SINTEF

TR A7619 - Åpen

# Rapport

## Evaluering av NVEs veileder til sikkerhet i AMS

NVE-Veileder nr. 7/2012

**Forfatter(e)**
Hanne Sæle
Maria Bartnes, Boye A. Høverstad, Martin Gilje Jaatun


**SINTEF Energi AS**
Energisystemer
2017-04-06

SINTEF Energi AS
Postadresse:
Postboks 4761 Sluppen
7465 Trondheim
Sentralbord: 73597200
Telefaks: 73597250
energy.research@sintef.no
www.sintef.no/energi
Foretaksregister:
NO 939 350 675 MVA

# Rapport

# Evaluering av NVEs veileder til sikkerhet i AMS

NVE-Veileder nr. 7/2012

EMNEORD:
AMS
Sikkerhet
Veileder
Forskrift

**VERSJON**
2.0

**DATO**
2017-04-06

**FORFATTER(E)**
Hanne Sæle
Maria Bartnes, Boye A. Høverstad, Martin Gilje Jaatun

**OPPDRAGSGIVER(E)**
NVE

**OPPDRAGSGIVERS REF.**
Øyvind Toftegaard

**PROSJEKTNR**
502001475

**ANTALL SIDER**
43

**SAMMENDRAG**
Denne rapporten er utarbeidet i forbindelse med prosjektet "Oppdatering av NVE veileder 7/2012 om "Veileder til sikkerhet i avanserte måle- og styringssystem" (AMS)".

Gjennom forskriftskrav er nettselskap ansvarlig for å installere AMS til målepunkt i sitt nett, og at AMS-infrastruktur skal være sikker mot misbruk av data og uønsket tilgang til styrefunksjoner. Veilederen omfatter innsamlingssystemet ("måleverdikjeden") og ble utarbeidet for å sette nettselskapene i best mulig stand til å oppfylle forskriftskravene om sikkerhet til AMS. Veileder ble utgitt i 2012, samme år som kravet om innføring av AMS ble innført i forskrift 301 om måling og avregning.

Dette prosjektet har evaluert dagens versjon av veileder og kommet med anbefalinger til mulige endringer. Evalueringen er basert på hva som er status for sikkerhetsarbeid i EU og erfaringer norske nettselskap har ved bruk av veileder.

**UTARBEIDET AV**
Hanne Sæle

SIGNATUR


**KONTROLLERT AV**
Andrei Z. Morch

SIGNATUR


**GODKJENT AV**
Knut Samdal

SIGNATUR


| RAPPORTNR | ISBN | GRADERING | GRADERING DENNE SIDE |
|---|---|---|---|
| TR A7619 | 978-82-594-3771-6 | Åpen | Åpen |

# Historikk

| VERSJON | DATO | VERSJONSBESKRIVELSE |
|---|---|---|
| 1.0 | 2016-12-15 | Endelig versjon |
| 2.0 | 2017-04-06 | Rapporten endret fra 'fortrolig' til 'åpen' |

SINTEF

# Innholdsfortegnelse

# 1 Innledning/Beskrivelse av oppdraget

Denne rapporten er utarbeidet for NVE i forbindelse med prosjektet Oppdatering av NVE veileder 7/2012 om "Veileder til sikkerhet i avanserte måle- og styringssystem" (AMS) ved SINTEF Energi og SINTEF IKT, høsten 2016. Prosjektet ble etablert etter en anbudsrunde høsten 2016.

## 1.1 Beskrivelse av oppdraget

Det er forskriftsfestet i ett av funksjonskravene til AMS at systemet skal «gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner», jf. § 4-2 bokstav g) i forskrift nr. 301 "Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv"[1].

Det er nettselskapene sitt ansvar å sikre sine AMS-relaterte systemer, herunder kommunikasjonsløsninger, mot uautorisert tilgang. Forskriftskravet til sikkerhet i AMS er generelt og overordnet, og det er derfor nettselskapenes ansvar å kartlegge de sårbarheter som måtte foreligge og iverksette de tiltak som er nødvendige for sikre sine AMS-systemer.

For å sette nettselskapene i best mulig stand til å oppfylle forskriftskravene om sikkerhet til AMS, utarbeidet NVE i 2012 veiledningen «Veileder til sikkerhet i avanserte måle- og styringssystem» (jf. NVE Veileder nr. 7/2012[2]).

Dette prosjektet skal svare på følgende punkter i utlysningen:

- Redegjøre for status om sikkerhetsarbeid/-krav i EU/EU-land relatert til AMS/Smart meters/grids.
- Gjennomgå og foreslå endringer i eksisterende veileder (NVE Veileder nr. 7/2012). Endringsforslag innbefatter både form og innhold.
- Under pkt. 2 skal det bl.a. vurderes sårbarheter/sikkerhetskrav knyttet til:
  - Innføring av Elhub
  - Tjenesteleverandører/leverandører av «tilleggstjenester»
  - Etablering av driftsselskap (f.eks. Valider AS og Smarthub AS)
  - Outsourcing av driftstjenester fra nettselskapene
  - Ulike modeller for drift, herunder bruk av skytjenester
  - Distribution management systems (DMS)
  - Andre/nye/uspesifiserte tjenester

[1] https://lovdata.no/dokument/SF/forskrift/1999-03-11-301
[2] http://webby.nve.no/publikasjoner/veileder/2012/veileder2012_07.pdf

## 1.2 Rapportstruktur

I kapittel 1 beskrives oppdraget slik det ble spesifisert i konkurransegrunnlaget fra NVE, og omfanget av arbeidet omtales i kapittel 2. I kapittel 3 blir det gitt en kort status om sikkerhetsarbeid/-krav i EU, relatert til AMS/Smart grids. I kapittel 4 beskrives arbeidsmetoden, dvs. hvordan arbeidsmøter har blitt gjennomført, og i kapittel 5 oppsummeres resultatet fra disse.

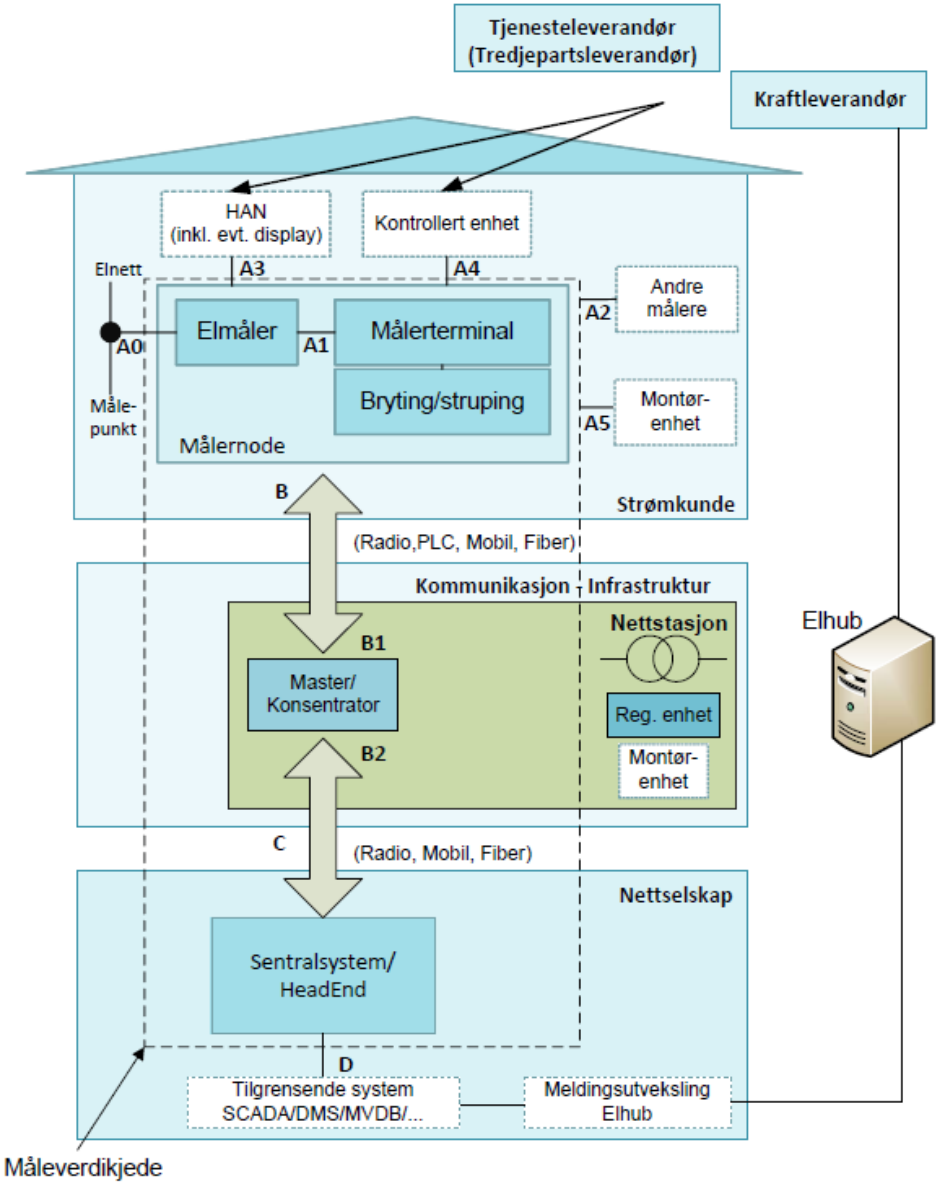
I anbudsforespørselen fra NVE ble det spesifisert noen ekstra punkter som også skal inngå ved vurdering av sårbarheter/sikkerhetskrav knyttet til AMS, og disse er omtalt i kapittel 6. I kapittel 7 presenteres SINTEF sine anbefalinger om endringer i dagens versjon av veileder, basert på diskusjoner på arbeidsmøtene.

Notater fra gjennomført arbeidsmøter er presentert i Vedlegg 1, og forkortelser brukt i rapporten er presentert i Vedlegg 2.

## 2 Omfang av dagens veileder

I dette prosjektet er det tatt utgangspunkt i dagens versjon av NVEs "Veileder til sikkerhet i avanserte måle- og styringssystemer", som ble publisert i september 2012. Dette var samme år som kravet om innføring av AMS ble innført i forskrift 301 om måling og avregning[3].

Dagens versjon av veilederen omfatter innsamlingssystemet ("måleverdikjeden") – fra målepunktet hos kundene til sentralsystemet hos nettselskap, samt kommunikasjonssystemet. En skisse til AMS-struktur er presentert i veileder. Vurderingen av dagens veileder er basert på dagens AMS-løsning og tilgrensede systemer, og en oppdatert skisse av AMS-infrastrukturen er presentert i figur 2.1



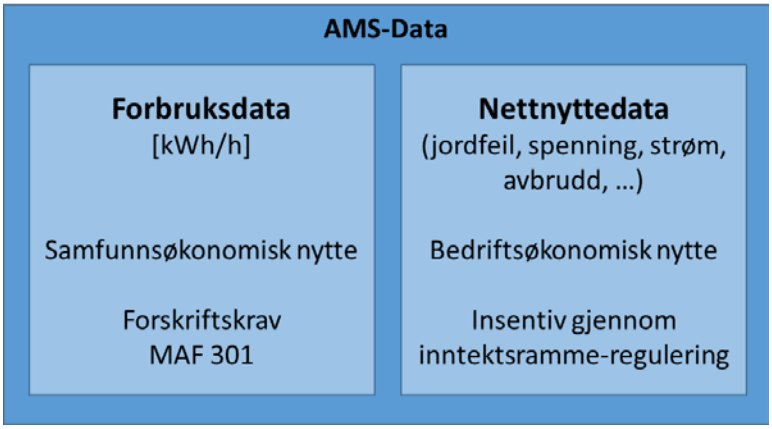

**Figur 2.1 Skisse AMS-infrastruktur**

[3] https://lovdata.no/dokument/SF/forskrift/1999-03-11-301

AMS-infrastruktur muliggjør innsamling av ulike type data. Gjennom forskrift om måling og avregning §4-2 er det krav om at AMS skal lagre måleverdier med en registreringsfrekvens på maksimalt 60 minutter (*punkt a)*) og at aktiv og reaktiv effekt i begge retninger skal registreres (*punkt h)*). Dette er forbruksinformasjon [kWh/h] som danner grunnlag for et velfungerende kraftmarked, og dermed har en samfunnsøkonomisk nytte.

I tillegg kan AMS-infrastruktur samle inn måleverdier som kan brukes direkte i nettdriften (dvs. nettnytte-data – spenning, strøm, avbrudd, alarm ved jordfeil o.l.). Nettnyttedata kan ha en bedriftsøkonomisk nytte og være et viktig bidrag for effektivisering av nettdriften.

Figur 2.2 viser ulike kategorier AMS-data.




**Figur 2.2 Ulike kategorier AMS-data**

Basert på NVE-rapporten "Smarte målere (AMS). Status og planer for installasjon og oppstart per 1. kvartal 2015"[4] har de fleste nettselskap vedtatt AMS-plan og inngått kontrakt med AMS-leverandør etter at veileder ble publisert i 2012. Det betyr at veilederen har vært tilgjengelig for nettselskap i prosessen med å spesifisere, forhandle og planlegge AMS-anskaffelse og utrulling.

Høsten 2016 har dette prosjektet vurdert gjeldende versjon av veileder til sikkerhet i AMS, med utgangs-punkt i at nettselskapene nå bl.a. har utarbeidet kravspesifikasjon for AMS, inngått allianser, valgt leverandør for AMS, startet utrullingen og begynt å få erfaring med drift av systemet.

