroll ikke har negativ innvirkning på AMS-løsningens operative funksjon, for eksempel ved å gi utilbørlig reduksjon av ytelse. Dette kontrollmålet kan ses i sammenheng med kontrollmål for sikker kommunikasjon (se B.7).

Eksempel: System for overvåking og avdekking av uautoriserte endringer
Nettselskapet har etablert et system for å avdekke uautoriserte endringer av programvare og informasjon, og slik oppdage om noen systemkomponenter har blitt kompromitterte eller korrupte. Dette systemet utfører integritetsskanning av AMS-løsningen, og sjekker integriteten på programvare ved oppstart, oppdatering og eksekvering.

Dette systemet skal også sørge for at enheten i AMS er sikret fysisk og logisk mot uautorisert oppdatering og endring av programvare, og at endringer av programvare skal være testet og godkjent før de gjennomføres. I tillegg skal enhetene i AMS kunne verifisere at alle spørringer og kommandoer er gyldige, har rett format og er foretatt fra autentisert og autorisert kilde.

Nettselskapet har satt opp systemet slik at kun autoriserte og autentiserte brukere er i stand til å utføre kommandoer. Dette medfører at det ikke er mulig å utføre kommandoer i AMS med mindre man har tilgang til den rette symmetriske krypteringsnøkkelen. I tillegg har de implementert et automatisk verktøy som varsler ved integritetsavvik.

B.7 Beskyttelse av kommunikasjon mellom AMS-måler og sentralsystemet (§4-6 c)

§

c. Kommunikasjon i nettverket mellom AMS-måler og sentralsystem skal være beskyttet med ende-til-ende-kryptering. Ved bruk av et eget datanettverk, stengt for uvedkommende, kan kravet om ende-til-ende-kryptering fravikes.

Beskrivelse av kravet

Dette kravet gjelder for kommunikasjon i nettverket mellom AMS-måler og sentralsystemet, og at denne kommunikasjonen skal beskyttes med ende-til-endre-kryptering. Hvis det brukes eget datanettverk for denne kommunikasjonen, hvor ingen uvedkommende har adgang, er det ikke krav om ende-til-ende-kryptering. Det er også mulig å benytte en løsning hvor deler av kommunikasjonen er beskyttet med kryptering og deler er beskyttet med bruk av et eget datanettverk som er stengt for uvedkommende.

!

Eget datanettverk for kommunikasjon mellom AMS-målere og sentralsystem

Dette er normalt aktuelt for AMS tilknyttet høyspenningsanlegg eller konsentratorer i nettstasjoner, og ikke AMS tilknyttet målepunkt hos sluttbruker i lavspenningsanlegg.

Ordforklaring

Sentralsystem	Se illustrasjon av AMS-system (Figur B.1)

Hvordan oppfylle kravet?

Beskyttelse av kommunikasjon mellom AMS-måler og sentralsystemet inkluderer følgende sikkerhetsområder:

- Sikkerhet i kommunikasjon i AMS-løsningen (B.7.1)
- Oppbevaring av sikkerhetssertifikater og krypteringsnøkler (B.7.2)

Sikkerhetsområdet er forklart med kontrollmål, hensikt, med påfølgende eksempler.

B.7.1 Sikkerhet i kommunikasjon i AMS-løsningen

Kontrollmål:	Vurdering av krav
a. All kommunikasjon mellom måler og sentralsystem og øvrig utstyr i AMS skal foregå på en sikker måte slik at innsyn, avlytting eller manipulering av signaler og informasjon ikke er mulig.	SKAL
b. Signalene og informasjonen bør krypteres ende-til-ende mellom måler og HES.	BØR

Hensikt
Kommandoer, målerdata og annen sensitiv informasjon som overføres i AMS løsningen skal beskyttes mot uautorisert innsyn, avlytting eller endring.

Utstedelsen av offentlige nøkkel-sertifikater skal skje gjennom en sertifikat-policy eller fra en anerkjent tjenesteleverandør. Nøkkelgenerering og -håndtering skal gjøres på en sikker måte for å forhindre at løsningen blir sårbar. Kryptografimoduler, algoritmer og nøkler må være sikret.

Eksempel:
Nettselskapet har tatt i bruk en AMS-løsning der hver måler har en unik symmetrisk krypteringsnøkkel, og sentralsystemet har en beskyttet database med oversikt over hvilken nøkkel som hører til hvilken AMS-måler. Den symmetriske nøkkelen brukes til gjensidig utfordring-svar-autentisering mellom sentralsystem og måler, og til å etablere en sesjonsnøkkel som i sin tur brukes til å kryptere all data som sendes mellom måleren og sentralsystemet.

B.7.2 Oppbevaring av sikkerhetssertifikater og krypteringsnøkler

Kontrollmål:	Vurdering av krav
a. Nettselskapet skal utarbeide retningslinjer for sikker oppbevaring av sikkerhetssertifikater og krypteringsnøkler som benyttes i AMS.	SKAL
b. Enheten skal lagre påloggingsinformasjon, sikkerhetssertifikater og annen sikkerhetsinformasjon sikkert.	SKAL
a. Autentisering bør gjøres ved bruk av flere faktorer	BØR

Hensikt
Forhindre kompromittering av krypteringsnøkler og sikkerhetssertifikater for AMS-løsningen .

Eksempel: Oppbevaring av sikkerhetssertifikater og krypteringsnøkler
Nettselskapet har etablert et system for oppbevaring av krypteringsnøkler til hver enkelt måler. Krypteringsnøklene oppbevares kryptert, og kun navngitte medarbeidere har tilgang via sentralsystemet etter autentisering.

Private nøkler til digitale sertifikater oppbevares kryptert i en maskinvarebasert sikkerhetsmodul (HSM), og er beskyttet av egne passord og autentiseringkode (multi-faktor autentisering).

Veileder
TOTP: Time-Based One-Time Password Algorithm

B.8 Oppdatering av programvare (§4-6 d)

§

d. Programvare i AMS skal være oppdatert. Før ny programvare installeres i AMS, skal nettselskapet eller nettselskapets leverandør kontrollere at programvaren er autentisk.

Beskrivelse av kravet
Dette kravet gjelder for oppdatering av programvare i AMS. Programvaren skal til enhver tid være oppdatert. Før en ny oppdatering gjennomføres, ved at ny programvare installeres i AMS, skal nettselskapet eller nettselskapet sin leverandør kontrollere at ny programvare er autentisk.

Hvordan oppfylle kravet?

Oppdatering av programvare inkluderer følgende sikkerhetsområder:

- Oversikt over versjoner i program- og maskinvare (B.8.1)
- Kontroll av ekthet av programvare (B.8.2)
- Kontroll med sårbarheter i programvare (B.8.3)

Hvert sikkerhetsområde er forklart med kontrollmål, hensikt, med påfølgende eksempler.

B.8.1 Oversikt over versjoner i program- og maskinvare

Kontrollmål:	Vurdering av krav
a. Nettselskapet skal ha en oppdatert oversikt over versjoner av all maskinvare, firmware, oppdateringer og programvare som benyttes i AMS løsningen. Oversikten skal oppdateres ved endringer og ved regelmessige gjennomganger.	SKAL

Hensikt
Forhindre at kjente sårbarheter finnes i nettselskapets systemer, ved kontinuerlig ha god oversikt over programvare og maskinvare. AMS vil for mange selskaper være en stor og kompleks løsning med mange komponenter. Må ses i sammenheng med B.8.3.

