Sikkerhetsanalyse i AMS

(Avansert Måle- og Styringssystem)

Sverre Andreas Larssen

Veiledere
Per-Oddvar Osland og Frank Li

This Master's Thesis is carried out as a part of the education at the University of Agder and is therefore approved as a part of this education.

University of Agder, 2011
Faculty of Engineering and Science
Department of Information and Communication Technology

Nøkkelord: AMS, Sikkerhet, Personvern, Nettselskap.

Sammendrag:

Automatisk Måle- og Styringssystem (AMS) skal innføres i alle norske bygg knyttet til strømnettet, innen 1. januar 2017. Dette er et system som i første omgang skal avlese elektrisk forbruk, styre strømtilførselen og gi forbrukere informasjon relatert til strøm. Dette gjøres ved å installere smartmålere, som er en strømmåler og kommunikasjonsenhet, i alle bygg. I EU skal det også avlese gass-, vann- og varmeforbruk og i Norge vil sannsynligvis vann- og fjernvarmeavlesning etter hvert bli implementert.

AMS er planlagt gjennomført i de fleste industrialiserte land og Norges Vassdrags- og Energidirektorat (NVE) ønsker å basere seg på standarden som er under utarbeidelse i Europa. Open Meter (OM) spesifiserer et AMS-system gjennom et standardiseringsarbeid for de europeiske landene. Dette arbeidet er ikke avsluttet, men det er grunn til å tro at de fleste anbefalingene er klare.

AMS er svært omfattende og uprøvd, men det har vært viktig for OM å bruke etablerte standarder i alle ledd når det gjelder selve infrastrukturen. Det garanterer for interoperabilitet og tilgang til utstyr fra mange leverandører. Overføring av data mellom systemkomponentene bruker utprøvde og avanserte krypteringsalgoritmer og protokoller.

En del hjem i Norge har og vil få hjemmenettverk (Home Area Network, HAN) som kan styre en del funksjoner i hjemmet. Dette dreier seg i første omgang om styring av elektriske apparater, lys og varme. AMS kan inkorporeres i dette hjemmenettverket og en del av det elektriske forbruket kan automatisk igangsettes, på tider av døgnet, når strømmen er rimeligere.

Sikkerhet er viktig i AMS fordi det berører både personvern og selve styringsfunksjonaliteten. Det kan derfor være interessant for norske nettselskap, og andre aktører, å få utredet enkelte sider ved sikkerhet og personvern i AMS:

- *Systemsikkerhet: Sider ved den overordnede sikkerheten når det gjelder drift av AMS.*
- *AMS-sikkerhet: Sikkerhet på komponentnivå i AMS.*
- *Er personvernet ivaretatt?*

NVE har i sitt siste høringsnotat til impliserte parter, foreslått en rekke krav som de ønsker i det norske AMS-systemet. Disse kravene blir knyttet opp mot en sikkerhets- og personvernvurdering.

Denne masteroppgaven omfatter analyse av sikkerhetsaspekter ved innføring av AMS og det er laget tabeller som viser hvor fokuset til nettselskapene bør ligge. Både valg av komponenter og håndteringen av informasjonssystemet kan ha avgjørende betydning for den totale sikkerheten. Det er også funnet en del uavklarte sider ved personvern.

Noen av tiltakene masteroppgaven foreslår:

- *Bruke anerkjent styringssystem for informasjonssikkerhet, for eksempel ISO 27001*
- *Forkaste NVEs krav i høringsnotatet, om tredjeparts adgang til smartmålere og HAN via AMS.*
- *Avklare enkelte personvernmessige implikasjoner.*

Versjonskontroll

Versjon	*Status*	*Dato*	*Endring*	*Forfatter*
0.1	UTKAST	2011-01-16	Nye kapitler lagt til	S.A.L.
0.2	UTKAST	2011-04-04	Til gjennomlesing	S.A.L.
0.3	UTKAST	2011-04-14	Kap 1 & Kap 3 bearbeides	S.A.L.
0.4	UTKAST	2011-04-28	KAP 3 & 4 bearbeides	S.A.L.
0.5	UTKAST	2011-05-04	KAP 2,3 & 4 bearbeides	S.A.L.
0.7	GRANSKING	2011-05-13	Alle kapitler bearbeides	S.A.L.
0.8	GRANSKING	2011-05-15	Kapittel 3-4-5 bearbeides	S.A.L.
0.9	GRANSKING	2011-05-18	Alle kapitler bearbeides	S.A.L.
1.0	ENDELIG	2011-05-25	Alle kapitler bearbeides	S.A.L.

Forord

Denne rapporten er hoveddelen av kurset IKT 590, Masteroppgaven, ved Universitet i Agder (Grimstad), Institutt for informasjons- og kommunikasjonsteknologi, Fakultet for teknologi og realfag.

Oppgaven er fremsatt av Devoteam A/S, Grimstad. Denne avdelingen av Devoteam jobber mot tele- og datakommunikasjon [1].

Devoteam A/S ønsker en bred analyse av sikkerhetsaspektet ved innføring av AMS. Jeg valgte denne oppgaven fordi det ville være en naturlig og utfordrende avslutning på utdannelsen innen spesialisering på sikkerhet.

Veileder hos Devoteam A/S var Dr. Per-Oddvar Osland og ved UiA, professor Frank Li. En stor takk til begge for verdifulle innspill og tilbakemeldinger.

Oppgaven har vært gjennomført i tidsrommet 7. januar 2011 til 25. mai 2011.

Lillesand

25. mai 2011

Sverre A. Larssen

Innhold

1 Innledning

Utviklingen går mot et samfunn der datamaskiner tar over for mer og mer når det gjelder styring av systemer, både store og små, offentlig og privat.

Vi ser en utvikling i bl.a. samferdsel, der datamaskiner tar over flere funksjoner for å avhjelpe menneskelige operatører. Det gjelder både fly, bil og jernbane. Etter hvert vil det bli mer vanlig med styresystemer i hjem og bygninger. Om noen få år skal det tas i bruk datamaskiner for å kunne regulere strømmarkedet bedre, gjøre avlesing av forbruk enklere og strømsparing mulig.

I husholdningene er det etter hvert blitt vanligere med fjernstyring av apparater og lys. Vi går mot såkalte smarte hus, dvs. et digitalisert hus som styres av datamaskiner. Dette innebærer at apparater slår seg på etter visse kriterier (lys på om kvelden, varmekabel på ved en viss temperatur eller tid osv). Disse mulighetene integreres i et såkalt HAN[1] (Home Area Network) som litt frem i tiden også vil omfatte eHelse (elektronisk Helse) [2]. eHelse er et distribuert helsetilbud der elektronisk overvåking og helserelatert informasjon om en pasient kan overføres fra hjemmet til sykehuset.

Selskap som driver strømnett i Norge har fått pålegg om å montere nye elektrisitetsmålere i alle bygg innen 1. Januar 2017 og 80 % av dette arbeidet skal være ferdig innen den 1. januar 2016. Disse nye målerne vil være digitale og ha en rekke nye funksjoner som Norges Vassdrags- og Energidirektorat (NVE [3]) har spesifisert.

1.1 Bakgrunn og motivasjon

AMS er en norsk forkortelse for Avansert Måle- og Styringssystem. I EU og andre engelsktalende land kalles det for Automatic Metering Infrastructure (AMI). AMS er en del av såkalte Smarte Nett/ Smart Grid som er et samlebegrep på et integrert strømnett og et digitalt nett. Det som spesielt kjennetegner smarte nett er evnen til kommunikasjon med målere og annet utstyr, slik at strømnettet automatiseres og også automatisk justeres og tilpasses etter oppståtte hendelser. Et eksempel kan være ved overforbruk av strøm i et område, der AMS-systemet automatisk stenger strømmen til enkelte forbrukere, for å unngå overbelastning av strømnettet.

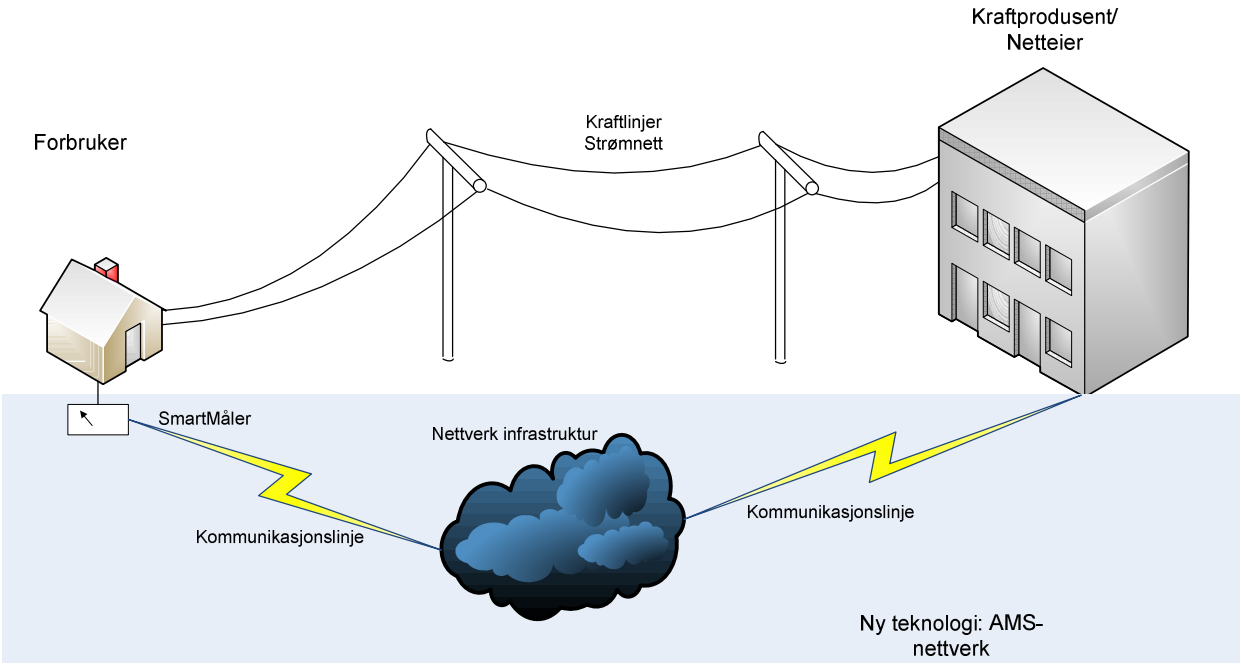
Den digitale delen består av en smartmåler (Smart Meter) og et datanettverk som kobler denne måleren til et nettselskap. Måleren er montert ute hos kundene og vil kunne lese forbruk (strøm, gass, varme og vann) i bygningene. Måleren skal også kunne overvåke strømkvaliteten, avdekke jordfeil, begrense strømtilførsel og stenge strømmen. Det skal også være mulighet for desentralisert strømproduksjon, slik at strøm kan produseres lokalt og mates inn i strømnettet. Smartmåleren vil da også kunne måle denne produksjonen. Smartmåleren, som består av en strømmåler og en kommunikasjonsmodul, skal også kunne gi kundene informasjon om strømpriser, tariffer, feilmeldinger og lignende, dersom kunden ønsker det. Figur 1-1 gir en forenklet oversikt over strømnettet og AMS, der den nye teknologien er vist med blå bakgrunn.

Den overordnede målsettingen med AMS, er i følge NVE, at systemet skal bidra til et mer samfunnsøkonomisk, rasjonelt kraftmarked, ved en mer effektiv avregning, enklere å bytte strømleverandør og tilpasning av forbruk og lokal produksjon.

[1] Det er få autoritative definisjoner på betegnelsen Home Area Network, HAN, men begrepet brukes i mange amerikanske publikasjoner. En del informasjon om protokollen er publisert av NIST[4].

Denne målsettingen er litt mindre ambisiøs enn EUs målsetting om reduksjon av strømforbruk og dermed drivhusgasser med 20 % innen 2020. AMI er en del av de såkalte 20-20-20-målene til EU-kommisjonen som slår fast [5]:

- *A reduction in EU greenhouse gas emissions of at least 20% below 1990 levels*
- *20% of EU energy consumption to come from renewable resources*
- *A 20% reduction in primary energy use compared with projected levels, to be achieved by improving energy efficiency.*



Figur 1-1 - Oversikt over systemet

Introduksjonen av AMS generelt og smartmålere spesielt i et datanettverk, krever innsikt i både smartmålerne og datanettverket. Enkelte nettselskap kan ha nytte av en anbefaling på hvordan AMS kan implementeres basert på en risikoanalyse med sikkerhet og personvern i fokus.

AMS er en del av utviklingen mot såkalte Smarte Hus. eHelse vil også være en del av en mer digitalisert fremtid for brukere. Det at eHelse og Smarte Hus blir en mer integrert del av hverdagen kan føre til implikasjoner for visse sider ved AMS.

Motivasjonen for denne rapporten er et ønske å gi en oversikt over AMS, både muligheter og begrensninger, med fokus på sikkerhet og personvern. Dette vil være nyttig for nettselskap og andre aktører som jobber med problemstillinger knyttet til AMS. Min bakgrunn er datasikkerhet og denne oppgaven går til kjernen av et slikt studium.

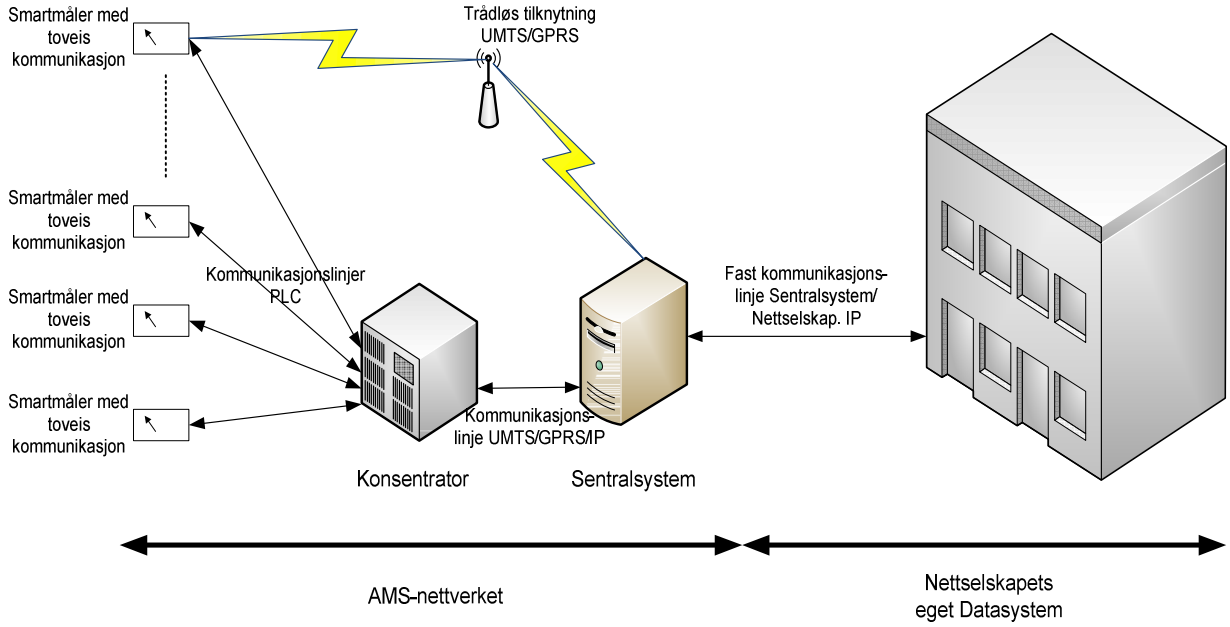
1.2 Problemdefinisjon

Nettselskap som skal innføre AMS i Norge kan ha nytte av en risikoanalyse av systemet før det implementeres. Denne rapporten skal konsentreres om sikkerhet i AMS-nettverket, sikkerhet sett

i et samfunnsperspektiv og personvern. Målet er da å identifisere problemområder og foreslå tiltak for å minimere disse problemene.

Selv om fokuset vil ligge på den tekniske delen av AMS, er det viktig å ha et bredt perspektiv på sikkerhet og forsyningsevne, siden strømforsyningen også er et samfunnsanliggende.

Figur 1-2 gir en oversikt over AMS-systemet. Denne rapporten vil konsentrere seg detaljert om AMS-nettverket, men ikke gå særlig inn på nettselskapets eget datasystem. Dette innebærer at implementeringen av nettselskapets datasystem ligger utenfor denne rapportens problemdefinisjon, men rapporten vil likevel komme litt inn på enkelte driftsrutiner ved dette interne datasystemet.



Figur 1-2 - Oversikt over AMS-systemet

Smartmåler og kommunikasjonsenhet er vanligvis montert sammen og vil være i alle bygninger som er tilknyttet strømnettet. Det er mulig å koble andre enheter til smartmåleren gjennom forskjellige grensesnitt. Smartmåleren kommuniserer med en konsentrator, som normalt er lokalisert i en transformatorstasjon. Konsentratoren kommuniserer så data til Sentralsystemet som er selve hjernen i AMS-nettverket. Sentralsystemet kommuniserer med nettselskapets datasystem, der måleverdier avleses og prosesser i AMS-systemet igangsettes.
Dersom det ikke er konsentrator tilgjengelig, eller det finnes andre grunner, vil kommunikasjonen mellom smartmåler og Sentralsystem foregå trådløst, direkte, slik det er skissert øverst i figuren. Kommunikasjonen foregår enten via konsentrator eller direkte til Sentralsystemet.

Netteieren vil være bekymret for om data (toveis kommunikasjon) mellom kunden og eget nettverk er riktige (integritet) og kommer fra riktig forbruker (autentisitet). Med en smartmåler installert i hver bygning, vil det åpnes muligheter for utenforstående folk/organisasjoner/produkter som ønsker å manipulere dette systemet. Det kan være alt fra ren svindel til mer alvorlige hendelser som å stenge strømmen til utvalgte bygninger eller områder. Smartmåleren kan også ha svakheter som gjør at det oppstår feil i systemet. Det kan også være betrodde medarbeidere med innsikt i AMS som ønsker å manipulere systemet på oppdrag fra tredjepart. Vi har med

andre ord flere menneskelig faktorer og systemfaktorer (teknisk) som kan bidra til ustablitet i AMS: Rapporten vil derfor ta for seg både et utvendig og innvendig trusselbilde.

Forbrukerne vil også ha en frykt for manipulering av AMS-systemet, slik at det blir feil med avregninger og uønskede effekter i strømnettet. Dessuten er det viktig at personvernet blir ivaretatt på en betryggende måte, slik at ikke informasjonen faller i feil hender (konfidensialitet).

Rapporten skal:

- Gi en grundig innføring og oversikt over krav som stilles i forbindelse med AMS, med utgangspunkt i NVEs høringsutkast og Open Meters standardiseringsarbeid.
- Se på kommunikasjonsløsninger som er foreslått i AMS, avdekke eventuelle svakheter og påpeke disse, der fokuset ligger på sikkerhet.
- Se på problemstillinger knyttet til driften av nettselskapets datanettverk. Dette er et samfunnsanliggende og går på samfunnssikkerhet.
- Se hvordan personvernet er ivaretatt.
- Se på andre indirekte problemstillinger knyttet til sikkerhet, herunder fare for liv og helse.

Det er et ønske fra oppdragsgiver av denne rapporten, at det skal gis en grundig oversikt over krav og standarder som gjelder for AMS. Kapittel 2, bakgrunn, vil derfor gå bredt ut og vil ta for seg det som er essensielt for sikkerhetsanalysen av AMS. En bred bakgrunnsanalyse kan også avdekke andre problemstillinger som også kan være av interesse i et AMS-prosjekt. Dette kan være problemstillinger som ikke direkte er sikkerhetsrealterte, men som kan være viktige å merke seg før AMS implementeres i stor skala.

Rapporten vil komme med en anbefaling av hvordan AMS kan implementeres på en sikrere måte og særlig påpeke svakheter eller uforståelige krav i NVE og Open Meters forslag til AMS. Hva som er viktig å fokusere på både når det gjelder sikkerhet i bred forstand og personvern.

Rapporten vil identifisere og foreslå løsninger på sikkerhetsproblemer som kan oppstå ved innføring av AMS. Sikkerhetsproblemer dreier seg hovedsakelig om beskyttelse av data og utstyr mot misbruk. Dette innebærer at sikkerhet må ivaretas på detaljnivå og overordnet nivå. Den skal også vise om personvernet i tilstrekkelig grad er ivaretatt.

1.3 Avgrensning og antagelser

Denne rapporten baserer seg på modellen som er utviklet av Open Meter (kapittel 2.2) og på de krav NVE har fremsatt i sitt høringsnotat (kapittel 2.1.1). Det er viktig å presisere at Open Meter ikke er ferdig med sitt arbeid, men det er god grunn til å anta at de tekniske spesifikasjonene er gitt, mens alle sikkerhetsaspekter ikke er tilstrekkelig gjennomgått.

Følgende avgrensninger gjelder og rapporten skal ikke:

- Analysere noe av nettselskapets datanettverk utover driftsrutiner.
- Foreslå noen særegne løsninger i AMS-systemet utover det som Open Meter jobber mot.
- Analysere praktiske eller økonomiske betraktninger rundt AMS.
- Analysere de foreslåtte kommunikasjonsprotokollene. Dette er grundig gjort i Open Meter og i masteroppgaven Kommunikasjonsalternativer i AMS [6].
- Se på sikkerhet i forbindelse med desentralisert (kundeprodusert) kraft.

1.4 Metode

AMS er delvis implementert i flere land og Italia er i mål med dette arbeidet. Likevel vil ikke denne masteroppgaven forholde seg til disse igangsatte og ferdige systemene i særlig grad, fordi de bygger delvis på proprietære standarder.

AMS, slik det er foreslått av Open Meter, er et nytt system som aldri tidligere har vært satt i drift. Selv om alle deler av systemet bygger på åpne, veldokumenterte standarder, finnes det ingen direkte erfaringer med dette systemet. Dette innebærer at en kvantitativ analyse ikke er mulig, slik at rapporten må bruke kvalitativ analyse.

Denne metoden innebærer at det må etableres en dyp forståelse for hele AMS og de enkelte enhetene i systemet, for å kunne gjennomføre en analyse. Kapittel 2 bakgrunn, blir derfor omfattende.

1.5 Presisering av begreper

Vedlegg A inneholder en komplett liste over begreper, forkortelser og definisjoner som er brukt i denne rapporten. Visse sentrale begreper går igjen i teksten og disse sammenfattes her for å gjøre det enklere å følge hovedlinjene i teksten uten å måtte sjekke vedleggene for en presisering.

AMI:
: Advanced Metering Infrastructure. Engelsk betegnelse på AMS-nettverket.

AMS:
: Automatisk Måle- og Styringssystem. Dette omfatter all maskinvare og programvare som trengs for å lese og regulere smartmålere og annen maskinvare, direkte eller indirekte, tilknyttet disse i et strømnett. Dette omtales i teksten som AMS og AMS-systemet. Det vil typisk bestå av smartmåler, konsentrator, sentralsystem og nettselskapets eget datasystem som styrer AMS-nettverket via Sentralsystemet. (Se Figur 1-2). AMS skal hente måledata fra smartmålerne og samtidig overvåke systemet. En del av overvåkingen skal være automatisk, slik at feil blir korrigert i sanntid av systemet. Alle målinger, alarmer og hendelser blir rapportert til nettselskapets datasystem via sentralsystemet.