[4] NVE-rapport 77/2015, "Smarte målere (AMS). Status og planer for installasjon og oppstart per 1. kvartal 2015", Arne Venjum, Cathrine Åsegg Hagen, http://publikasjoner.nve.no/rapport/2015/rapport2015_77.pdf

# 3 Status om sikkerhetsarbeid og -krav i EU relatert til AMS/Smart Grids

I forbindelse med prosjektet er det utført en kort litteraturstudie for å kartlegge status for sikkerhetsarbeid og -krav for AMS/smart grids i andre europeiske land. Relevante dokumenter ble identifisert gjennom nettsøk og konsultasjoner med nasjonale og internasjonale eksperter innen AMS, smart grids og informasjons-sikkerhet. I det følgende beskrives funnene for sikkerhetsarbeid og -krav fra sentrale EU-instanser, og deretter for utvalgte land.

## 3.1 EU og sentrale europeiske instanser

*The Smart Grids Task Force* (SGTF) ble satt opp av Europakommisjonen i 2009, og har siden da vært rådgivende overfor Europakommisjonen innenfor temaer knyttet til utvikling og utrulling av smart grid, herunder også innføringen av smarte målere[5]. SGTF er organisert i fem ekspertgrupper, hvorav ekspert-gruppe 2 fokuserer på personvern, datasikkerhet og cybersikkerhet i smart grid.

SGTF ekspertgruppe 2 publiserte i 2011 en rapport til EU-kommisjonen med anbefalinger til regelverk og retningslinjer for datasikkerhet i smart grid[6]. Rapporten ble etterfulgt av anbefaling 2012/148/EU fra EU-kommisjonen, som omhandler forberedelser til utrulling av smarte målere. Sikkerhetsarbeid er det ene av tre hovedtemaer i denne anbefalingen (metodikk for kost-nytte-vurderinger og funksjonelle krav er de to andre)[7].

Anbefaling 2012/148/EU erklærer at risikoelementer i utvikling av smart grid kan identifiseres ved å gjennomføre såkalte *data protection impact assessments* (DPIA). 2012/148/EU annonserte utviklingen av en mal for DPIA som skal hjelpe i dette arbeidet. Denne ble publisert av SGTF ekspertgruppe 2 i 2014[8], sammen med anbefaling 2014/724/EU[9]. DPIA-malen er nå inne i en 2-åring testfase som ble påbegynt i 2015[10].

Anbefaling 2012/148/EU omtales i mer detalj i kap. 3.1.2.

[5] https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force
[6] Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection: Recommendation to the European Commission, 2011. https://ec.europa.eu/energy/sites/ener/files/documents/Recommendations%20regulatory%20requirements%20v1.pdf
[7] 2012/148/EU: Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012H0148&from=EN
[8] https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf
[9] 2014/724/EU: Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.300.01.0063.01.ENG
[10] https://ec.europa.eu/energy/en/test-phase-data-protection-impact-assessment-dpia-template-smart-grid-and-smart-metering-systems

### 3.1.1 Overordnete betraktninger

De ovennevnte aktivitetene og aktørene fokuserer spesifikt på smart grid, hvor utrullingen av smarte målere er av særskilt betydning når det gjelder hensynet til personvern og datasikkerhet. Det er imidlertid viktig å påpeke to særskilte og nært relaterte aspekter som utpeker seg i alt arbeidet knyttet til cyber-sikkerhet for smart grid i EU: hensynet til personvernet, og viktigheten av å se smart grid- og AMS-spesifikke regelverk i lys av en større kontekst.

Moderne smarte målere tilbyr så høy oppløsning, både geografisk og i tid, at EU regner dataene de samler inn som personlige data. Innledningen til DPIA-malen illustrerer viktigheten av dette ved å påpeke at innføringen av smarte målere er den første virkelig store "testen" på *Internet of Things*[11].

Dette medfører blant annet at sikringen av disse dataene kan omfattes av EUs Personverndirektiv (Data Protection Directive 95/46/EC[12]). I motsetning til anbefalingene nevnt over, har direktiver normalt direkte innvirkning på norsk lovgivning. Personverndirektivet vil bli avløst av Personvernforordningen (Forordning 2016/679), som skal tre i kraft i 2018. Denne vil styrke retten til vern av og kontroll over personlige data ytterligere. Personvernforordningen vil automatisk gjelde også i Norge hvis den inkluderes i EØS-avtalen, og kan komme til å ha betydning for både sikring og utnyttelse av AMS-relaterte data.

I tillegg til Personverndirektivet og -forordningen, vil håndteringen av data fra smarte målere kunne påvirkes av lovverk fra NIS-direktivet[13] (2016/1148). For å styrke implementasjonen av disse lovene, påbegynte EUs Generaldirektorat for Energi i 2015 utviklingen av en helhetlig plattform for cyber-sikkerhet i hele energi-sektoren (*Energy Expert Cyber Security Platform – EECSP*)[14]. EECSP skal bestå av en ekspertgruppe og et forum. Vi har i skrivende stund ikke kunnet finne noe informasjon om status på arbeidet i ekspertgruppen.

### 3.1.2 Anbefaling fra EU-kommisjonen (2012/148/EU)

I EU er det krav om at smarte målere skal installeres for å muliggjøre at kunder kan delta i markedene for elektrisitet og gass, forutsatt at det ligger en positiv kost-/nytte-vurdering bak. Totalt skal slike smarte målere installeres hos 80% av kundene innen 2020[15].

I rapporten "Benchmarking smart metering deployment in the EU-27 with a focus on electricity"[16] er det beskrevet status for utrulling av smarte målere i EU-landene. Rapporten anbefaler at de nye målerne skal tilfredsstille følgende krav:

- Minimums funksjonskrav tilsvarende det som er spesifisert i [2012/148/EU][7]
- Ivareta personvern og sikkerhet
- Muliggjøre forbrukerfleksibilitet og andre energitjenester, og
- Sikre markedsbasert nytteverdi for kunde og energisystemet.

I anbefalingen vedrørende utrulling av smarte målere [2012/148/EU][7] er det definert et minimum funksjons-krav for de nye målere og det er spesifisert flere tiltak knyttet til bl.a. sikkerhet/security[17] for å sikre en

[11] "Internet of Things – New security and privacy challenges", https://www.researchgate.net/profile/Rolf_Weber3/publication/222708179_Internet_of_Things_-_New_security_and_privacy_challenges/links/0c96053cab03fee371000000.pdf
[12] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l14012&from=EN
[13] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[14] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3341
[15] https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters
[16] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0356&from=EN

konsekvent tilnærming i ulike land og anbefalinger for å sikre at informasjonssikkerhet ivaretas når data behandles i AMS-systemet, spesielt personopplysninger. Gjennom utførelse av *data protection impact assessments* (DPIA) skal risikoelementer identifiseres. Tiltak for å ivareta datasikkerhet og informasjons-sikkerhet skal bygges inn i AMS-systemet før det rulles ut ("security and data protection by design"), og benyttes i stor utstrekning.

Under kapitlet for beskyttelse og sikring av data anbefales det blant annet at "beste tilgjengelige teknikker" skal anvendes for personvern og datasikkerhet, samt at eksisterende og fremtidige komponenter må tilfreds-stille alle "sikkerhetsrelevante standarder", inkludert de relevante aspektene av *Smart Grid Architecture Model* (M/490 SGAM). Videre påpekes kravet om at alle aktiviteter må oppfylle kravene i EUs rammeverk for databeskyttelse, og at de nødvendige grep for å sikre personlige data inkluderes i systemet allerede fra designfasen.

På lik linje med NVEs veileder, påpeker anbefalingen at ansvaret for sikkerheten knyttet til smarte målere ligger hos nettverksoperatørene (§27).

Det anbefales også minimums funksjonskrav for å ivareta sikkerhet. Dette inkluderer sikret kommunikasjon i alle ledd, og mekanismer for å både unngå og oppdage sikkerhetsbrudd (svindel, hacking, etc.).

### 3.1.3 Andre europeiske aktører

Stiftelsen *The European Network for Cyber Security* (ENCS) bringer sammen aktører innen kritisk infrastruktur og sikkerhetseksperter for å hjelpe aktørene i kraftbransjen å imøtekomme anbefalingene og direktivene fra nasjonale og europeiske myndigheter, og på den måten sikre kraftnett og infrastruktur i Europa.

European Union Agency for Network and Information Security (Enisa) laget i 2014 en rapport om de forskjellige regimene for sertifisering av smartgrid-teknologi som eksisterte i Europa[18]. De konkluderte med at fragmentering og forskjeller mellom de forskjellige landene bidro til det største gapet mellom nåtilstanden og en fremtidig harmonisert sertifiseringsordning. De påpekte også at ingen av de eksisterende regimene kan dekke hele tillitskjeden fra design til utrulling, samt at hele kjeden ikke kan dekkes av alle smartgrid "use cases".

De viktigste anbefalingene fra rapporten omfatter:

- Utarbeidelse av harmonisert smartgrid sikkerhetspraksis i EU,
- Nasjonal implementering av spesifikke smartgrid use cases basert på en tillitskjede, og
- Opprettelse av en styringskomite for å ha overoppsyn med smartgrid sertifisering i EU.

[17] "COMMISSION RECOMMENDATION of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU)", http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012H0148&from=EN

[18] "Smart Grid Security Certification in Europe", https://www.enisa.europa.eu/publications/smart-grid-security-certification-in-europe

## 3.2 Eksempler fra ulike land i Europa

Dette avsnittet tar for seg sikkerhetsarbeidet og sikkerhetskrav knyttet til AMS-utrullingen i ulike land i Europa. Avsnittet gir et kort innblikk i status og sentrale aktører, men går ikke i detalj på de konkrete kravene i de enkelte land. Teksten er ment å fungere som et utgangspunkt for innhenting av mer detaljert informasjon direkte fra referansene.

**Østerrike**
Østerrike har utarbeidet et sett med krav (kravkatalog) til produsenter av AMS-komponenter[19]. Disse kravene inneholder også en veiledning for nettselskap som skal ta AMS i bruk, hvor hvert krav har en "implementation guidance" med f.eks. anbefalinger om type dokumentasjon produsentene bør stille til rådighet for kundene (dvs. nettselskapene). Enkelte av disse kan brukes som innspill til NVE-veilederen.

**Tyskland[20]**
Det tyske *Bundesamt für Sicherheit in der Informationstechnik* (BSI) legger opp til at det skal utføres en full sikkerhetsevaluering av alle målere etter kriteriene i den internasjonale standarden ISO[21]/IEC[22] 15408 (Common Criteria)[23]. BSI har utarbeidet en Protection Profile for gateways for smarte strømmålere, samt en egen Protection Profile for sikkerhetsmodulen til en AMI Smart Meter Gateway. Imidlertid kan vi merke oss at det ikke er laget noen Protection Profile for måleren selv.

Så langt er det bare en modul som er sertifisert:

- Security Module for a Smart Meter Gateway BSI-DSZ-CC-0957-2015 TCOS Smart Meter Security Module Version 1.0 Release 1/P60C144PVA T-Systems International GmbH 09.02.2015

Ytterligere åtte ulike Smart Meter Gateways er under evaluering.

Kravene er således rettet primært mot produsenter av utstyr, og ikke mot nettselskaper som skal ta dem i bruk. BSI har imidlertid også publisert retningslinjer Technische Richtlinie TR-03109, som omfatter interoperabilitet til kommunikasjonsenheten (TR-03109-1), interoperabilitet til sikkerhetsmodulen (TR-03109-2), kryptografiske forutsetninger (TR-03109-3), administrasjon av sertifikater (TR-03109-4), og administrasjon av gateway (TR-03109-6). Disse kan gi innspill til NVEs veileder, men ikke alle delene er fritt tilgjengelige.

[19] http://oesterreichsenergie.at/branche/stromnetze/sicherheitsanforderungen-fuer-smart-meter.html?file=files/oesterreichsenergie.at/Downloads%20Netze/Smart%20Meter/20150614%20E2E-Sicherheit-Anforderungskatalog-EN.PDF
[20] Informasjonen om Tyskland er hentet fra disse kildene:
- https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/UebersichtSP-TR/uebersicht_node.html
- https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/smartmeter_node.html
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0073b_pdf.pdf;jsessionid=E1D3288E56D99A6ECA11389E7058EA89.2_cid359?__blob=publicationFile&v=1

[21] ISO = International Organization for Standardization
[22] IEC = International Electrotechnical Commission
[23] http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341

**Storbritannia**
Storbritannia har valgt en modell for utrulling og drift av smarte målere hvor de forskjellige oppgavene i stor grad håndteres av utvalgte nasjonale aktører[24]:

- Offentlige myndigheter leder og overvåker utrullingen, og har også definert reglene og standardene som skal ivareta datasikkerhet og personvern. Arbeidet ble tidligere ledet av *The Department of Energy & Climate Change* (DECC), som i 2016 inngikk som en del av det nyopprettede *Department for Business, Energy & Industrial Strategy* (BEIS).
- Modellen for AMS-systemet og sikkerheten i dette har blitt designet i samarbeid med *Government Communications Headquarters* (GCHQ). Arbeidet videreføres av *The National Cyber Security Centre* (NCSC), en datterorganisasjon av GCHQ som ble opprettet i oktober 2016, med spesielt fokus på cybersikkerhet[25]. Artikkelen i fotnote 25 gir en god oversikt over prinsippene bak det valgte designet.
- Regulatoren Ofgem har et ansvar med likheter til NVEs i Norge, og energileverandører (el og gass) har ansvar for den fysiske installasjonen og driften av målerne.
- I motsetning til i Norge håndteres hele infrastrukturen for håndtering av AMS-data av et enkelt frittstående selskap: *The Data Communications Company* (DCC), som også er regulert av Ofgem.
- DCC må tilfredsstille kravene i *The Smart Energy Code* (SEC), på linje med andre aktører i energisystemet.