Eksempel:
Nettselskapet har en database med oversikt over alle måler-ID-er, som inneholder type og modell/versjon av måler, versjon av firmware, når den ble installert, og eventuelle tidligere versjoner av firmware som er tilgjengelig på måleren. Databasen omfatter også eventuelle konsentratorer og annet nettverksutstyr mellom måleren og sentralsystemet. Dessuten finnes det en database med oversikt over maskinvare som brukes i sentralsystemet, versjon av operativsystem, installerte oppdateringer med dato, og versjon av HES programvare samt oppdateringer med dato.

B.8.2 Kontroll av ekthet av programvare

Kontrollmål:	Vurdering av krav
a. Nettselskapet skal ha muligheten til å verifisere at programvare, firmware og tilhørende oppdateringer er ekte	SKAL

Hensikt

Forhindre at en angriper kan introdusere manipulert programvare eller firmware på endesystem eller måler. Dette kontrollmålet gjelder kun oppdateringer fra leverandør, ikke programvare etc. som allerede er installert (dette dekkes av B.6.3).

Eksempel:

Nettselskapet har valgt en leverandør av AMS-system som sørger for at all programvare, firmware og oppdatering er signert med en digital signatur. Leverandørens offentlige nøkkel er signert av en anerkjent Certification Authority (CA), og nettselskapet har lastet ned det offentlige sertifikatet til leverandøren og verifisert ektheten til det. Før ny programvare installeres på endesystemet, verifiseres det at den digitale signaturen på programvaren fra leverandøren er korrekt. Det samme gjøres ved nedlasting av oppdatert firmware til AMS-måler. I tillegg vil også AMS-måleren verifisere at signaturen er korrekt før ny firmware tas i bruk på AMS-måleren.

B.8.3 Kontroll med sårbarheter i programvare

Kontrollmål:	Vurdering av krav
a. Nettselskapet skal ha prosesser for å fange opp eventuelle kjente programvaremessige sårbarheter i sitt AMS-miljø.	SKAL
b. Dersom man blir kjent eller varslet om sårbarheter, skal disse evalueres og eventuelt håndteres umiddelbart.	SKAL

Hensikt

Forhindre at kjente sårbarheter ikke blir vurdert eller håndtert.

Det kan være nødvendig at man vurderer om sikkerhetsoppdateringene kan utgjøre en trussel mot funksjonaliteten til AMS. Derfor bør man ha tett dialog med leverandøren omkring sikkerhetsoppdateringer.

Det er viktig at lukking av sårbarheter ikke gjøres på en måte som medfører for stor risiko for nettselskapet eller kraftsystemet.

Eksempel:

Nettselskapet abonnerer på varsler fra KraftCERT, og har laget en prosess som automatisk filtrerer ut varsler som er relevant for deres AMS-miljø. Sårbarheter i sentralsystemet oppdateres i samråd med leverandør så snart dette er praktisk mulig. Sårbarheter i firmware for AMS-målere håndteres så snart firmwareoppdatering fra leverandør er tilgjengelig og testet hos nettselskapet.

Veileder
Grunnprinsipper for IKT-sikkerhet 2.0 – Ivareta en sikker konfigurasjon
Grunnprinsipper for IKT-sikkerhet 2.0 – Oppdag og fjern kjente sårbarheter og trusler

B.9 Sikkerhetshendelser (§4-6 e)

e. Hendelser som kompromitterer sikkerheten i en AMS-måler, eller dens kommunikasjon med sentralsystemet, skal ikke kompromittere sikkerheten i andre AMS-målere, deres kommunikasjon med sentralsystemet, eller sentralsystemet i seg selv.

Beskrivelse av kravet
Dette kravet omhandler å hindre eskalering av sikkerhetshendelser. Det betyr at hvis en hendelse kompromitterer sikkerheten i en AMS-måler, eller i kommunikasjonen mellom AMS-måler og sentralsystemet, skal ikke sikkerheten i andre AMS-målere kompromitteres. Tilsvarende skal ikke sikkerheten i kommunikasjonen fra andre AMS-målere til sentralsystemet, eller selve sentralsystemet kompromitteres.

Ordforklaring

Kompromittere	Kompromittere betyr at noen har kommet seg forbi sikkerhetsløsningene på en eller flere enheter i AMS-systemer.

Hvordan oppfylle kravet?
Sikkerhetshendelser inkluderer følgende sikkerhetsområder:

- Logging og overvåking (B.9.1)
- Uavhengighet (B.9.2)

Hvert sikkerhetsområde er forklart med kontrollmål, hensikt, med påfølgende eksempler.

B.9.1 Logging og overvåking

Kontrollmål:	Vurdering av krav
a. Nettselskapet skal ha satt opp løsning og rutiner for sikkerhetslogging i den totale AMS-løsningen.	SKAL

Hensikt
Logger er et svært viktig verktøy for å kunne påvise unormal aktivitet i systemet. Som et supplement bør nettselskapet vurdere å etablere et automatisk analyseverktøy for logger, slik at man raskt får et varsel dersom man får unormal trafikk.

Eksempel:
Nettselskapet har installert et inntrengningsdeteksjonssystem (IDS) som en del av sentralsystemet, og IDS overvåker både lokale logger og nettverkstrafikk til/fra HES.

Veileder
Grunnprinsipper for IKT-sikkerhet 2.0 – Etabler sikkerhetsovervåking

B.9.2 Uavhengighet

Kontrollmål:	Vurdering av krav
a. Sikkerhetsfunksjonalitet i AMS-løsningen skal ikke påvirkes ved feil i AMS eller feil konfigurasjon av annen funksjonalitet.	SKAL
b. Hvis man kompromitterer en måler, skal ikke dette ha noen konsekvenser for andre målere eller sentralsystemet.	SKAL

Hensikt
Dersom det oppstår en feil i et system eller i kommunikasjonsløsningen til AMS, så skal dette ikke påvirke informasjonssikkerheten ved at for eksempel kundedata eller annen informasjon blottlegges. Dersom noen får fysisk tilgang til en måler, og mulighet til å hente ut informasjon fra denne (som f.eks. krypteringsnøkler), skal ikke dette kunne brukes til å få tilgang til informasjon fra (eller påvirke) andre målere eller hente ut informasjon fra sentralsystemet.

Eksempel:
Nettselskapet har sørget for at alle AMS-målere har en unik symmetrisk nøkkel som brukes for å autentisere måleren mot HES (og omvendt) samt for å etablere sesjonsnøkler for ende-til-ende-kryptering. Nettselskapet overvåker at det kun er en måler som kommuniserer med en gitt måler-ID/nøkkel-kombinasjon, og dersom det oppdages at flere enheter bruker samme ID/nøkkel, blir den angjeldende nøkkel gjort ugyldig, og måleren må byttes.

B.10 Tilgjengelig funksjonalitet (§4-6 f)

§

f. AMS skal til enhver tid kunne utføre de oppgaver systemet er designet for. Nettselskapet eller nettselskapets leverandør skal deaktivere funksjonalitet i AMS som ikke skal benyttes.

Beskrivelse av kravet
Dette kravet omfatter oppgavene som AMS-systemet skal utføre. Det er kun funksjonalitet som er i bruk til ett eller flere formål, som skal være aktiverte. Funksjonalitet som ikke benyttes, skal deaktiveres.