AMS-enheter:
: De enkelte bestanddelene i et AMS-nettverk. Det er Smartmåler, Konsentrator, Sentralsystem og kommunikasjonslinjer.

AMS-Nettverket:
: AMS-nettverket er den delen av AMS som er utenfor nettselskapets datasystem. Dette er logisk adskilt fra nettselskapets lokaliteter og denne delen av AMS-systemet omtales som AMI (Advanced Metering Infrastrucure) på engelsk.

AMS-Systemet:
: Samme som AMS.

Display:
: En skjerm for fremvisning av målerverdier, tariffer, informasjon o.s.v. fra nettselskap eller kraftleverandør. Koblet til smartmåler med toveis eller enveis kommunikasjon.

HAN:
Home Area Network er et nettverk som knytter forskjellige digitale enheter sammen i hjemmet eller andre bygninger. Dette kan være styring av for eksempel vaskemaskiner, oppvaskmaskiner, tørketromler, varmtvannsberedere, varmeovner og lys. HAN vil ofte være koblet til Internett slik at man kan fjernstyre hytta eller hjemmet utenfra.

Konsentrator:
Maskinvare som vanligvis vil være lokalisert i transformatorstasjoner og så kommuniserer og samler inn måledata fra flere smartmålere i et tilknyttet område. Disse verdiene blir så sendt videre til Sentralsystemet.

Kraftleverandør:
De som står for salg av elektrisk kraft. Dette kan være kraftprodusenter eller en tredjepart som selger kraft fra forskjellige kraftprodusenter.

Nettselskap:
De som står for distribusjon av elektrisk kraft og er eiere av kraftnettet og AMS.

Nettselskapets datasystem:
Et datasystem som styrer AMS, har kunderegister med forbruk og kundedata knyttet til smartmålerne.

Sentralsystemet:
Dette er hovedprosesseringsenheten i AMS-nettverket. Her samles alle måledata inn fra alle konsentratorer (eller direkte fra smartmålerne): Strømforbruk, feilmeldinger, hendelser, alarmer. Dette kan gjøre AMS-nettverket delvis autonomt, slik at det kan overvåke og ta forholdsregler ved feil i AMS-nettverket. Sentralsystemet blir kontrollert av nettselskapets datasystem og rapporterer også målerverdier, hendelser o.s.v. tilbake til dette. Sentralsystemet er logisk adskilt fra nettselskapets datasystem, men er ofte fysisk plassert i samme lokaliteter. Betegnelsene Front End og Central Access Server (CAS) brukes også, men ikke i denne rapporten.

Smartmåler:
En måler- og kommunikasjonsenhet som erstatter de gamle elektromekaniske strømmålerne i bygninger. Den toveis kommunikasjonsenheten skal blant annet kommunisere forbruk og gi informasjon til forbruker via Display, regulere strømforbruk, avstenge strøm, overvåke strømkvalitet og jordfeil. Smartmåleren kan være en enhet eller separert i to: Strømmåler og kommunikasjonsenhet.

Systemsikkerhet:
Sikkerhet på et overordnet nivå knyttet til bl.a. drift, driftsrutiner og trusler fra personer og organisasjoner som ønsker å manipulere AMS-systemet.

1.6 Litteraturstudie

AMS har vært på agendaen i Norge i flere år og det er NVE som setter føringer på når og hvordan dette skal implementeres. Med utgangspunkt i dette er NVEs publikasjoner [7] en viktig kilde til å få en oversikt over problemstillingene som tas opp her. NVE har mange referanser til EU og Open Meter, slik at disse dokumentene også må danne bakgrunn for denne rapporten. Publikasjonene fra NVE og Open Meter er oppsummert i kapittel 2 der også flere referanser er nevnt.

Amerikanske National Institute for Standards and Technology (NIST) har også en rekke publikasjoner angående AMI [8]. (AMS-nettverket kalles AMI på engelsk).

Videre er bøker og rapporter om datasikkerhet, bedriftssikkerhet og samfunnssikkerhet viktige for bakgrunnsforståelsen. I denne rapporten er bøkene Computer Security [9], Network Security [10], IT Governance [11] og Håndbok i Datasikkerhet [12] brukt som bakgrunnsmateriale.

1.7 Rapportstrukturen

Kapittel 2 i rapporten gir en bakgrunn for å kunne forstå AMS og hvilke sikkerhetsmekanismer som ligger i anbefalte løsninger. I kapittel 2.1 går jeg gjennom AMS i Norge og i kapittel 2.2 går jeg gjennom spesifikasjoner og krav fra Open Meter. I kapittel 2.3 vil det være noe bakgrunnsstoff fra datasikkerhet, systemsikkerhet og personvern.

Kapittel 3 vil vise hvordan et AMS-system er tenkt satt opp, påpeke svakheter ved enkelte sider og foreslå løsninger eller sette fokus på disse svakhetene som er avdekket. Kapittelet er organisert slik at det blir en inndeling etter problemområder.

Kapittel 4 vil drøfte og problematisere enkelte sider ved funn og valgte løsninger.

Kapittel 5 er en konklusjon av oppgaven, der de viktigste funnene blir sammenfattet.

2 Bakgrunn

Dagens strømnett er gammeldags og har ikke tatt innover seg de siste årenes muligheter som data og datakommunikasjon gir. Neste generasjons strømnett vil integrere kraftforsyning og datakommunikasjon og vi får såkalte Smarte Nett (SN). (Fra engelsk, Smart Grid). I Norge brukes begrepet AMS om den digitale biten av dette systemet.

AMS er et toveis kommunikasjonssystem mellom forbrukere og kraftleverandører. Systemet skal kunne måle forbruk hyppig, rapportere uregelmessigheter ved strømsituasjonen og kunne stenge strømtilførselen til forbrukeren.

AMS skal kunne gi forbrukeren bedre oversikt over aktuell strømpris og dermed oppmuntre til et mer differensiert forbruk. Ved prisstrategier kan nettselskapene påvirke en del kunder til å forskyve strømforbruket fra perioder med høy pris til perioder med lav pris. Nettselskapene ønsker en større utjevning i strømnettet, slik at toppene i forbruksmønsteret unngås.

Innføring av AMS kan gjøre både forbrukere og nettleverandører mer sårbare for manipulasjon. Det er derfor viktig å ha en bred analyse av sikkerhetsaspektet når et slikt system skal implementeres.

Norges Vassdrags- og Energidirektorat (NVE) er ansvarlig for forskrifter i forbindelse med igangsetting av AMS i Norge. Disse forskriftene er stort sett av teknisk natur og overlater i hovedsak ansvaret for personvern og sikker kommunikasjon til nettleverandøren [13]:

NVE understreker at de systemer og tekniske løsninger som nettselskapene velger må ta tilstrekkelig høyde for de krav til personvern som følger av personopplysningsloven. Selskapene må også sørge for at nødvendige krav til sikkerhet ved kommunikasjon og grensesnitt oppfylles, samtidig må de generelle kravene til nøytralitet og ikkediskriminering overholdes.

NVE har i sine anbefalinger støttet seg på arbeidet til OPEN meter [14], som er et prosjekt finansiert av EU-kommisjonen, for innføring av AMS i Europa.

2.1 AMS i Norge

NVE har hatt som mål en fullstendig utrulling av AMS innen utgangen av 2018, men i en pressemelding [15] fra Olje- og Energidepartementet (OED) har prosessen blitt fremskyndet to år, til utgangen av 2015. (Eller 1.1.2016).

NVE kom med sitt forslag om innføring av AMS i forskrift 11. mars 1999, nr. 301 [16] *om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester.* I disse dager ligger foreløpig siste høringsnotat [13] ute med høringsfrist 6.mai 2011. Det har vært ute to høringsnotater tidligere, men NVE har ikke fattet en endelig beslutning om innføring av AMS ennå, men det er sannsynlig at OEDs anbefaling blir fulgt:

Bakgrunnen har vært et behov for å avvente EUs standardiseringsmandat (M/441) [17] men også at NVE har funnet det nødvendig å gjøre ytterligere utredninger […flere funksjonskrav…]

Dette siste høringsnotatet blir brukt som utgangspunkt for arbeidet med denne rapporten. Dette vil knyttes opp mot relevant informasjon fra EUs OPEN meter og andre lands erfaringer,

planlegging og innføring av AMS. Forskriftene som vil komme som følge av høringsnotatet vil være minimumskrav, slik at nettselskapene kan implementere flere tjenester også.

2.1.1 AMS Høringsnotat

Jeg vil i dette kapittelet ta for meg de kravene som er foreslått i høringsnotatet [13]. Noen av kravene i notatet er allerede ferdig utarbeidet, mens andre krav ønskes det innspill om. Innspill ønskes i hovedsak fra nettselskap, energiselskap og forbrukerorganisasjoner. Videre har NVE samarbeidet med Justervesenet, Post- og teletilsynet, Direktoratet for Sikkerhet og Beredskap (DSB), Datatilsynet og vært representert i Council of European Energy Regulators (CEER) [18].

AMS har tre hovedfunksjoner: Måling, kommunikasjon og styring

Med måling menes registrering av elektrisk forbruk. Kommunikasjon skal være toveis og også ta høyde for kommunikasjon med eksternt utstyr fra andre leverandører. Styringsfunksjonen skal muliggjør begrensninger av uttak til sluttbruker og bedre styringsmuligheten totalt for nettet.

AMS har to hovedoppgaver: Effektivisere avregning og tilrettelegge for kraftmarkedet.

Oppgaven med å effektivisere avregning, vil si å avlese forbruk automatisk. Tilrettelegging for kraftmarkedet innebærer å ha et system som kan brukes av andre tjenesteleverandører også.

NVE setter også krav til at det ikke skal brukes særnorske løsninger. NVE ønsker derfor ikke krav i forskriftene som går utover det andre land tilbyr. Dette for å kunne bruke utstyr som allerede er tilpasset et regelverk og som allerede er tilgjengelig. NVE ønsker også at nettselskapene foretar en nytte- og kostnadsvurdering for å finne ut hvor mye de vil implementere utover minimumskravene. NVE anbefaler at nettselskapene går ut over disse minimumskravene. Nettselskapene har også ansvar for å overholde Personopplysningsloven, Forskrift om krav til elektrisitetsmålere og Forskrift om elektriske forsyningsanlegg.

NVE ønsker å knytte standardiseringen av AMS opp mot del 1 av EUs standardiseringsmandat som ventes å være tilgjengelig første halvdel av 2011. Et forskriftsvedtak vil derfor komme etter at denne delen er tilgjengelig. NVE har innblikk i EUs arbeid og bruker de forventede kravene i dette høringsnotatet.

CEER har laget en rapport med funksjonskrav til AMS som NVE i høringsnotatet siterer. Oppsummert punktvis skal følgende krav være tilfredsstilt:

- Kunden bør stå som eier av måledata, bør selv kunne velge hvordan disse skal benyttes og skal kunne få kjennskap til hvilken informasjon som lagres hos nettselskapet,
- kunden bør ha enkel og kostnadsfri tilgang til informasjon om faktisk forbruk og priser og kostnader knyttet til dette
- kunden bør kunne få tilgang til informasjon på forespørsel (on demand) om forbruks- og kostnadsdata,
- kunden bør ha mulighet til å motta informasjon i ulike media (for eksempel sms, Internett, kundetelefon etc.),
- alle tjenesteleverandører (inkludert nettselskap og kraftleverandør) bør ha rask tilgang til måledata slik at det blir lettere å skifte leverandør, flytte eller endre kontrakt,
- faktura bør være basert på faktisk forbruk,
- kunder skal ha tilgang på historiske data som vil gjøre det lettere med

klagebehandling),
- kraftavtaler bør reflektere faktisk forbruk og registreringsfrekvens bør i hvert fall være timebasert,
- måleren bør kunne bryte og begrense effektuttaket i det enkelte målepunkt,
- måler bør kunne måle både forbruk og produksjon,
- kunden bør få umiddelbar informasjon ved avbrudd,
- kunden bør få umiddelbar informasjon ved ekstreme situasjoner (for eksempel ved ekstremt høyt forbruk),
- måleren bør være utstyrt med eller tilknyttet en åpen og standardisert gateway for å gjøre det mulig for kunden å benytte tilleggstjenester fra andre tjenesteleverandører,
- målerens software bør kunne oppdateres fjernstyrt slik at man kan ta høyde for utviklingen fremover.

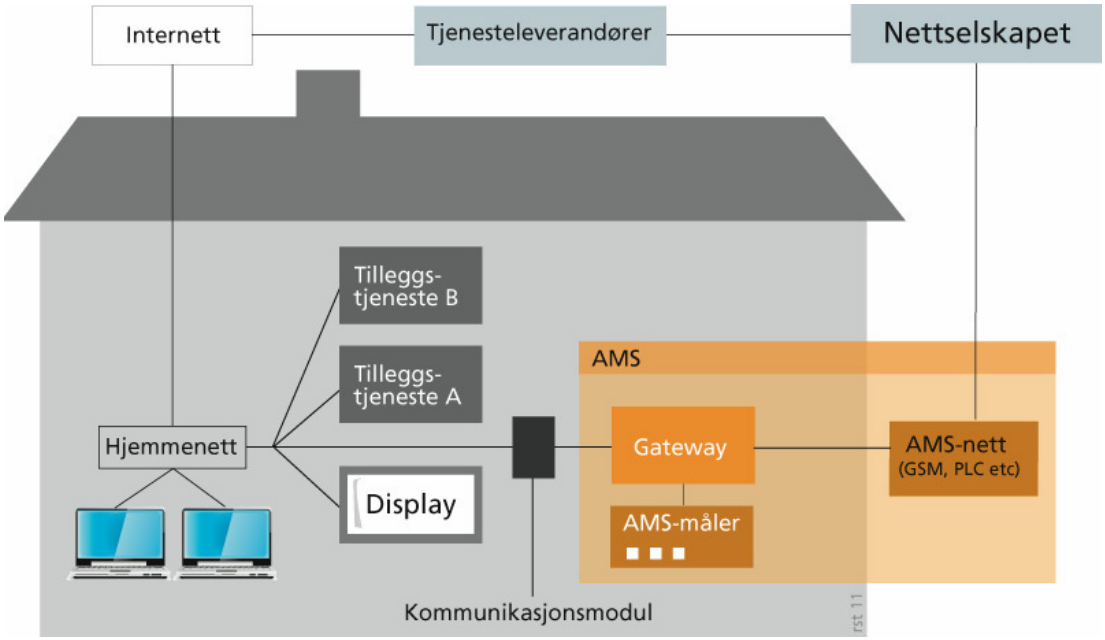
I kapittel 3 i høringsnotatet konkretiserer NVE funksjonskravene og oppgavene som AMS i Norge må oppfylle. Disse er:

1. Registrering og Innhenting av målerverdier:
    - Registrering og tidsoppløsning: All registrering av måledata må kunne lagres hos kunden inntil de er overført til nettselskapet. Det skal foretas avlesing av forbruk minst hvert 60. minutt justerbart ned til hvert 15. minutt. Dersom utstyret ikke kan justeres skal avlesning foretas hvert 15. minutt.
    - Momentan avlesning: Ved hjelp av toveis kommunikasjon skal nettselskapet kunne avlese en måler når som helst.
    - Overføringsintervaller: Elektrisk forbruk skal overføres minst en gang pr. døgn fra kunde til nettselskap. Måleverdiene siste døgn, skal være tilgjengelig for sluttbrukere og kraftleverandører innen kl. 09 neste dag. Dette for at kraftleverandøren kan tilpasse sin produksjon og at de kan lettere vite hva de kan tilby spotmarkedet.
    - Kommunikasjonsløsninger: NVE går ikke inn på de forskjellige kommunikasjons-protokollene som foreligger: Internett, Power Line Communication (PLC), mobile løsninger (GSM-GPRS) o.s.v. Kommunikasjonen må kunne oppfylle de punktvise kravene i denne listen.

2. Brytefunksjonalitet: Netteieren skal kunne styre strømuttaket i hvert målepunkt. Videre skal målepunktet også kunne stenges. NVE har ikke tatt endelig standpunkt til bryte- og strupefunksjonalitet, men anbefaler (med henvisning til M441) at det bør foreligge en bryterfunksjon.
3. Måling av egenprodusert kraft: Sluttkunder som produserer egen kraft skal kunne levere dette gjennom AMS-systemet. Dersom dette krever ekstra kostnader, skal kunden belastes disse.

4. Tjenesteleverandører og tilleggsfunksjoner:
    - Tilrettelegging for kunde og tjenesteleverandører: NVE forutsetter at kommunikasjonsløsningene som velges av nettselskapene vil ha en høy grad av sikkerhet. Nettselskapene må legge til rette for at også andre tjenesteleverandører kan koble seg inn på AMS-systemet og benytte den kommunikasjonsplattformen som velges. Disse tjenestene og behovene er foreløpig ikke spesifisert.
    - Kommunikasjon mellom eksternt utstyr og AMS: AMS skal kunne brukes til å kommunisere med andre målere som vann, fjernvarme, gass, hvitevarer, styringssignaler, alarmer, jordfeil og pris-/tariffdata. Annen informasjon (styring og energieffektivisering) skal også kunne videreformidles og nettselskapene må derfor ta høyde for at kommunikasjonsløsningen som velges må kunne sende styringssignaler

og motta informasjon fra kraftleverandører og andre energitjenesteleverandører. (Figur 2-1 er hentet fra samme notat):



Figur 2-1 - NVEs skisse til AMS og tilleggstjenester

For å muliggjøre tilleggstjenester må kommunikasjonen være basert på IP. Dette for å sikre standardiserte kommunikasjonsløsninger. Det er viktig at alle tjenestetilbydere får tilgang til kommunikasjonsløsningen på ikke-diskriminerende vilkår (§ 7-1 i avregningsforskriften - Se vedlegg B). Kommunikasjonen skal foregå i et lukket datanettverk eller kryptert. Også tilleggstjenester og tilleggsfunksjoner skal følge den valgte metoden og kan tilbys andre tjenesteleverandører (for eksempel vannverk, vannmålere). Nettselskapene må foreta en risikovurdering av AMS-systemet. NVE vil på et senere tidspunkt utarbeide rutiner for dette.
Det er viktig at datagrensesnittene i AMS er IP-baserte og dermed tilgjengelig for de fleste kjente kommunikasjonsprotokoller. Dette for å sikre andre tjenesteleverandører innpass på energiselskapets nettverk.

5. Tilgang på informasjon:
   - Informasjon som skal være tilgjengelig lokalt: Lokale måleverdier skal kunne hentes ut i samme bygning ved å koble til eksternt utstyr til AMS-måleren. Dette eksterne utstyret skal også være IP-basert. Kunden får dermed oversikt over eget forbruk og kan med det riktige eksterne utstyret også lagre data og få en historisk oversikt over forbruket. Disse data kan kunden senere bruke i forbindelse med energirådgivning og/eller endringer til et mer gunstig forbruk.
   - Distribusjon av informasjon til sluttbruker og tjenesteleverandører: Måleverdiene skal innhentes minst en gang i døgnet og skal også være tilgjengelig for andre tjenesteleverandører med samtykke fra kunden. Nettselskapene skal også gjøre forbruket i et større område tilgjengelig for kraftprodusentene, slik at disse kan bedre beregne produksjon og overskudd til spotmarkedet. Måledata som produseres i et AMS-system skal være tilgjengelig for godkjente aktører uten forsinkelser. I enkelte tilfeller trengs en korreksjon av data til kunden. Da må også historiske data endres samtidig, slik at det blir samsvar i faktureringen. Sluttbruker skal ha tilgang på egne data på energinettverkets hjemmeside. Bransjen skal selv velge et Internettformat eller grensesnitt for en slik presentasjon. Det er ønskelig at bransjen selv velger en

standard, slik at data fra alle landets energiverk kan samkjøres til en nasjonal database for måleverdier. Kraftprodusentene skal ha tilgang til måleverdiene i sine distrikter, men NVE har ikke tatt endelig stilling til om andre tjenesteleverandører, med kundens samtykke, skal registreres og autoriseres av NVE.

- Display: AMS-systemet skal muliggjør tilkobling av display som viser energiforbruk, kraftpriser, nettariffer og totalkostnader ved forbruk. Dette displayet skal være tilgjengelig for de kunder som ønsker dette og kostnadene for nødvendig utstyr og installasjon skal belastes kunden direkte og ikke gjennom økt nettleie. Nettselskapet skal være prisbevisste i forhold til løsninger de tilbyr kundene.

6. Informasjonssikkerhet:
   - Generelt: Kommunikasjonskanaler til alle sluttbrukere, energiforbruk og mulighet for fjernstenging av abonnementet setter store krav til datasikkerhet, datalagring, konfidensialitet og dataanonymisering.
   - Lagring av måleverdier: For å kunne utnytte potensialet som ligger i AMS er det viktig at resultatene gjøres tilgjengelig. Det er ønskelig at nettselskapene skal kunne lagre data så lenge at de kan presenteres som time-, måneds- og årsforbruk. Det er ikke tatt stilling til hvor lenge man kan lagre historiske data, men det henvises til datalagringsdirektivet.

     NVE ønsker at timeverdier skal kunne lagres i 3-15 måneder:
     - Dette vil gjøre faktureringen riktigere ved at prisen på forbruk gjenspeiles i den aktuelle kraftprisen. Videre bør data lagres minimum til etter at faktura er betalt.
     - Kraftleverandørene kan bedre regulere produksjon med tilgang til (anonymiserte) timeverdier.
     - Ved bruk av timeverdier basert på historiske data kan sluttbrukeren selv tilpasse forbruket til et rimeligere mønster, ved å utnytte prisvariasjonen som oppstår gjennom døgnet.
     - Nettselskapene kan bruke generelle eller egendefinerte lastprofiler. Egendefinerte lastprofiler lages på bakgrunn av timeverdier over minimum et år.

     Videre foreslår NVE at månedsverdier for de tre siste år skal lagres. Dette for å kunne gi en oversikt til sluttbruker over sesongvariasjonene.

     Måleverdier knyttet til personopplysninger hører inn under personopplysningsloven og alle aktører som har tilgang til disse data må overholde denne. Anonymiserte måleverdier skal kunne brukes utover begrensninger i personopplysningsloven. NVE og datatilsynet vil informere om hvordan man skal forholde seg i henhold til denne loven.
   - Sikkerhet mot inntrenging, misbruk og manipulering: AMS er et stort og omfattende system som også gjør kunder, nettselskaper og samfunnet mer sårbart. Nettselskapene må derfor utarbeide risikovurderinger og gjøre tiltak i henhold til disse vurderingene slik at ikke uautoriserte får tilgang til systemene.
   - Kostnad og risiko knyttet til brukerfunksjonalitet: Nettselskapene må gjøre en særskilt trussel- og risikovurdering for uautorisert tilgang på bryterfunksjonalitet. Dersom bryterfunksjonalitet integreres i det øvrige AMS-systemet, skal tilgang til driftskontrollsystemet sikres i henhold til § 6.4 i forskrift om beredskap i kraftforsyningen.

7. Inndeling i kundesegmenter: Generelt ønsker ikke NVE at ulike kundegrupper skal ulike AMS-løsninger. Det åpnes likevel for at noen kunder har særskilte behov og dermed kan kreve alternative AMS-løsninger. Dette åpnes det for i punkt 10, under.