Seksjon G av SEC definerer de sikkerhetsmessige kravene DCC må oppfylle, herunder krav til å oppdage og håndtere uautoriserte aktiviteter og hendelser, krav til håndtering av svakheter, data, sårbarheter samt krav til kryptering og sikring[26, 27].

Utrullingen av AMS i Storbritannia har fått betydelig negativ oppmerksomhet, blant annet på grunn av et sikkerhetshull som ble oppdaget hvor alle britiske målere delte samme krypteringsnøkkel[28]. Noe av den negative oppmerksomheten rettes også mot manglende tillit til hvorvidt myndighetene vil utnytte AMS-systemene for overvåkning og etterretning, da også dette inngår i ansvarsområdet til GCHQ[29].

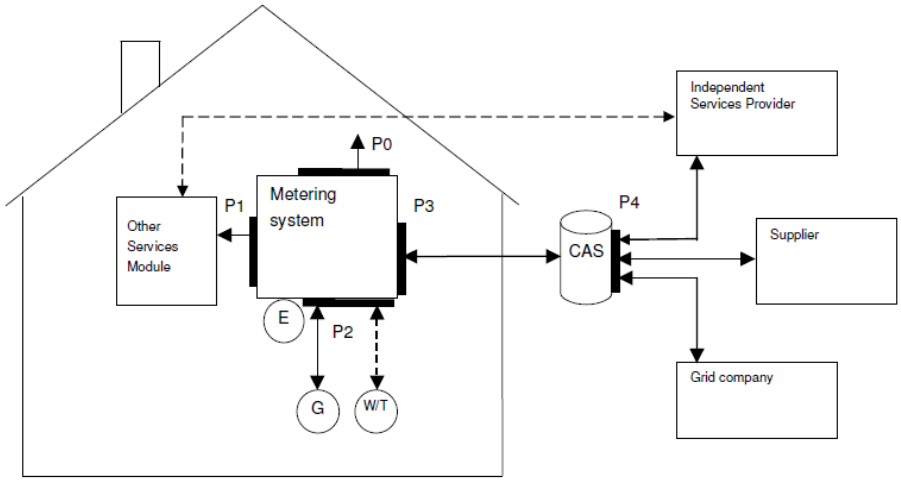
**Nederland**[30]
ENCS gjennomførte i 2015 et større prosjekt sammen med en bransjeorganisasjon for nettselskaper hvor de studerte sikkerhet i smarte målere som allerede var installert. Undersøkelsen dekket både funksjonell sikkerhet, robusthet og innbruddstesting. Resultatene ble brukt til å forbedre sikkerheten i smarte målere.

Bransjeorganisasjonen har publisert flere kravdokumenter for smarte målere:

- Dutch Smart Meter Requirements: P1 Companion Standard (*Krav til grensesnittet mellom AMS-infrastruktur og andre energimålere som f.eks. gass, fjernvarme, vannmåler.*)
- Dutch Smart Meter Requirements: P3 Companion Standard (*Krav til grensesnittet mellom måler og kommunikasjonssystemet.*)
- Dutch Smart Meter Requirements: GPRS Companion Standard

[24] https://www.smartenergygb.org/en/the-bigger-picture/about-the-rollout/roles-and-responsibilities/government
[25] https://www.ncsc.gov.uk/articles/smart-security-behind-gb-smart-metering-system
[26] https://www.smartenergycodecompany.co.uk/sec/sec-and-guidance-documents
[27] SEC 5.0, November 2016: https://www.smartenergycodecompany.co.uk/docs/default-source/sec-documents/sec-5.0/sec-5-0---8th-november-2016.pdf?sfvrsn=6
[28] https://www.google.no/search?q=gchq+smart+meter, http://www.theinquirer.net/inquirer/news/2451793/gchq-intervenes-to-prevent-catastrophically-insecure-uk-smart-meter-plan
[29] https://www.techdirt.com/articles/20160927/09585335643/uk-government-says-smart-meters-can-definitely-be-trusted-because-gchq-designed-their-security.shtml
[30] http://www.netbeheernederland.nl/themas/dossier/documenten/?pageindex=3

Figur 3.1 viser oversikten over de ulike grensesnitt i måleverdikjeden (i Nederland), hvor det er definert kravdokumenter.




**Figur 3.1 Oversikt over grensesnitt på måler (Nederland)[31]**

[31] "P1 Companion Standard. Dutch Smart Meter Requirements", http://read.pudn.com/downloads145/doc/633047/DSMR%20v2.2%20final/Dutch%20Smart%20Meter%20Requirements%20v2.2%20final%20P1.pdf

# 4 Metodebeskrivelse – Innhenting av data for evaluering av veileder nr. 7/2012

For å evaluere dagens versjon av veileder nr. 7/2012, var det viktig å få innspill fra aktører som bruker veilederen. Det ble derfor valgt å kartlegge erfaringer fra bruken av den ved å arrangere to arbeidsmøter, hvor representanter fra ulike nettselskap, tjenesteleverandører og NVE deltok. Arbeidsmøtene ble arrangert hos SINTEF Energi i Trondheim, 31. oktober og 3. november. Tabell 4.1 viser en oversikt over deltakerne på de gjennomførte arbeidsmøtene.

**Tabell 4.1 Oversikt over deltakere på arbeidsmøtene**

| 31. oktober | | 3. november | |
|---|---|---|---|
| **Selskap** | **Ant. deltakere** | **Selskap** | **Ant. deltakere** |
| Agder | 1 | Lyse | 1 |
| Eidsiva | 1 | Nettalliansen | 1 |
| Haugaland | 1 | NTE | 1 |
| TrønderEnergi | 3 | Valider | 1 |
| NVE | 1 | KraftCERT | 1 |
| SINTEF | 4 | SINTEF | 4 |

SINTEF har skrevet rapporten basert på innspill og diskusjoner på de gjennomførte arbeidsmøtene, supplert med skriftlige tilbakemeldinger i etterkant av møtene.

## 4.1 Strukturering av arbeidsmøtene

Hvert arbeidsmøte var delt i to sesjoner. I første sesjon fikk deltakerne anledning til å presentere sitt system for innsamling og håndtering av AMS-data. Andre sesjon fokuserte eksplisitt på opplevde styrker og svakheter ved dagens veileder, samt en diskusjon rundt mulige forbedringer i en evt. oppdatert versjon av veileder.

Gjennom en kreativ sesjon med idémyldring og bruk av gule lapper, ga alle deltakerne sine tilbakemeldinger på dagens versjon av veilederen. Tilbakemeldingene omhandlet både Form/Struktur, Tema (A-I) og Innhold (Detaljer). Deretter ble "tilleggspunktene" (kap. 2) diskutert i plenum, opp mot dagens versjon av veileder.

Notater fra de gjennomførte arbeidsmøtene er presentert i Vedlegg 1.

## 4.2 Erfaringer fra gjennomførte arbeidsmøter

Det er store forskjeller blant selskapene angående hvor mye de har benyttet veilederen for sikkerhet i AMS. Noen har brukt den som en sjekkliste for å se at de har dekket de viktigste tiltakene i sin egen kravspesifikasjon, mens andre ikke har sett på den i det hele tatt.

# 5 Evaluering av veileder til sikkerhet i AMS

I dette kapitlet beskrives tilbakemeldinger på dagens versjon av veileder 7/2012, basert på erfaringer innhentet i arbeidsmøtene. Dette vil være et viktig grunnlag for evaluering av veileder.

Det presenteres både positive og negative (dvs. forbedringsmuligheter) tilbakemeldinger knyttet til hhv. form/struktur, tema (A-I) og innhold (detaljer).

## 5.1 Form/struktur

Hoveddelen av dagens veileder er ***kapittel 5 Sikkerhetsområder og kontrollmål***. Kapitlet er inndelt i ni tema (A-I), og for hvert tema er det beskrevet 1-6 sikkerhetsområder med ett eller flere kontrollmål.

Det er strukturen knyttet til sikkerhetsområdene som er behandlet i denne rapporten, og disse består av følgende punkter:

- *Kontrollmål*: Beskriver ulike sikkerhetsområder som veileder omhandler (Målbart krav).
- *Eksempler for å oppnå kontrollmål*: Beskriver hvordan de ulike kontrollmål kan oppnås (tiltak/prosedyrer/...)
- *Hensikt*: Beskrivelse av hvorfor kontrollmålet er inkludert i veileder.
- *Supplerende veiledning*: Ekstra veiledning der det er funnet hensiktsmessig.

I tillegg er det i vedlegg gitt en tabellarisk fremstilling av kontrollmålene, med mulighet for leser å begrunne hvorfor/hvorfor ikke et kontrollmål er valgt.

I arbeidsmøtene ble deltakerne bedt om å vurdere hvorvidt strukturen er hensiktsmessig eller om det er endringer som bør gjøres for at veilederen skal bli enklere å benytte.

Tilbakemeldingen fra arbeidsmøtene var at strukturen i dagens veileder oppleves som god, oversiktlig og logisk. Kontrollmålene i veileder hjelper til med å konkretisere hva man skal fokusere på angående sikkerhet. Veilederen er enkel å bruke som sjekkliste og et ryddig oppsett gjør det enkelt å vurdere hvorvidt spesifikke kontrollmål er fulgt opp. Det oppleves også som nyttig at det er med mange konkrete eksempler som nettselskap kan relatere seg til.

Det ble kommentert at sikkerhet i AMS er et viktig område og at det derfor er bra med en egen veileder, og at dette ikke er noe som er gjemt i en altomfattende bok. Dagens versjon av veilederen er kompakt og overkommelig, og dette er noe som bør ivaretas videre.

Når det gjelder rekkefølgen på punktene under hvert sikkerhetsområde, er dette ikke konsistent i dagens veileder (f.eks. varierer rekkefølgen på ***Hensikt*** og ***Supplerende veiledning*** for ulike sikkerhetsområder). I tillegg benyttes ulik betegnelse på punktene (f.eks. Eksempler for å oppnå kontrollmål/Eksempler for å oppnå kontrollmålet/Eksempler på aktivitet for å oppnå kontrollmål). Dette er noe som bør ryddes opp i, i en evt. oppdatert veileder.

*Det anbefales å presentere hensikten med sikkerhetsområdet først, før supplerende veiledning nevnes, og at det benyttes lik tekst i overskrift til hvert underpunkt.*

## 5.2 Tema/sikkerhetsområder

Dagens kapittel 5 i veilederen er delt inn i følgende ni tema:

A. Krav til nettselskapet i henhold til forskrift
B. Overordnet sikkerhetsarbeid rundt AMS
C. Kontroll med tilgang til system og utstyr
D. Overvåking og håndtering av hendelser
E. Endrings- og versjonskontroll
F. Fjerntilgang til AMS-løsningen
G. Fysisk beskyttelse av AMS-løsningen
H. Bryte- og strupefunksjonalitet
I. Elektromagnetisk interferens (EMI)

Dagens veileder beskriver ni tema, med underliggende sikkerhetsområder. Disse områdene har blitt vurdert som dekkende i forbindelse med utrulling av AMS. Andre sikkerhetsområder kan være relevante for en veileder som skal gjelde for perioden etter idriftsettelse av AMS, men siden utrulling av AMS ikke er ferdig enda, kom det ikke noen konkrete forslag på dette.

En oppdatering av veileder bør ikke ha tilbakevirkende kraft på allerede kjøpt AMS-teknologi, men heller stille krav til videre levetid og håndtering av sikkerhet.

I arbeidsmøtene ble deltakerne bedt om å vurdere hvorvidt de omtalte temaene, med underliggende sikkerhetsområder, er relevante og om det er flere tema/sikkerhetsområder som burde inkluderes.

Innholdsfortegnelsen er god og nyttig til et overordnet sikkerhetsarbeid, og både temaene og sikkerhets-områdene som inngår, oppleves som relevante. Veilederen har vært nyttig i forbindelse med å inkludere krav til sikkerhet i kravspesifikasjon for AMS. Sjekklisten bakerst i veilederen gir en bra oversikt og oppleves som et nyttig hjelpemiddel. Erfaringer tilsier at dagens versjon av veileder og tema/sikkerhetsområder som er inkludert, er dekkende i forbindelse med både utrulling og drift av AMS.

*Det er en fare for at relevante tema eller konkrete tiltak oversees, dersom de ikke er nevnt blant disse ni sikkerhetsområdene eller dekket av nevnte kontrollmål og/eller eksempler. Dette vil imidlertid alltid være en risiko ved bruk av en slik veileder.*

## 5.3 Innhold (detaljer)

I arbeidsmøtene ble deltakerne bedt om å gi både positive og negative tilbakemeldinger til veilederen og med det også vurdere hvorvidt det er behov for revidering/fjerning av tema, kontrollmål, eksempler og/eller beskrivelse av hensikt.

**Hensikt med veileder**
Veilederen oppfattes generelt sett som god. Hensikten er fornuftig, og det er bra at den er såpass kort og spisset mot et konkret tema. Det er lett å forstå hva den kan brukes til. En konkret tilbakemelding er at forkortelsen "AMS" burde være med i navnet på veilederen, og dermed på forsiden, for å tydeliggjøre så godt som mulig hva den inneholder.