Ordforklaring

Deaktivere	Gjøres utilgjengelig for bruk/Settes ut av drift

Hvordan oppfylle kravet?
Kontroll på sikkerhet i AMS med tilgjengelig og deaktivert funksjonalitet inkluderer følgende sikkerhetsområde:

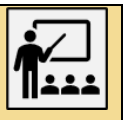
- Kontroll på sikkerhet med deaktivert eller ikke brukt funksjonalitet (B.10.1)
- Avviks- og hendelseshåndtering (B.10.2)
- Katastrofehåndtering og -øvelser (B.10.3)
- Sikkerhetskopier og gjenoppretting (B.10.4)

Sikkerhetsområdet er forklart med kontrollmål, hensikt, med påfølgende eksempler.

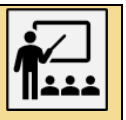
B.10.1 Kontroll på sikkerhet med deaktivert eller ikke brukt funksjonalitet

Kontrollmål:	Vurdering av krav
a. Funksjonalitet i AMS som ikke er i bruk skal deaktiveres	SKAL
b. Funksjonalitet som er deaktivert eller ikke tilgjengelig for bruk skal ikke påvirke sikkerheten i løsningen.	SKAL

Hensikt
Forhindre at funksjonalitet som ikke er i bruk er aktivert og kan utnyttes av en angriper. Ideelt sett burde all kode som ikke er i bruk fjernes, da dette vil redusere kompleksiteten, og gjøre analyser lettere. Utover dette vil all kode potensielt kunne representere et angrepspunkt for en inntrenger, og ved å deaktivere kode som ikke brukes vil man minimalisere angrepsflaten til AMS.



Eksempel:
Nettselskapet har ikke tatt i bruk muligheten for struping i deres AMS-løsning. De gjennomfører egne tester for å verifisere at det ikke er mulig å strupe strømmen hos sluttbrukere fra sentralsystemet.



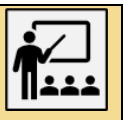
Eksempel:
Nettselskapet har ikke åpnet for bruk av serviceport (optisk kommunikasjonsport) i deres AMS-løsning. De gjennomfører egne tester for å verifisere at det ikke er mulig å koble til serviceporten eller på noe vis å påvirke AMS-løsningen via den deaktiverte serviceporten.

B.10.2 Avviks- og hendelseshåndtering

Kontrollmål:	Vurdering av krav
a. Nettselskapet skal etablere en dokumentert prosess for avviks- og hendelsesregistrering.	SKAL
b. Nettselskapet skal etablere en dokumentert prosess for hendelseshåndtering.	SKAL

Hensikt
Å registrere og håndtere avvik er en svært viktig funksjon for å kontrollere at sikkerheten er tilstrekkelig ivaretatt, samtidig som man raskt kan se trender som forteller om det er uvanlig aktivitet rundt AMS.

Ved en konkret hendelse er det viktig at nettselskapet har klare rutiner og prosedyrer for hvordan hendelsen skal håndteres, slik at man unngår misforståelser, uklare ansvarsforhold og at man på en mest mulig effektiv måte får normalisert situasjonen.



Eksempel:
Nettselskapet har etablert en prosess for registrering og håndtering av avvik og hendelser hvor forskjellige hendelser er klassifisert i følgende kategorier:

1. Uautorisert tilgang til informasjon
2. Kompromittering
3. Forsøk på kompromittering
4. Tjenestenekt
5. Rekognosering/informasjonsinnsamling
6. Annet

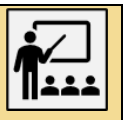
Nettselskapet har dokumentert roller og ansvar, og har en plan for håndtering og avklaring av hendelser, og rutiner for eskalering. Alle hendelser i kategori 1-5 over rapporteres til KraftCERT via MIPS-plattformen, andre hendelser vurderes individuelt om de skal rapporteres. Avvik som det ikke gjøres noe med, skal godkjennes av nettselskapets sikkerhetsansvarlig. Alle avvik fra egne og eksterne krav dokumenteres, og alle avvik som ikke er lukket følges opp til de lukkes.

Veileder
Grunnprinsipper for IKT-sikkerhet 2.0 – Forbered virksomheten på håndtering av hendelser
Grunnprinsipper for IKT-sikkerhet 2.0 – Vurder og klassifiser hendelser
Grunnprinsipper for IKT-sikkerhet 2.0 – Kontroller og håndter hendelser

B.10.3 Katastrofehåndtering og –øvelser

Kontrollmål:	Vurdering av krav
a. Nettselskapet skal ha beredskapsplaner og forberedte løsninger for å sikre beredskap, kontinuitet og evne til å håndtere katastrofer knyttet til informasjonssikkerhet og AMS.	SKAL
b. Det skal jevnlig gjennomføres øvelser for å håndtere omfattende sikkerhetshendelser og -katastrofer.	SKAL

Hensikt
Beredskapsplaner og øvelser er helt nødvendig for at nettselskapet effektivt kan håndtere en katastrofe, og raskt kan gjenopprette AMS-løsningen ved en større hendelse. For mer informasjon og beredskapsplaner og øvelser, se eksempler i "Veiledning til forskrift om beredskap i kraftforsyningen".



Eksempel:
Nettselskapet har en beredskapsplan som også omfatter sikkerhetshendelser i AMS. Nettselskapet gjennomfører årlig en beredskapsøvelse som tester de vesentlige momentene i beredskapsplanen. Alle tjenesteleverandører som er involvert i AMS hos Nettselskapet deltar i øvelsen.

Veileder
Veiledning til forskrift om beredskap i kraftforsyningen

B.10.4 Sikkerhetskopier og gjenoppretting

Kontrollmål:	Vurdering av krav
a. Det skal foreligge sikkerhetskopier av all kritisk programvare, konfigurasjoner, dokumentasjon av alle relevante komponenter i AMS-løsningen.	SKAL
b. Det skal foretas jevnlig sikkerhetskopiering av måledatabasen.	SKAL
c. Sikkerhetskopiene bør lagres på et sikkert sted /et annet fysisk sted enn der originalene befinner seg.	BØR
d. Sikkerhetskopiene bør umiddelbart gjenopprettes på et test/skyggesystem for å verifisere at de er korrekt generert.	BØR

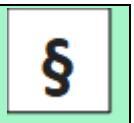
Hensikt
Ved katastrofale feil i systemet, er det svært viktig at nettselskapet har rask tilgang på sikkerhetskopier for å unngå unødig lang nedetid og eksponering av AMS-løsningen for mulige sårbarheter.

Eksempel:
Nettselskapet har sikkerhetskopi av HES programvare og alle HES konfigurasjonsfiler samt de tre siste versjoner av firmware for alle AMS målertyper i sitt nett. Sikkerhetskopiene oppbevares off-line hos

nettselskapets leverandør av IT-tjenester. Hver gang det tas sikkerhetskopi av HES og tilhørende konfigurasjon skal det verifiseres at dette kan gjenopprettes korrekt på et test/skyggesystem.

Veileder
Grunnprinsipper for IKT-sikkerhet 2.0 – Etabler evne til gjenoppretting av data

B.11 Tilgangsbegrensning i målepunkt (§4-6 g)



g. I målepunkt for sluttbrukere i lavspenningsanlegg skal tilgang til AMS-målerens grensesnitt begrenses for andre enn sluttbruker, nettselskapet og andre aktører med legitimt behov. I øvrige målepunkt skal kun nettselskapet og andre aktører med legitimt behov ha tilgang til AMS-måleren.