8. Valg av måler: Det er nettselskapene som står for drift, innkjøp og montering av målere. NVE kan likevel bestemme at andre enn nettselskapet skal få velge måler. (Dette gjelder i hovedsak eiere av gatelys, som ønsker målere på hvert lyspunkt). Alle målere skal ha samme krav til nøyaktighet og følge justervesenets krav til godkjenning og brukskontroll.

9. Ombygging av sikringsskap: Sikringsskap er kundens eiendom og dersom plassen til montering av AMS-utstyret er for liten, skal kunden belastes en eventuell ombygging av sikringsskapet. Nettselskapet skal ta hensyn til målerens størrelse, slik at behovet for ombygging minimaliseres.

10. Dispensasjon. Unntaksregler: I utgangspunktet skal AMS installeres i alle målepunkt. Nettselskapene kan gjøre unntak på anlegg med svært lavt kraftforbruk eller anlegg med svært jevnt kraftforbruk. Videre skal nettselskapene ta hensyn til 'strømfølsomme' kunder ved valg av løsninger. Noen kunder vil vegre seg for trådløse løsninger pga. stråling.
    NVE oppfordrer nettselskapene til å gjøre færrest mulig unntak og de må uansett ikke komme i konflikt med kravet om nøytral og ikke-diskriminerende opptreden. Unntak skal kunne redegjøres for og ved tvist om unntaksregler mellom kunde og nettselskap kan NVE avgjøre saken.

Kapittel fire i høringsnotatet omhandler utrulling og finansiering. AMS skal være ferdig installert innen den 01.01.2017 og 80% skal være ferdig installert innen den 01.01.2016. Pga. anstrengt kraftsituasjon i midt-Norge (Møre og Romsdal, Nord- og Sør-Trøndelag) ønsker man å forsere utbyggingen av AMS, slik at 80% skal være installert innen 01.01.2014. Sluttfristen for de gjenværende 20% er den samme som landet for øvrig.

NVE ønsker å følge utrullingen og vil i 2011 utarbeide et elektronisk rapporteringsskjema og nettselskapene på rapportere regelmessig fra 2012. NVE ønsker opplysninger om:

- Plan for utrulling av nye målere fordelt på år.
- Antall og hvilke målepunkt som unntas fra utrullingen.
- Antall kunder som har mekaniske målere og antall kunder som har fått nye målere på Rapporteringstidspunktet.
- Hvilke kategori kunde som har fått installert nye målere (fritid, husholdning, næring).
- Hvor mange kunder som avleses automatisk.
- Overslag på kostnader på nye målere.
- I hvilken grad internettløsninger er etablert.
- Avvik fra planer. Årsak til eventuelle avvik.

Når det gjelder finansiering ønsker NVE at selskapene ikke bruker en egen finansieringsmodell for AMS. De mener det kan slå uheldig ut på enkelte nettselskaper. Man skal sette en årlig inntektsramme som dekker investeringer i nettet (herunder AMS) og gir en avkastning. NVE har laget økonomiske modeller som viser få ulemper for store nettselskaper kontra små ved bruk av nåværende reguleringsmodell for inntektsrammer. Det er heller ingen fordeler ved å investere senere i perioden.

Det vil komme endringer i forskriftene når det gjelder avregning ved bruk av AMS. I første omgang vil NVE endre punkter i forskriftene som er til hinder for installering av AMS, samt lage tillegg for AMS-målere. Disse tilleggene skal utnytte timeverdier ved måling og avregning.

Tillegg til avregningsforskriften:

Forslag til nytt tredje ledd, § 3-3:
For målepunkt med timemåler skal timeverdier benyttes ved måling og avregning.

NVE foreslår å fjerne hele § 3-4 den 01.07.2011, fordi alle vil etter hvert få timemålere:

§ 3-4. Nettselskapets og sluttbrukers adgang til timemåling
Sluttbruker kan kreve timemåling.
Nettselskap kan timemåle i alle tilfeller.

Videre skal de tre siste leddene i § 3-6 strykes slik at fra og med den 01.01.2011 står igjen med:

§ 3-6. Dekning av kostnader ved timemåling
Ved timemåling av energiuttak i henhold til § 3-3 syvende ledd skal kostnadene dekkes av nettselskapet.

Når det gjelder fakturering til husholdninger ønsker NVE et tredje punkt i § 6-1, gjeldene fra 01.07.2012, slik at det faktureres på bakgrunn av faktisk forbruk:

Forslag til endring av § 6-1, tredje ledd:

> *Det kan faktureres på bakgrunn av stipulert forbruk dersom innhenting av målerstand medfører urimelig kostnad eller ulempe for nettselskapet. Det skal opplyses på fakturaen at forbruket er stipulert. Husholdninger med timemåler skal faktureres på bakgrunn av faktisk forbruk.*

Det vil være overgangsbestemmelser i forbindelse med kundeinformasjon og hele § 4 vil først tre i kraft den 01.01.2017. (Nytt forslag til § 4 er tatt med i tillegg E). I en overgangsperiode ønsker NVE å la kunder med timemålere om å faktureres for timeforbruket. (§ 3-3 og § 6-1 over). Videre skal konsumenter i midt-Norge kunne inngå kraftpriskontrakter basert på timeverdier fra den 01.01.2012.

Fra den 01.01.2014: Alle kunder skal ha løpende tilgang på eget forbruk ved hjelp av PC, mobil og lignende. Eget display skal tilbys kunder som ønsker det. Kunden skal også ha tilgang på egne data som er samlet inn hos nettselskapet. Denne forbruksinformasjonen skal være tilgjengelig på Internett.

Tilslutt i kapittel sju i høringsnotatet nevnes økonomiske og administrative konsekvenser:

For sluttbrukere vil det innebære enklere avregning, mindre sannsynlighet for feil, fakturering etter faktisk forbruk, grunnet bedre oversikt over forbruk; bedre konkurranse om kundene, bedre energiøkonomisering og kraft- nettleieavtaler bedre tilpasset forbruket. Kostnadene forbundet med installasjon av AMS må bæres av sluttbrukere gjennom økt nettleie og er anslått til å være ca. kr. 380 pr. bruker.

Nettselskapene vil få reduserte måle- og avregningskostnader, enklere nettplanlegging, bedre driftskontroll og overvåking, reduserte drifts- og vedlikeholdskostnader, færre klager fra kunder, flere tilleggstjenester, enklere leverandørbytte og bedre omdømme. Investeringskostnadene for AMS må nettselskapene ta, men det er kundene som får sluttregningen i form av økt nettleie. Det stilles større krav til nettselskapenes datanettverk som følge av innføring av AMS.

Kraftleverandørene vil få enklere rutiner for leverandørbytte og kan lettere tilpasse produksjonen med tilgang til bedre måledata. Kraftleverandørene får ingen direkte kostnader tilknyttet

innføringen av AMS, men det er forventet å medføre økt konkurranse, slik at fortjenestemarginene blir mindre.

AMS-systemet skal være modulært slik at andre tilleggstjenester skal kunne integreres på et senere tidspunkt. Dette kan for eksempel være alarm- eller sikkerhetstjenester.

AMS er en forutsetning for å installere fremtidens energisystem, der kraftmarkedet, IKT og Internett integreres. Dette kalles ofte Smart Grid. Slike smarte, integrerte systemer vil gjøre det lettere å samarbeide om kraftmarkedet internasjonalt. Videre regner man med færre klagesaker som følge av AMS: Myndighetene kan også regulere forbruket til sluttbrukere når strøm må rasjoneres.

2.2 EU – Open Meter

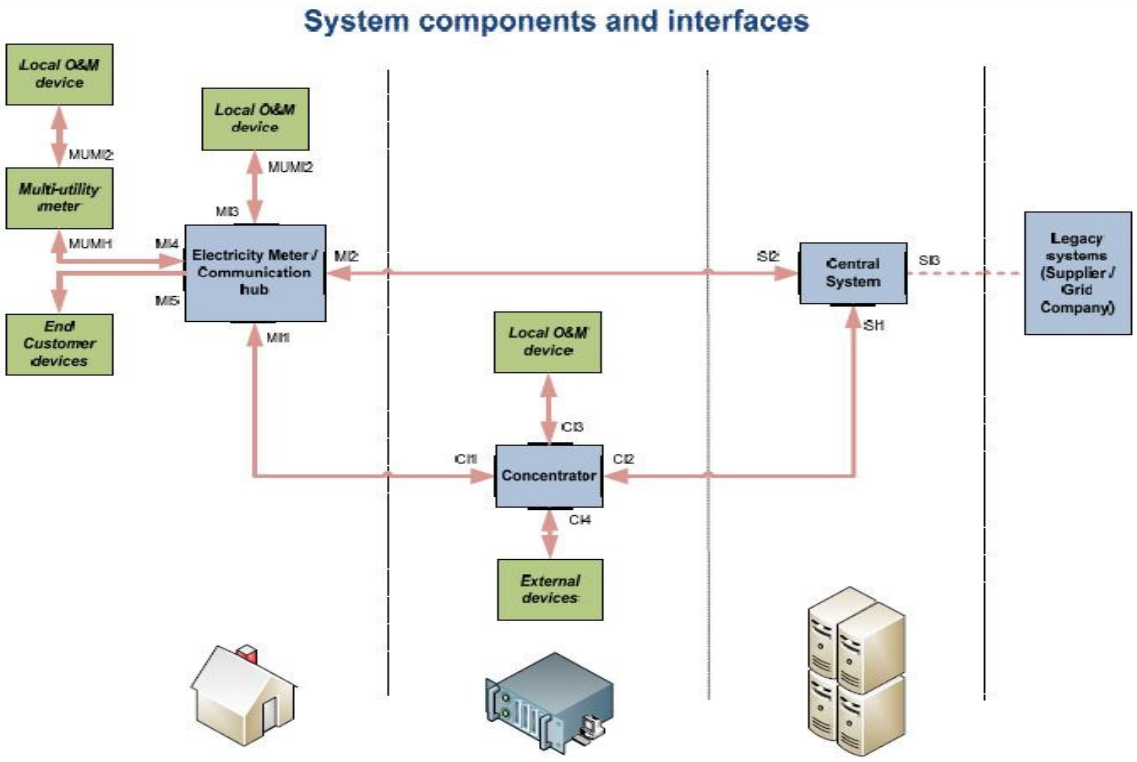
Open Meter er en organisasjon finansiert av den europeiske kommisjon[2] (European Commision, EC) for å komme med anbefalinger i forbindelse med implementering av intelligente strømnett, smarte nett. Den er satt sammen av ulike aktører i forskjellige land. Hovedmålsettingen for Open Meter er å spesifisere et omfattende utvalg av åpne standarder for bruk i Advanced Metering Infrastructure (AMI). Et AMI-system består av en smartmåler (smart meter), et toveis kommunikasjonssystem (infrastructure) og en sentral som bearbeider data. Utenfor denne sentralen styrer nettselskapets datamaskin hele systemet ved hjelp av Automatic Metering Management (AMM). I Norge brukes betegnelsen AMS om AMI- og AMM-systemet. Forløperen til AMI var Automatic Reading Meter (AMR) og kunne bare lese forbruk, d.v.s. enveis kommunikasjon.

Open Meter har som målsetting å bruke flest mulig etablerte standarder innenfor kommunikasjon og målerdrift, men noen må nødvendigvis videreutvikles for å tilpasses AMI. Ved å spesifisere behov, krav, standarder og velge åpne løsninger, ønsker Open Meter å tiltrekke seg mange utstyrsleverandører, slik at det blir en reell konkurranse på pris og ikke på utstyrsspesifikasjonene.

Open Meter jobber i seks arbeidsgrupper (Work package, WP), som publiserer utgivelser dokumenter (Deliverables) på prosjektets hjemmeside [19]. Disse dokumentene er svært omfattende og detaljerte og vil være viktige redskaper for nettselskaper som ønsker å implementere AMS i Norge. De neste delkapitlene vil ta for seg disse arbeidsgruppene og sammenfatter de viktigste punktene i disse dokumentene.

En oversikt over systemet med komponenter og grensesnitt er gitt i Figur 2-2. De enkelte enheter er forklart under figuren og er hentet fra WP-3.1. Denne figuren brukes som referansemodell for alle arbeidsgruppene.

[2] Project Funded by the European Commission under the 7th Framework Programme



Figur 2-2 Open Meter: Oversikt over AMI

Strømmåleren/kommunikasjonsenheten (Electricity meter/Communication hub) er en elektronisk smart-enhet som har to oppgaver: Den registrerer strømforbruk (og annet strømrelatert) og fungerer som en kommunikasjonsenhet for annet utstyr. Som kommunikasjonsenhet har strømmåleren som oppgave å lagre/sende data til det eksterne AMI-nettverket, samt innhente/skrive data til eksterne enheter i bygningen. Den kan fungere som en proxy-server, dvs. at den innhenter data fra andre enheter, lagrer disse og gjør dem tilgjengelige for AMI-systemet ved behov. Den kan også operere som en gateway, der AMI-systemet kan lese av de enkelte målerne direkte, ved behov. Dette siste er kanskje ikke mulig, siden eksterne (batteridrevne) målere pga. strømsparing ikke vil være tilgjengelige hele tiden. De operer i en slags dvaletilstand mellom avlesningene. Derfor vil en proxy-løsning være mest sannsynlig, der måledata bufres for avlesing fra sentralenheten eller konsentrator. Strømmåleren må også ha inngående buffer for å kunne håndtere forespørsler fra det sentrale AMI-systemet.

Konsentratoren (Concentrator) er et element som er plassert mellom elektrisitetsmåleren og sentralenheten (Se fig. 2.2). Denne brukes dersom man bruker strømnettet som kommunikasjonsmedium og er vanligvis lokalisert i transformatorbokser. Hovedoppgaven til en konsentrator er å bygge opp, vedlikeholde og styre PLC-kommunikasjonen med strømmålere, å utveksle data med strømmåleren via grensesnitt CI1 og sentralsystemet via CI2, og evt. tilby data til andre systemer via CI4. Også konsentratoren kan operere som proxy (innsamler av data) eller tilby sentralsystemet direkte tilgang til målerne.

Sentralsystemet (Central System) har ansvaret for styring av all informasjon og datainnsamling i forbindelse med smartmålerne. Den kan også være ansvarlig for all konfigurering, operasjoner,alarmer, hendelser og kontroll av alle systemkomponenter via grensesnittene SI1 og SI2. Sentralsystemet er tilknyttet nettselskapets datanettverk gjennom SI3. Sentralsystemet mottar og utfører handlinger i nettverket igangsatt av netteselskapet datanettverk. Resultatet av

disse operasjonene sendes tilbake sammen med en bekreftelse. Når sentralsystemet mottar et ønske via grensesnitt SI3 må det kunne:

- Oversette kundens (måler-) ID til en nettverksadresse ved å bruke en database over disse rute-sammensetningene, tilgjengelige noder og nettverksarkitektur.
- Oversette nettselskapets kommandoer til en riktig kommandoprotokoll basert på aktuelt grensesnitt og involverte enheter.
- Sende resultater av tidligere handlinger mot nettverket.

Ved innkommende beskjeder og data fra målernettverket, skal sentralsystemet sende disse til nettselskapets datanettverk.

Nettselskapets datanettverk (Legacy system) er ansvarlig for styring av hele AMI-systemet samt kundeportefølje, tariffer, registrering av kunder og maskinvare i systemet. Selve kommunikasjonen med målerne tar sentralnettverket seg av og datanettverket trenger ikke kjenne til denne kommunikasjonen (infrastruktur og protokoller). Kommunikasjonen med sentralsystemet foregår via grensesnitt SI3.

Måle- og vedlikeholdsinstrumenter (Local O&M devices) brukes til å konfigurere, operere og vedlikeholde systemet gjennom forskjellige dedikerte grensesnitt: Strømmåleren bruker MI3, multimetere bruker MUMI2 og konsentratoren CI3. Disse instrumentene kan være av spesielt utviklet til formålet, bærbare PC'er eller PDA'er og kobles til grensesnittene via kabel eller et trådløst system med kort rekkevidde.

Multimetere (Multi-utility meters) brukes i hovedsak i forbindelse med kommunikasjon av de andre målerne i systemet: Vann, gass og varme. Disse er koblet til måleren gjennom MUMI1 og multimetere bruker grensesnitt MUMI2.

Kundeutstyr (End Customer Device) er utstyr kunden kan koble til måleren for å få tilgang til måledata og lastenheter innenfor bygningen. Dette utstyret har ingen innvirkning på AMI-systemet og er tilleggsutstyr. Dette kan brukes til kommunikasjon med forbruker (fra nettselskapet) og også være til hjelp for kunden ved å vise forbruk/pris/tariffer til strømsparing (evt. sparing av gass/varme/vann). Kundeutstyret kobles til måleren gjennom MI5-grensesnittet.

Eksternt utstyr (External Devices) er utstyr tilknyttet konsentratoren. Dette kan være sensorer/systemer og er typisk installert i nærheten av konsentratoren. Dette kan for eksempel være måling av overforbruk og systemet kan da strupe tilgangen av strøm til forbrukere. Kommunikasjonen med eksternt utstyr kan være fast eller trådløst og grensesnitt CI4 brukes.

2.2.1 Arbeidsgruppe 1 – Funksjonelle krav og reguleringsbestemmelser

Denne gruppen er ledet av ENDESA, det største nettselskapet i Spania, og skal definere de tekniske krav som tilfredsstiller reguleringsbestemmelsene i de ulike europeiske land.

Denne gruppen ga ut et dokumentet med tittelen "D1.1 – Report on the identification and specification of functional, technical, economical and general requirements of advanced multimetering infrastructure, including security requirements", den 01.07.2009. [20]

Figur 2-2, viser komponenter og grensesnitt slik det er definert i Open Meter Project.

Dokumentet er delt opp i tre deler: Systemfunksjoner, Generelle krav og Økonomiske krav. Siden denne oppgaven omhandler sikkerhetsanalyse, vil jeg ikke gå inn på den tredje delen: Økonomiske krav.

2.2.1.1 Systemkrav

En oversikt over systemkravene (system Requirements) fra Open Meter er gitt i Tabell 2-1 under. En beskrivelse av tabellen følger etterpå.

Tabell 2-1 - Oversikt over systemkrav fra Open Meter

ID	Beskrivelse	Virkeområde	Kategori
OM-SR-1	Målerregistrering	Måte å inkorporere målere til det fjernbetjente informasjonsnettverket.	Minimum
OM-SR-2	Tariffprogrammering	Måte å fjernprogrammere måleren til å bruke parametere relatert til tariff, kalender og kontraktkraft.	Minimum
OM-SR-3	Måleravlesning (Ved behov)	Måte å innhente avlesning på etter behov.	Minimum
OM-SR-4	Måleravlesning (for fakturering)	Måte å innhente avlesning på for avregning. (Periodisk avlesning).	Minimum
OM-SR-5	Fjernstyrt fra-/tilkobling	Mulighet for å fra- eller tilkoble forbrukeren på en bestemt dato.	Minimum
OM-SR-6	Kraftkontroll	Aktivering eller deaktivering av den krevde kraftkontrollen i målere.	Minimum
OM-SR-7	Klokkesynkronisering	Mulighet til å justere de interne klokkene i målerutstyret.	Minimum
OM-SR-8	Fjernoppgradering av program- og maskinvare.	Mulighet for oppgradering av utstyr fra sentralt hold.	Minimum
OM-SR-9	Håndtering av alarmer og hendelser.	Måte å håndtere hendelser og alarmer gitt av tilkoblet utstyr.	Minimum
OM-SR-10	Avbruddsinformasjon	Måte å motta informasjon om avbrudd.	Minimum
OM-SR-11	Avdekking av svindel	Måte å avdekke svindelforsøk.	Minimum
OM-SR-12	Fjerntilgang til konsentratorer	Mulighet for å fjernbetjene konsentratorene.	Minimum
OM-SR-13	Behandling av lastprofiler	Måte å fjernprogrammere og innhente lastprofiler	Minimum
OM-SR-14	Automatisk tilpasning til endringer i nettverket	Endringer i nettverkets topologi registreres automatisk.	Avansert
OM-SR-15	Målertilgjengelighet	Mulighet for sjekk av kommunikasjon med måleren.	Avansert
OM-SR-16	Energibalanse	Mulighet for å oppnå energibalanse.	Frivillig/Tillegg
OM-SR-17	Lastbehandling	Mulighet for å aktivere/deaktivere kraftkontrollen i visse situasjoner.	Frivillig/Tillegg
OM-SR-18	Styring av kundeenheter	Sende data basert på kundens forbruk av energi.	Frivillig/Tillegg
OM-SR-19	Styring av kvaliteten på kraft	Måte å foreta målinger av kvaliteten på kraften.	Frivillig/Tillegg
OM-SR-20	Forhåndsbetaling	Muliggjøre en funksjonalitet for forhåndsbetaling.	Frivillig/Tillegg

Målerregistrering: Sentralenheten skal automatisk oppdage en ny måler i systemet. Dersom det er konsentrator installert skal denne også bli informert. Sentralenheten skal informeres av nettselskapets datanettverk om at en ny måler installeres. Når sentralenheten er informert om ny måler og har automatisk oppdaget denne, skal den nye måleren gjøres tilgjengelig for operasjon.

Tariffprogrammering: Ulike kundegrupper vil ha ulike tariffer. Parametere for dette bestemmes hos nettselskapene og må kunne skrives/lagres i målerutstyret hos sluttbrukerne. Ved feil i overføringen av tariffparametere må sentralenheten kunne kommunisere med håndholdt utstyr, slik at feilen kan bli rettet.

Måleravlesning (ved behov): Nettselskapets datanettverk (ND) skal kunne lese en måler ved behov. Måler-ID og data returneres. Ved feillesing skal siste lagrede data i konsentrator returneres. Ved feil ved kommunikasjonen skal sentralenheten eller ND kunne kommunisere med et håndholdt instrument koblet til MI3.

Måleravlesning (for fakturering): Nettselskapets datanettverk (ND) setter opp en periode som overføres til sentralenheten. Denne leser periodiske verdier fra konsentrator, som igjen avleser målerne. Dersom noen målere ikke har avgitt nye verdier, skal de foregående verdiene i konsentratoren brukes. Ved feil ved kommunikasjonen skal sentralenheten eller ND kunne kommunisere med et håndholdt instrument koblet til MI3.

Fjernstyrt fra-/tilkobling: Nettselskapet eller kraftleverandøren kan bestemme å koble fra eller til strømmen av forskjellige grunner; Ubetalte regninger, nettvedlikehold, fraflyttet eiendom, ny innflytting eller av sikkerhetsgrunner. Nettselskapets datanettverk (ND) skal derfor kunne frakoble og tilkoble strømmen hos kundene og en dato skal brukes som inndata i denne prosessen. Måleren skal returnere målerverdien til ND. Ved tilkobling kan man bruke grensesnitt MI4 for å koble til en kommunikasjonsenhet, slik at kunden kan bekrefte tilkobling. Ved utkobling skal måleren KUN kunne tilkobles når den får beskjed om det fra ND. Ved feil ved kommunikasjonen skal sentralenheten eller ND kunne kommunisere med et håndholdt instrument koblet til MI3.
Måleren må kunne oppdage feil i denne prosessen og gi beskjed til ND, dersom fra- eller tilkoblingen svikter.