**Veilederens levetid**
En tilbakemelding vedrørende relevansen for veilederen, er at den oppleves som svært relevant ved *innføring* av AMS, men på et arbeidsmøte ble det stilt spørsmål ved relevansen *etter utrulling* – hvorvidt det er behov for andre fokusområder og å framheve andre krav til denne neste fasen. Veileder bør generelt beskrive hvilken fase den gjelder for.

Det savnes en slags "utløpsdato" eller gyldighetsperiode for veilederen. Dette er imidlertid vanskelig å fastsette pga. raske teknologiendringer. Det vil også være en utfordring å utarbeide en veileder som ser tilstrekkelig langt framover. Dagens fokus på funksjonalitet forlenger levetiden til veileder.

**Bruk av veileder**
På arbeidsmøtene ble det gitt tilbakemelding om at veilederen er et viktig dokument for å sikre et kontinuerlig forbedringsarbeid knyttet til sikkerhet i AMS. Tema og sikkerhetsområdene er bra og fokuserer både på hardware og software.

Det ble poengtert viktigheten av at sikkerhet til AMS ikke må bli en sak for "AMS-folket", men at temaet gjelder også for andre deler av nettselskapet.

**Detaljnivå**
Detaljnivået oppfattes stort sett som passelig, basert på tilbakemeldinger fra arbeidsmøtene, og det er bra at det er fokus på funksjonalitet, og ikke spesifikke produkter og tekniske detaljer. Ett forslag til forbedring er å skille på eksempler til henholdsvis store og små nettselskaper – hva er minimumskrav for at de ulike selskapene skal kunne oppfylle forskriften. Veileder kan ha referanse til spesifikke eksempler på hvordan kontrollmål blir løst, uten at dette trenger være førende, men angi hva som er ønsket sikkerhetsnivå for AMS.

Samtidig oppfattes veilederen som uforholdsmessig spisset og detaljert i forhold til andre områder i nettvirksomheten (som ikke er forskriftsregulert, f.eks. nettnytte). Dette kan skape (et inntrykk av) skjevhet i det totale sikkerhetsarbeidet.

**Tydeliggjøring av ansvar**
Det er bra at nettselskapenes ansvar er tydelig beskrevet i dagens veileder (kapittel 1, 2.1, 2.3 og 3.1). Likevel er det ønske om en mer utdypende tekst om nettselskapets ansvar. Dette er særlig viktig når det oppstår allianser som ivaretar en del av oppgavene som i utgangspunktet ligger hos nettselskapet. *Kompleksitet som følge av outsourcing til flere tjenesteleverandører, inkludert skyløsninger og tilleggs-tjenester, burde beskrives nærmere – med særlig vekt på at til tross for allianser og outsourcing, ligger ansvaret fortsatt hos nettselskapet.*

Veilederen er (sammen med aktuelle forskrifter) til god hjelp for å stille krav til både leverandører og egen ledelse.

**Tydeliggjøring av krav**
Veilederen inneholder strenge krav, noe som oppleves som bra, da sikkerhet i AMS er et viktig område. I tillegg er kravene konkrete, hvilket gjør det enklere å kommunisere dem til leverandører og følge opp. Spesielt er det positivt at det kreves at leverandørene varsler ved kjente sårbarheter (D.1).

Det savnes imidlertid en tydeliggjøring av hvorvidt "Eksempler for å oppnå kontrollmål" er *skal*-krav eller *bør*-krav. Da forskriften sier særdeles lite om dette, burde veilederen være klarere i sitt budskap. Det er vanskelig å overse eksempler hvor det står *skal/må*, samtidig som det er uklart hvorvidt det faktisk er et *skal*-

krav. På arbeidsmøtene ble det ytret ønske om en nærmere spesifisering av hvilke forskriftskrav, andre enn §4-2 g) i forskrift om måling og avregning, som dekkes ved bruk av denne veilederen.

I veilederen er det ikke gjort noen vurdering av hvor kritiske de ulike kontrollmålene er. Ved bruk av veileder som grunnlag for en kravspesifikasjon, ville det ha vært til stor hjelp om det var skilt mellom *skal*-krav og *bør*-krav, da det er vanskelig å finne leverandører som kan innfri alle kravene.

**Referanse til lovgivning/forskrifter**
Veilederen burde være tydeligere på krav knyttet til personvern, inkludert referanser til lovgivningen (andre forskrifter en "Forskrift om måling og avregning"). Dersom allerede eksisterende veiledere er gode nok, bør det kryssrefereres. Det savnes også referanser til andre relevante veiledere og standarder, både fra NVE/ bransjen og internasjonale ressurser (f.eks. NorSIS, NorCERT, NSM, ISO, ITIL, etc.). Veilederen kan gjerne inkludere referanser til forskriftsparagrafer i kontrollmålene, der dette er relevant.

Hele bransjen, inkludert leverandørene, forholder seg til NVE som primær informasjonskilde for gjeldende lover og krav. Med den kommende endringen i personvernlovgivningen fra 2018 etterspørres det en klargjøring av hvordan nettselskap skal forholde seg til dette. Lovverk og eventuelle begrensninger for bruk av skyløsninger etterspørres. Det er dessuten behov for å harmonisere regelverk på tvers innen bransjen.

I dagens veileder stilles det visse krav til AMS som virker inkonsekvente med tilsvarende problemstillinger i nettdriften generelt – for eksempel kreves vandelsattest for håndtering av sensitive systemer og informasjon i AMS (C.1), mens tilsvarende ikke er gjeldende for håndtering av personopplysninger i KIS[32]. Det finnes også et krav knyttet til bruk av mobile enheter for en avgrenset aktivitet, men i praksis bør de kunne brukes til flere aktiviteter i sammenheng. Krav og veiledere må henge sammen med virkeligheten hvor nye teknologiske løsninger innføres i høyt tempo.

Veileder bør ha referanser til gjeldende lovverk, noe som innebærer at man inkluderer nye referanser når det kommer nye forskrifter/lover, men også at man fjerner referanser til forskrifter/lover som ikke gjelder lenger, som f.eks. referansen til kompetanseforskriften som finnes i dagens versjon av veileder.

Det anbefales å avstemme veileder mot andre veiledere, rundskriv og forskrifter nettselskapet må forholde seg til (jfr. generell avstemming opp mot gjeldende lovverk).

**Tilgjengelighet AMS-data**
Tilgjengelighet er et viktig aspekt ved informasjonssikkerhet, men dette er ikke godt nok dekket av dagens kontrollmål. Veilederen har i dag et større fokus på å hindre at uvedkommende trenger inn i systemene, men tilgjengelighet av data blir viktigere jo mer AMS-data brukes til planlegging og nettnytte.

**Beskrivelse av kommunikasjonsteknologi**
Teksten om kommunikasjonsteknologier oppleves som utdatert. Den er skrevet før forskriften kom, og bør derfor oppdateres. Spesielt stilles det spørsmål til om andre tjenesteleverandører skal kunne kommunisere over AMS. Dette var en viktig diskusjon da veileder ble utarbeidet (2012), men dette oppleves ikke lenger som et aktuelt tema.

På et arbeidsmøte ble det også kommentert at det var beskrevet feil angående kryptering på 2G. Det står at kryptering 2G er lett å hacke – dette stemmer for GSM, men ikke nødvendigvis for GPRS. Unøyaktige

[32] KIS = KundeInformasjonsSystem

formuleringer bør korrigeres. Generelt bør betegnelser oppdateres, hvor f.eks. MBB (Mobilt bredbånd) er et mer generelt begrep som bør benyttes i stedet for GSM.

**Tilgangskontroll**
I veileder er det spesifisert tilgangskontroll for bryter i AMS-måler hos kunde. I forskrift om måling og avregning er det spesifisert at det skal være mulig å bryte og begrense effektuttaket i det enkelte målepunkt (unntatt trafomålte anlegg), og i dagens veileder er det tatt høyde for at bryte- og strupefunksjonalitet skal kunne brukes for masseutkoblinger. På et arbeidsmøte ble det kommentert at det er bra at veileder anbefaler at kritiske operasjoner ikke skal kunne utføres av én person alene. For å ivareta sikkerhet ytterligere, er det også viktig å presisere at den som gir tilgang til en kritisk operasjon ikke selv kan utføre tilsvarende funksjon.

**Aktører**
Nettselskap er ansvarlig for sikkerhet i AMS, noe som også presiseres i veileder. Veilederen burde imidlertid være mer tydelig på krav som nettselskap bør stille til leverandører for at sikkerhet skal ivaretas. I dagens veileder er det ingen begrensninger med hensyn til tjenesteutsetting til underleverandører. Det er ingenting i veileder som begrenser underleverandørenes mulighet til å delegere videre til egne underleverandører, eller som spesifiserer hvilke krav man skal stille for å begrense/unngå/kontrollere dette.

Veilederen er utarbeidet for nettselskap som drifter hele måleverdikjeden selv. Beskrivelsen av driftsselskap i veilederen tar ikke høyde for alliansene som nå er inngått (bl.a. Soria og Nettalliansen). I veilederen bør det være beskrivelse av hvordan slike allianser vil kunne påvirke sikkerheten, og hvordan nettselskapenes bør forvalte dette.

I dagens veileder er det ikke godt nok beskrevet hvordan leverandørkjeden skal følges opp. For å kunne ivareta sikkerhet i AMS, bør nettselskapene ha en god prosjektorganisasjon/ -gjennomføring for å ivareta dette.

**Sikkerhet/Risiko – avtaleverk og testing**
Underleverandører får normalt tilgang inn i nettselskapenes systemer, eksempelvis for oppdatering av programvare. Dette kan være mulige sikkerhetshull. Flere nettselskap har løst dette ved å etablere VPN-tunnel som manuelt aktiveres på forespørsel fra leverandør, og deaktiveres umiddelbart etter at det aktuelle oppdraget er utført.

Det oppleves som vanskelig å få leverandører til å fokusere tilstrekkelig på sikkerhet (spesielt proaktiv sikkerhetsovervåking). Nettselskap erfarer at feil som fikses i en versjon, har dukket opp igjen i neste. På et av arbeidsmøtene kom det opp at et nettselskap har erfart at 50% av sikkerhetsfeil dreier seg om konfigurasjon.

Det må være mulig å oppgradere sikkerhet i AMS-systemet, og dette bør tas med i veileder (og senere inkluderes i kravspesifikasjon.). Et eksempel på dette er at ved anskaffelse av AMS, er det 50% ledig kapasitet i CPU for å ta høyde for fremtidige oppgraderinger.

Veilederen bør ha større fokus på hendelseshåndtering, bl.a. siden AMS har en bryter. Hvis dette inkluderes, bør man også beskrive hva hendelseshåndtering betyr.

Avhengigheter mellom ulike deler av systemet bør inngå i ROS-analyser og verdivurdering. Dette bør speiles i veileder.

# 6 Tilleggspunkter

Evalueringen av veilederen inkluderer også en vurdering av nye problemstillinger, som har blitt relevante eller endret karakter etter utgivelsen av veilederen. Konkret nevnes innføring av Elhub, tilleggstjenester, driftsselskap, outsourcing av driftstjenester, ulike driftsmodeller (inkl. skytjenester) og DMS, samt eventuelt andre tjenester (f.eks. nettnytte).

Dette avsnittet tar for seg de nevnte problemstillingene, og drøfter hvorvidt og hvordan de kan påvirke dagens veileder. Punkter fra arbeidsmøtene som er relevante for de nye problemstillingene oppsummeres også.

**a. Innføring av Elhub**

Elhub er en datahub som skal omfatte alle måledata for strøm i Norge, og det er Statnett som har fått i oppdrag fra NVE å etablere denne. Elhub vil fungere som et bindeledd mellom nettselskap og kraftleverandører, for å bidra til et velfungerende kraftmarked. Elhub vil være en IKT-infrastruktur for sluttbrukermarkedet for kraft i Norge. Elhub er planlagt satt i drift i oktober 2017.

Nettselskap skal overføre kvalitetssikrede måleverdier til Elhub innen kl. 07:00 hver dag. Disse måleverdiene vil være tilgjengelig for kraftleverandører, leverandørbytter, flytting, opphør og sammenstilling til balanseavregning og avviksunderlag. Kraftleverandører vil få tilgang til kvalitetssikrede måledata fra alle sine kunder via Elhub, og trenger ikke forholde seg til det enkelte nettselskap eller hvor kunden er geografisk lokalisert.

I tillegg vil 3. part kunne hente ut måledata fra Elhub (etter fullmakt fra kunde) og kunder skal kunne logge seg på via sin side hos kraftleverandøren og få tilgang til sine måledata lagret i Elhub.

I veilederen omtales dette som felles IKT-tjenester som skal utredes av Statnett (side 8). Siden arbeidet med Elhub nå er godt i gang, bør kapittel 2.3 i veilederen oppdateres ut fra hva som er faktisk status for Elhub.

I forskrift om endring i forskrift om måling og avregning[33] er det foreslått et nytt punkt §6-21 ang. Sikkerhet i Elhub, og noen av avsnittene i denne paragrafen kan være relevante for AMS (Se tabell 6.1).