Beskrivelse av kravet
Dette kravet omfatter tilgang til målepunkt hvor AMS-måler er installert. For målere tilknyttet lavspenningsanlegg og tilknyttet en sluttbruker, er det kun sluttbruker, nettselskapet og andre aktører med legitimt behov som skal ha tilgang til grensesnittet på AMS-måler. I øvrige målepunkt (dvs. ikke tilknyttet en sluttbruker), er det kun nettselskap og andre aktører med legitimt behov som skal ha tilgang.

Ordforklaring

Sluttbruker i lavspenningsanlegg	Strømkunde (f.eks. husholdningskunde, hyttekunde, næringskunde, …)

Veileder
AMS + HAN - om å gjøre sanntids måledata tilgjengelig for forbruker. Vedlegg 1 - HAN personvern
Krysskobling til andre paragrafer og regelverk
Lov om behandling av personopplysninger (personopplysningsloven),
https://lovdata.no/dokument/NL/lov/2018-06-15-38

Hvordan oppfylle kravet?
Tilgangsbegrensning i målepunkt inkluderer følgende sikkerhetsområde:

- Beskyttelse mot uautorisert fysisk tilgang til AMS-utstyr (B.11.1)

Sikkerhetsområdet er forklart med kontrollmål, hensikt, med påfølgende eksempler.

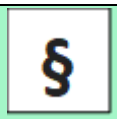
B.11.1 Beskyttelse mot uautorisert fysisk tilgang til AMS-utstyr

Kontrollmål:	Vurdering av krav
a. Det skal være tiltak for å forhindre misbruk av HAN-port, port for andre målere og serviceport	SKAL

Hensikt
AMS-måler er utstyrt med flere porter som gir fysisk tilgang. Det gjelder HAN-port, port for andre målere og serviceport. Det skal være implementert tiltak som forhindrer at disse portene kan misbrukes av uautoriserte som kan få tilgang til lokalene hvor AMS-måler er montert.

Eksempel: HAN-port
Nettselskapet har i utgangspunktet deaktivert HAN-porten i alle AMS-målere. Kunder kan aktivere HAN-porten slik at den begynner å sende ut forbruksdata ved å gå inn på "min side" i Nettselskapets kundeportal. Når kunder flytter eller sier opp leveransen av strøm fra nettselskapet, blir HAN-porten automatisk deaktivert. Kunden må evt. manuelt åpne HAN-port igjen på den nye adressen.

B.12 Opprettholdelse/forbedring av sikkerhetsnivå i AMS ved tilkobling av andre enheter eller systemer (§4-6 fjerde ledd)



Dersom nettselskapet eller nettselskapets leverandør kobler andre enheter eller systemer til AMS, skal sikkerhetsnivået i AMS opprettholdes eller forbedres. Tilsvarende gjelder dersom sluttbruker eller tredjepart kobler seg til AMS.

Beskrivelse av kravet
Dette kravet omfatter tilkobling av andre enheter eller systemer til AMS, og at dette kun kan gjøres hvis sikkerhetsnivået i AMS kan opprettholdes eller forbedres. Dette gjelder både for nettselskap, nettselskapets leverandør, sluttbruker eller tredjepart.

Hvordan oppfylle kravet?
Opprettholdelse/forbedring av sikkerhetsnivå i AMS ved tilkobling av andre enheter eller systemer inkluderer følgende sikkerhetsområder:

- Tilkobling av eksternt utstyr (B.12.1)
- Tilkobling av utstyr i AMS lokalisert hos sluttbruker (B.12.2)

Sikkerhetsområdene er forklart med kontrollmål, hensikt, med påfølgende eksempler.

Krysskobling til andre paragrafer og regelverk
HAN+AMS – om å gjøre sanntid måledata tilgjengelig for forbruker - NEK

B.12.1 Tilkobling av eksternt utstyr

Kontrollmål:	Vurdering av krav
a. Nettselskapet skal eksplitt godkjenne alle enheter som kobles til AMS	SKAL
b. Enheter som kobles til AMS skal ikke påvirke sikkerheten negativt	SKAL

Hensikt
Kun utstyr som er eksplisitt godkjent av nettselskap skal kobles til andre deler av AMS enn HAN-porten. Nettselskapet skal også eksplisitt godkjenne evt. utstyr som kobles til slike "andre enheter eller utstyr".

Eksempel:
Nettselskapet inngår avtale med kommunens vann- og avløpsverk om å koble automatiske vannmålere til AMS-målere i kommunen. Nettselskapet påser at datamengden fra vannmåleren ikke kan overstige en nærmere angitt maksimumsgrense, slik at vannmåleren ikke kan utgjøre en risiko for tilsiktet eller utilsiktet tjenestenekt. Data som overstiger denne grensen, skal avvises i AMS-måleren. Vannmåleren skal ha tilsvarende adgangsbegrensninger som AMS-måleren, dvs. at sluttbrukere kun får koble til enveis (kun lese) grensesnitt, og ingen ytterligere enheter kan kobles til vannmåleren uten at dette er eksplisitt godkjent av nettselskapet. Vannmåleren får kun kommunisere måleverdier via AMS-måleren, og vannmåleren får ikke anledning til å sende kommandoer eller på annet vis påvirke AMS-måleren.

B.12.2 Tilkobling av utstyr i AMS lokalisert hos sluttbruker

Kontrollmål:	Vurdering av krav
a. Enheter som sluttbrukere kobler til AMS skal kun kunne lese fra, ikke skrive til AMS	SKAL

Hensikt
Sluttbrukere skal kun ha mulighet til å koble seg til HAN-porten, og hvis HAN-porten er ukryptert kun dersom de eksplisitt har bedt om at den skal åpnes. HAN-porten skal være enveis, dvs. det skal kun være mulig å lese ut av porten, ikke sende data til den. Sluttbrukere kan koble til utstyr fra tredjeparter til HAN-porten, men ettersom HAN-porten er enveis, vil ikke dette kunne påvirke AMS.

Eksempel:
Sluttbrukeren har kontaktet Nettselskapet for å få åpnet HAN-porten, og har koblet den til en tredjeparts enhet for å administrere strømsparing i boenheten. HAN-porten sender ut forbruksdata i henhold til fastlagt skjema, men det ikke mulig å skrive data til HAN-porten.

Tilkobling av utstyr til AMS lokalisert hos sluttbruker

Dette gjelder kun tilkobling av utstyr til HAN-port på AMS-måler tilknyttet sluttbrukere i lavspenningsanlegg, eller tilsvarende port for AMS-måler tilknyttet sluttbrukere i høyspenningsanlegg.

B.13 Internkontrollsystem (§4-6 femte ledd)

Nettselskapet skal dokumentere oppfyllelse av krav i første til fjerde ledd i et internkontrollsystem.

Ordforklaring

Internkontroll	Bedriftens egenkontroll.
Internkontrollsystem	Et kvalitetssystem, styringssystem eller ledelsessystem for etterlevelse av regelverk.

Beskrivelse av kravet

Dette kravet krever at nettselskapet skal etablere et internkontrollsystem, for å kunne dokumentere hvordan krav i §4-6 første til fjerde ledd er oppfylt. Systemet skal være et oversikts- og styringsverktøy for virksomheten. Systemet skal kunne gi en rask og korrekt dokumentasjon over status i forhold til alle relevante bestemmelser etter denne forskriftsparagraf.

Hvordan oppfylle kravet?