Kraftkontroll: Dersom ND (via sentralenheten) setter måleren i kraftkontroll-modus, kan ND kontrollere mengden kraft forbrukeren får. Strømmen vil da termineres hvis forbrukeren overskrider en viss mengde kraft. Kunden kan selv, manuelt, eller gjennom et tilknyttet panel, sette i gang strømmen igjen. Måleren må kunne registrere alle hendelser i forbindelse med kraftkontroll: Grenseverdi, avkobling og tilkobling. Disse data skal returneres til ND.
Ved feil ved kommunikasjonen skal sentralenheten eller ND kunne kommunisere med et håndholdt instrument koblet til MI3.

Klokkesynkronisering: Sentralenheten skal periodisk (eller etter hendelser) sjekke tid og dato på målerne og synkronisere disse. Ved bruke av konsentratorer skal også disse synkroniseres. Sentralenheten kan da delegere synkroniseringsansvaret til konsentratorene. Et instrument koblet til MI3 skal sjekke tid og dato på måleren før det kan brukes, og synkronisere målerklokken med instrumentet dersom det er avvik.

Fjernoppgradering av program- og maskinvare: Oppgradering må ta hensyn til at lagrede data ikke må endres i prosessen. Oppgraderingen må ha sikkerhetsmekanismer som garanterer at ingen deler av måleren skades. Det er sentralenheten som foretar oppgraderinger og det skal settes en dato for dette. Ved feil ved oppgraderingen skal et håndholdt instrument koblet til MI3 kunne oppgradere måleren.

Håndtering av alarmer og hendelser: Alle enheter koblet til systemet må kunne gi alarmer eller beskjed om hendelser. Disse skal rapporteres til sentralenheten eller ND (via konsentrator om

den finnes). Alarmer og hendelser skal kunne mottas ved krav eller rapporteres automatisk. Følgende alarmer skal rapporteres:

- Kritisk feilfunksjon i måler eller konsentrator.
- Kritisk klokkeavvik.
- Modifisering av data i måleren, særlig knyttet til fakturering og forbruk.
- Programvare- og maskinvareversjoner med nøyaktig tid for installasjon og modifikasjon.
- Bortfall og tilstedeværelse av spenning.
- Uautorisert forsøk på tilgang til enhetene.

Hendelser som skal rapporteres er:

- Kraftkontroll
- Bortfall, planlagte avbrudd.
- Ny oppgradering av enheten(e).
- Påvirkninger.
- Alarmer sendt til forbrukere
- Annet

Avbruddsinformasjon: Måleren skal kunne registrere alle avbrudd og presentere disse for kunden. Disse data skal ikke mistes og må som et minimum inneholde tid, dato og varighet på avbruddet.

Avdekking av svindel: Måleren må kunne oppdage følgende forsøk på manipulasjon: Åpning av måleren, oppgradering av måleren (software) og magnetisk påvirkning. Disse hendelsene skal registreres i måleren og kunne leses av sentralenheten. Systemet skal også tillate at det blir utført en energibalanseringsanalyse slik at svindel i et område kan avdekkes.

Fjerntilgang til konsentratorer: Ved installering av ny konsentrator skal sentralenheten få beskjed fra ND om dette. Sentralenheten skal selv oppdage ny konsentrator og sende data, slik at den kan aktiveres. Ved feil skal sentralenheten eller ND tillate at et instrument kobles til CI3 og oppgraderer konsentratoren. Sentralenheten skal kunne oppgradere og kommunisere med konsentratoren.

Behandling av lastprofiler: En lastprofil viser forbruk over tid og må derfor imøtekomme de enkelte lands begrensninger for datalagring. ND skal kunne legge inn lastprofilene i måleren og kontrollen med lastprofilene gjøres av sentralenheten (via konsentrator om den finnes). ND skal avlese lastprofilene, lagre disse og levere dem til ND ved behov.

Automatisk tilpasning til endringer i nettverket: Systemet bør kunne oppdage nye målere i nettet og ved bruk av konsentratorer bør de kjenne til alle målerne som er tilkoblet. Sentralenheten får beskjed fra konsentratorene ved endringer, eller hvis en annen konsentrator har tatt over målere (fordi en konsentrator har falt ut, vedlikehold o.s.v.) ND oppdateres med den nye topologien fra Sentralenheten.

Målertilgjengelighet: Sentralenheten skal periodisk sjekke om målerne er tilgjengelige, temporært utilgjengelige eller permanent utilgjengelige. Sentralenheten skal utarbeide statistikk på denne bakgrunnen og bruke statistikken slik at den leser måleren når det er størst sjanse for tilgjengelighet. Ved permanent utilgjengelighet skal sentralenheten varsle ND.

Energibalanse: For å kunne bestemme energibalansen til alle målerne koblet til en konsentrator, må sentralenheten/konsentratoren periodisk lese energiforbruket til målerne over tid, samt

forbruket (egen måler) på transformatorstasjonen som forsyner forbrukerne. Informasjonen om energibalansen skal gjøres tilgjengelig for ND.

Lastbehandling: Systemet skal kunne redusere forbruk når det er (lovlig eller nødvendig) behov for dette. ND setter lastverdier og målerne i lastkontrollmodus, via sentralenheten (og eventuelle konsentratorer). Måleren må kunne registrere alle hendelser i forbindelse med kraftkontroll: Grenseverdi, avkobling og tilkobling. Disse data skal returneres til sentralenheten eller ND. Ved feil ved kommunikasjonen skal sentralenheten eller ND kunne kommunisere med et håndholdt instrument koblet til MI3.

Styring av kundeenheter: ND skal (via sentralenheten/konsentratorer) kunne sende beskjeder til målerdisplay eller annet utstyr koblet til MI5. Disse beskjedene kan være markedsinformasjon, informasjon om forbruk, varsel om stenging, varsel om begrensninger i kraftforbruk o.s.v.

Styring av kvaliteten på kraft: Nettselskapet skal garantere forbrukerne en spesifisert kvalitet på den elektriske kraften. Målerne må kunne registrere avvik på den avtalte kvaliteten og rapportere dette til ND.

Forhåndsbetaling: Ved bruk av forhåndsbetaling skal måleren ha et dedikert register som holder rede på kreditten, målt i Wh. (Watt timer). Måleren skal presentere kreditten for forbruker og justere denne kreditten etter forbruket og forhåndsbetaling. Kraftleverandøren har ansvaret for dette og nettselskapet effektuerer avtalen mellom forbruker og kraftleverandør. Sentralenheten (eller konsentratorene) bruker oppgitt kreditt og debet (overforbruk) for å styre tilgangen av kraft til forbrukerne.

2.2.1.2 Generelle krav

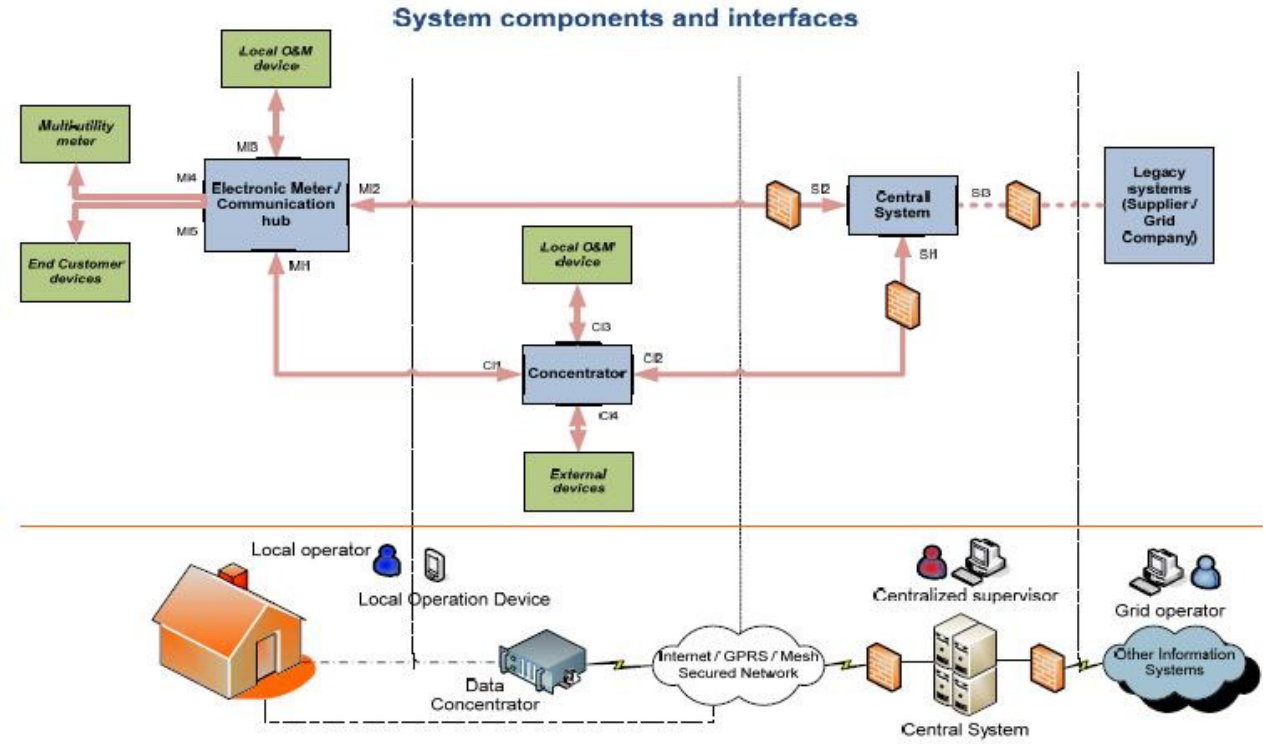
Innen Open Meter opereres det med forkortelser, der generelle krav (General Requirements) er listet på formen OM-GR-X. Alle de generelle kravene er listet i dette kapittelet og dette er kategorisert som minimumskrav, avanserte og frivillige krav.

Management eller styring innen AMI går på aktiviteter, metoder, prosedyrer og verktøy som opprettholder drift, administrasjon og klargjøring av et AMI-system.

Sikkerhet er av avgjørende betydning og EU jobber for tiden med spesielle direktiver angående datasikkerhet i kritiske samfunnsmessige infrastrukturer. AMI er en slik infrastruktur og derfor er også sikkerhet fokusert i alle ledd i et AMI-system. For en operatør av et slikt system er det fare for:

- Tilgang eller endring av informasjon av en uautorisert person.
- Villet handling fra en inntrenger, som modifiserer oppsett eller stenger kundens strømtilgang og dermed setter offentlig helse og tillit i fare.
- Denial of Service (DoS)-angrep på komponenter/systemet som fører med seg et utilgjengelig system og dermed et ustabilt og mindre sikkert system.
- Personvern skal beskyttes i et AMI-system.

Inntrenging kan lage kritiske problemer for kunder og nettselskap og derfor må AMI-systemet beskyttes og tilby sikkerhetsmuligheter for data, nettverk og alle komponenter det består av.



Figur 2-3 Open Meter: Oversikt Systemkomponenter og grensesnitt

Det er ønskelig at det brukes allerede utviklede IT-systemer og ikke gjenoppfinner ny teknologi når det gjelder AMI. Hvert lag i infrastrukturen skal ha sikkerhet, såkalt "dybdeforsvar". Sikkerhetskravene til AMI er i henhold til "Welmec Software Guide 7.2, utgave 3" og er som følger:

Sikkerhetsantagelser:

- Ved fysisk inntrenging i måler eller datakonsentrator skal ikke inntrenging i en enhet få følger for resten av systemet.
- Sensitiv informasjon og kommandoer skal beskyttes strengt.
- Maskinvareenheter skal støtte kryptografiske algoritmer. Enheter bør kunne bruke både symmetriske og asymmetriske algoritmer, men minimum symmetriske. Bruk av anerkjente krypteringsalgoritmer, slike som er innbakt i prosessoren i smartkort, bør overveies, siden de er vanskelige å manipulere.
- Tilgjengelige sikkerhetsstandarder for IT, automatisering og kontroll, skal brukes for hele systemkonseptet og distribusjon av enhetene.

Fundamentale sikkerhetskrav. Et globalt AMI-system skal forhindre:

- Uautorisert tilgang, tyveri eller misbruk av konfidensiell informasjon, dvs. data kan ikke leses eller endres i måleren eller under transport i HELE nettverket.
- Tap av integritet eller pålitelighet av prosessdata og produksjonsinformasjon.
- Tap av systemtilgjengelighet. Dvs. at man skal sikre nettselskapets datanettverk og dataprosessering.
- Invadering og illegale endringer. For eksempel ulovlig programvareoppdatering.
- Oppsett av prosesser som medfører kapasitets- eller funksjonalitetsproblemer.

Identifiserte krav for å imøtekomme de ovennevnte kravene er:

- Tilgangs- og brukskontroll
- Dataintegritet

- Datakonfidensialitet
- Ressurstilgjengelighet

De 22 generelle kravene (General Reqirements) er listet i Tabell 2-2 under:

Tabell 2-2 - Oversikt over generelle krav fra Open Meter

ID	Beskrivelse	Virkeområde	Kategori
OM-GR-1	Systemet må tillate operasjoner, administrasjon og klargjøring gjennom tilgangsmetoder og styringsprotokoller gjennom moderne standarder.	System	Minimum
OM-GR-2	Systemet må være i stand til å autentisere brukere og enheter og må være i stand til å tillate eller avvise disse, men også grupper av brukere og enheter. Dette kravet skal gjelde alle AMI-grensesnitt, dvs. GUI, WAN, andre IT-systemer, Datakonsentrator osv. For å hindre inntrenging i systemet er det nødvendig å sikre at brukere eller utstyr som har tilgang til AMI virkelig er autorisert for tilgang.	System	Minimum
OM-GR-3	Systemet må være i stand til å håndtere tilgangsrettigheter for alle komponentene med en adekvat granularitet (forfinethet). Brukere skal bare bli autentisert og autorisert til de komponentene i systemet de har rettigheter til. Sterk autentisering skal brukes til kritiske kommandoer, som for eksempel stenging av strøm.	System	Minimum
OM-GR-4	Systemet må være i stand til å garantere dataintegritet over alt der det er påkrevet. Det er nødvendig å forsikre at data ikke er modifisert eller kompromitert av utenforstående ved kommunikasjon eller lokal tilgang av disse data. Dette kan løses ved hash-funksjon eller symmetriske og asymmetriske algoritmer.	System	Minimum
OM-GR-5	Utstyret skal tilby funksjonalitet for å kunne lagre data og krypteringsnøkler konfidensielt.	System	Minimum
OM-GR-6	Utstyret skal tilby funksjonalitet for å sørge for integritet av lagrede data og programvare for utstyret (firmware).	System	Minimum
OM-GR-7	Systemet og utstyret skal tilby funksjonalitet som hindrer avlytting. Systemet må være i stand til å kryptere kommunikasjonen med de beste krypteringsalgoritmene som er tilgjengelig, slik at konfidensialiteten ivaretas.	System	Minimum
OM-GR-8	Systemet skal være i stand til å avverge at tidligere kommandoer blir tatt opp og brukt igjen. (Message replay). Dette for å forhindre at noen bruker kritiske kommandoer (som stenging av strøm) om igjen. Dette løses ved å bruke kryptering og tid eller nummerering for å identifisere at kommandoen er unik.	System	Minimum

OM-GR-9	Kringkastede (Broadcast) kommandoer skal gjøres på en sikker måte. Disse kommandoene får større virkninger i AMI, siden de berører mange komponenter samtidig. Derfor må slike kommandoer ha gode mekanismer for autentisering, integritet og hindre bruk av opptak.	System	Minimum
OM-GR-10	En overvåkning av systemet bør være mulig slik at unormale hendelser oppdages og en automatisk reaksjon til disse iverksettes. Det er ønskelig at unormale hendelser oppdages når systemet svikter, eller at systemet blir påvirket til feil. For eksempel hvis flere enn et gitt antall frakoblingskommandoer gis innen et gitt antall minutter, så bør systemet si fra om dette.	System	Avansert
OM-GR-11	Utstyret skal tilby funksjonalitet for håndtering av nøkler. Krypteringsnøkler må bli håndtert slik at de kan genereres, byttes, lagres, brukt og erstattet på en sikker måte.	System	Minimum
OM-GR-12	Fysisk tilgang til utstyret skal være vanskelig. Utstyret må være i stand til å oppdage fysisk inntrenging og gi alarm ved unormale hendelser.	System	Minimum
OM-GR-13	Alle ubrukte fysiske grensesnitt på utstyret skal være stengt i utgangspunktet. Av sikkerhetsgrunner bør det være mulig å styre disse grensesnittene, slik at de ikke kan brukes hvis ikke de er åpnet sentralt.	System	Frivillig (Avansert)
OM-GR-14	Forsøk på å få tilgang til et lokalt grensesnitt for vedlikehold blir logget og dette grensesnittet skal automatisk kobles ut en gitt tid. Feil autentisering resulterer dermed i at denne lokale porten blir stengt en viss tid.	System	Avansert
OM-GR-15	Etablerte standarder for IT-teknologi og Automasjonssystemer skal brukes for å lage sikre AMI-systemer. Standarder fra ISO, IEC, NIST, NERC, ISA, IETF og IEEE skal brukes overalt der det er mulig.	System	Minimum
OM-GR-16	Bruk av sertifikater for å muliggjøre funksjoner er sterkt anbefalt. Bruk av sertifikater muliggjør sikkerhetstjenester som autentisering, integritet, konfidensialitet, tidsstempling og feil avsender (repudiation).	System	Minimum
OM-GR-17	Alle deler av nettverket må være under kontroll, overvåkning og administrasjon. Av sikkerhetsgrunner er det viktig å bruke etablert teknologi for å kunne gjøre dette.	System	Minimum
OM-GR-18	Interoperabilitet er svært viktig i AMI. Det er særlig et krav i grensesnittene MI1, MI2 og MI4.	System	Minimum
OM-GR-19	AMI-systemet skal være robust på den måten at det skal ha maksimal tilgjengelighet, pålitelighet og feiltoleranse. Det skal også være i stand til å automatiske reorganisere seg når det skjer endringer i topologien.	System	Minimum

OM-GR-20	AMI-systemet skal være skalerbart, fleksibelt og kunne oppgraderes ved at det er enkelt å legge til nytt utstyr, nye lagringsmuligheter og ny topologi.	System	Minimum
OM-GR-21	Det er viktig å velge utstyr og løsninger som reduserer vedlikehold. Det meste av vedlikeholdet skal skje automatisk og fjernstyres, slik at det manuelle vedlikeholdet er minimalt.	System	Minimum
OM-GR-22	AMI-systemets design og implementering skal gi best mulig ytelse.	System	Minimum

2.2.1.3 Funksjonelle krav

Følgende definisjoner av ord er brukt i dette delkapitlet:

- Tidsstempling: Indikerer et tidspunkt på formatet ÅÅÅÅ-MM-DD H24:min:sek
- Produksjons-ID: Alt utstyr som lages har en unik identifikasjon. Denne id'en er en del av utstyrets konfigurasjonsinformasjon.
- Målerdata: Målerdata er data som er produsert med en viss frekvens og avlest fra målere for strøm, gass, vann og varme.

Denne arbeidsgruppen har satt opp 200 funksjonelle krav. De fleste av disse kravene går på spenningsnivå, måledata, avlesningshyppighet, andre målere og fakturering. De kravene som går på sikkerhet, direkte eller indirekte, er tatt med i Tabell 2-3.

Tabell 2-3 - Funksjonelle krav (Functional Requirements) fra Open Meter

ID	Beskrivelse	Virkeområde	Kategori
OM-FR-1	Smartmåleren må avvise ulovlige forespørsler og gi en feilmelding.	Smartmåler	Minimum
OM-FR-8	Strømmåleren skal ved periodisk avlesning, kunne gi indikasjon dersom det er registrert feil eller svindelforsøk .	Strømmåler	Minimum
OM-FR-10	Strømmåleren skal gi feilmelding om det ikke er registrert måleravlesning fra smartmåleren innen de siste n timene, der n kan konfigureres.	Strømmåler	Minimum
OM-FR-25	Alt målerutstyr skal oppdage forsøk på fysisk inntrenging.	Smartmåler	Minimum
OM-FR-26	Alt målerutstyr skal oppdage forsøk på magnetisk påvirkning, hvis de kan påvirkes av magnetisme.	Smartmåler	Frivillig
OM-FR-27	Målerutstyr skal tilby et konfigurerbart antall oppdagede forsøk på manipulering.	Smartmåler	Minimum
OM-FR-28	Smartmåleren skal tilby funksjonalitet for å fjernbetjene fra- og tilkobling på en spesfisert dato og tid.	Strømmåler	Minimum
OM-FR-29	Den elektriske bryteren som brukes til fra- og tilkobling skal ikke kunne betjenes manuelt.	Strømmåler	Minimum

OM-FR-30	Strømmåleren skal lagre loggeinformasjon for hver fra- og tilkobling.	Strømmåler	Minimum
OM-FR-31	Strømmåleren skal tilby loggeinformasjon for et konfigurerbart antall fra- og tilkoblinger.	Strømmåler	Minimum
OM-FR-32	Strømmåleren skal gi en logisk feilmelding om fra- eller tilkobling ikke kunne gjøres angitt dato.	Strømmåler	Minimum
OM-FR-33	Strømmåleren skal tilby en funksjonalitet som gjør at det er mulig å sette en grense på maksimalt effektuttak. Ved en CLEAR-kommando går måleren tilbake til vanlig operasjon.	Strømmåler	Minimum
OM-FR-34	Strømmåleren skal logge hendelser der grensen settes eller fjernes.	Strømmåler	Minimum
OM-FR-35	Strømmåleren skal automatisk koble inn ”Use case 9: (Dis)connect E”, hvis effektgrensen overskrides.	Strømmåler	Minimum
OM-FR-36	Strømmåleren skal tilby funksjonalitet til kunden slik at det er mulighet å manuelt koble seg til strømnettet igjen.	Strømmåler	Minimum
OM-FR-43	Strømmåleren skal tilby funksjonalitet til å fremvise standardbeskjeder.	Strømmåler	Minimum
OM-FR-44	Dersom MI5-grensesnittet er tilgjengelig skal strømmåleren tilby funksjonalitet for å presentere ferdigdefinerte beskjeder til kundens utstyr.	Strømmåler	Minimum
OM-FR-45	Dersom MI5-grensesnittet er tilgjengelig skal strømmåleren tilby funksjonalitet for å kunne motta lange beskjeder.	Strømmåler	Minimum
OM-FR-46	Dersom MI5-grensesnittet er tilgjengelig skal strømmåleren tilby funksjonalitet for å kunne videresende lange beskjeder til kundens utstyr.	Strømmåler	Minimum
OM-FR-56	Produsenten av programvare til utstyret, firmware, skal tilby dokumentasjon til hvert leverte produkt.	Strømmåler, kommunikasjonsenhet, smartmåler, konsentrator	Minimum
OM-FR-57	Utstyret skal tilby funksjonalitet for å kunne laste opp ny programvare.	Strømmåler, kommunikasjonsenhet, smartmåler, konsentrator	Minimum
OM-FR-58	Utstyret skal kunne kjøre den nye programvaren til en gitt dato og tid. Dersom dato ikke er oppgitt, skal oppgraderingen kjøres øyeblikkelig.	Strømmåler, kommunikasjonsenhet, smartmåler, konsentrator	Minimum
OM-FR-59	Utstyret skal gi en logisk feilmelding om den nye programvaren er ufullstendig eller inneholder feil.	Strømmåler, kommunikasjonsenhet, smartmåler, konsentrator	Minimum
OM-FR-60	Utstyret skal logge informasjon om installasjonen av den nye versjonen (av programvaren) var vellykket.	Strømmåler, kommunikasjonsenhet, smartmåler, konsentrator	Minimum