[33] "Forskrift om endring i forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester", FOR-2015-06-12-705, https://lovdata.no/dokument/SF/forskrift/2015-06-12-705

**Tabell 6.1 Nytt punkt §6-21 i forskrift om måling og avregning, som kan være relevante for AMS**

| Avsnitt | Forskriftstekst | Kommentar |
|---|---|---|
| 1 | Elhub skal ikke inneha funksjoner som kan påvirke, utføre eller overta overvåking og styring av elektriske anlegg i energiforsyningen, jf. energiloven § 1-3 første ledd og energilov-forskriften § 1-1. | Dette innebærer bl.a. at Elhub ikke skal inngå i eller erstatte funksjon i AMS-infrastruktur, men kun motta måledata fra nettselskap. |
| 2 | Elhub skal ikke inneha funksjoner for å kunne strupe eller bryte effektuttaket i noen målepunkt. | Bryterfunksjonaliteten som inngår i AMS-infrastruktur skal fortsatt håndteres av nettselskap (Omtalt i C.1 i dagens veileder). |
| 4 | Avregningsansvarlig skal sørge for at all informasjonsutveksling i henhold til Ediel er kryptert. | Informasjon som sendes fra nettselskap til Elhub er kryptert. (Krav om kryptert informasjonsutveksling er også spesifisert i A.2/C.6 i dagens veileder). |

Elhub vil bli en sentral database hvor AMS-data (forbruksdata) lagres. En database med forbruksdata for alle kunder i Norge, vil ha stor fokus på sikkerhet. Det forventes at Elhub er implementert etter prinsippene for "innebygd sikkerhet" og "innebygd personvern", gjennom eget mandat gitt til de som er ansvarlig for etablering av Elhub.

I forbindelse med arbeidsmøtene gjennomført høsten 2016, ble systemskissene for AMS-infrastruktur og tilgrensede systemer hos nettselskap presentert og diskutert. På disse skissene gikk normalt informasjons-utvekslingen mot Elhub fra en egen EDI-server (via EDI-format), etter at måleverdier var eksportert fra sentralsystemet til en egen måleverdiserver.

Informasjonsutvekslingen mot Elhub er ikke knyttet direkte til AMS-infrastruktur (dvs. måleverdikjeden fra målepunktet hos kunden til sentralsystemet hos nettselskap), og dette er også skissert i figur 2.1. Det vurderes ikke som nødvendig å oppdatere dagens veileder med nye temaer/sikkerhetsområder knyttet til Elhub, men det anbefales å oppdatere beskrivelsen av Elhub i veileder til sikkerhet i AMS (kap. 2.3).

**b. Tjenesteleverandører/leverandører av «tilleggstjenester»**

Veilederen nevner innledningsvis at "nettselskapene [skal] legge til rette for at ulike tilleggstjenester kan tilknyttes AMS i fremtiden. For å sikre dette foreslår NVE at nettselskapet skal gi andre tjenesteleverandører mulighet til å kommunisere over AMS", men drøfter ikke sikkerhetsaspekter ved denne tilleggstjenesten ytterligere i veilederen.

Begrepet "tilleggstjenester" kan tolkes til å inkludere både tilknytning av andre målere, jfr. AMS-forskriftens funksjonskrav §4.2 c), og tilknytning av display eller andre former for uthenting av data gjennom "HAN-porten", jfr. AMS-forskriftens funksjonskrav §4-2 b).

Grensesnittet for uthenting av data gjennom HAN-porten var ikke ferdig spesifisert da dagens veileder ble skrevet. Siden da har både den fysiske utformingen, kommunikasjonsprotokollen og dataene som skal overføres, blitt vedtatt[34,35].

[34] "AMS + HAN: Om å gjøre sanntid måledata tilgjengelig for forbruker", NEK (Aanensen, Fines og Ek), 2015.
[35] "Informasjon til kundene via HAN-grensesnittet i AMS-måleren. OBIS-koder", brev fra NVE, 2016.

Tilknytningen av andre målere skiller seg fra "HAN-porten" ved at hele AMS-infrastrukturen er involvert, siden denne brukes til å samle *inn* måleverdier, mens det for HAN-porten utelukkende dreier seg om å sende data *ut* fra AMS-måleren til sluttbruker (push).

I veilederen bør det beskrives hva som kan være tilleggstjenester, og hvilke forventninger som stilles til sikkerhet for hver av disse. Spesielt bør sikkerhetskravene ved tilknytning av andre typer målere (vann, fjernvarme, etc.) beskrives, inkludert en beskrivelse av hvordan man skal håndtere det at man utfører måling for andre selskaper. Alternativt bør det gjøres eksplisitt at veilederen ikke dekker dette aspektet ved AMS, til tross for at det er forskriftsfestet.

I dagens veiler er det i kontrollområde C.2 allerede spesifisert at det skal *implementeres mekanismer for å autentisere og autorisere enheter i AMS før det opprettes forbindelse mellom enheten og resten av AMS*. Det er også presisert at ekstra sterk autentisering bør foretas før det opprettes forbindelse mellom enheten og resten av AMS. Det virker naturlig å vurdere om tilsvarende krav også bør stilles til andre målere, samt til grensesnittet mot disse (A2 på systemskissen i dagens veileder).

I den grad kontrollområdet i C.2 er ment å dekke tilkoblinger over HAN-porten, er dette delvis i konflikt med tilrådingen fra NEK, hvor det påpekes at valget av kryptering avhenger av kundens ønske og målerens plassering (s. 26)[34].

Med bakgrunn i diskusjonen over, kan det være hensiktsmessig å være tydeligere på hvilke grensesnitt som adresseres i eksempelvis veilederens kapittel C.2. Det er også verdt å påpeke at begrepet "HAN" både kan forstås som "HAN-porten" på AMS-måleren med tilstøtende teknologi, og et lokalt IP-nettverk innenfor husets fire vegger (Home Area Network).

**c. Etablering av driftsselskap (f.eks. Valider AS og Smarthub AS)**

Gjennom forskrift om måling og avregning[36] er alle nettselskap pålagt å installere AMS i alle målepunkt i sitt nett, med unntak av målepunkt hvor forbruket er lavt og forutsigbart og installasjon er til vesentlig og dokumenterbar ulempe for sluttbruker. Til tross for et felles krav, er det ulike måter dette har blitt gjennomført på. I forbindelse med etablering og drift av AMS-infrastruktur er det bl.a. etablert egne driftsselskap for å håndtere dette, f.eks. Valider AS og Smarthub AS.

Smarthub[37] AS ble etablert i 2012 av 10 nettselskaper i Møre og Romsdal for å ivareta AMS for sine eierselskaper. Smarthub skal utføre datainnsamling, kvalitetskontroll, distribusjon og administrasjon av målerservice,ihht. forskrift om AMS.

Valider AS er et driftsselskap med 27 nettselskap på eiersiden, som representerer 700 000 AMS-målere[38]. De største selskapene er BKK Nett, TrønderEnergi, NTE Nett, Haugaland Kraft og Nordlandsnett.

Et slikt driftsselskap drifter AMS-infrastruktur på vegne av sine eierselskaper, men fremdeles er det nettselskapet som er ansvarlig for AMS-infrastruktur i sitt konsesjonsområde. Hvert nettselskap på eiersiden bør ha egne avtaler med driftsselskap, knyttet til hvordan tjenesteutsetting skal håndteres (Dekket av sikkerhetsområde A.3 ang. utsetting til tredjepart i dagens veileder, men som i kap. 7.2 er foreslått som eget sikkerhetsområde for tjenesteutsetting).

[36] https://lovdata.no/dokument/SF/forskrift/2011-06-24-726?q=forskrift om måling avregning fakturering
[37] http://smarthub.no/smarthub-as
[38] http://www.valider.no

**d. Outsourcing av driftstjenester fra nettselskapene**

Med *outsourcing* menes bruk av eksterne aktører til leveranse av en tjeneste, et system, kompetanse eller lignende. Alle former for outsourcing/tjenesteutsetting må reguleres gjennom gode avtaler som inkluderer forhold som er relevante for informasjonssikkerhet. Vi foreslår et eget, eller flere, kontrollmål knyttet til Tjenesteutsetting innunder tema B, som beskrevet i kap. 7.2.

Problemstillinger knyttet til aktører og ansvar er beskrevet tidligere, i kap. 5.3.

**e. Ulike modeller for drift, herunder bruk av skytjenester**

Dagens veileder dekker ikke nyere trender som skybaserte løsninger. Det bør refereres til annet lovverk som spesifiserer lokalisering av servere som brukes i skyløsninger.

Lovkrav knyttet til personopplysninger er likt i Norge som i EU. Dette inkluderer krav til databehandler-avtaler. Lokale lovverk gjelder i det landet det data lagres, og kan påvirke krav som bør stilles for skytjenester.

Bruk av skytjenester er en form for outsourcing, og kontrollmål for skytjenester hører dermed til under det nye punktet Tjenesteutsetting innunder tema B, som vi har foreslått til den nye versjonen av veilederen (se kap 7.2).

Tilsvarende som bruk av skytjenester, vil også outsourcing av tjenester til utlandet være underlagt lovverket i det landet hvor operatør oppholder seg.

**f. Distribution management systems (DMS)**

Parallelt med utrullingen av AMS, er det flere nettselskap som anskaffer driftskontrollsystemer for distribusjonsnettet (DMS), som muliggjør bruk av AMS-data til mer effektiv nettdrift. Gjennom å kombinere informasjon fra ulike fagsystemer (nettinformasjon, kart og kundeinformasjon), kan nettselskapene få oppdatert informasjon om status i nettet, hvilke kunder som mangler strøm, hvordan effektflyten er i distribusjonsnettet, hvordan spenningsforhold i distribusjonsnettet er, o.l.

Nytteverdien av DMS forventes å kunne øke betydelig ved å inkludere såkalte *nettnyttedata* som samles inn via AMS, men som ikke dekkes av AMS-forskriften. Det anbefales å være eksplisitt på at disse aspektene ikke inngår i forskriften og følgelig ikke dekkes av veilederen, men at de kan berøres av annen lovgivning knyttet til personvern, datasikkerhet eller beredskap. Dette beskrives ytterligere i neste avsnitt.

**g. Andre/nye/uspesifiserte tjenester**

Etter at dagens veileder ble utgitt, har det blitt en økende fokus på bruk av AMS for å effektivisere nettdriften. AMS er også en viktig brikke i fremtidens intelligente distribusjonsnett, og da er det mer enn kWh-verdier som registreres. Disse tilleggsdata betegnes ofte som *nettnyttedata*. Eksempler på nettnyttedata og bruksområde er vist i tabell 6.2.

**Tabell 6.2 Eksempler på nettnyttedata og bruksområde for disse**

| Nettnyttedata | Bruksområde |
|---|---|
| Måling av spenningens 1 minutts RMS-verdi | Spenningsmåling gir mulighet for:<br>• Oversikt over tilstanden i nettet<br>• Oversikt over utnyttelsen av nettet<br>• Mulighet til raskere kundebehandling<br>• Mulighet til å kvalitetssikre nettdokumentasjonen |
| Registrering av jordfeilstrøm | Raskere deteksjon og retting av jordfeil |
| Måling av aktiv og reaktiv effekt | Grunnlag for å utføre lastflyt med målte timesverdier |
| Varsling ved avbrudd | Raskere deteksjon og retting av avbrudd |

Veileder var opprinnelig tenkt for kWh-data, men i dag er det også nettnytte-data som samles inn via AMS. Nettnyttedata nevnes ikke i dagens versjon av veileder, men krav til sikkerhet i AMS-infrastruktur gjelder for alle data registrert av AMS.

Dagens forskrift spesifiserer også at AMS skal "kunne sende og motta informasjon om kraftpriser og tariffer". Det er uklart hvordan og over hvilket grensesnitt (A2, A3, A4) dette skal skje. Veilederen bør om mulig og nødvendig omtale behovet for sikring av denne kommunikasjonen.

# 7 Anbefaling om endringer

I dette kapitlet beskrives SINTEF sine anbefalinger om endringer i og tillegg til dagens versjon av NVE-veilederen basert på litteraturstudie og diskusjoner på arbeidsmøtene. Vurderingene er gjort med utgangspunkt i erfaringer fra bruk og innhold/struktur.

## 7.1 Generelt

Veileder til sikkerhet i AMS må avstemmes mot andre veiledere, rundskriv og forskrifter som nettselskapene må forholde seg til (jfr. generell avstemming opp mot gjeldende lovverk).

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. Endringstakten er høy, og det er krevende for NVE å alltid ligge i forkant. Det er svært viktig at ikke forskriftskrav hindrer nettnytte.

Det er et stort behov for å få leverandører til å bli mye bedre på å levere sikre løsninger. Innebygd sikkerhet og sikkerhetstesting er områder som er underprioritert så langt. Det er ikke hensiktsmessig at hvert enkelt nettselskap skal gjøre den samme jobben med sikkerhetstesting på vegne av leverandørene.

## 7.2 Form/struktur

Tilbakemeldingen fra arbeidsmøtene var at dagens veileder har en god, oversiktlig og logisk struktur, og det anbefales at denne videreføres. For å få en mer gjennomført beskrivelse for de ulike sikkerhetsområdene, anbefales det *å presentere hensikten med sikkerhetsområdet først, før supplerende veiledning nevnes, og at det benyttes lik tekst i overskrift til hvert underpunkt.*

En oversikt over hvilke sikkerhetsområder dette medfører endringer i, er presentert i tabell 7.1.

**Tabell 7.1 Forslag til endringer av form/struktur i dagens veileder**

| Sikkerhetsområde | Dagens veileder | Endres til |
|---|---|---|
| A.2 | *Supplerende veiledning* kommer før *Hensikt* | Rekkefølge endres, slik at *Hensikt* presenteres før *Supplerende veiledning* |
| A.3, B.1, B.2, B.3, B.4, C.1, C.4 | Eksempler for å oppnå kontrollmål**et** | Eksempler for å oppnå kontrollmål |
| C.6, D.2, G.1, I.1 | Eksempler **på aktivitet** for å oppnå kontrollmål | |
| D.2 | Hensikt**en med kontrollmålet** | Hensikt |

Veilederen er ment som et hjelpemiddel for at nettselskap skal kunne oppfylle krav §4-2 punkt g) i forskrift om måling og avregning. Det er derfor uhensiktsmessig at det er et eget tema A hvor det spesifiseres at dette gjelder krav i henhold til forskrift. Kontrollområdene i kapittel A er temamessig relevant for andre temaer, og det anbefales at kontrollområdene flyttes.