Internkontrollsystem inkluderer følgende sikkerhetsområde:

- Internkontrollsystem for sikkerhet (B.13.1)

B.13.1 Internkontrollsystem for sikkerhet

Kontrollmål:	Vurdering av krav
a. Nettselskapet skal ha et dokumentert internkontrollsystem for sikkerhet som omfatter AMS.	SKAL

Hensikt

Sikre at nettselskapet etablerer et system som legger til rette for at personvern, konfidensialitet, integritet og tilgjengelighet ivaretas for alle aspekter av driften.

Den enkelte virksomhet må selv bestemme hvor omfattende systemet skal være. Bestemmelsen gir ingen avgrensning med hensyn til å bruke eller tilpasse allerede etablerte internkontrollsystemer, så lenge bestemmelsens vilkår er oppfylt gjennom å dokumentere at alle krav til beredskap i lov og forskrift er oppfylt. Internkontrollsystemet må for eksempel gi informasjon om når siste sikkerhetsvurdering ble utført

for et anlegg eller system, hvem som godkjente analysen og hvem som deltok i arbeidet, hvor analysen ligger og hva som er neste planlagte revisjonsdato med videre.

Eksempel: Etablering av internkontrollsystem

For å være sikre på å kunne dokumentere hvordan krav i §4-6 første til fjerde ledd er oppfylt, har nettselskapet valgt å etablere et eget internkontrollsystem i henhold til anbefalinger fra Datatilsynet. Nettselskapet skaffer seg tilstrekkelig kunnskap om personvern og informasjonssikkerhet gjennom å engasjere en ekstern konsulent for å gjennomføre et opplæringsopplegg, og ledelsen tar ansvar for at det utarbeides retningslinjer/rutiner og at internkontrollaktiviteter gjennomføres. Formålet med internkontrollen dokumenteres, sammen med vurdering av lovlighet, nødvendighet og proporsjonalitet av tiltak. Nettselskapet beskriver de overordnede rammer for internkontrollen, og tilhørende plikter. Nettselskapet bruker malene til Datatilsynet for å lage styrende, gjennomførende, og kontrollerende dokumentasjon, og sørger for at malene tilpasses nettselskapets lokale forhold.

Maler
Datatilsynet Måler og støtteverktøy for etablering av internkontroll
Standarder
ISO/IEC 27001 – Beskrivelse (Digitaliseringsdirektoratet)
Veileder
Veiledning til kraftberedskapsforskriften Kapittel 2
Datatilsynet – Hvordan gjennomføre internkontroll i praksis
Krysskobling til andre paragrafer og regelverk
Kraftberedskapsforskriften §2-10 Internkontrolllsystem

B.14 "Sjekkliste"

Tabell B1 Krav til nettselskapet i henhold til forskrift (§4-6 første og andre ledd) (SKAL-krav er beskrevet i vanlig font, og *BØR-krav er beskrevet i kursiv*.)

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Etablering og oppfølging av sikkerhetskrav		
a. Nettselskapets ledelse skal utarbeide og godkjenne overordnede sikkerhetskrav til AMS-løsningen. Disse skal dekke alle prosesser og systemer som påvirker AMS og eventuelt kraftforsyningen. Kravene skal være målbare og dokumenteres. *b. Nettselskapet ledelse bør etablere et system for å følge opp og forbedre sikkerhetskravene for AMS.*	• Nettselskapets ledelse dokumenterer sitt engasjement for å få utarbeidet sikkerhetskravene og oppfølgingen av dem. • Nettselskapet skal sørge for å ha nødvendig tilgang på kompetanse på eget sikkerhetsarbeid knyttet til AMS. • Nettselskapet skal utpeke en informasjonssikkerhetsansvarlig for AMS. Denne personen skal gis nødvendig myndighet, ansvar og opplæring samt få avsatt tilstrekkelig tid og ressurser slik at funksjonen kan ivaretas på en tilfredsstillende måte. • Det må gjennomføres tilstrekkelig opplæring på informasjonssikkerhet for alle nettselskapets egne og innleide ressurser. • Kravene skal baseres på risiko- og sårbarhetsanalyse, og være tilstrekkelige for å oppnå et akseptabelt risikonivå. • Sikkerhetskravene skal gjennomgås minimum årlig for å klarlegge om kravene er hensiktsmessige i forhold til nettselskapets behov, og kontrollere etterlevelse av forskriftskrav. • Konkretiser sikkerhetskrav i konkurransegrunnlag og kontrakt med leverandør	

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Risiko- og sårbarhetsanalyse		
a. Det skal gjennomføres risiko- og sårbarhetsanalyse eller annen hensiktsmessig sikkerhetsvurdering av AMS med den hensikt å identifisere risiko forbundet med drift og sikkerhet av AMS. *b. Konfigurasjon og oppsett for kritiske kommandoer, målerdata og annen informasjon i AMS løsningen bør være basert på risiko.*	• I analysen skal alle forhold vurderes som for eksempel kan hindre korrekt avregning, hindre tilfredsstillende funksjonalitet, sette informasjonssikkerheten i fare eller hindre kraftforsyning til sluttbrukere. • Det skal fastsettes akseptabelt risikonivå som risikoene i risiko- og sårbarhetsanalysen skal vurderes mot. Der hvor risikonivå er høyere enn akseptabel risiko skal tiltak etableres slik at akseptabelt risikonivå oppnås. Omfang av og type sikkerhetstiltak skal være tilpasset risiko. • Dersom større tiltak er nødvendig for å oppnå akseptabelt risikonivå, skal tilstrekkelige midlertidige kompenserende tiltak iverksettes inntil permanente tiltak er på plass. • Risiko- og sårbarhetsanalysene skal utføres og gjennomgås årlig og ved endringer i løsninger eller i trusselsituasjon som påvirker drift og sikkerhet i AMS.	
Sikkerhetsområde: Sikkerhetsavtaler		
a. Nettselskapet skal inngå sikkerhetsavtaler med alle leverandører eller enkeltpersoner som ikke er ansatt i nettselskapet dersom de skal utføre enhver form for arbeid på sentrale løsninger eller komponenter i AMS-løsningen.	• Underskrevne avtaler.	
Sikkerhetsområde: Tjenesteutsetting av utrulling og/eller drift av AMS-løsningen til tredjepart		
a. Sikkerheten i AMS skal ikke påvirkes ved at utrulling eller drift av AMS settes ut til ekstern tjenesteleverandør.	• Nettselskapet må påse at de selv har tilstrekkelig kompetanse til å sette krav til sikkerhet i AMS gjennom kravspesifikasjonen, og også kunne kontrollere at kravene blir etterlevd i driftssituasjonen. • Nettselskapet må sette målbare krav til leverandørene.	