OM-FR-61	Ny programvare skal ikke resultere i modifikasjon eller fjerning av måledata, konfigurasjonsparametre eller andre operasjonelle parametere i utstyret.	Strømmåler, kommunikasjonsenhet, smartmåler, konsentrator	Minimum
OM-FR-62	En oppgradering i målerinstrumentene skal ikke influere på de målertekniske bestanddelene av instrumentene.	Strømmåler, kommunikasjonsenhet, smartmåler, konsentrator	Minimum
OM-FR-63	Utstyret skal logge at en ny versjon av programvaren ble gjennomført.	Strømmåler, kommunikasjonsenhet, smartmåler, konsentrator	Minimum
OM-FR-64	Utstyret skal tilby en funksjonalitet for selv-sjekk og sende resultatet videre.	Strømmåler, kommunikasjonsenhet, smartmåler, konsentrator	Minimum
OM-FR-65	Utstyret skal forkaste den nye versjonen av programvaren om den ikke er komplett eller har feil.	Strømmåler, kommunikasjonsenhet, smartmåler, konsentrator	Minimum
OM-FR-66	Utstyret skal tilby funksjonalitet for selv-sjekk og presentere resultatet på det lokale grensesnittet.	Strømmåler	Minimum
OM-FR-67	Strømmåleren skal ha en standardisert lokal port for installasjon og vedlikehold (MI3).	Strømmåler	Minimum
OM-FR-76	Hvis grensesnitt MI4 er tilgjengelig skal strømmåleren tilby funksjonalitet for å kunne identifisere andre komponenter som er tilkoblet gjennom MI4	Strømmåler	Minimum
OM-FR-96	Strømmåleren eller smartmåleren som bruker batterier skal være i stand til å bestemme gjenværende levetid for disse.	Strømmåler, smartmåler	Frivillig
OM-FR-97	Ved installasjon skal tidspunktet for batterialarm kunne konfigureres.	Strømmåler, smartmåler	Frivillig
OM-FR-98	Smartmåler som bruker batterier skal gi en normal feilmelding når levetiden når en angitt terskel.	Smartmåler	Frivillig
OM-FR-111	Konsentratoren skal være i stand til å håndtere minst 3000 endepunkter.	Konsentrator	Minimum
OM-FR-117	Konsentratoren skal tilby funksjonalitet for å kunne hente ut konsentratorens konfigurasjon.	Konsentrator	Minimum
OM-FR-118	Konsentratoren skal tilby funksjonalitet for å kunne hente ut konsentratorens operasjonelle parametere.	Konsentrator	Minimum
OM-FR-119	Konsentratoren skal tilby logginformasjon og feilmeldinger i et gitt intervall.	Konsentrator	Minimum
OM-FR-120	Konsentratoren skal lagre all interaksjon med eksternt utstyr.	Konsentrator	Minimum
OM-FR-121	Konsentratoren skal tilby nok informasjon fra interaksjonen slik at loggeinformasjonen kan tolkes.	Konsentrator	Minimum

OM-FR-122	Konsentratoren skal automatisk foreta en selv-sjekk når strømmen kommer tilbake etter strømbrudd.	Konsentrator	Minimum
OM-FR-128	Konsentrator som bruker batterier skal være i stand til å bestemme gjenværende levetid på batteriene.	Konsentrator	Frivillig
OM-FR-129	Konsentratorer som bruker batteri skal sende en logisk feilmelding når forventet levetid er mellom 1,5 og 2,5 år.	Konsentrator	Frivillig
OM-FR-130	Konsentratorutstyret skal verifisere at kommunikasjonskanalene som er tilkoblet er tilgjengelige for bruk.	Konsentrator	Minimum
OM-FR-131	Konsentratorutstyret skal gi en logisk feilmelding hvis en kanal i nettverket er utilgjengelig.	Konsentrator	Minimum
OM-FR-132	Konsentratoren skal indikere om selv-sjekk lyktes eller mislyktes.	Konsentrator	Minimum
OM-FR-133	Konsentratorutstyret skal tilby funksjonalitet for å kunne avgjøre om utstyr er tilkoblet direkte eller indirekte.	Konsentrator	Minimum
OM-FR-134	Konsentratorutstyret skal tilby funksjonalitet som rapporterer hva slags utstyr som er tilkoblet og styrt av den.	Konsentrator	Minimum
OM-FR-138	Konsentratorutstyret skal tilby funksjonalitet som informerer smartmåleren at den er autorisert til å styre smartmåleren.	Konsentrator	Minimum
OM-FR-139	Konsentratorutstyret skal tilby funksjonalitet for å kunne registrere egen utstyrs-ID.	Konsentrator	Minimum
OM-FR-140	Konsentratorutstyret skal tilby funksjonalitet for å registrere utstyr den håndterer.	Konsentrator	Minimum
OM-FR-141	Konsentratorutstyret skal tilby funksjonalitet for å avregistrere utstyr den håndterer	Konsentrator	Minimum
OM-FR-145	Utstyr skal logge all aktivitet som endrer tilstanden til utstyret.	Strømmåler, smartmåler, konsentrator	Minimum
OM-FR-148	Utstyret skal gi feilmelding dersom programvaren inneholder feilfunksjon.	Strømmåler, smartmåler, konsentrator	Minimum

2.2.1.4 Tekniske krav.

Tabell 2-4 gir en oversikt over noen av de 80 tekniske kravene som arbeidsgruppe 1 (WP-1) har listet opp i sine dokumenter. De kravene som er listet i tabellen er relatert til sikkerhet, direkte eller indirekte og til NVEs høringsnotat.

Tabell 2-4 - Tekniske krav fra Open Meter

ID	Beskrivelse	Virkeområde	Kategori
OM-TR-1	Effektforbruket i målere som går på batterier skal minimeres.	Smartmåler	Minimum
OM-TR-2	Utstyr med kommunikasjonsgrensesnitt MI2 eller CI2 må ha en strømforsynings-backup slik at alarm kan sendes ved strømbortfall.	Strømmåler, konsentrator	Avansert
OM-TR-3	Målerinstrumentene skal være immune mot påvirkning fra vanlige magnetiske felt.	Smartmåler	Minimum
OM-TR-4	Målerinstrumentene skal avgi alarm hvis de blir utsatt for magnetiske feilt som kan påvirke dem.	Smartmåler	Frivillig
OM-TR-6	Den målertekniske funksjonaliteten av målerinstrumentet skal ikke forstyrres av strømforstyrrelser.	Smartmåler	Minimum
OM-TR-16	Tilvirkere av utstyr skal tilby resultater av effekten av feil som kan oppstår. (Failure Mode Effect Analysis – FMEA).	Strømmåler, smartmåler, konsentrator	Frivillig
OM-TR-18	Utstyr levert av forskjellige produsenter skal være interoperatibelt.	Strømmåler, smartmåler, konsentrator	Minimum
OM-TR-19	Utstyret skal tilby funksjonalitet for å unikt kunne identifisere kilden til datakommunikasjonen over egne grensesnitt.	Strømmåler, smartmåler, konsentrator	Minimum
OM-TR-20	Utstyret skal tilby funksjonalitet for å autorisere tilkobling til et gitt grensesnitt.	Strømmåler, smartmåler, konsentrator	Minimum
OM-TR-21	Alle kommunikasjonsgrensesnitt skal deaktivere protokoller som ikke trengs i kommunikasjonen med annet utstyr	Strømmåler, smartmåler, konsentrator, lokalt testutstyr.	Minimum
OM-TR-22	Alle kommunikasjonsgrensesnitt skal takle uautorisert kommunikasjon uten at det skal gå ut over utstyret ellers.	Strømmåler, smartmåler, konsentrator	Minimum
OM-TR-23	Utstyret skal tilby funksjonalitet for å rapportere tap av integritet i datalager eller utstyrets programvare.	Strømmåler, smartmåler, konsentrator	Minimum
OM-TR-24	Utstyret skal tilby funksjonalitet som sikrer at kun autorisert og autentisert registrering og avregistrering av målere kan skje.	Smartmåler	Minimum
OM-TR-25	Endring/utskifting av en enhet til en av konsentratorens grensesnitt må oppdages, logges og en alarm må sendes til sentralenheten.	Konsentrator	Minimum
OM-TR-26	Alle ubrukte Konsentrator-grensesnitt er deaktivert i utgangspunktet utenom vedlikeholdsgrensesnittet.	Konsentrator	Minimum

OM-TR-27	Disse (se over) deaktiverte grensesnittene kan aktiveres ved å gå inn på vedlikeholdsgrensesnittet og endre konfigurasjonen.	Konsentrator	Minimum
OM-TR-28	Hvis enheten er passordbeskyttet må passordet for tilgang til konsentratorens grensesnitt være minst 8 tegn.	Konsentrator	Minimum
OM-TR-30	Kommunikasjonsgrensesnitt i konsentratoren som blir åpnet lokalt, må deaktiveres etter en konfigurerbar tid.	Konsentrator	Minimum
OM-TR-39	Det å installere en smartmåler skal gjøres innen en begrenset tidsfrist.	Smartmåler	Frivillig
OM-TR-77	Kommunikasjonsutstyr som bruker IP-adresser må støtte dynamisk tildeling av IP-adresser.	Konsentrator	Minimum

2.2.1.5 Kommunikasjonskrav

Tabell 2-5 gir en oversikt over noen av de 26 kommunikasjonsmessige kravene (Communication Requirements) som arbeidsgruppe 1 (WP-1) har listet opp i dokumentet D-1. De kravene som er listet i tabellen er relatert til sikkerhet, direkte eller indirekte og til NVEs høringsnotat.

Tabell 2-5 - Kommunikasjonskrav fremsatt av Open Meter

ID	Beskrivelse	Virkeområde	Kategori
OM-CR-1	Strømmåleren/kommunikasjonsenheten må ha enten et PLC eller et trådløst grensesnitt.	Kommunikasjon	Minimum
OM-CR-2	PLC-teknologien må være i stand til å adressere minst 3000 endepunkter.	Kommunikasjon	Minimum
OM-CR-3	PLC må ha en båndbredde på minst 2400 bps for å ha pålitelig kommunikasjon.	Kommunikasjon	Minimum
OM-CR-14	Smartmåleren skal ha et IP-basert trådet eller trådløs grensesnitt.	Kommunikasjon	Frivillig
OM-CR-20	Smartmåleren skal ha et enveis grensesnitt til kundens utstyr.	Kommunikasjon	Frivillig
OM-CR-21	Et IP-basert grensesnitt skal brukes i konsentrator.	Kommunikasjon	Minimum
OM-CR-21	Kommunikasjonen mellom eksterne målere og smartmåleren må optimaliseres for å maksimere batterilevetiden til de eksterne målerne.	Kommunikasjon	Minimum

2.2.2 Arbeidsgruppe 2 – Identifisere svakheter i kunnskap og teknologi

Denne arbeidsgruppen er ledet av Current Technologies International, et Sveitsisk firma som driver med utvikling, produksjon og salg av kommunikasjonsutstyr. Disse skal gjennomgå dagens teknologi, identifisere svakheter og foreslå den beste kommunikasjonsløsningen for AMI. Den skal også foreslå forskningsområder der det er mangler med teknologi eller kunnskap.

Denne arbeidsgruppen har delt opp arbeidet i flere utgivelser [19], der D2.1 (overview) gir en oversikt over arbeidet i gruppen. Videre har D2.1 (i flere deler, part1-4) en oversikt over aktuelle teknologier. Det blir en oppsummering av disse først, der det vektlegges de teknologiene som D2.2 (se under) anbefaler.

D2.2 gir en anbefaling av tilgjengelige teknologier og foreslår generelle krav, protokoller og datastrukturer. Denne utgivelsen, med henvisninger til D2.1 og D2.3, vil bli brukt som ramme for dette kapittelet.

D2.3 kommer med forslag om forskningsbehov, men det blir ikke referert fra dette dokumentet.

Dokumentet D2.2 inneholder det som er relevant for denne masteroppgaven, mens D2.1 består av bakgrunnsstoff for D2.2. Kapittel 2.2.2.1 og kapittel 2.2.2.2 må derfor ses på som en oversikt over teknologiene og en forklaring til at Open Meter har tatt de valgene som ble gjort. Disse to kapitlene kan være nyttig lesing for nettselskap som ønsker å gå utenom Open Meters anbefalinger.

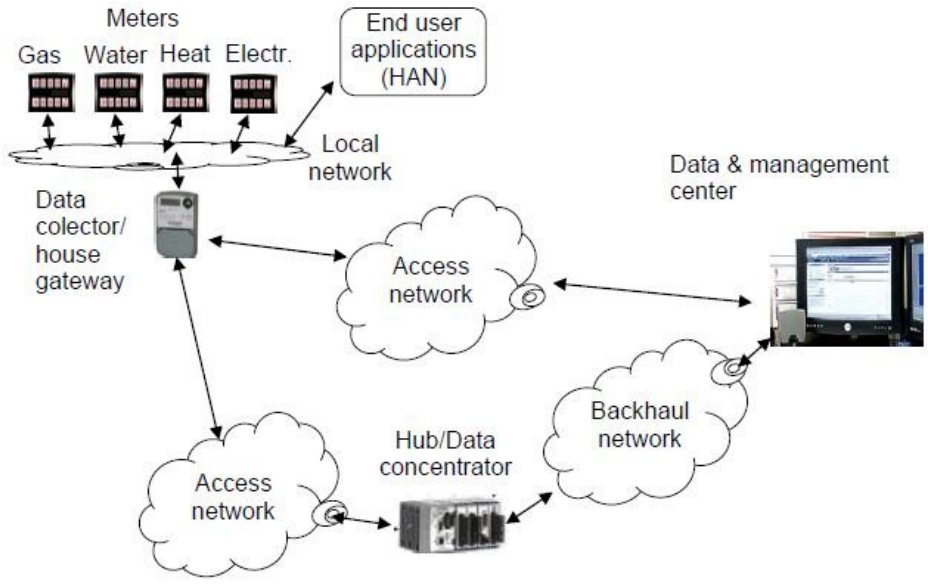
De fleste lesere kan gå direkte til kapittel 2.2.2.3 uten at forståelsen for arbeidet og konklusjonene i denne masteroppgaven vil lide.

2.2.2.1 Oversikt over tilgjengelig teknologi (D2.1)

AMI-arkitekturen kan deles inn i tre deler:

- Lokalt nettverk.
- Tilgangsnettverk. (access network)
- Tilknyttende nettverk (backhaul network).

Se Figur 2-4.



Figur 2-4 – Open Meter: Oversikt over nettverk

Det lokale nettverket knytter sammen AMI-målere og annet utstyr hos forbrukeren. Dette utstyret kan være koblet til et såkalt HAN-nettverk (Home Area Network).
Tilgangsnettverket knytter sammen forbrukerens kommunikasjonsenhet (Gateway) med konsentrator eller datasenteret (om systemet ikke har konsentrator).
Det tilknyttende nettverket kobler sammen konsentrator med datasenteret. (Data & Management Center).

Det lokale nettverket bruker typisk følgende teknologier:

• Euridis bus (IEC 62056-31 standard) over tvinnede par.
• M-bus (Meter bus), (EN13757 Series standard) over tvinnede par eller radio.
• D-bus (Dialogue bus) for store fasiliteter
• Ibus EIB (ABB).
• RS-485 over tvinnede par med standard eller proprietære protokoller.
• Echelon LONworks (ANSI/CEA-709.1) over proprietære kraftlinjer, tvistede par eller radio.
• Ethernet.

Tilgangsnettverket (access) kan bestå av følgende teknologier:

• ZigBee basert på IEEE 802.15.4 MAC & PHY som operer på ulisensierte 2.4 GHz
• WiFi/PWLAN basert på IEEE 802.11 som operer i 2.4 GHz eller 5 GHz båndet.
• Proprietære eller industrielle radio standarder som for eksempel operer i VHF- ellerr UHF-båndet. (174 MHz, 433 MHz, 868 MHz) for eksempel Plextek såkalte Ultrasmalt Bånd (UNB-telemetri).
• ,Offentlige mobilnett, 2G GSM/GPRS
• Proprietær eller industriell standard kraftlinjekommunikasjon, lik løsninger basert på Echelon LONworks (ANSI/EIA-709) eller Intellon/homePlug, osv.
• Analoge modem standarder over PSTN (vanlig telefonlinje) eller xDSL (datalinje).

Tilknyttende nettverk (backhaul) bruker vanligvis:

• Offentlig tilgjengelige mobilnett (2G GSM/GPRS, 3G UMTS)
• Kjernteknologi fra mobilnett om dette brukes.
• Proprietær eller industriell standard kraftlinjekommunikasjon
• Mikrobølger.
• WiMAX IEEE 802.16
• Analoge modem standarder over PSTN or xDSL

Trådløse løsninger er alltid mest attraktivt å ta i bruk, siden dette forenkler installasjonsprosessen (og dermed gjør den billigere). Dette kan ikke brukes overalt, siden svært mange bygninger har montert målerne i en betongkjeller som har dårlige forutsetninger for trådløs kommunikasjon. PLC (Power Line Communication) er en teknologi som heller ikke trenger ny kabling, men trenger en del investeringer, siden teknologien er lite brukt.

Av proprietære trådløse teknologier nevnes Wavenis, Plextek (UNB) og Everblu. Siden EU ønsker mest mulig åpne standarder, går jeg ikke inn på de tekniske spesifikasjonene på disse teknologiene.

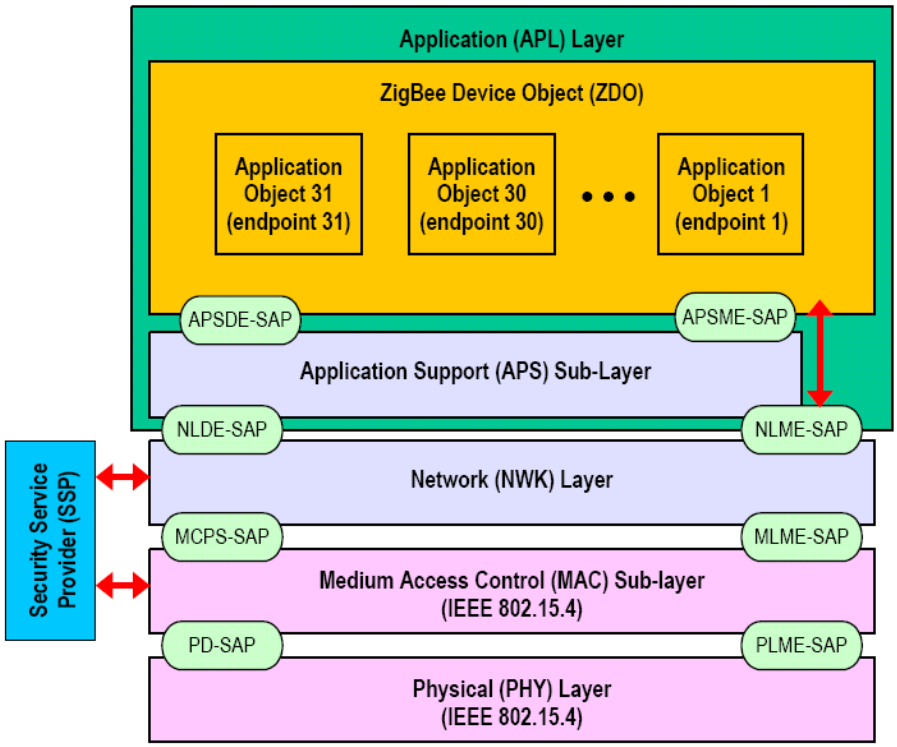
Av åpne trådløse standarder har vi:

- IEEE 802.15.1 (Blåtann): Åpen standard for datautveksling mellom enheter på kort avstand. Disse bruker radiosignaler (og er dermed ikke avhengig av fri sikt). Deles inn i forskjellige klasser etter rekkevidde: Klasse 1: 1 meter. Klasse 2: 10 meter. Klasse 3: 100

meter. Teknologien (den siste versjonen) er svært avansert og har innebygde mekanismer for kryptering, fornying av passord, informasjon om enhetene, automatisk opprettelse av sikker kommunikasjon osv.

- IEEE 802.15.4 (Wireless Personal Area Network, WPAN): Denne standarden spesifiserer det fysiske laget og Media Access Control- (MAC) laget for WPAN med lav datarate. Kommunikasjonsradiusen er på 10-75 meter og raten er på 250 kbps. Standarden definerer ikke et nettverkslag og kan derfor ikke brukes til ruting direkte, men kan løses med et ekstra lag. Også sikkerhet løses med øvre lag, som da kan bruke nøkler for kryptering. Denne protokollen er basis for ZigBee, 6loWPAN, WirelessHART eller MiWi, som definerer de øvre lag.

- ZigBee: Dette er en kommunikasjonsprotokoll basert på punktet over (IEEE 802.15.4) og har mange egenskaper som er ideelle for målere: Lave kostnader, lavt effektforbruk, selvhelende egenskaper, selvkonfigurerende og interoperabilitet mellom ZigBee-enheter.



Figur 2-5 -OM: ZigBee kommunikasjonsprotokoll

Av figuren over går det frem at ZigBee definerer de øverste lagene (NWK og APS) i protokollen og også selve applikasjonsobjektene (ZDO).
Nettverkslaget (NWK) kan etablere nye nettverk, bli med/melde seg ut av et nettverk, konfigurere nye enheter, gi adresser til nye ZigBee-enheter, synkronisere nettverket, kryptere/dekryptere data med AES, og rute data til riktig mål.
Applikasjonsstøtten (APS) binder sammen NWK og ZDO, samt støtter sikker kommunikasjon og definerer rollen ZigBee-enheten skal ha i nettverket.
ZDO er program som er spesielt utviklet tilpasset miljøet ZigBee skal operere i: Styring av hjemmeunderholdning, overvåking av enheter og smartmålere. Det utvikles stadig nye anvendelsesområder.

- 6loWPAN: (IPv6 over laveffekts WPAN). Dette er en standard utarbeidet av IETF og optimaliserer IVv6 til bruk med teknologier som IEEE 802.15.4, WPAN). Optimaliseringen

går ut på at hodet i datagrammet komprimeres. IP-protokollene/lagene er basert på en robust, utprøvd teknologi og dette gjør 6loWPAN attraktiv. Merk at ZigBee ikke er en direkte konkurrent til denne standarden, fordi ZigBee kan brukes som øverste laget i OSI-modellen. (Også kalt IP-modellen).