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.
- *A.2. 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.

I tillegg anbefales det at dagens kap. A.3 endrer navn til "Tjenesteutsetting". Dette kan da inkludere allianser, skytjenester o.l..

## 7.3 Tema/sikkerhetsområder

Veilederen oppfattes som god, og det er fornuftig med en egen veileder vedrørende sikkerhet i AMS.

For ytterligere tydeliggjøring av at veilederen gjelder AMS, bør forkortelsen "AMS" være med i navnet på veilederen, og dermed på forsiden (Tabell 7.2).

**Tabell 7.2 Forslag til endringer for å spesifisere hensikt med veileder**

| Endringspunkt | Dagens veileder | Endres til |
|---|---|---|
| Tittel på veileder | Veileder til sikkerhet i avanserte måle- og styringssystem | Veileder til sikkerhet i avanserte måle- og styringssystem **(AMS)** |

## 7.4 Veilederens levetid

Levetid på veilederen ble diskutert på arbeidsmøtene (se kap. 5.3), bl.a. om den var mest aktuell i forbindelse med utrulling, og kanskje ikke like relevant etter utrulling.

Dagens veileder er funksjonsorientert og omfatter tema/kontrollområder som er relevante for drift av AMS-infrastruktur. 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.

## 7.5 Bruk av veileder

Veilederen er et viktig dokument for å sikre et kontinuerlig forbedringsarbeid knyttet til sikkerhet i AMS. Sikkerhetsområdene er gode og fokuserer både på hardware, software og prosesser. Til tross for at dette er en veileder knyttet til AMS, er det viktig at dette ikke kun blir en sak for "AMS-folket".

Dette er en anbefaling som heller medfører en endring i oppfatning av veileder og ikke direkte endring i tekst.

## 7.6 Detaljnivå

På et av arbeidsmøtene ble det diskutert om man bør ha egne krav for henholdsvis små og store nettselskap. SINTEF mener at dette ikke er å anbefale, fordi sikkerhet i AMS må være likt for alle kunder i Norge uavhengig av hvor de bor. Temaene/kontrollmålene bør derfor gjelde for alle nettselskap. Den utstrakte bruke av allianser i AMS er også med på å viske ut skillet mellom små og store nettselskap i denne sammenhengen.

Til tross for like kontrollmål i veileder, vil det likevel være lokale forhold som påvirker valg av løsninger, siden hvert nettselskap skal gjennomføre egne ROS-analyser for AMS. Forskjellene mellom små og store nettselskap, og omfang av sikkerhetstiltak, vil da bli ivaretatt.

## 7.7 Tydeliggjøring av ansvar

Nettselskapenes ansvar er tydelig beskrevet i dagens veileder (kapittel 1, 2.1, 2.3 og 3.1). Til tross for dette er det et ønske om en mer utdypende beskrivelse, og da spesielt når det oppstår allianser som ivaretar en del av oppgavene som i utgangspunktet ligger hos nettselskapet.

**Tabell 7.3 Forslag til endringer i kontrollmål for å tydeliggjøre ansvar**

| Sikkerhetsområde | Dagens veileder | Forslag til tilleggstekst |
|---|---|---|
| A.3 | Sikkerheten i AMS skal ikke påvirkes ved at utrulling eller drift av AMS settes ut til ekstern tjenesteleverandør. | Ansvaret for sikkerhet i AMS ligger fortsatt hos nettselskapet, til tross for at deloppgaver er satt ut til ekstern tjenesteleverandør, evt. allianser. |

## 7.8 Referanse til lovgivning/forskrifter

I veileder bør det være referanser til relevante gjeldende lovverk (andre enn forskrift 301 §4-2 g)), og det anbefales å avstemme veileder mot andre veiledere, rundskriv og forskrifter nettselskapet må forholde seg til. Noen forslag til dette er presentert i tabell 7.4.

I ett av eksemplene under sikkerhetsområdet C.1 i veilederen er det krav om "bakgrunnssjekk av personell som skal ha tilgang til å håndtere sensitive systemer og informasjon". På arbeidsmøtene kom det frem at dette oppleves som inkonsistent med eksempelvis håndtering av personopplysninger i KIS, hvor bakgrunnssjekk ikke er påkrevd.[39]

I risikoevalueringen som lå til grunn for veilederen ble det imidlertid påpekt at skadepotensialet ved utro tjenere er betydelig[40]. Dette fremheves også i NOU 2016:19 Samhandling for sikkerhet[41]. Utredningen påpeker videre at det norske samfunnet og arbeidslivet er i endring, blant annet gjennom økt mangfold og

[39] Jfr. oppsummering fra arbeidsmøtene på s. 19, samt notater fra disse på s. 37.
[40] Line M B, Johansen G, Sæle, H. "Risikovurdering av AMS: Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS." SINTEF F21615, 2012.
[41] NOU 2016:19, Samhandling for sikkerhet: Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid

globalisering. Dette kan føre til økt sårbarhet, og at behovet for bakgrunnssjekk kan være økende. Endelig påpekes et behov for harmonisert sikkerhetsnivå på tvers av samfunnssektorer.

SINTEF ønsker på bakgrunn av dette ikke å anbefale 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. Eksempelvis kan det være aktuelt å begrense kravet til å bare gjelde visse typer og nivåer av tilgang. Det er opp til NVE å bestemme nøyaktig hvor denne grensen skal gå. Et alternativ kan være å knytte kravet om bakgrunnssjekk opp mot risikoevaluering hos de enkelte aktører, for å opprettholde fleksibilitet i forhold til hvordan de forskjellige AMS-systemene er implementert når det gjelder administrasjon av tilganger og rettigheter.

**Tabell 7.4 Forslag til referanser til annen lovgivning/forskrifter**

| Anbefalt referanse | Sikkerhetsområde | Foreslått endring/Kommentar |
|---|---|---|
| Krav knyttet til personvern, inkludert referanser til lovgivningen | C.1? | Generell henvisning til Datatilsynet. |
| Referanser til andre relevante veiledere og standarder, både fra NVE/bransjen og internasjonale ressurser (f.eks NorSIS, NorCERT, NSM, ISO, ITIL, etc.) | Kan henvises fra innledningen, "for den som vil lese mer" | ISO/IEC 27001 Ledelsessystem for informasjonssikkerhet.<br>ISO/IEC 27035 Information security incident management[42].<br>Datatilsynet om personvernforordningen fra 2018. NorSIS: https://norsis.no/publikasjoner/<br>NSM: www.nsm.stat.no – de har en rekke publikasjoner. Det blir fort utdatert om veilederen skal lenke til konkrete dokumenter. |
| Endringen i personvern-lovgivningen fra 2018 | | Det vil nok komme diverse veiledninger om denne framover. En generell referanse til Datatilsynet er det riktigste og mest varige. |
| Lovverk og eventuelle begrensninger for bruk av skyløsninger etterspørres. | | Tilleggstjenester. Lovverk knyttet til overføring av person-opplysninger til andre land er veldig klart beskrevet av Datatilsynet. Hvorvidt det er/skal være begrensninger på overføringer av andre typer data til utlandet, er nok ikke like klart definert og må vurderes ut ifra hva slags type data det er snakk om, hvilke konsekvenser evt. uønskede hendelser kan ha, og hvem som kan få tak i data. |
| Vandelsattest for håndtering av personopplysninger i AMS. | C.1 | Tilsvarende krav er ikke tidligere stilt til personell som håndterer data i KIS, DMS og andre fagsystemer som kommer til å bruke AMS-data (forbruksdata og nettnyttedata). Krav om vandelsattest kan være hensiktsmessig, men det bør i så fall være konsekvent for personell som skal ha tilgang til sensitive systemer og informasjon av en viss kritikalitet, uavhengig hvilket system de får slik tilgang gjennom. |

[42] ISO/IEC 27035 gir en hensiktsmessig beskrivelse av hvordan man kan organisere arbeidet med håndtering av cyber-hendelser i AMS og tilgrensende systemer.

| Anbefalt referanse | Sikkerhetsområde | Foreslått endring/Kommentar |
|---|---|---|
| Eksternt utstyr/ mobile enheter skal kun brukes for oppgaver mot AMS. | C.3 | Dette begrenser mulig nytte ved bruk av mobile enheter. I praksis bør de kunne brukes til flere aktiviteter i sammenheng. |
| Fjerne referanser som ikke gjelder lenger, f.eks. kompetanse-forskriften. | A.3 | Teksten under ***Hensikt*** endres til:<br>Denne målkontrollen er basert på kravene i **energilovforskriften §3-6 Tilgang til personell** som går på både evne til å ivareta nettforvaltningsoppgaver og oppgaver innenfor måling og avregning. En viktig del av nettforvaltning er sikkerhet og beredskap. |
| Avviks- og hendelseshåndtering | D.3 | Referanse til ISO/IEC 27035[42] Information security incident management |
| Katastrofehåndtering og –øvelser | D.4 | Referanse til ISO/IEC 27035[42] Information security incident management |

## 7.9 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. Hensikt med et slikt sikkerhets-område vil være å sikre at informasjon er tilgjengelig til bruk til daglige driftsformål.

## 7.10 Beskrivelse av kommunikasjonsteknologi

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. Da veilederen ble utarbeidet var det en viktig diskusjon om tredjepart skulle få tilgang til å kommunisere over AMS-infrastruktur, men dette oppleves ikke lenger å være et aktuelt tema. Dette er ikke samme funksjonalitet som at nettselskap henter inn måleverdier fra andre målere (vann, fjernvarme, gass, ...) via AMS-infrastruktur på vegne av tredjepart. Det foreslås derfor at dette tas bort fra kap. 1 *Innledning*.

**Tabell 7.5 Forslag til endringer i beskrivelse av kommunikasjonsteknologi**

| Sikkerhetsområde | Dagens Veileder | Foreslått endring/Kommentar |
|---|---|---|
| A.2 | *Eksempler for å oppnå kontrollmål:*<br>Det er ikke tilstrekkelig å benytte den innebygde krypteringsløsningen i GSM.<br>*Supplerende veiledning:*<br>Krypteringsløsningen som benyttes i GSM (2G) er såpass lett å knekke at det anses ikke som en sikker løsning alene for å sikre kommunikasjonen i AMS. | Kommentarer knyttet til en spesiell kommunikasjonsteknologi bør vurderes fjernet fra *Supplerende veiledning* under kontrollmålet. |
| C.2 | Begrepsbruk i veileder bør oppdateres. | Mobilt bredbånd (MBB) bør brukes i stedet for spesifikk betegnelse av teknologi (GSM, GPRS, UMTS, EDGE, HSDPA, LTE, ..., 5G) |
| C.6<br>(Anbefales inkludert i ny A.2) | Det er overlapp mellom A.2 og C.6. På grunn av overlappende temaområde anbefales det at disse sikkerhetsområdene slås sammen. Dette gir en utvidet versjon av tematikken ang. krypteringsnøkler, noe som er relevant med referanse til alvorligheten av en eventuell kompromittering, og med den nylig avdekkede situasjonen i Storbritannia som bakteppe (Se kap. 3.2). | Mulige eksempler på tiltak for å oppnå kontrollmål under ny A.2 (kombinert med C.6) kan inkludere bruk av separate nøkler for hver AMS-måler, egne nøkler og prosedyrer for bryterstyring, prosedyrer for håndtering av nøkler hos tredjepart (inkludert montører), rutiner for sikkerhetstrening og risikoevaluering, o.s.v.<br><br>Nye eksempler som foreslås tatt med:<br>• Krypteringsløsninger i AMS skal være i henhold til god praksis mht. krypteringsalgoritmer og nøkkellengder.<br>• Private nøkler som tilhører sertifikater skal lagres kryptert<br>• Det skal være separate nøkler for hver AMS-måler<br>• Det skal være egne nøkler (og prosedyrer) for bryterstyring – dvs. nøkkelen som beskytter sending av målerverdier er ikke den som gjøre det mulig å koble ut/strupe måleren<br>• Nettselskapet skal konkretisere/ inngå egen avtale med tredjepart vedrørende håndtering av nøkler der dette er nødvendig |

## 7.11 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 (Se tabell 7.6).

**Tabell 7.6 Forslag til endringer i beskrivelse av tilgangskontroll**

| Sikkerhetsområde | Dagens veileder | Forslag til endret tekst |
|---|---|---|
| C.1 | *Eksempler for å oppnå kontrollmål (femte kulepunkt):*<br>Ha prosedyrer og tekniske løsninger som skal sikre at kritiske operasjoner ikke kan kunne utføres av én person alene. | Ekstra tekst: Den som gir tilgang skal ikke kunne utføre tilsvarende funksjon som vedkommende gir tilgang til. |

## 7.12 Aktører

I dagens veileder er det ingen begrensninger med hensyn til tjenesteutsetting til underleverandører.

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.

I dagens veileder er det heller ikke godt nok beskrevet hvordan leverandørkjeden skal følges opp. Behovet for en god prosjektorganisasjon og -gjennomføring for å ivareta sikkerhet i AMS bør tydeliggjøres.