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
	• Kravene må følges opp regelmessig. • Nettselskapet må ha innsyn og forståelse av sikkerhetstiltakene som etableres og risikoen tjenesteutsettingen medfører. • Nettselskapet må ha realistisk mulighet til å trekke tilbake avtalen ved avtalebrudd, uakseptabel risiko eller endringer i regulering. • Tjenesteutsettingen må ikke påvirke risiko for kraftforsyningen negativt.	
Sikkerhetsområde: Elektronisk beskyttelse mot ondsinnet programvare og inntrengning		
a. Det skal etableres et system for overvåking og beskyttelse av programvaren i AMS med hensikten å oppdage og stanse ondsinnet programvare.	• Virusbeskyttelse eller tilsvarende • Beskyttelse mot målrettede og tilfeldige angrep • Implementering av ”Intrusion detection system” eller ”Intrusion prevention system” • Brannmurbeskyttelse • Logisk eller fysisk segmentering/soneinndeling av ulike deler av nettverk etc.	
Sikkerhetsområde: Beskyttelse mot uautorisert fysisk tilgang til AMS-utstyr		
a. Alle rom som inneholder utstyr som er kritisk for AMS skal være egen adgangskontrollert sone. b. Komponenter i AMS utenfor adgangskontrollerte soner skal beskyttes mot uautorisert fysisk tilgang. c. Alle forsøk på å få uautorisert tilgang til utstyr i AMS-løsningen eller rom med kritisk AMS-utstyr skal oppdages straks registreres og varsles så snart som mulig.	• Ved forsøk på uautorisert fysisk adgang skal det sendes et varsel til nettselskapet. Varselet skal logges og inneholde tidspunkt for utløsning av varselet. • Det skal kunne bevises dersom det har blitt utført uautorisert tilgang, for eksempel ved at det etterlates fysiske merker eller andre typer spor dersom noen bryter opp enheten. • Kommunikasjonsinstallasjoner og - skap skal beskyttes mot uautorisert fysisk adgang. Ved forsøk på og uautorisert adgang skal varsel sendes til nettselskapet. Nettselskapet skal undersøke og iverksette aktiviteter tidsriktig.	

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
	• Varsel om uautorisert fysisk adgang skal følges opp av nettselskapet.	

Tabell B2 Godkjenning av enheter og brukere som skal kommunisere til eller i AMS (§4-6 a)

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Tilgangskontroll for system		
a. Nettselskapet skal ha prosedyrer og kriterier for tildeling, endring, sletting og verifikasjon av korrekt tilgang til kundedata samt AMS-funksjonalitet	• Ha prosedyrer som sikrer at kun autoriserte personer kan få tilgang til, endre, slette eller utlevere målerdata eller annen sensitiv kundeinformasjon. Prosedyrene skal inkludere både intern og ekstern tilgang. • Nettselskapet skal foreta tilstrekkelig bakgrunnssjekk av personell som skal ha tilgang til å håndtere sensitive systemer og informasjon. Med tilstrekkelig menes for eksempel som minimum vandelsattest (hvis mulig), kredittsjekk og referansesjekk. • Tilgang skal administreres på basis av forhåndsdefinerte roller og tilgangsnivåer. • Tilganger skal tildeles, endres, fjernes og revideres basert på tjenstlig behov. • Ha prosedyrer og tekniske løsninger som skal sikre at kritiske operasjoner ikke kan kunne utføres av én person alene. Den som gir tilgang til funksjonen, skal ikke kunne utføre tilsvarende funksjon. • Ha prosedyrer som sikrer at maskinvare som inneholder sensitiv informasjon skal avhendes på en sikker måte.	

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
	• Ha tekniske løsninger for å oppdage uautorisert endring i målerdata eller personopplysninger • Ha tekniske løsninger for å forhindre uautorisert utlevering av målerdata eller personopplysninger • Ha tekniske løsninger for å loggføre dersom det utføres endringer i allerede registrerte målerdata • Ha tekniske løsninger for å loggføre dersom målerdata eller annen kundeinformasjon utleveres til autorisert tredjepart.	
Sikkerhetsområde: Identifisering og autorisasjon av enheter		
a. Det skal implementeres mekanismer for å autentisere og autorisere enheter i AMS før det opprettes forbindelse mellom enheten og resten av AMS. *b. Ved bruk av nettverk som nettselskapet ikke kontrollerer, f.eks. Mobilt Bredbånd (MBB), bør ekstra sterk autentisering foretas.*	• Det skal ikke tillates tilkobling av enheter uten at disse er autorisert og autentisert • *Hver enhet i AMS skal tildeles et unikt sikkerhetssertifikat som kontrolleres før det sendes/mottas data fra enheten.* • Der man ikke får kontrollert eller verifisert enheten, skal enheten nektes tilgang til nettverket. • *Sikkerhetssertifikatet skal benyttes for å autorisere enheter i AMS*	
Sikkerhetsområde: Identifisering og autorisering av eksternt utstyr		
a. Håndholdte enheter (feltutstyr) må være autorisert og skal autentiseres av AMS - løsningen. Bruker skal være autorisert og autentisert.	• Det skal ikke tillates tilkobling av eksternt utstyr uten at disse er autorisert og autentisert • Hver enkelt enhet skal utstyres med et sikkerhetssertifikat som kontrolleres ved oppkobling mot enheter i AMS. • *Det bør sperres for at eksternt utstyr benyttes til annet enn oppgave mot AMS.*	

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
	• Autoriseringsprosessene skal være formaliserte i form av instrukser/ prosedyrer. • Det skal være mulig å fjerne/endre autorisering av håndholdte enheter sentralt.	
Sikkerhetsområde: Fjerntilgang til AMS fra tredjepart eller leverandør		
a. Det skal etableres prosedyrer for godkjenning, administrering og overvåking av eksterne tilkoblinger for vedlikehold og diagnostiske aktiviteter på alle komponenter i AMS-systemet.	• Det skal ikke opprettes tilkobling til tredjepart eller leverandør uten eksplisitt avtale med selskapet. • Tredjepart må forpliktes til å etterleve relevante sikkerhetskrav. • Tredjepart må benytte en sikker løsning for fjerntilgang. • *Fjerntilgang bør kun tillates fra sikre lokasjoner som ikke medfører økt risiko.* • Når eksternt vedlikehold er fullført, skal det fra nettselskapet eller fra AMS-komponenten avslutte alle økter og eksterne tilkoblinger som er opprettet.	

Tabell B3 Sporbarhet av endringer av programvare og konfigurasjon av dataprogram (§4-6 b)

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Sporing av endringer		
a. Nettselskapet skal dokumentere prosedyrer for å planlegge og utføre endringer i AMS-miljøet. b. Sentralsystemet skal logge alle endringer i programvare og konfigurasjon i AMS	• Alle endringer i AMS-løsningen skal dokumenteres. • Alle endringer skal testes og godkjennes før de rulles ut. • Alle endringer skal vurderes i forkant om endringen kan medføre risiko for kritiske AMS-funksjoner eller medføre konsekvenser for kraftforsyningen. • All ny programvare som innføres i AMS løsningen skal sikres slik at integritet ivaretas. • Enheter skal kunne verifisere at oppdatering av firmware er autorisert og at firmwaren er umodifisert og godkjent før den oppdateres. • Sentralsystem med personlig innlogging og tofaktor autentisering	
Sikkerhetsområde: Oppdatert dokumentasjon av AMS-løsningen		
a. Det skal til enhver tid foreligge fullstendig og oppdatert dokumentasjon av AMS-løsningens komponenter og konfigurasjoner.	• Alle sikkerhetsrutiner og sikkerhetstiltak skal være dokumentert. • *Dokumentasjonen bør være systematisert og sporbar* • Det skal klart fremkomme gyldighet, eierskap og endringshistorikk. • Dokumentasjonen skal være beskrevet og komplett på en slik måte at enhver (både internt og evt leverandør) effektivt kan utføre vedlikehold eller feilretting. • Dokumentasjonen skal oppbevares separat fra AMS-løsningen • Utførte kontrolltiltak skal være dokumenterte og etterprøvbare.	