- IEEE 802.11 (WLAN, WiFi): WLAN er blitt svært populært med årene og tilbyr de samme tjenestene som et trådet nettverk (LAN). Disse operer i 2,4 GHz- og 5 GHz-båndet og har høy bitrate. Dette er en utprøvd teknologi som nå tilbyr gode krypteringsløsninger. WLAN er installert mange offentlige steder, men også her kan det oppstå problemer med AMI som er montert i kjellere, pga. dårlig signaltilgang.
- IEEE 802.16 (WiMAX): Dette er en bredbåndsstandard som skal kunne overføre data opptil 72 Mbps begge veier og kunne kommunisere over fra noen få km (ved hindringer) til 50 km (ved fri sikt). Den skal selv kunne justere dataoverføringshastigheten, der det er nødvendig. Standarden ble utviklet som en konkurrent til den trådete teknologien xDSL. Systemet har visse svakheter i forbindelse med frekvensområdet det jobber under og er heller ikke særlig utbygd. Det anbefales ikke brukt i et AMI-system dersom det ikke allerede er tilgjengelig.
- 2G/2,5G GSM/GPRS/EDGE: I Europa er bebodde områder nær dekket med 100 % av denne mobilteknologien. Overføringshastigheten er mellom 9,6 kbps (2G) til 237 kbps (2,5G) og er derfor velegnet for AMI. AMI er ikke særlig båndbreddekrevende. Også her kan det være problemer å nå målere i kjellere slik at selve mobilkommunikasjonsenheten må plasseres over kjellernivå. Man må da strekke kabel eller bruke et innendørs trådløst system for å nå måleren i kjelleren. Dette er et utbygd og velprøvd system som ikke krever investeringer i infrastruktur.
- 3G UMTS: En videreutviklet mobilteknologi som ikke er helt utbygd, men som tilbyr raskere overføringshastigheter og er utviklet med henblikk på datatransport. UMTS som operer i 2 GHz-båndet var liten gjennomslagsevne for signalene og har dermed de samme problemene som over når det gjelder signaltilgang i kjellere.
- 4G LTE: En ny standard som er IP-basert og vil gi enda høyere båndbredde. Eksisterer bare i noen få større byer.
- Satellittsystemer: Det finnes selskaper som tilbyr toveis satellittkommunikasjon med lav båndbredde. Dette kan brukes der ingen annen kommunikasjon er mulig.

Av vanlige (trådete) teknologier har vi:

- PSTN (Public Switched Telephone Network): Telefonnettverkene har utviklet seg til å bli digitale og kan tilby svært høye overføringshastigheter ved bruk av telefonlinjer. Ved å bruke modem på disse kan data overføres mellom nesten alle europeiske hjem og nettselskapet. Ulempen er at kunden må betale for bruken av linjen mens modemet er i bruk.
- xDSL: Denne teknologien bruker også telefonlinjer, men bruker andre frekvenser enn et vanlig digitalt PSTN, slik at båndbredden er større. Svært mange brukere er tilknyttet ADSL og har dermed allerede en nettverkstilgang. ADSL kan i dag ikke støtte forbindelser fra punkt til multipunkt. (Båndbredde kan ikke deles mellom to ADSL-modemer, der det ene er dedikert til AMI). En enhet som kan dele tilgangen mellom forbruker og AMI må derfor utvikles.
- FTTB, FTTH: Dette er fiberteknologi som gir optisk kommunikasjon direkte til bygningene eller hjemmet. Det finnes en del på større steder.
- M-Buss (Meter-Bus): Dette er en europeisk standard spesielt utviklet for å kommunisere med enkeltmålere og sensorer. Bussen kan også gi strøm til enheten den kommuniserer med. Den er spesielt utviklet for bruk med målere og fokus har vært enkel installasjon og lite strømforbruk.

PLC (PowerLine Communication) er også en trådet teknologi, men står i en særstilling, siden den er tilgjengelig i alle bygninger der AMI-målere skal installeres. Det eksisterer en del proprietære og åpne standarder for PLC. PLC deles gjerne inn i smalbånd (148,5 KHz) og bredbånd (2-30 MHz), der kun smalbåndsbruk er vanlig akseptert hos nettselskapene. Et problem som kan oppstå med PLC er når operatørene av strømnettverket ruter strømmen annerledes pga. vedlikehold og lignende. Da vil også kommunikasjonen måtte følge den nye ruten og et AMI-system må kunne tilpasse seg slike endringer i topologien.

Ikke-standardiserte smalbånd PLC-teknologier:

- Echelon og andre: Echelon er et amerikansk system med lav båndbredde, spesielt utviklet til AMR og med lave installasjonskostnader. De har også utviklet en standard, som er akseptert i USA, Europa og Kina, som kalles LonWorks/LonTalk. Båndbredden regnes som for lav for fremtidens AMI-systemer.
- PRIME (Power line Intelligent Metering Evolution): Dette er en spesifikasjon som skal gjelde de lavere lag i en kommunikasjonsprotokoll og være gratis å benytte. Den kan, avhengig av implementasjon operere i området 21,4 kbps til 128,6 kbps.
- Telegestore-DLC og ZIV: To proprietære systemer der detaljert informasjon ikke er tilgjengelig.

Åpen standard smalbånd PLC-teknologier:

- IEC 61334-5-1 S-FSK: Dette er den eneste standarden støttet av IEC. Den har flere robuste mekanismer for sikker dataoverføring, men datahastigheten kan være for lav for fremtidens AMI-systemer.
- IEC 61334-5-2: Beskriver et fysisk lag i en PLC-protokoll som kan operere på 600 til 1200 bps. Dvs. svært liten båndbredde.
- IEC 61334-5-4: Samme som over, men med hastighet opptil 4,5 kbps.
- CENELEC EN50090 (KNX – PL): Dette er en godkjent protokoll for hjemmeautomatisering som kan operere i området 1,2 – 2,4 kbps.

Ikke-standardiserte bredbånd PLC-teknologier (Broadband Power Line, BPL):

(Merk at operasjoner i MHz-båndet ikke er vanlig akseptert hos nettselskapene).

- HomePlug: En industristandard utviklet av 70 selskap der bruken er fokuserert på hjemmenettverk (LAN). Den er nylig blitt publisert i den internasjonal standarden TIA-1113. Den er blitt brukt i smarte nettverk og sluttbrukerapplikasjoner i USA. Teknologien har muligheter til å lage egne ad-hoc-nettverk og støtter robust dataoverføring < 1 Mbps ved forskjellige nettverksspenninger. Den er antatt å være velegnet til AMI. Foreløpig er det en dyr teknologi, hovedsakelig pga. maskinvaren. Standarden har blitt overført til IEEE, slik at det kan bli en åpen standard.
- Panasonic: Dette er en teknologi utviklet av Panasonic hovedsakelig for å kunne distribuere lyd og bildesignaler via PLC i et hjem.
- OPERA/UPA (DS2): Dette er en industristandard utviklet av Universal Powerline Association (UPA) og er spesifisert av Open PLC European Research Alliance (OPERA) som er EU-finansiert. Den operer i forskjellige hastigheter fra 2 MHz til 32 MHz og har robuste mekanismer for dataoverføring < 1 MHz. Det jobbes mot en ny løsning (på bakgrunn av denne) som skal være spesialtilpasset AMI. Der skal hver celle kunne støtte opptil 300 noder. OPERA/UPA har blitt sendt til IEEE og ETSI for å bli en åpen standard.

Åpen bredbånd PLC-teknologier:

- IEEE P1901: Denne standarden er under utarbeidelse og fokuserer på effektiv bruk av PLC, interoperabilitet og skal tilby sikkerhetsmekanismer for å sikre datakommunikasjon mellom brukere. Siden standarden er under utarbeidelse er det vanskelig å kvantifisere kostnadene forbundet med implementering.
- ITU-T G.hn: G.hn er en gruppe under ITU-T som jobber med høyhastighetsnettverk basert på PLC, telefonlinje og på coax-kabling. Anbefaling G9960 ble akseptert av ITU-T i 2008 og har et stort omfang av industrielle produkter, tilbydere og tjenester som allerede er utviklet til formålet. Teknologien imøtekommer alle krav til et AMI-system med sikker dataoverføring, kryptering (AES), lavt effektforbruk o.s.v. Det forventet at dette vil bli en hjemmestandard og smarte nett kan forvente lave kostnader på komponenter, som følge av det.

D2.1 – Part 2 behandler PLC-systemer svært grundig. Jeg vil derfor ikke referere fra denne i rapporten, siden det hovedsaklig er en teknisk beskrivelse av PLC-teknologien og ikke spesifikt omhandler sikkerhet.

D2.1 – Part 3 er en grundig gjennomgang av aktuelle trådløse teknologier, der det er lagt vekt på frekvensbånd, applikasjoner og kostnader. I part 1 av D2-1 har jeg allerede skrevet om sikkerhetsaspektene i aktuelle trådløse teknologier og kommer også tilbake til dette under D2-2.

For teknisk personell i et nettselskap som planlegger AMI, vil disse to delene (D2.1-Part 2 og Part 3) gi verdifull bakgrunnsinformasjon.

2.2.2.2 Data- og applikasjonsmodell (D2.1-Part 4)

Denne modellen beskriver prinsippene slik objekter blir laget. Et objekt består av attributter og metoder. Ved å følge disse spesifikasjonene kan maskinvare og programvare fra forskjellige firma operere sammen.

Ved bruk av proprietære systemer, kan det installeres ”drivere” som knytter utstyr fra forskjellige leverandører. Mange nettselskap er i besittelse av slikt leverandørspesifikt utstyr.

Et åpent system som er klassifisert i IEC 62056-61/62 COSEM, definerer både applikasjonsmodellen og et enhetlig Object Identification System (OBIS). COSEM-standarden definerer applikasjonene uavhengig av kommunikasjonsmedia og protokoller.

Dokumentet beskriver kommunikasjonsprotokoller og datastrukturer som er i bruk i AMR- og AMI-systemer, samt andre aktuelle protokoller som ikke er spesielt utviklet for AMI.

Fra figur 2.2 er følgende grensesnitt definert som:

- Port MI1: Kommunikasjon mellom målerinstallasjonen og Datakonsentrator (DC).
- Port MI2: For kommunikasjon mellom målerintsllasjon og sentral server (CAS).
- Port MI3: For kommunikasjon mellom målerinstallasjonen og eksternt utstyr til bruk under installasjon og vedlikehold.
- Port MI4: For kommunikasjon mellom målesystemet og et eller flere målerinstrument eller utstyr fra nettselskapet. Datamodellen og protokollen er beskrevet under.
- Port MI5: For kommunikasjon mellom målerinstallasjonen og ISP-modulen eller tilleggsutstyr, med en begrensning på antall utstyrsenheter. MI5 skal være toveis og kan for eksempel brukes til et display. Datamodellen og protokollen er beskrevet under.
- Port SI3 er en port som uavhengige tilbydere og nettselskap kan benytte for å få tilgang til CAS: Denne porten blir ikke behandlet i dette dokumentet.

Oversikt over kommunikasjonsprotokoller og datastrukturer:

IEC 61334 S-FSK profilen er en del av IEC 61334 standarden Det er en smalbåndet PLC-teknologi og er støttet av mange maskinvareprodusenter. Denne standarden spesifiserer også de øverste lag i ISO-modellen: Et ekstra nettverkslag, applikasjonslag og DLMS applikasjonsprotokoll. Denne profilen er brukt av franske og nederlandske nettselskap på MI1-grensesnittet mellom måleren og DC. S-FSK PLC er regnet som en robust protokoll og sammen med DLMS/COSEM er den velegnet til AMI.

IEC 62056-31 EURIDIS er en praktisk og god protokoll for AMI. I dag er dette standardiserte grenesnittet det eneste for å kunne lese måler over avstand gjennom en tvinnet kobberledning ved bruk av bæresignaler. EURIDIS kan lese/skrive data med stor integritet og sikkerhet. Den er rimelig, kan opere med 100 m mellom aksesspunkter, er lett å integrere og er en åpen, internasjonal standard. Hovedfunksjonene er fjernlesing av registere, fjernprogrammering, alarmhåndtering, støtte til annet utstyr (som for eksempel vannmålere), automatisk registrering av nytt utstyr og sikret mot fysisk inntrenging.
Man ønsker å utvikle denne protokollen til å kunne bruke datamodellen DLMS/COSEM og øke overføringshastigheten (fra dagens 1200 bps) til 9600 bps.

DLMS/COSEM: IEC 62056, EN 13757-1 er en internasjonal standard for datautveksling mellom såkalt intelligent utstyr. Modellen er utviklet av nettselskap og utstyrsleverandører til AMI. Datautvekslingen kan baseres på mange kommunikasjonsprotokoller; TCP-IP, S-FSK-PLC, M-buss og EURIDIS. Datasikkerhet er ivaretatt både som tilgangssikkerhet og transportsikkerhet. Det er valgt en AES-GCM-128 symmetrisk nøkkelalgoritme som bør ha en levetid til etter 2030. Spesifikasjonene til DLMS/COSEM er basert på COSEM-datamodell, OBIS identifikasjonssytem og DLMS teksttjenester og bør kunne være en kjernestandard i et AMI-system.

M-BUS EN 13757 er en europeisk busstandard benyttet for enveis og toveis kommunikasjon med målere. Den kan også benyttes til sensorer og fjernstyring. M-BUS spesifiserer alle egne lag i en 3-lags (forenklet) OSI-struktur, men kan også benyttes sammen med DLMS/COSEM. Protokollen er optimalisert for målere og tilbyr lave kostnader og lavt effektforbruk. Den har også mulighet for trådløs overføring. En revisjon av standarden er ventet etter krav fa tyske og nederlandske prosjektgrupper. Datasikkerhet er i varetatt ved å kryptere M-BUS-telegrammene ved hjelp av DES eller AES. Tilgangskontroll er ikke implementert. I dag brukes bussen hovedsakelig for gass- og varmemålere.

Smart Message Language (SML): er en kommunikasjonsprotokoll som er utviklet og brukt av flere store nettselskap/kraftleverandører. Den er utviklet med henblikk på smarte nettverk og er gratis tilgjengelig (Ikke- proprietær). Protokollen definerer kun applikasjonslaget i OSI-modellen og er dermed uavhengig av transportlaget. SML er på vei til å bli en internasjonal standard (IEC). Sikkerheten er ivaretatt på transportlaget.

IP Telematric Protocol E-DIN 43863-4. Dette er en protokoll som er utviklet for telleravlesning og elektrisk forbruk. Den blir mest brukt mellom teknisk utstyr og er en DIN-standard. Den tyske DIN-standarden er åpent tilgjengelig og det er søkt om internasjonal standardisering. Poenget med standarden er å kunne integrere IP-baserte tjenester i protokollen. (Man kan bruke applikasjoner basert på IP som allerede er utviklet). Protokollen er ikke spesielt utviklet til AMI, men kan brukes i et slikt system.

IEC 60870-5 er en kommunikasjonsprotokoll for å sende kontrollbeskjeder mellom to systemer. Spesifikasjonene er omfattende og det er definert mange kontrolloppgaver protokollen kan gjøre. Den kan (kun) baseres på lokal buss som kommunikasjonsmedium. Det er en internasjonal standard.

IEC 61968-9. Denne standarden spesifiserer mange kommandotyper som kan brukes i et AMI-system. Standarden er utviklet for å kunne utveksle meldinger mellom et målersystem og resten av nettverket. Det er foreløpig et utkast til standard.

SITRED. Dette er en proprietær protokoll utviklet av ENEL (italiensk distributør) og implementerer lag 1, 2 og 7 i OSI-modellen.

PRIME (Powerline Intelligent Metering Evolution) er definert på de lavere lag i OSI-modellen. (Fysiske og mediatilgangslaget (MAC)). Det er en åpen og gratis standard.

IEC 68150 består av en konsistent datamodell, integrasjon av automatiserings- og kraftkontrollsystemer og bruk av kjente industriprodukter.

KNX (Konnex) er en protokoll for hjem og bygninger som er godkjent som europeisk, amerikansk (USA), kinesisk og internasjonal standard. Dette er den eneste standarden i verden godkjent for offentlige og private bygg. Alle produkter merket KNX (fra forskjellige leverandører) kan jobbe sammen. KNX kan fjernstyre det meste i en bygning og kan også brukes til målere, overvåking, sikkerhet o.s.v.

ZigBee SmartEnergyProfile består av flere høynivå kommunikasjonsmodeller som er basert på digitale radioer med lav effekt (IEEE 802.15.4). ZigBees SmartEnergyProfile er en ferdig utviklet pakke for enkel måleravlesning, respons og lasthåndtering.

6LoWPAN er, som ZigBee også en trådløs kommunikasjonsprotokoll bygget på IEEE 802.15.4. Den er basert på IPv6, men med mindre pakker og hoder.

Homeplug er en teknisk spesifikasjon for PLC som går på de lavere lag i OSI-modellen.

Z-Wave er en trådløs proprietær standard som er utviklet for automatisering i hjemmet. Den tilbyr en rekkevidde på 30 meter og en kommunikasjonshastighet på 9600 bps.

Wavenis er en trådløs teknologi som går på de nedre lagene i OSI-modellen. Den kan dermed støtte mange applikasjonsprotokoller. Den har lang rekkevidde og svært lavt effektforbruk.

EverBlu er et automatisk måleravleser (AMR-)system basert på trådløs teknologi. Den har lang rekkevidde (300 meter) og ultralavt effektforbruk. AMI er støttet, men ikke hjemmeautomatisering.

2.2.2.3 Anbefaling av telekommunikasjonsteknologier (D2.2)

(Originaltittel på dokumentet: 'Assessment of potentially adequate telecommunications technologies' elaborated within OPEN meter WP2 'Identification of Knowledge and Technology Gaps').

Det er fremdeles diskusjoner om mulige teknologier som kan benyttes, men denne gruppen har kommet frem til to kandidater for hvert grensesnitt.

PLC-teknologier

Rapporten slår fast, på generelt grunnlag at PLC-teknologien ikke er moden nok ennå og at evalueringsresultatene denne gruppen fremsetter i dette henseende er vage. Videre har de kun valgt smalbåndsløsninger for PLC (NPL) fordi disse samsvarer med CENELEC EN 50065.

Anbefalt PLC-teknologi brukt i AMI-systemet er i Tabell 2-6. (Tabellen hos Open Meter er feil, det er rettet i tabellen under).

Tabell 2-6: Anbefalte PLC-teknologier

Grensesnitt	MI1-CI1	MI4-MUMI1	CI2-SI1
Beste løsning	PRIME	IEC 61334-5-1	Smalbånds-PLC over MV
Nest beste løsning	IEC 61334-5-1	KNX-PL	-

Trådløse teknologier

En oppsummering er i Tabell 2-7 under. Se Figur 2-2 for referanse til grensesnittene.

Tabell 2-7: Trådløse teknologier

Grensesnitt	MI4-MUMI1	MI3-CI3-MUMI2	CI4	MI2-SI2	CI2-SI1	MI5
Beste løsning	IEEE802.15.4	IEEE802.15.4	ZigBee	UMTS	UMTS	Blåtann
Nest beste løsning	IEEE802.11	IEEE802.11	WiFi	GPRS	GPRS	ZigBee

Protokoller

Arbeidsgruppen vil ikke gå gjennom IP-protokoller (6LoWPAN), fordi de mener at dette er en del av systemarkitekturen og henviser til Arbeidsgruppe 3 og 4 (WP 3 & WP 4). En del proprietære og ikke ferdigutviklede protokoller blir heller ikke gjennomgått. Anbefalningene er oppsummert i Tabell 2-8 under:

Tabell 2-8: Oversikt over anbefalte protokoller

Grensesnitt	MI4-MUMI1	MI3-CI3-MUMI2	CI4	MI2-SI2	CI2-SI1	MI5
Beste løsning	DLMS/COSEM over M-BUS DLMS/COSEM over EURIDIS	DLMS/ COSEM over PRIME PLC	DLMS/ COSEM over IEC 62056-31	DLMS/ COSEM over UMTS/ GPRS/IP	DLMS/ COSEM over UMTS/ GPRS/IP	DLMS/ COSEM over IEC 61025-31
Nest beste løsning	DLMS/COSEM over ZigBee SML	SML	SML	SML	SML	SML ZigBee SEP

Oppsummering

Tabell 2-9 oppsummerer tabellene nevnt over. Det er verdt å merke seg at for grensesnittet MI1-CI1 er det kun PLC-teknologi som er anbefalt. Dette innebærer at forskningsfokuset fremover (for Open Meter) er PLC-teknologi, siden de mener det er en teknologi som ikke er moden nok, slik den fremstår i dag. En referanse til grensesnittene er i Figur 2-2.

Tabell 2-9: Oppsummering av valgt teknologi, protokoller og standard.

Grensesnitt	Valgt teknologi	Valgt standard	Valgt protokoll
MI1-CI1	PLC	PRIME IEC 61334-5-1	DLMS SML
CI2-SI1	Trådløs	UMTS GPRS	DLMS SML
MI2-SI2	Trådløs	UMTS GPRS	DLMS SML
MI3-CI3 & MUMI2	Trådløs	IEEE802.15.4 IEEE802.11	DLMS SML
MI4-MUMI1	Trådløs	IEEE802.15.4 IEEE802.11	DLMS SML
CI4	Trådløs	Zigbee Wifi	DLMS SML
MI5	Trådløs	Bluetooth Zigbee	DLMS ZigBee SEP

2.2.3 Arbeidsgruppe 3 – Global arkitektur og komponenter.

Denne arbeidsgruppen er ledet av Iberdrola, et privat spansk energiselskap og bygger på arbeidet til arbeidsgruppe 1 og 2. Dokumentet gir en komplett arkitektur for et AMI-system, bygget på OSI-konseptet.

Denne arbeidsgruppen har delt opp arbeidet i to utgivelser [19], der D3.1 viser hvordan open meter mener systemarkitekturen skal se ut. D3.2 er en svært inngående drøftelse av protokoller og med mange eksempler på hvordan de skal implementeres og brukes. D3.2 er utenfor denne rapportens definisjonsområde.

2.2.3.1 Kommunikasjonsprofiler for open meter systemgrensesnitt (D3.1)

Dokumentet slår fast at strømmåleren er den eneste måleren i en bygning som hele tiden har tilgang til strøm. Gass, vann og varme er målere som vil bruke batterier og det er strengere krav til sikkerhetsprotokoller for disse, siden de er eksterne. Strømmåleren er en integrert del av kommunikasjonsenheten. D3.1, global arkitektur og komponenter, er lagt inn i introduksjonen av open meter og er knyttet til figur 2.2. D3.1, kommunikasjonsprofiler for open meter systemgrensesnitt, følger under. De skal oppfylle kravene til Integritet, Tilgjengelighet og Konfidensialitet. Sikkerhetskravene er oppsummert i tabellen under:

Tabell 2-10 - Kommunikasjonsprofiler for systemgrensesnitt

Funksjonskategori	Sikkerhetskrav	Beskrivelse	D1.1-referanse
Minimum	Tilgangs- og brukerkontroll	Systemet må kunne autentisere enheter	OM-GR2
Minimum	Tilgangs- og brukerkontroll	Systemet må kunne håndtere brukertilgang til alle komponenter	OM-GR-3
Minimum	Dataintegritet	Systemet må garantere at riktige data blir utvekslet	OM-GR-4

Minimum	Datakonfidensialitet	Utstyret må garantere konfidensialitet til lagrede data.	OM-GR-5
Minimum	Dataintegritet	Systemet må garantere integritet til lagrede data og maskinvare	OM-GR-6
Minimum	Datakonfidensialitet	Systemet og utstyret må hindre mulighet for avlytting	OM-GR-7
Minimum	Dataintegritet	Systemet skal kunne implementere en mekanisme slik det er beskyttet mot omsending av data	OM-GR-8
Minimum	Tilgangs- og brukerkontroll Dataintegritet	Kringkastet kommunikasjon skal skje på sikker måte	OM-GR-9
Minimum	Tilgangs- og brukerkontroll Dataintegritet Datakonfidensialitet	Utstyret skal kunne håndtere krypteringsnøkler	OM-GR-11
Minimum	Tilgangs- og brukerkontroll Dataintegritet	Fysisk tilgang til enheter skal vanskeliggjøres	OM-GR-12
Minimum	Tilgangs- og brukerkontroll Dataintegritet Datakonfidensialitet	Etablerte standarder for IT og automatisering skal brukes	OM-GR-15
Minimum	Tilgangs- og brukerkontroll Dataintegritet Datakonfidensialitet	Bruk av sertifikater til sikkerhetsoppsettet er sterkt anbefalt	OM-GR-16
Minimum	Ressurstilgjengelighet	Hele nettverket må være under kontroll, overvåking og administrering	OM-GR-17
Avansert	Ressurstilgjengelighet	En overvåkning av systemet bør være mulig slik at unormale situasjoner kan oppdages og (til en viss grad) automatisk korrigeres.	OM-GR-10
Avansert	Tilgangs- og brukerkontroll Dataintegritet	Bruk av grensesnitt til testutstyr blir loggført	OM-GR-14
Tillegg	Tilgangs- og brukerkontroll	Alle fysiske grensesnitt som ikke er i bruk holdes avstengt i standardoppsettet	OM-GR-13

2.2.3.2 Sikkerhet i DLMS/COSEM

DLMS står for: Distribution Line Message Spesification eller Distribution Language Message Spesification.
COSEM står for: COmpanion Spesification for Energy Metering.