**Tabell 7.7 Forslag til endringer i beskrivelse av aktører og avtaler**

| Sikkerhetsområde | Dagens veileder | Forslag til endret tekst |
|---|---|---|
| Nytt B.5 (Tidligere A.3, se kap. 7.2) | Dette punktet finnes ikke i dagens veileder, foreslås som et tillegg. | B.5 Tjenesteutsetting. Sikkerhetsområdet må beskrive at ansvaret fortsatt hører til hos nettselskapet, både ved deltakelse i allianser og ved bruk av eksterne leverandører. |

## 7.13 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).

**Tabell 7.8 Forslag til endringer i beskrivelse av risiko**

| Sikkerhetsområde | Dagens veileder | Forslag til endret tekst |
|---|---|---|
| A.1 | *Kontrollmål c)*<br>Konfigurasjon og oppsett for kritiske kommandoer, målerdata og annen informasjon i AMS løsningen skal være basert på risiko. | *Kontrollmål c)*<br>Konfigurasjon og oppsett for (...) skal være basert på basert på **dokumenterte risiko- og sårbarhetsvurderinger**. |
| | | Målerdata endres til **måledata** |
| A.1 | *Eksempler for å oppnå kontrollmål, første kulepunkt:*<br>Utstrakt testing av funksjonalitet i et begrenset testmiljø. | ...Utstrakt testing av **sikkerhets**funksjonalitet[43] i et begrenset testmiljø. |
| B.2 | *Eksempler for å oppnå kontrollmål, andre kulepunkt:*<br>... Nivå på sikkerhetstiltak skal være basert på risiko. | ... Nivå på sikkerhetstiltak skal være basert på **dokumenterte risiko- og sårbarhetsvurderinger**. |
| B.2 | Sikkerhetsområdet omhandler Risiko- og sårbarhetsanalyser, men betegnelsen "ROS" er ikke forklart. | Endret overskrift på B.2 til "Risiko- og sårbarhetsanalyse (ROS)" |
| B.2 | Forslag til nytt kulepunkt | Krav til vurdering av avhengigheter knyttet til både fysiske og logiske verdier, samt personell. Dette må gjøres i en risikovurdering. |
| B.2 | Supplerende veiledning | Oversikten oppdateres bl.a. med referanse til SINTEF--rapport som er ment å skulle støtte gjennomføring av risikovurderinger for informasjonssikkerhet og personvern i kraftbransjen. Dette er et tillegg til bransjens veileder for ROS-analyser. "Støtte til gjennomføring av ...", http://infosec.sintef.no/wp-content/uploads/2014/09/St%C3%B8tte-til-gjennomf%C3%B8ring-av-risikovurdering-v1.1.pdf |
| D.2 | Logging og overvåking bør skilles i to sikkerhetsområder. Dagens kontrollområde D.2 inneholder kun en beskrivelse av logging. Man bør også få inn krav om proaktiv overvåkning og analyse av data, for å være i forkant av evt. hendelser/feil som måtte inntreffe. | *Forslag til oppdatert kontrollmål:*<br>Nettselskapet skal ha satt opp løsning og rutiner for sikkerhetslogging **og overvåkning** i den totale AMS-løsningen". |
| | | *Forslag til nytt eksempel som legges til som tredje kulepunkt:*<br>Proaktiv overvåkning og analyse vil gi muligheten til å være i forkant av evt. sikkerhetshendelser. |

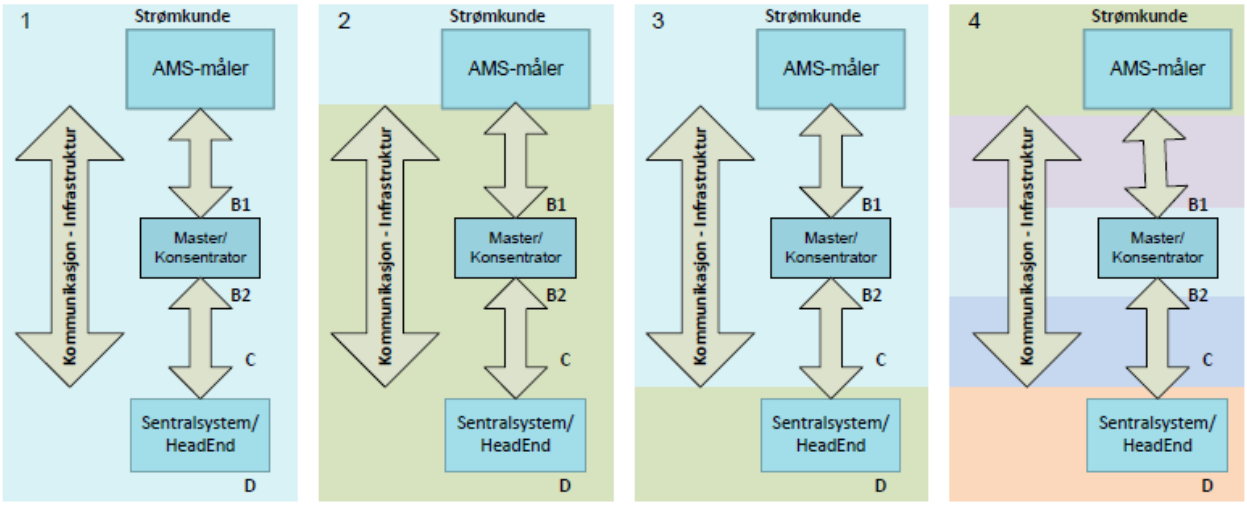
[43] Spesifiseringen er gjort for å holde fokus på sikkerhet og unngå misforståelse med funksjonalitet i AMS (måling, styring, ...)

## 7.14 Tilleggspunkter

Flere av de nye problemstillingene som er nevnt i prosjektbeskrivelsen gjelder tjenesteutsetting på ett eller annet vis: b) tilleggstjenester, c) driftsselskap/allianser, d) outsourcing av drift, e) ulike driftsmodeller, f.eks skyløsninger, g) andre tjenester. Den nye versjonen 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. Dette er ikke utfordringer som særskilt gjelder kraftbransjen, det er generelle problemstillinger som gjelder i alle situasjoner hvor tjenester leveres av eksterne parter.

Figur 7.1 viser eksempler på ulik grad av outsourcing for måleverdikjeden/AMS-infrastruktur. De skraverte områdene viser deler som er outsourcet. Økende grad av outsourcing stiller økende krav til avtaler, samtidig som det er nettselskapet som har ansvaret for sikkerheten i hele måleverdikjeden.




**Figur 7.1 Eksempler på ulik grad av outsourcing**

**1: Nettselskapet drifter hele måleverdikjeden selv,**
**2: Driftsselskap –Ansvarlig for sentralsystem og kommunikasjonsinfrastruktur,**
**3: Skyløsning for sentralsystem,**
**4: Outsourcing av alle enheter til ulike aktører**

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.

# Vedlegg 1 Notater fra gjennomførte arbeidsmøter

## V1.1 Arbeidsmøte 1 (2016-10-31)

**Positive tilbakemeldinger på dagens veileder**

- Hensikt
  - Hensikt ok
  - Fint at det er en egen veileder og ikke noe som er gjemt i en altomfattende "bok"

- Struktur
  - Ryddig oppsett. Enkelt å kontrollere om punkter er fulgt opp
  - Oversiktlig oppbygging
  - Bra struktur
  - Struktur ok

- Innhold
  - Bra at sårbarheter i programvare er tatt fram og at leverandører skal varsle ved kjente sårbarheter
  - Bra utgangspunkt for starten på en ROS-analyse
  - Fokus på endrings- og versjonskontroll. Grunnlag for å stille krav til leverandør.
  - Nettselskapet har ansatt egen ressurs => Ansvar for informasjonssikkerhet
  - Stiller strenge krav/mål – dette er jo et viktig område
  - Fokus på ansvar. Ansvar er tydeliggjort (Eksempel: Selskapene har ansvar for sikkerheten (3.1), ansvar for lokale løsninger selg om Elhub kommer (2.3))
  - Mange bra punkter
  - Bra med eksempler på hvordan kontrollmål kan oppnås
  - Bra med krav til dokumentasjon
  - Fokus på mange sikkerhetsområder
  - Gir konkrete krav til leverandører

Notater, ang. **positive tilbakemeldinger**:

- Viktig område, bra med strenge krav
- Fokus på kommunikasjon og sårbarhet i program

**Tilbakemeldinger på mulige forbedringer av dagens veileder**

- Innhold
  - Bør være "(AMS)" i dokumenttittel (?)
  - Trenger ytterligere forenkling
  - Noen eksempler er i overkant spesifikke
  - Vanskelig å overse eksempler der det står "skal/må"
  - Eksempler med "skal" – krav eller veiledning/eksempler
  - Bedre på ansvar. Samarbeid
  - Eierskap og ansvar skal ikke smuldre. (Spesielt små nettselskap)
  - Bedre på personvern/lovgiving
  - Kontrollspm.
  - Uklart hva som er krav og hva som er veiledning. (Veileder beredskap -> krav skal/bør).
    - Tydeliggjøre hva som er nødvendig minimumstandard

- Tydeliggjøre hva som er krav og hvem som er ansvarlig.
  - Tosider "nettselskapets ansvar"?
- Forskriftskrav + siste setning kap. 1 => Ikke tydelig at dette er krav til sikkerhet
- Veileder skal angi ønsker sikkerhetsnivå.
- Strengere disiplin på ordbruken i veileder.
- Tydeligere begreper
- Et nettselskap har tolket veilederen og dens detaljnivå/sikkerhetsnivå som et signal om hva som vil komme av krav og forventninger til sikkerheten i resten av nettdriften.
- NVE: ser på veilederen som en indikasjon på det NVE mener må til for å nå et sikkerhetsnivå som møter forskriften.

- Henvisninger/referanser
  - Kunne hatt mer henvisninger/koblinger til eksisterende lovverk (ref. personvern)
  - Personopplysningsloven –mer tydelig, mer konkrete krav enn andre forskrifter fra NVE
  - Leverandørene forholder seg til NVE, ikke annen lovgivning. Oppdatere informasjon hos NVE, evt. linke til informasjon fra andre lovgivende organer
  - Personopplysning – knyttet til lovverket. Ta med i veileder
  - Ny personvernlovgivning
    - Mer komplisert
    - Mer uoversiktlig
    - Hvordan skal nettselskap forholde seg til dette?
  - Tydeligere kobling mot annen lovgivning (eks. personopplysningsloven).
  - Behov for harmonisering av regelverk på tvers: DMS, flåtestyring, etc.

- Eksempler
  - Tilgjengelighet (data). Fokus på å hindre at uvedkommende trenger inn i systemet. Hva med tilgjengelighet av data?

- Kommunikasjonsteknologi
  - Skal andre tjenesteleverandører kommunisere over AMS? Teksten henviser til før forskrift kom. Andre tjenesteleverandører kommuniserer over AMS-kanal. Mer aktuelt før.
    - Bør oppdateres ihht. Forskriftstekst

- Aktører
  - Få frem ansvaret til nettselskapet tydeligere.
    - Spesielt ved tjenesteleveranser.
    - Konsekvenser
  - Ingen begrensninger mtp tjeneste-utsetting (underleverandører og underleverandørers underleverandører)
  - Samarbeid, Eierskap-ansvar osv.
  - Utfordring for allianser.
  - Mangler figur som illustrerer kompleksitet med flere tjenesteleverandører
    - Hvordan forholder spesielt de minste nettselskapene seg til sikkerhet i AMS? Overlater de ansvaret til Soria/Valider?
  - 27 nettselskap i en "sekk" hos Valider – innebærer dette en risiko i seg selv?
  - Veileder og forskrifter er til god hjelp for å stille krav til både leverandører og egen ledelse (jfr. også punktet om tydeliggjøring av forholdet mellom krav, anbefalinger og eksempler i veilederen).
  - Valider overtar mye, inkludert mye forvaltning av sikkerhet.
  - Mye av kommunikasjonen går over fiber, som leveres av et annet selskap i konsernet (jfr. bruk av underleverandører, eksempelvis for radiokommunikasjon).

- Et nettselskap bruker generelt mye tredjepartsleverandører for leveranse og drift av IKT-systemer
- Beskrivelsen av driftsselskap i veilederen tar ikke høyde for alliansene som nå er inngått (Soria og Nettalliansen). Vil disse fremstå som enda en aktør, mellom nettselskapene og tredjepart (f.eks. Valider)? Hvordan vil dette påvirke sikkerheten, og nettselskapenes opplevelse av ansvar og anledning til å forvalte dette?
- Betydelig avhengighet til telekomoperatørene (jfr. bl.a. gjeninnkobling).