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Kontroll med integriteten til programvare		
a. Det bør etableres et system for overvåking og avdekking av uautoriserte endringer av programvare og informasjon.	• *Utføre integritetsskanning av AMS-løsningen* • *Integriteten på programvare bør sjekkes ved oppstart, oppdatering og eksekvering.* • *Enheten skal være sikret fysisk og logisk mot uautorisert oppdatering og endring av programvare* • *Endringer av programvare bør være testet og godkjent* • *Implementering av automatiske verktøy som varsler ved integritetsavvik.* • *Enhetene i AMS skal kunne verifisere at alle spørringer og kommandoer er gyldige, har rett format og er foretatt fra autentisert og autorisert kilde.* • *Sikkerhetssertifikatet bør benyttes for verifikasjon av kommandoeksekvering*	

Tabell B4 Beskyttelse av kommunikasjon mellom AMS-måler og sentralsystemet (§4-6 c)

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Sikkerhet i kommunikasjon i AMS-løsningen		
a. All kommunikasjon mellom måler og sentralsystem og øvrig utstyr i AMS skal foregå på en sikker måte slik at innsyn, avlytting eller manipulering av signaler og informasjon ikke er mulig. *b. Signalene og informasjonen bør krypteres ende-til-ende mellom måler og HES.*	• *Krypteringsalgoritmer som benyttes for sikker kommunikasjon skal som minimum være FIPS-godkjent (eller ekvivalent).* • *Krypteringsløsningen bør støtte PKI (Public Key Infrastructure) nøkkelkryptografi* • Påloggingsinformasjon som krypteringsnøkler, sikkerhetssertifikat etc skal kunne oppdateres sentralt. • *Sertifikatnøkler skal lagres kryptert.* • Det er ikke tilstrekkelig å benytte den innebygde krypteringsløsningen i MBB	

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Oppbevaring av sikkerhetssertifikater og krypteringsnøkler		
a. Nettselskapet skal utarbeide retningslinjer for sikker oppbevaring av sikkerhetssertifikater og krypteringsnøkler som benyttes i AMS. b. Enheten skal lagre påloggingsinformasjon, sikkerhetssertifikater og annen sikkerhetsinformasjon sikkert. *c. Autentisering bør gjøres ved bruk av flere faktorer*	• Dokumentasjon av retningslinjer • *Ved tilgang til private nøkler til sertifikater benyttes både passord og TOTP-basert sikkerhetskode*	

Tabell B5 Oppdatering av programvare (§4-6 d)

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Oversikt over versjoner i program- og maskinvare		
a. Nettselskapet skal ha en oppdatert oversikt over versjoner av all maskinvare, firmware, oppdateringer og programvare som benyttes i AMS løsningen. Oversikten skal oppdateres ved endringer og ved regelmessige gjennomganger.	• Etablere en form for sentral liste med oversikt over maskinvare, versjoner av programvare som disse benyttes etc. • Alle endringer i konfigurasjoner og programvare skal logges. • Fast prosedyre og klare ansvarsforhold for oppdatering av listen ved endringer. • Automatiske systemer som gir oversikt over programvareversjoner og som kan rulle ut oppdateringer.	
Sikkerhetsområde: Kontroll av ekthet av programvare		
a. Nettselskapet skal ha muligheten til å verifisere at programvare, firmware og tilhørende oppdateringer er ekte	• Programvareoppdateringer er signert av leverandøren, og kan verifiseres av leverandørens offentlige nøkkel	

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Kontroll med sårbarheter i programvare		
a. Nettselskapet skal ha prosesser for å fange opp eventuelle kjente programvaremessige sårbarheter i sitt AMS-miljø. b. Dersom man blir kjent eller varslet om sårbarheter, skal disse evalueres og eventuelt håndteres umiddelbart.	• Avtaler om varsling fra leverandør(ene) eller andre relevante samarbeidspartnere dersom det oppdages sårbarheter i sine system. • Regelmessig sårbarhetsscanning av enheter og infrastruktur. • Interne prosedyrer for hvordan slik informasjon skal behandles og sårbarheter håndteres. • Prosedyrer som sørger for at sikkerhetsoppdateringer blir utført så raskt som praktisk mulig på en sikker måte.	

Tabell B6 Sikkerhetshendelser (§4-6 e)

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Logging og overvåking		
a. Nettselskapet skal ha satt opp løsning og rutiner for sikkerhetslogging i den totale AMS-løsningen.	• Alle nettverkskomponenter, AMS enheter, operativsystemer, databaser, applikasjoner med videre skal settes opp med rett loggnivå for sikkerhet. • Endringer, feil, normal og unormal aktivitet og sikkerhetshendelser skal logges. • Loggene skal sikres og overvåkes sentralt for å fange opp eventuelle uønskede sikkerhetshendelser. • Logger skal kunne lagres lokalt dersom kommunikasjon mot sentralsystem ikke er tilgjengelig. Lokal logg må være av tilstrekkelig omfang stor for å kunne håndtere forventet maksimal nedetid på kommunikasjonsløsning. • Lokale og sentrale logger skal sikres mot uautoriserte endringer.	

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Uavhengighet		
a. Sikkerhetsfunksjonalitet i AMS-løsningen skal ikke påvirkes ved feil i AMS eller feil konfigurasjon av annen funksjonalitet.	• Utstrakt testing av funksjonalitet i et begrenset testmiljø. • Foreta regelmessig sikkerhetstesting • Ha prosess og prosedyrer for regelmessig identifikasjon og feilretting av sikkerhetssvakheter • Overvåking og varsling av unormal bruk eller trafikk	
b. Hvis man kompromitterer en måler, skal ikke dette ha noen konsekvenser for andre målere eller sentralsystemet.	• Alle AMS-målere skal bruke unike symmetriske nøkler	

Tabell B7 Tilgjengelig funksjonalitet (§4-6 f)

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Kontroll på sikkerhet med deaktivert eller ikke brukt funksjonalitet		
a. Funksjonalitet som er deaktivert eller ikke tilgjengelig for bruk skal ikke påvirke sikkerheten i løsningen.	• Utstrakt testing av funksjonalitet i et begrenset testmiljø. • Foreta regelmessig sikkerhetstesting • Ha prosess og prosedyrer for regelmessig identifikasjon og feilretting av sikkerhetssvakheter • Overvåking og varsling av unormal bruk eller trafikk	
Sikkerhetsområde: Avviks- og hendelseshåndtering		

a. Nettselskapet skal etablere en dokumentert prosess for avviks- og hendelsesregistrering og -håndtering.	• Alle avvik skal følges opp.
	• Prosessen skal inneholde retningslinjer for hvordan avvik skal behandles. De kan for eksempel være;
	  ○ klassifisering av hendelser,
	  ○ roller og ansvar
	  ○ plan for håndtering og avklaring
	  ○ eskalering
	  ○ terskel for varsling til NVE	