Sikkerhetskravene til systemet er omfattende og berører både moduler og grensesnitt. For protokollen DLSM/COSEM gjelder to sikkerhetsaspekt ved transport og tilgang til data:

- Sikkerhetskontroll ved datatilgang styres av en DLMS/COSEM-server.
- Sikkerhet av datatransport oppfylles med at avsender kan kryptere applikasjonspakkene som blir sendt. Mottager kan dekryptere eller sjekke disse.

Denne sikkerhetsmekanismen er delvis implementert i applikasjonslaget og delvis implementert i selve objektet i COSEM. To applikasjoner (Applikasjonsassosiasjon AA) kan etableres (av en Application Control Service Element (ACSE) i en applikasjonskontekst eller en autentiseringskontekst. Applikasjonskonteksten bestemmer om kryptering skal brukes eller ikke. Autentiseringskonteksten bestemmer sikkerhetsnivå. Merk at informasjonsbærerne i applikasjonslaget (Application Layer Portable data unit, APDU) fra ACSE ikke er kryptert, men at de kan transportere kryptert informasjon.

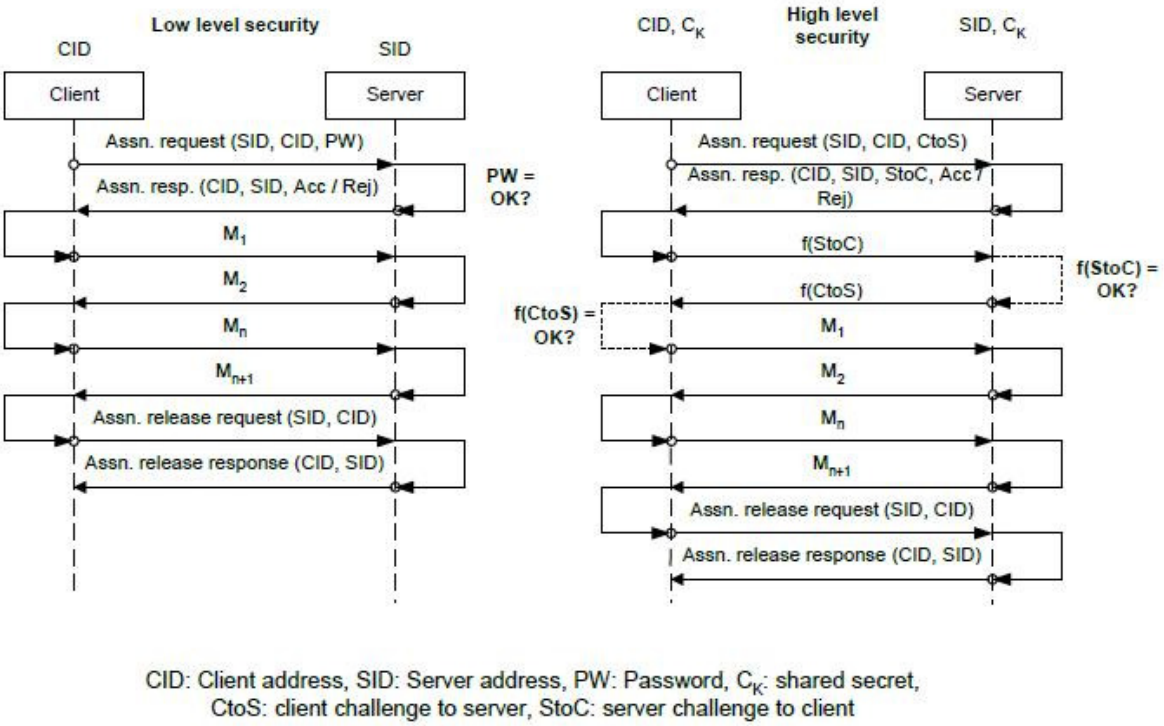
Når en AA er etablert kan COSEM-tjenester brukes til å få tilgang til attributter i COSEM-objekter. Sikkerheten i meldingsutvekslingen er basert på NIST og IETF.

Datatilgangssikkerhet

Denne er bygget på en rollebasert modell for tilgang til data i en DLMS/COSEM-enhet. Den er basert på objekter som er assosiert med logisk navn (LN) og kort navn (Short Name SN). Hver COSEM-server (dvs. logisk enhet) kan støtte AA med forskjellige klienter som har forskjellige oppgaver og dermed forskjellige tilgangsrettigheter. Hver AA identifiseres gjennom lavere lags adresser. Hvert assosierende objekt har en liste over AA'er som er tilgjengelige i denne AA'en og tilgangsrettigheter for deres attributter. For å få tilgang til data må klienten autentiseres med serveren. Det finnes tre sikkerhetsnivå det kan forhandles om:

- Laveste sikkerhetsnivå (Ingen sikkerhet): Brukes til utveksling av basisinformasjon og gir tilgangsrettigheter til serveren med de rettigheter som er i den gitte AA'en
- Lavnivå sikkerhet (LLS): Klienten autentiseres med passord, men server autentiseres ikke. Dette nivået brukes når kommunikasjonskanalen allerede tilbyr beskyttelse mot avlytting og gjentagende passord.
- Høynivå sikkerhet (HLS): Både server og klient autentiseres.

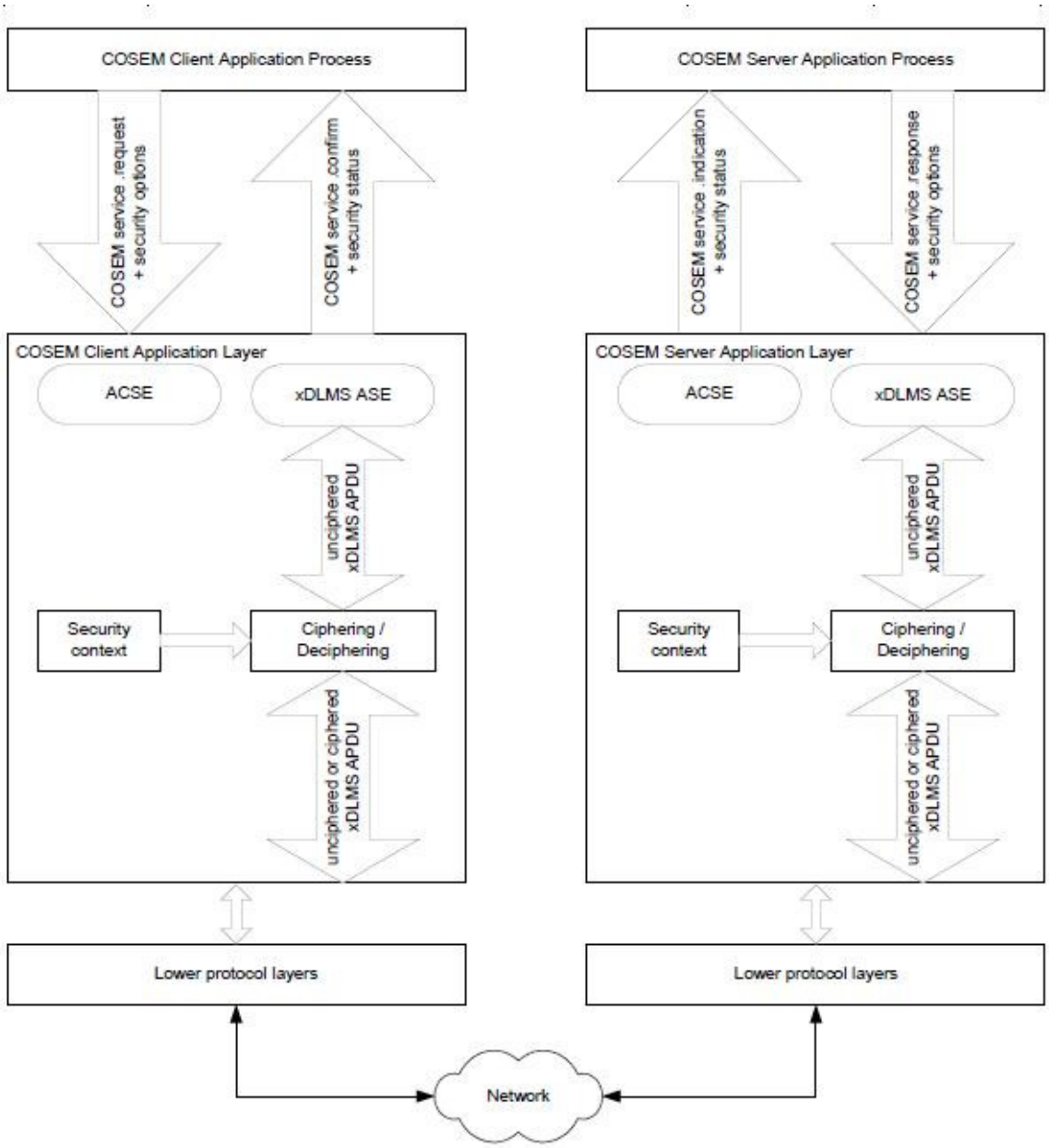
Autentiseringsprosessen for LLS og HLS er i figuren under.



Figur 2-6 - Autentiseringsprosess for LLS og HLS

Datatransportsikkerhet

Datatransportsikkerhet kan ivaretas ved at kryptering foretas før det sendes en xDLMS APDU (informasjonskapsel i DLMS-format). Dette avgjøres av sikkerhetsnivået som er valgt. (Dette dokumentet, D3, tar ikke for seg kryptering i lagrede data). Kryptering og dekryptering gjøres i applikasjonslaget i COSEM-protokollen. En oppsummering av hvordan dette foregår mellom en COSEM-klient og en COSEM-server er gitt i figuren under.



Figur 2-7 - OM: Datatransport mellom klient og server i COSEM

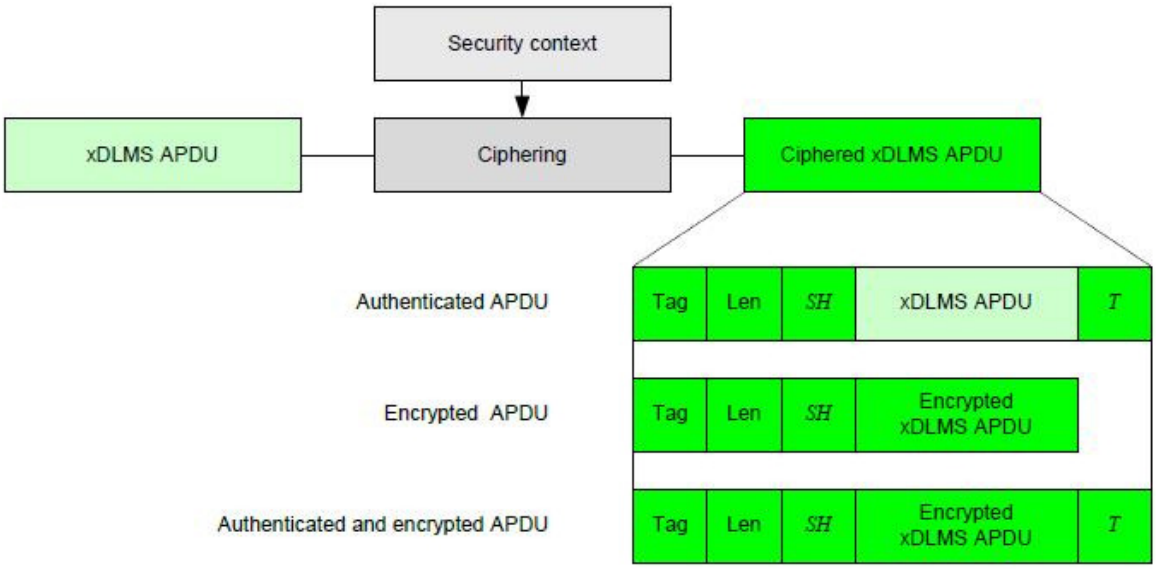
Sikkerhetskontekst

Denne definerer sikkerhetsattributtene som er relevante for krypterings- og dekrypteringsprosessen. Den består av:

- Sikkerhetspolitikk som er valgt: Denne består av fire muligheter:
    1. Usikret
    2. Alle beskjeder/informasjon er autentisert
    3. Alle beskjeder er kryptert
    4. Alle beskjeder er autentisert og kryptert

- Sikkerhetspakken som spesifiserer sikkerhetsalgoritmene: Foreløpig er kun en algoritme spesifisert. AES-GCM-128. Globale nøkler er beskyttet ved å bruke AES-128 key wrap.

Elementene i sikkerhetsmaterialet består av en blokkchiffernøkkel EK, en autentiseringsnøkkel AK, en initieringsvektor IV og en tekst som skal sikres M. EK,AK og IK bestemmes av sikkerhetsnivået og teksten som skal krypteres er xDLMS APDU. (Informasjonskapsler). Strukturen til en kryptert APDU avhenger av valgt kryptering og er oppsummert i figur og tekst under.



Figur 2-8 - OM: Innholdet i informasjonskapsler APDU

En autentisert APDU inneholder en APDU-merkelapp (TAG), lengde (Len), Sikkerhetshode (SH), den opprinnelige APDU'en og en T for autentisering. Teksten i APDU er her ukryptert. En APDU har en lengde som går opp i en oktett (8 bit) og lengdefeltet viser lengden for oktett-strengen.

En kryptert APDU er som over, men har ikke autentiseringsflagget T satt. Teksten er her kryptert.

En autentisert og kryptert APDU er som over, med autentiseringsflagget T, satt.

Sikkerhetshodet en rammeteller (FC) og en sikkerhetskontroll (SC). SC består av 8 bit der bit 0-3 er ID'en til sikkerhetspakken som er valgt. (Kun AES-GCM-128 er mulig foreløpig og denne har ID=0). Bit 4 indikerer at APDU er autentisert. Bit 5 at den er kryptert. Bit 6 satt til 0 innebærer at nøkler distribueres en-til-en (Unicast) eller en-til-flere (broadcast). Bit 7 er foreløpig udefinert. FC brukes internt av sender og mottager.

Sikkerhet i lavere lag.

Det finnes behov for å kunne beskytte for eksempel nettverksadresser i et AMI-system. Senere publikasjoner fra WP-3 vil ta opp slike problemstillinger og komme med anbefalinger for alle kommunikasjonsprofiler.

Oversikt over grensesnitt

MI1-CI1 er grensesnittet mellom smartmåleren og konsentratoren. Data- og kontrollinformasjon går over PLC. Kontrollinformasjon blir delegert til konsentratoren fra Sentralsystemet, hvis

konsentrator blir brukt. Det er antatt at PLC-teknologi har lavere kostnader og er mer robust enn å bruke GPRS/UMTS i disse grensesnittene.
Grensesnitt: PLC-PRIME eller PLC-S-FSK.
Protokoll: DLMS/COSEM

MI2-SI2 er grensesnittet mellom smartmåleren og Sentralsystemet. Dette brukes dersom det er ønskelig med en direkte kobling mellom disse to og MI1-CI1 ikke brukes. Data- og kontrollinformasjon går over GPRS/UMTS.
Grensesnitt: GPRS eller UMTS.
Protokoll: DLMS/COSEM

MI3 er et grensesnitt på smartmåleren som brukes til test og vedlikehold (Operations & Maintenance). Dette kan ha et optisk eller "current loop" grensesnitt.
Grensesnitt: Optisk.
Protokoll: DLMS/COSEM

MUMI2 er grensesnittet på de eksterne målerne (ikke strømmåleren) og brukes til test og vedlikehold på disse. Det anbefales ikke at MUMI2 skal brukes, men at man kan bruke smartmålerens grensesnitt MI4 koblet til MUMI1, slik at test og vedlikehold kan fjernstyres fra denne eller konsentrator/Sentralsystem.
Grensesnitt: Ikke bruk
Protokoll: ***

MUMI1-MI4 er grensesnittet mellom eksterne målere og smartmåleren. Dette er det eneste grensesnittet eksterne målere kan kommunisere med Sentralsystemet.
Grensesnitt: M-Bus, Trådløs M-Bus, Euridis 2, IEEE 802.15.4 radio eller ZigBee
Protokoll: DLMS/COSEM

MI5 er grensesnittet mellom smartmåler og utstyr hos kunden som for eksempel 'display'.
Grensesnitt: ZigBee, Bluetooth.

CI2-SI1 er grensesnittet som gir sentralsystemet tilgang til alle konsentratorene. Her er det ikke tatt stilling til hva slags kommunikasjonsmåte som skal brukes (de lavere lag av OSI-modellen). Det kreves at et IP-basert nettverk er tilgjengelig.
Grensesnitt: GPRS, UMTS eller annet IP-basert nettverkslag.
Protokoll: sFTP, SNMPv3 eller Web-tjeneste
(Dette grensesnittet er basert på WAN-teknologi og har dermed mange standarder tilgjengelig).

CI3 er grensesnittet som brukes for test og vedlikehold av konsentratoren. Instrumenter som brukes her må kunne hente ut alle data fra konsentratoren og kunne gjøre det som er Sentralsystemets oppgave, hvis forbindelsen til dette er brutt.
Grensesnitt: Optisk.
Protokoll: DLMS/COSEM

CI4 er et grensesnitt på konsentratoren for tilkobling av eksternt utstyr, som for eksempel sensorer. Det er tenkt at eksternt utstyr skal være i samme bygg som konsentratoren. Denne arbeidsgruppen analyserer ikke dette grensesnittet videre.

2.2.4 Arbeidsgruppe 4 – Testing

Denne gruppen, ledet av KEMA som er et nederlandsk konsulentselskap innen energisektoren, skal utarbeide testprosedyrer og også teste nylig utviklede løsninger. Arbeidet til denne arbeidsgruppen faller utenfor fokus for denne rapporten. (Dokumentet D4: [19])

2.2.5 Arbeidsgruppe 5 – Spesifikasjoner og forslag til standard

Denne arbeidsgruppen er ledet av Landis+Gyr, et sveitsisk selskap som bl.a. utvikler målerutstyr. Disse skal bruke de andre arbeidsgruppenes resultater til å foreslå formelle spesifikasjoner for AMI. Nye standarder skal rapporteres til relevante standardorganisasjoner. Arbeidet til denne arbeidsgruppen faller utenfor fokus for denne rapporten. (Dokumentet D5: [19])

2.2.6 Arbeidsgruppe 6 – Formidling

Arbeidsgruppen er ledet av DLMS brukerorganisasjon, KEMA og Iberdrola og skal se på hvordan prosjektresultatene blir formidlet av/til alle involverte parter. Arbeidet til denne arbeidsgruppen faller utenfor fokus for denne rapporten. (Dokumentet D6: [19])

2.3 Sikkerhet, sårbarhet og personvern

Innføring av AMS gjør samfunnet og aktørene mer sårbare. Dette setter nødvendigvis store krav til sikkerhet når det gjelder implementeringen av AMS. Dette kapittelet tar opp bakgrunnen for informasjonssikkerhet, samfunnssårbarhet og personvern. Dette gjøres på en summarisk måte og er ikke tenkt som en innføring i disse kategoriene, men mer som oppsummering av sentrale begreper og definisjoner.

2.3.1 Informasjonssikkerhet

Innen informasjonssikkerhet opereres med tre sentrale begreper:

- Konfidensialitet: Bare rett person skal ha tilgang til informasjonen. Disse skal identifiseres og autentiseres i AMS-systemet. Konfidensialitet består av datakonfidensialitet og personvern.
- Integritet: Dataintegritet innebærer at informasjonen er korrekt og bare kan endres av autoriserte personer. Systemintegritet vil si at systemet fungerer slik det er ment og at det ikke manipuleres av utenforstående. Informasjonen i systemet skal være riktig og gyldig.
- Tilgjengelighet: Informasjonen skal være tilgjengelig ved behov for autoriserte brukere/program.

Disse tre begrepene utgjør kjernen av informasjonssikkerhet, men de senere årene har det blitt foreslått ytterligere to begrep som gjør bildet mer komplett:

- Autentisitet: Opphavet er ekte og kan verifiseres og stoles på. Dette innebærer å vite at brukerne er den de sier de er og at data inn i systemet kommer fra en verifisert kilde.
- Ansvarlighet: Hendelser skal kunne spores til den som var opphavet til disse hendelsene. Det er et ønske om å spore hendelsene som skjer i et datasystem mot den som er ansvarlige for dem.

Internet Engineering Task Force (IETF) [21] spesifiserer i rfc 2828 [22] sikkerhetsterminologien som brukes i datasystemer. Noen sentrale begrep er:

- Adversary - Motstander eller trusselagent: En enhet som angriper eller en trussel mot systemet.
- Attack - Angrep: En manipulering med systemet som skyldes en intelligent trussel, d.v.s. en villet handling. Slike angrep kan komme fra innsiden og utsiden. De kan også være aktive eller passive. Aktive angrep manipulerer systemet, mens passive angrep ønsker bare å hente ut informasjon.
- Countermeasure - Mottiltak: Et tiltak, elektronisk enhet, prosedyre eller teknikk som reduserer en trussel, en sårbarhet eller et angrep ved å minimisere skadene disse kan gjøre mot systemet.
- Risk - Risiko: En forventning av tap som skjer når det ved en viss sannsynlighet oppstår en trussel som utnytter sårbarhet og som resulterer i et skadelig resultat.
- Security Policy – Sikkerhetspolitikk:En mengde regler og etablert praksis på hvordan et system eller en organisasjon tilrettelegger for sikkerhetstjenester for å beskytte sensitive eller kritiske systemressurser.
- System resources (Asset) – Systemressurser (Utstyr/tilbehør): Dette er data i et informasjonssystem eller i en tjeneste tilknyttet systemet, muligheter i systemet som

prosesseringskraft eller båndbredde, en systemkomponent som maskinvare, programvare, operativsystem, og dokumentasjon eller fasilitetene der utstyret og operasjonene på dette blir utført.
- Threat – Trussel: Et potensial for å ødelegge sikkerheten som eksisterer når det er en omstendighet, hendelse eller mulighet som bryter sikkerheten og lager problemer. Trussel er en mulig fare som utfordrer sårbarheten.
- Vulnerability – Sårbarhet: En feil eller svakhet i systemdesignen, implementasjonen, operasjon eller ledelsen av datasystemet, som kan utnyttes for å skade systemets sikkerhetspolitikk.
- Value – Verdi: En vekting av informasjonen som er utsatt for risiko, fra lav til høy (0.1-1.0).