- Sikkerhet/risiko
  - Ikke bare én person ift. bryterstyring?. Tilgangskontroll
  - Bryterstyring – krav til antall personer som involveres. Er dette tilstrekkelig?
  - Hvordan forventes test?
    - Nivå
    - Scope
  - Fysiske soner?
  - Under kap. C er det en del krav som ikke lar seg realisere pr. i dag. Teknisk løsning skal oppdage/hindre -> kan ikke realiseres
  - Tilgangskontroll
    - Kundedata i AMS
    - Tekniske løsninger...
  - Kundedata AMS - Håndtering. Spesifikke krav som ikke gjelder andre systemer, bl.a. at den som har adgang til disse data skal levere vandelsattest. Tilsvarende krav er ikke gitt for de som har tilgang til data i KIS.
  - Autorisering & Autentisering av håndholdte enheter => Sperres for andre oppgaver. Noen eksempler er for spesifikke. Håndholdt enhet skal være sperret for annen funksjon. Hvordan skal dette håndteres? (Kravet bør bort?)
  - DMS/SCADA
    - System "Sammenkoblet med". Hva betyr det? Hva er en "Kobling"? Definere begreper?
  - Nettselskap "anerkjenner betydelig risiko ved outsourcing av tjenester".
  - Underleverandører får normalt tilgang inn i nettselskapenes systemer, eksempelvis for oppdatering av programvare. Mulig sikkerhetshull. Dette er løst overfor leverandør ved å etablere VPN-tunnel som manuelt aktiveres forespørsel fra leverandør, og deaktiveres umiddelbart etter at det aktuelle oppdraget er utført.
  - Et nettselskap opplever veilederen som veldig god, men kanskje uforholdsmessig spisset og detaljert i forhold til andre områder i nettvirksomheten. Kan skape (et inntrykk av) skjevhet i det totale sikkerhetsarbeidet. Eksempel: C.1 s. 15, "vandelsattest, kredittsjekk og referansesjekk". Inkonsistent med krav ellers i nettdriften. **Anbefaling**: avstemme veileder mot andre veiledere, rundskriv og forskrifter nettselskapet må forholde seg til (jfr. generell avstemming opp mot gjeldende lovverk).
  - Et nettselskap har brukt mye tid på sikkerhetstesting, bl.a. av hele kjeden fra måler til KIS, og har funnet mye feil.
  - Det oppleves som vanskelig å få leverandører til å fokusere tilstrekkelig på sikkerhet (spesielt proaktiv sikkerhetsovervåking).
    - Har drevet voksenopplæring av leverandører
    - Har opplevd at feil som fikses i en versjon dukker opp igjen i neste
    - 50% av sikkerhetsfeil dreier seg om konfigurasjon

- Bruk av veileder
  - Logging og overvåking bør skilles og få inn krav til proaktiv overvåkning og analyse
  - Uklart hva som er krav og hva som er råd
  - Testing – hvor detaljert? Hva er akseptabelt minimumsnivå?
  - Veilederen inneholder mye bra, men Agder bruker den ikke aktivt per i dag. Forklares blant annet med timing: de hadde allerede kommet langt i AMS-arbeidet da veilederen ble publisert.
    - Flere av eksemplene er ikke relevante

- Nye tjenester
  - Dekker ikke senere trender som driftsallianser og skybaserte løsninger
  - Ansvar felles IKT-løsning, side 8 (dvs. Elhub), Omformulere kap. 2.3 – gjelder Elhub
  - Nettnyttedata var i liten grad en del av diskusjonen (og av figurene nettselskapene viste). Dekkes også i liten grad av veilederen (og er eksplisitt utelatt fra den underliggende risikovurderingen). Får dette for lite fokus i sikkerhetsarbeidet?
  - Tilleggstjenester: hva ligger egentlig i dette? Hvor utbredt kan det forventes å bli? Må avstemmes mot ekom-lovverket(?) – NVE har laget rundskriv om HAN-porten.
  - Spesielle problemstillinger knyttet til plusskunder?
  - Outsourcing av stengerett i forbindelse med ny modell for gjennomfakturering?

- Ekstra punkter
  - Allianser – med flere involverte
  - Tilleggstjenester
    - Fjernvarme
  - eComm. Lovverk – tilby for andre
  - Utkobling laster hos kunde
  - Sanntidsinformasjon fra måler? Hvordan? HAN (A3) – definert, finnes utstyr
  - Plusskunder?
  - Utkobling – fra en-og-en til mange?
  - Masseutkobling av målere er en bekymring. Det samme gjelder muligheten for gjeninnkobling.
  - Skytjenester – Tjenesteutsetting. Hva må være i Norge/Europa? Spesifisert i lovverket
  - Figur må oppdateres. Et nettselskap bruker konsentrator med maks 200 kunder under hver, unngår med andre ord "single point of failure". Innhenting av nettnyttedata fra nettstasjon vil være i et helt separat system.
  - Inkludere aktører i oversiktsfiguren?
  - Mange problemstillinger knyttet til personvern (avtaler med kunder, hva kan dataene brukes til, omfattes nettnyttedata av avtalene, personvernlovgivning, etc). (*Er dette egentlig utenfor scope til veilederen*?)

Ytterligere notater

- Hovedinntrykk: veilederen er et godt verktøy, med potensiale for å få mer slagkraft gjennom å bli tydeligere:
  - Tydeligere på skille mellom krav, anbefaling og eksempel. Presis språkbruk ("skal" vs. "kan").
  - Justere strukturen til å ha hensikt/formål først, og eksemplene til slutt.
  - Inkludere forskjellige eksempler på mulig tilnærming for store og små nettselskaper (og evt. tredjepartsleverandører).
  - Regelverket omtaler "kobling" og "integrering" av systemer. Hva betyr egentlig en "kobling"?
  - Skytjenester: hva ligger i dette begrepet? Må tydeliggjøres og dekkes av veilederen.

## V1.2 Arbeidsmøte 2 (2016-11-03)

**Positive tilbakemeldinger på dagens veileder (gule lapper + notater)**

- Sjekklisten i vedlegg
- Det er bra med henvisning til forskriftskrav, kanskje enda mer spesifisere hvilke forskriftskrav som dekkes ved bruk av veileder?
- Dagens veileder er kompakt og overkommelig. Dette bør ivaretas videre.
- Innhold
    - Temaene er i utgangspunktet gode.
    - Gode punkter i innholdsfortegnelsen -> til overordnet sikkerhetsarbeid
- Form
    - Struktur oversiktlig
    - Lettfattelig, overordnet
    - Oversiktlig
    - Oversiktlig
    - Logisk form/struktur
- Eksempler
    - Innhold: Tabell over kontrollmål må endres/tilpasses
    - Kontrollmål hjelper å konkretisere
    - Bra med konkrete eksempler
    - Bra med mange eksempler som man kan relatere seg til.
    - Innhold: Overordnet sikkerhetsarbeid
    - Hjelp til utarbeidelse av kravspesifikasjon
    - Overordnet sjekkliste, helikopterperspektiv. Sjekkliste gir en bra oversikt.
- Ansvar
    - Hvem er ansvarlig
    - Krav til nettselskap som første tema
- Detaljnivå
    - Ikke for detaljert
    - Innhold:
        - Passelig detaljert
        - Fokus på funksjon, ikke spesifikke produkt/detaljer
    - Bra: Innhold
        - Konkret på innhold, uten å være teknologispesifikk
- Tema
    - Gode tema
    - Veldig relevant for AMS og nettselskapene i en oppstartsfase (kravspec. Etc.) (Grunnlag for utarbeidelse av kravspesifikasjon)
    - Relevante sikkerhetsområder
    - Relevant for innføring av AMS. Tidsrett.
        - For installasjon/utrulling. Mulig litt annen fokus etter utrulling?

**Tilbakemeldinger på mulige forbedringer av dagens veileder (gule lapper + notater)**

- Innhold
  - Oppdaterte krav ift. kommunikasjon?
  - Urealistisk med tanke på leverandørsituasjon?
  - Ikke vurdering av hvor kritiske punktene er. Trengs en overordnet beskrivelse av hva som er kritisk å oppnå. Det er vanskelig å finne leverandører som tilfredsstiller alle punktene i veileder.
  - Fare for at viktige områder overses (pga. detaljerte kontrollmål og eksempler). Gjelder områder utenom A-I, men også underpunkter under disse.
  - Spesifisere om forbedringer bør inngå i ROS? Oppdatere ROS-veileder? (Tillegg laget i DeVID).
- Henvisninger/referanser
  - Henvise til forskriftskrav der det gjelder
  - Fjerne henvisning til kompetanseforskrift (s. 12)
  - Henvise til forskriftsparagraf i kontrollmål
  - Lite referanser til eksterne kilder som gjelder sikkerhet, f.eks. NorSIS, NSM, CERT, iTIL Foundation osv.
- Eksempler
  - Det er bra at veileder har en overordnet fokus, og fokus på funksjonalitet.
    - Kan ha referanse til spesifikke eksempler på hvordan kontrollmål blir løst, uten at dette trenger å være førende.
    - Kan ha flere konkrete eksempler i vedlegg? Det spørs på levetid til slike eksempler.
- Kommunikasjonsteknologi
  - Oppgraderbarhet av enheter på kommunikasjonsteknologi ("komt"?). Typisk for å tette sikkerhetshull
  - "Feil" angående kryptering på 2G (A5/4?). Det står at kryptering 2G er lett å hacke – dette stemmer for GSM, men ikke for GPRS. Unøyaktige formuleringer bør korrigeres.
    - Benyttes kun på linjeswitch mobil kommunikasjon, ... A5/3, GEAx
  - Oppdatere begrepsbruk i veileder. "GSM" skal være "MBB" (mobilt bredbånd) (GPRS, UMTS, EDGE, HSDPA, LTE, ... 5G).
  - Er kravene til kommunikasjon gode nok?
- Aktører
  - Tydeligere ansvar nettselskap – leverandør
  - Hvordan følge opp leverandørkjeden? Dette er ikke godt nok beskrevet. Følge opp på en god nok måte. Forutsetter en god prosjektorganisasjon/-gjennomføring hos nettselskap.
- Levetid
  - Tidsvinduet til veileder. Anbefaling -> spesifikke på hva veileder gjelder for
  - Revisjon/oppdatering. Utløpsdato/Tidsbegrensning?
  - Veileder gjelder i dag, men ser man nok framover?
- Sikkerhet/risiko
  - Hva betyr egentlig "sikkerhetsavtale"? Fokus leverandør-nettselskap
    - Forståelse
    - Forventninger
  - Større fokus på hendelseshåndtering, bl.a. siden AMS har en bryter.
    - Beskrive hva hendelseshåndtering betyr?
  - "Nye" trusler: RansomeWare etc. se finansbransjen
  - Hva er forventningene til sikkerhet i nettverket?

    - A.1 "Basert på risiko". Hva menes?
    - Det må være mulig å oppgradere sikkerhet. Dette bør tas med i veileder (og senere inkluderes i kravspesifikasjon.) Eksempel: Valider har 50% ledig kapasitet i CPU for å ta høyde for fremtidige oppgraderinger.
    - Avhengigheter – bør inngå i ROS og verdivurdering
        - Fysisk
        - Logisk
        - Personell
- Bruk av veileder
    - Kontinuerlig oppfølging av arbeid ihht. Veileder (treffer brukerne av veileder)
    - Kan lett bli en sak for "AMS-folket", men gjelder også for andre deler av nettselskapet. Hva med tilgrensende organisasjon?
    - Kontinuerlig forbedringsarbeid. Prosess hardware/software
    - Krav til kontinuerlig oppfølging av arbeidet
    - Prosess og prosjektoppfølging
    - Kompetanseoverføring
- Nye tjenester
    - Stenging/struping fra KIS. Svakheter i dag.
    - Hva med nettnyttedata? (Veileder opprinnelig tenkt for kWh-data. I dag er det mye annen data.)
    - Tilpasses driftssituasjon og nye tjenester
    - Grensesnitt mot DMS m.m. (DERMS, ...)
    - Hva med DMS/SCADA?
    - Elhub (Oppfølging av sertifisering). Elhub er ikke nevnt i veileder. Alle selskaper skal sertifiseres (ref. Elhub). Hvordan følge opp dette?
    - Smarthus, Big Data, Nettnytte
    - Skytjenester – Hvordan følge opp?
    - Ekstra punkter
        - Andre målere (vann, fjernvarme, ...). Tilknyttet ofte via M-bus (kostbart). Andre målere kan inngå i radio-mesh.
            - Hvordan håndtere at man måler for andre?
            - Hvor ligger da sikkerhetsnivået? (Nettverk/link/...)
        - Hvilke forventninger til sikkerhet i nettverk? (ref. tilgang for andre)

Krav om sikkerhetstesting må veldig tydelig inn i veilederen. Kompetanse på sikkerhetstesting er et stort behov hos leverandører (og nettselskaper). Kraftbransjen begynner å bli bedre bestillere, men veilederen bør kunne hjelpe i dialogen med leverandører.

## Vedlegg 2 Forkortelser

| | | |
|---|---|---|
| AMI | - | Advanced Metering Infrastructure |
| AMS | - | Avanserte Måle- og Styringssystem |
| BEIS | - | Department for Business, Energy & Industrial Strategy |
| BSI | - | Bundesamt für Sicherheit in der Informationstechnik |
| DCC | - | The Data Communication Company |
| DECC | - | Department of Energy & Climate Change |
| DMS | - | Distribution Management System (driftskontrollsystem for distribusjonsnettet) |
| DPIA | - | Data Protection Impact Assessments |
| EECSP | - | Energy Expert Cyber Security Platform |
| ENCS | - | The European Network for Cyber Security |
| GCHQ | - | Government Communications Headquarters |
| GPRS | - | General Packet Radio Services |
| GSM | - | Global System for Mobile communication |
| HAN | - | Home Automation Network |
| IEC | - | International Electrotechnical Commission |
| ISO | - | International Organization for Standardization |
| KIS | - | Kundeinformasjonssystem |
| MBB | - | Mobilt Bredbånd |
| MVDB | - | Måleverdidatabase |
| NCSC | - | The National Cyber Security Centre |
| NIS | - | Nettverks og informasjonssikkerhet (EU-Direktiv 2016/1148) |
| ROS | - | Risiko- og sårbarhetsanalyse |
| SCADA | - | Supervisory Control And Data Acquisition (driftskontrollsystem) |
| SEC | - | The Smart Energy Code |
| SGAM | - | Smart Grid Architecture Model |
| SGTF | - | Smart Grids Task Force |
| VPN | - | Virtual Private Network |

Teknologi for et bedre samfunn

**www.sintef.no**