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
	• Avvik som det ikke gjøres noe med, skal godkjennes • Alle avvik fra egne og eksterne krav skal dokumenteres. • Alle avvik som ikke er lukket skal følges opp til de lukkes. • Utstrakt testing av funksjonalitet i et begrenset testmiljø. • Foreta regelmessig sikkerhetstesting • Ha prosess og prosedyrer for regelmessig identifikasjon og feilretting av sikkerhetssvakheter • Overvåking og varsling av unormal bruk eller trafikk	
Sikkerhetsområde: Katastrofehåndtering og –øvelser		
a. Nettselskapet skal ha beredskapsplaner og forberedte løsninger for å sikre beredskap, kontinuitet og evne til å håndtere katastrofer knyttet til informasjonssikkerhet og AMS. b. Det skal jevnlig gjennomføres øvelser for å håndtere omfattende sikkerhetshendelser og -katastrofer.	• Beredskapsplanene og løsningene skal evalueres regelmessig og i forbindelse med evaluering av øvelser. • Planene for og resultatene fra øvelsene skal dokumenteres. Avdekkes gap eller mangler etter øvelsene, skal det tas hensyn til dette i evalueringen eller oppdateringen av beredskapsplaner. • *Øvelser bør inkludere feilsituasjoner, sikkerhetshendelser i kombinasjon med ekstremvær eller andre relevante hendelser.* • *Øvelsene bør inneholde elementer av gjenoppretting etter katastrofer.* • Som et minimum skal det gjennomføres årlige øvelser.	
Sikkerhetsområde: Sikkerhetskopier og gjenoppretting		
a. Det skal foreligge sikkerhetskopier av all kritisk programvare, konfigurasjoner, dokumentasjon av alle relevante komponenter i AMS-løsningen.	• Dokumentasjon av sikkerhetskopieringsrutiner • *Nettselskapet bør med jevne mellomrom teste at gjenoppretting av sikkerhetskopiene fungerer etter hensikten.*	

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
b. Det skal foretas jevnlig sikkerhetskopiering av måledatabasen. *c. Sikkerhetskopiene bør lagres på et sikkert sted et annet fysisk sted enn der originalene befinner seg.* d. *Sikkerhetskopiene bør umiddelbart gjenopprettes på et test/skyggesystem for å verifisere at de er korrekt generert.*		

Tabell B8 Tilgangsbegrensning i målepunkt (§4-6 g)

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
a. Det skal være tiltak for å forhindre misbruk av HAN-port, port for andre målere og serviceport	• HAN-port stengt i utgangspunktet, åpnes kun ved anmodning, og stenges automatisk ved flytting	

Tabell B9 Krav til tilkobling av andre enheter eller systemer til AMS (§4-6 fjerde ledd)

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Tilkobling av andre enheter eller systemer til AMS		
a. Nettselskapet skal eksplitt godkjenne alle enheter som kobles til AMS b. Enheter som kobles til AMS skal ikke påvirke sikkerheten negativt	• Alle enheter må autentisere seg mot sentralsystemet • Kommunikasjon fra enheter som ikke er autentisert ignoreres	
Sikkerhetsområde: Tilkobling av andre enheter eller systemer til AMS		
Enheter som sluttbrukere kobler til AMS skal kun kunne lese fra, ikke skrive til AMS	• Dokumentasjon av funksjonalitet av HAN-port • Testing av HAN-port i et begrenset testmiljø	

Tabell B10 Krav til nettselskapet om Internkontrollsystem (§4-6 femte ledd)

Sikkerhetsområde/Kontrollmål	Eksempler for å oppnå kontrollmål	Status/evaluering
Sikkerhetsområde: Internkontrollsystem for sikkerhet		
Nettselskapet skal ha et dokumentert internkontrollsystem for sikkerhet som omfatter AMS.	• Dokumentasjon	

B.15 Kobling mellom sikkerhetskrav i Avregningsforskriften og tiltak i NSM sine grunnprinsipper

NSMs grunnprinsipper for IKT-sikkerhet (Tabell B11) anbefales for alle norske virksomheter, og bl.a. kraftberedskapsforskriftens krav til informasjonssikkerhet er i stor grad basert på grunnprinsippene. Grunnprinsippene er i stor grad anvendbare på industrielle systemer som smart grid.

Tabell B11 NSMs grunnprinsipper for IKT-sikkerhet

Identifisere og kartlegge		Beskytte og opprettholde		Oppdage		Håndtere og gjenopprette	
1.1	Kartlegg styrings-strukturer, leveranser og understøttende systemer	2.1	Ivareta sikkerhet i anskaffelses- og utviklings-prosesser	3.1	Oppdag og fjern kjente sårbarheter og trusler	4.1	Forbered virksomheten på håndtering av hendelser
1.2	Kartlegg enheter og programvare	2.2	Etabler en sikker IKT-arkitektur	3.2	Etabler sikkerhetsover-våkning	4.2	Vurder og klassifiser hendelser
1.3	Kartlegg brukere og behov for tilgang	2.3	Ivareta en sikker konfigurasjon	3.3	Analyser data fra sikkerhetsovervåkning	4.3	Kontroller og håndter hendelser
		2.4	Beskytt virksomhetens nettverk	3.4	Gjennomfør inntrengnings-tester	4.4	Evaluer og lær av hendelser
		2.5	Kontroller dataflyt				
		2.6	Ha kontroll på identiteter og tilganger				
		2.7	Beskytt data i ro og i transitt				
		2.8	Beskytt e-post og nettleser				
		2.9	Etabler evne til gjenoppretting av data				
		2.10	Integrer sikkerhet i prosess for endringshåndtering				

Grunnprinsippene er delt i 4 kategorier (Identifisere og kartlegge; Beskytte og opprettholde; Oppdage; Håndtere og gjenopprette), og hvert prinsipp er detaljert i et antall tiltak. Tabell B12 viser kobling mellom sikkerhetskrav i avregningsforskriften og relevante tiltak fra NSMs grunnprinsipper.

Tabell B12 Kobling mellom sikkerhetskrav i Avregningsforskriften og tiltak i NSMs grunnprinsipper

Forskriftskrav	Kort beskrivelse	Tiltak i NSMs grunnprinsipper	I hvilken grad dekker tiltakene forskriftskravet?
§4-6 a)	Godkjennelse av enheter og brukere som skal kommunisere til eller i AMS	1.2.1 1.2.2 1.2.3 1.3.1 1.3.2 2.6.2 2.6.3 2.6.6	Dekkes fullt ut
§4-6 b)	Loggføring av endringer av programvare og konfigurasjon av dataprogram i AMS	1.2.4 2.2.1 d) 2.10.1	Dekkes i stor grad, men sier ikke eksplisitt at endringer skal spores tilbake til enkeltbruker
§4-6 c)	Ende-til-ende kryptering i kommunikasjonen mellom AMS-måler og sentralsystem	2.4.2 2.7.1 2.7.2 2.7.4	Dekkes i stor grad, selv om ende-til-ende-kryptering ikke angis eksplisitt. Imidlertid vil ikke ende-til-ende-kryptering være et krav dersom nett-selskapet kontrollerer (og kan forhindre uvedkommendes tilgang til) alle steder informasjonen er ukryptert
§4-6 d)	Oppdatering av programvare i AMS	2.1.2 2.10.4 3.1.3 2.3.1	Dekkes fullt ut
§4-6 e)	Sikkerhet i AMS-målere skal ikke påvirkes av hverandre	2.2.5 2.3.4 2.5.3 2.7.1	Dekkes i stor grad, men sier ikke eksplisitt at alle målerne skal ha forskjellige symmetriske nøkler
§4-6 f)	Funksjonalitet i AMS skal fungere til enhver tid. Funksjoner som ikke brukes, skal deaktiveres	2.3.3 2.9.1	Andre del av kravet dekkes fullt ut
§4-6 g)	Kontroll på tilgang til AMS-målerens grensesnitt		Dekkes ikke (for spesifikt til å dekkes av grunnprinsipper)