2.3.2 Kryptering

Kryptografi er en teknikk for å endre formatet på informasjonen, slik at det blir utilgjengelig for utenforstående å lese. Prosessen må være reversibel. En tekst som blir endret ved hjelp av en nøkkel og krypteringsalgoritme, kalles chiffertekst.

2.3.2.1 Symmetrisk kryptering

Symmetrisk kryptering innebærer at man bruker samme nøkkel for å kryptere enn melding som for å dekryptere den. Dette setter særlige krav til oppbevaring av nøkler og at krypterings-algoritmen er god. I dag regnes Advanced Encryption Standard [23] (AES) som den beste algoritmen for symmetrisk kryptering, og denne er også valgt av Open Meter. Størrelsen på nøkkelen er avgjørende for hvor vanskelig det er å knekke koden for utenforstående. Open Meter har valgt en nøkkellengde på 128 bit og dette regnes som en rimelig sterk nøkkel.

2.3.2.2 Asymmetrisk kryptering

Asymmetrisk kryptering kalles også kryptering med offentlig nøkkel. Her er det to nøkler, en offentlig og en privat. Den offentlige nøkkelen gis til den som skal kryptere meldingen og bare den som besitter den private nøkkelen kan da lese chifferteksten. Det er med andre ord ikke mulig å dekryptere chifferteksten med samme nøkkel som den ble kryptert med.

Offentlige nøkler brukes i Digitale Signaturer, Offentlige sertifikater og utveksling av symmetriske nøkler.

Open Meter ønsker en nøkkelutveksling i AES, der den nye nøkkelen pakkes inn i en melding (Key Wrap) og den gamle (symmetriske) nøkkelen brukes til å åpne pakken med den nye nøkkelen. Den aller første nøkkelen kunne utveksles med asymmetrisk kryptering.

2.3.2.3 DoS-angrep

Denial of Service (DoS), eller tilgangsnekt, er en handling som hindrer autoriserte brukere å bruke nettverket, systemet eller applikasjonene. Et slikt angrep iverksettes ved å overbelaste prosessoren (CPU, hukommelsen (RAM), båndbredden og harddiskkapasiteten.

Den vanligste formen for DoS-angrep er å legge beslag på båndbredde i systemet ved å sende flere forespørsler og generere mer datatrafikk enn motparten kan håndtere. (Flooding). En annen

metode er å angripe svakheter i motpartens system, slik at motpartens system blir opptatt med å behandle forespørsler fra angriperen.

Hvis flere systemer går sammen om å angripe et tredje system har vi et Distribuert DoS, eller DDoS-angrep. Dette øker datakraften og kompleksiteten i angrepene.

2.3.3 Samfunnssårbarhet

Bondevik-regjeringen tok i 1999 initiativ til å kartlegge samfunnets sårbarhet mht. IKT og komme med en strategi for å redusere denne sårbarheten. Et regjeringsoppnevnt utvalg presenterte rapporten NOU2000:24 "Et sårbart samfunn" [24], som danner bakgrunn for den videre strategien for å redusere samfunnets sårbarhet.

I denne rapporten slås det fast at IKT og kraftforsyning er blant bærebjelkene i samfunnets infrastruktur og at det må sikres robuste systemer i denne kritiske infrastrukturen.

Kraftomsetning og produksjon er åpnet for fri konkurranse, mens nettjenestene er monopolistiske og regulert av NVE. Rapporten påpeker at utviklingen går mot at funksjonaliteten i strømnettet øker og at dette går på bekostning av sikkerheten:

Den direkte følgen av dette er i første omgang lavere pris til kundene. I dette ligger ingen oppmuntring til å bygge robuste infrastrukturer som tåler utfordringer utover det som fredssituasjoner tilsier. Derimot bidrar dette til ensidig fokusering på kostnadsbesparelser. Gjennom sentralisering av virksomheter og funksjoner, nedbemanning og økt bruk av informasjons- og kommunikasjonssystemer, øker sårbarheten i systemene som helhet fordi tidligere reserver i personell og materiell bygges ned, tilgang på fagkompetanse blir redusert og kompleksiteten øker.

Det er en uttalt bekymring for at myndighetene har et for sterkt fokus på priskonkurranse og at dette går på bekostning av beredskap og sårbarhet. Det fastslås at bortfall av strøm vil ramme både folk og samfunn negativt.

Styring av infrastruktur ved hjelp av IKT gjør det også mulig for utenforstående å overta kontrollen over nettet. Dette kan gjøres indirekte med såkalte DoS-angrep, der driftssentralene mister kontrollen over styringen. Ved store svingninger i kraftforbruket kan dette få fatale følger fordi det må være en balanse mellom forbruk og produksjon i nettverket, for å unngå nettsammenbrudd.

Rapporten hevder videre at det finnes få relevante sikkerhetskrav til nettselskapene som sikrer et tilfredsstillende sikkerhetsnivå.

Forsvarets Forskningsinstitutt ga i 2001 ut rapporten [25] BAS3, "En sårbar kraftforsyning", der det fastslås at kraftforsyningen er kritisk for samfunnet og at i en tid med effektivisering, internasjonalisering og ukjent trusselbilde må det iverksettes tiltak for å redusere sårbarheten.

Denne rapporten går inn på flere fysiske tiltak som er viktige for å beskytte infrastrukturen. Men den fastslår også at innføring av IKT i kraftforsyningen har medført at fremtidens driftspersonell vil være dårligere i stand til å håndtere kriser, fordi de blir avhengige av datasystemene. Sårbarhet i kraftforsyningen blir dermed direkte relatert til sårbarhet i IKT fordi driftspersonellet ikke lenger har god kjennskap om kraftforsyningen de styrer.

2.3.4 Personvern

Personvern i den store sammenhengen er retten den enkelte har til privatliv, selvbestemmelse og selvutfoldelse. Det som er vesentlig i denne rapporten er det som Fornyings-, Administrasjons- og Kirkedepartementet kaller personopplysningsvern [26]:

Et vesentlig element i personvernet er at personer i utgangspunktet skal kunne bestemme hva andre skal få vite om hans eller hennes egne personlige forhold. Vi kan i denne sammenhengen snakke om "personopplysningsvern", og det er primært denne dimensjonen som er underlagt omfattende lovregulering som for eksempel personopplysningsloven, helseregisterloven, regler om taushetsplikt mv.

Det er viktig å presisere at personvernet ikke er ukrenkelig. Samfunnets interesser kan i enkelte tilfeller veie tyngre enn personlige interesser og da kan personvernet krenkes.

I Norge er det Datatilsynet som er utnevnt til å påse at personopplysningsloven blir fulgt. Denne loven skal beskytte den enkelte mot krenking av personvernet. Datatilsynet skal også hjelpe bransjer med å utarbeide retningslinjer for adferd og gi råd om sikring av personopplysninger.

Datatilsynet utga 25.11.2010 en "Veileder for behandling av personopplysninger ved bruk av automatiske målesystem i energisektoren" [27].

Denne veilederen tar ikke for seg tilleggstjenester men kun behandling av opplysninger i forbindelse med fakturering for nettselskapet. Det skal bare behandles personopplysninger om strømforbruk og at avlesningshyppigheten må tilpasses avtalen nettselskapet har med kunden. En avtale om fastpris medfører dermed lav avlesningshyppighet.

Videre skal det foretas en risikovurdering for å sikre at personopplysninger ikke blir misbrukt internt og eksternt.

Personopplysninger som ikke lenger er nødvendige for fakturering skal slettes, men kan brukes til andre forhold dersom det foreligger rettslig grunnlag. Informasjonen kan også brukes i anonym statistikk.

Det er også krav om internkontroll i forbindelse med å sikre personopplysningenes kvalitet. Datatilsynet har utarbeidet flere veiledere [28] for slik kontroll som må implementeres i nettselskapene.

2.4 Oppsummering av bakgrunn

Kapittel 2 har gitt en grundig innføring i bakgrunnen for denne rapporten. I kapittel 2.1.1 har jeg gjennomgått NVEs høringsnotat og skrevet et sammendrag fra dette. Kapittel 2.2 er et omfattende sammendrag av Open Meters arbeidsgrupper 1,2 og 3 (WP 1,2 og 3). Resultater og anbefalinger fra Open Meters arbeidsgrupper har jeg savnet i andre norske rapporter. Denne rapporten bygger i hovedsak på resultater fra Open Meter og krav fra NVE.

Tilslutt, i kapittel 2.3 har jeg tatt for meg sikkerhet, samfunnssårbarhet og personvern, som et bakteppe for hva analysen handler om.

3 Analyse av sikkerhet og personvern ved innføring av AMS

For å kunne implementere AMS i stor skala, må også sikkerhet og personvern være ivaretatt. Sikkerhet i denne sammenheng går på sikkerhet i AMS-nettverket, systemsikkerhet og personsikkerhet. Følgende problemstillinger er knyttet til disse:

- Sikkerhet i AMS-nettverket: Utstyr og kommunikasjon skal være sikret mot sabotasje slik at data ikke kan endres, avlyttes eller være fra feil avsender. Videre må tilgang til data være begrenset og veldefinert innen nettselskapenes datasystem. Denne rapporten tar for seg sikkerhet i AMS-nettverket og ikke nettselskapets datasystem.

- Systemsikkerhet og personvern: Dette bør være definert av NVE slik at det stiller krav til utforming av implementeringen av AMS, både når det gjelder ansvarsstrukturer (nettselskapets datanettverk) og selve infrastrukturen (montering av utstyr og lignende). Nettselskapene må også ha katastrofeplaner, der de tar høyde for at kommunikasjonsutstyr er svært sårbart. Personvernet må ivaretas etter Datatilsynets anbefalinger.

- Personsikkerhet går på sikkerhet i bygg når det gjelder innføring av AMS. AMS kan bidra til økt sikkerhet ved bl.a. å avdekke jordfeil, men frem i tid vil AMS sannsynligvis bidra til et endret forbruksmønster. Strømkrevende utstyr i hjem og industri, som ikke er døgnkritiske, vil igangsettes automatisk om natten når strøm presumptivt er billigere. Dette øker brannfaren og konsekvensene blir alvorligere, når folk ikke er til stede eller sover. Også struping eller stenging av kraft kan påvirke liv og helse.

Denne sikkerhetsanalysen vil i hovedsak være av kvalitativ natur. Det innebærer at man ser på de enkelte sidene ved AMS og finner styrker og svakheter ved de foreslåtte standardene. En kvantitativ analyse ville ha brukt allerede installerte AMS-systemer som bakgrunnsdata (empiriske data) for en sikkerhetsanalyse. Siden Open Meter ennå ikke er ferdig med sine anbefalinger, finnes det heller ingen AMS-systemer bygget etter disse. Enkelte land har installert AMS etter delvis proprietære standarder og der det er naturlig vil erfaringer fra disse knyttes inn i teksten.

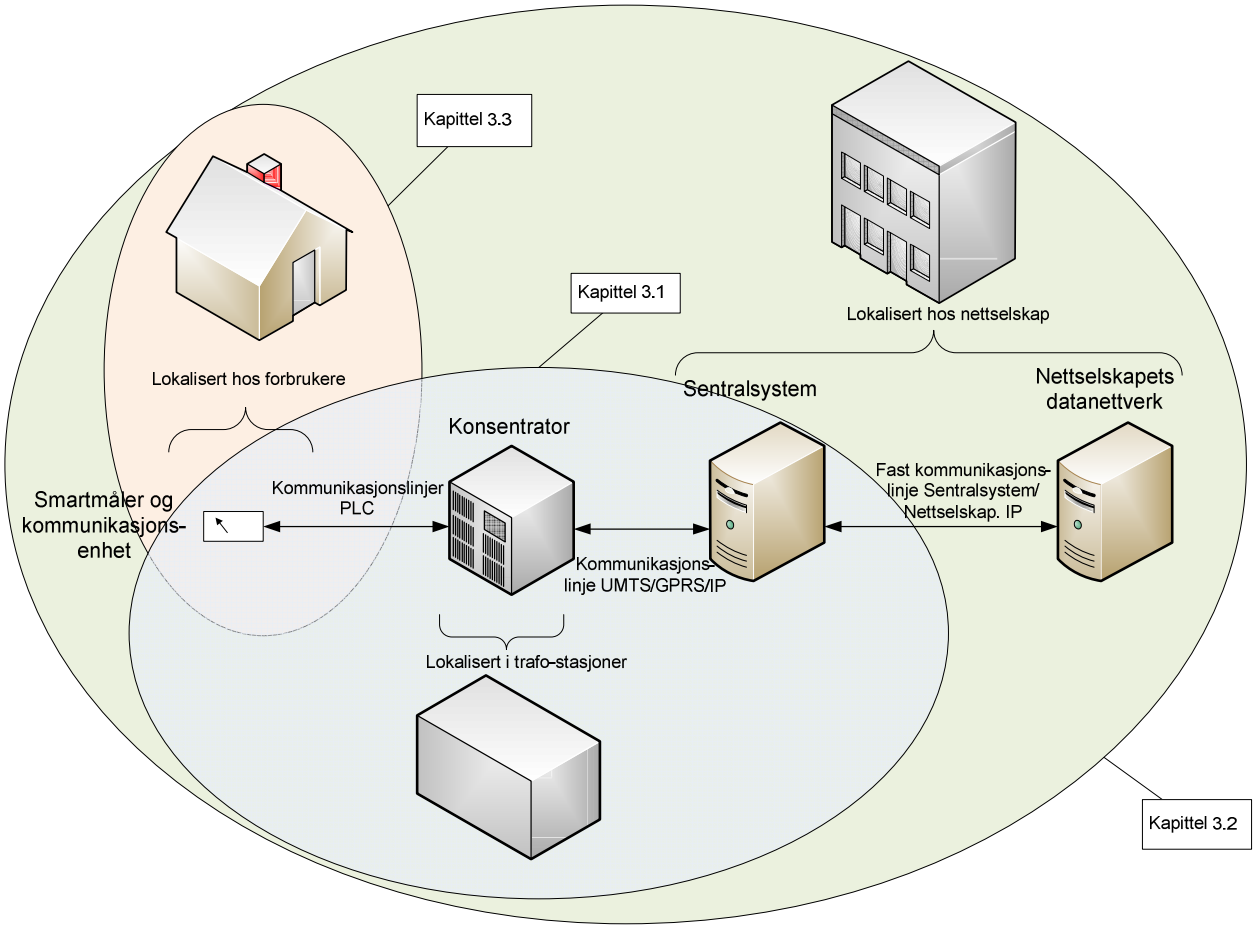
Nasjonal sikkerhetsmyndighet [29] (NSM) bruker følgende formel for risiko:

$$\text{Risiko} = \frac{\text{Trussel} \times \text{Sårbarhet}}{\text{Mottiltak}} \text{Verdi}$$

Variablene er behandlet i kapittel 2.3.1, men kort oppsummert er *Risiko* det vi ønsker å minimere, *Trussel* er mulig fare, *Sårbarhet* er feil eller svakhet i systemet, *Verdi* er vekting av informasjonen som er utsatt for en trussel og *Mottiltak* er måte å hindre forventede angrep på systemet.

I en kvalitativ analyse er det vanskelig å tallfeste størrelsene. Derfor er oppgaven med å minimere risikoen først og fremst basert på å minske sårbarheten og øke mottiltakene. Det er ikke mulig for meg å foreta en vekting av *Verdi*, slik at dette må nettselskapene som leser rapporten selv avgjøre. Denne rapporten peker på svakheter, men rangerer ikke disse etter *Verdi.*

Figur 3-1 viser en grovinndeling av problemområdene som er skissert punktvis over. Grensene er ikke så kategoriske som det fremgår av figuren, men viser hvor fokuset ligger i de enkelte delkapitlene.



Figur 3-1 - Grovinndeling av problemområder og referanse til kapitler

3.1 Sikkerhet i AMS-nettverket

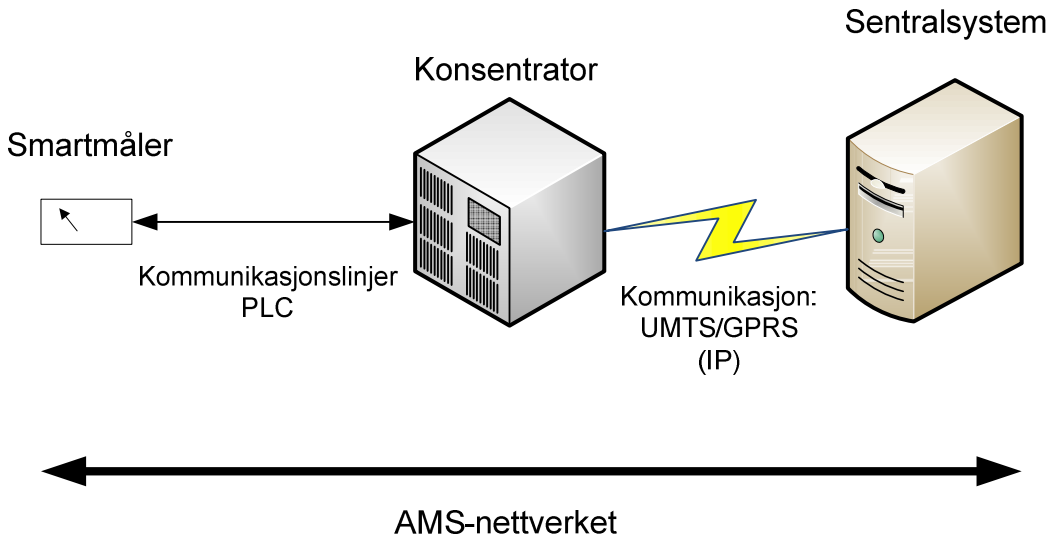
Med bakgrunn i kapittel 2.2 vil dette underkapitlet ha fokus på de enkelte delene som utgjør et AMS-nettverk. Figur 3-2 viser en forenklet utgave av AMS-nettverket som behandles i dette kapitlet. Det er verdt å merke seg at AMS Sentralsystem logisk er en del av AMS-nettverket, men er (i regelen) fysisk lokalisert hos nettselskapet. Smartmåleren kan også kommunisere trådløst til Sentralsystemet via UMTS/GPRS, hvis konsentrator ikke er tilgjengelig. Dette er ikke tegnet inn i figuren.

En viktig del av dette systemet er et overvåkningssystem (Intrusion Detection System, IDS) som skal overvåke og registrere uregelmessigheter. Dersom man prøver å magnetisk påvirke, fysisk åpne eller fjerne noen av AMS-enhetene vil dette registreres som ”hendelser/alarmer” i Sentralsystemet. De foreslåtte kommunikasjonsprotokollene brukt i AMS-nettverket har svært lav båndbredde (fra 2400 og inntil 128 kbps). Dette kan lage problemer for et Intrusion Detection System (IDS) og det er derfor viktig at dette overvåkingsssystemet er så enkelt (og robust) som mulig. IDS-kommunikasjonen skal også krypteres i tillegg til at AMS-måleravlesninger krypteres. All kryptering tar ekstra båndbredde i AMS-nettverket. (Et kortfattet og oversiktlig dokument om IDS i AMS ligger under referanse [30]).

Denne infrastrukturen gjør AMS-nettverket autonomt og det kan operere selvstendig uavhengig av nettselskapets datasystem. Det er ikke mulig å få tilgang til nettverket eller komponenter utenom gjennom nettselskapet. Det finnes innvendinger mot denne infrastrukturen.

I følge høringsnotatet fra NVE ønskes et IP-basert AMS-system slik at andre tilleggstjenester fra andre tilbydere kan muliggjøres. Det er ønskelig med tredjeparts tilgang, på ikke-diskriminerende vilkår, til AMS-systemet. Dette er problematisk og tas opp i kapittel 3.2.1.4.

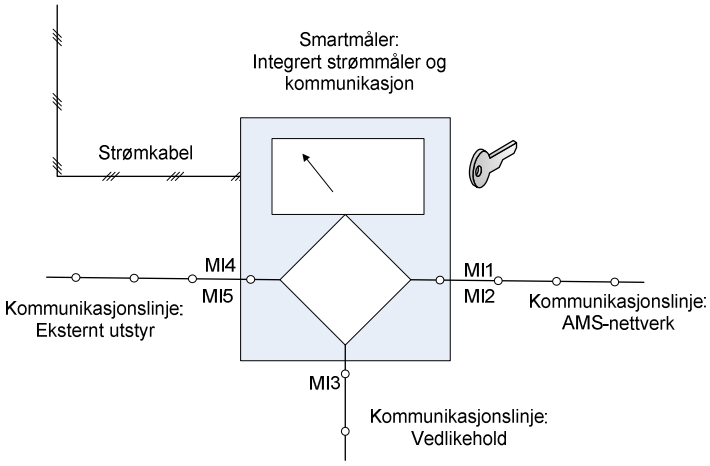
Dette kapittelet bruker Open Meters infrastruktur som utgangspunkt. Open Meter foreslår en anbefaling og det er dermed ikke nødvendigvis slik alle nettselskap vil implementere dette systemet slik det foreligger.



Figur 3-2 - Oversikt av komponenter i et AMS-nettverk

3.1.1 Smartmåler

Smartmåleren består av en integrert strømmåler og en kommunikasjonsenhet. Måleren er forsynt av strømmen fra strømnettet og har flere grensesnitt for tilkobling av eksternt utstyr. Se Figur 3-3



Figur 3-3 - Smartmåler og grensesnitt

Når en smartmåler installeres i et AMS-nettverk, vil nettverket automatisk registrere denne. Nettselskapets datasystem har på forhånd registrert den nye måleren i AMS-systemet (Sentrasystemet) . Sentralsystemet sammenligner den nyoppdagede AMS-måleren med den forhåndsregistrerte måleren og på bakgrunn av denne informasjonen opprettes en kommunikasjon, eller måleren forkastes som en del av systemet.

Smartmåleren er forsynt med en nøkkel ved installasjon, som brukes til kryptering av informasjon og kommunikasjon. Den har videre to grensesnitt for kommunikasjon med AMS-nettverket: Dersom det brukes en konsentrator vil kommunikasjonen foregå gjennom MI1, som er anbefalt å være en PLC-linje, det vil si at strømkabelen brukes til kommunikasjon. Ved direkte tilkobling til Sentralsystemet brukes grensenitt MI2, som er anbefalt å være en mobiltelefoniløsning. MI3 brukes til testing og vedlikehold av smartmåleren og er forbeholdt servicepersonell. For tilkobling av andre målere (vann, gass og varmeforbruk) brukes MI4. Ekstra kundeutstyr, som for eksempel display, kobles på grensesnitt MI5.

3.1.1.1 Nøkler

All kommunikasjon mellom de forskjellige enhetene i AMS-systemet skal foregå kryptert. Til dette brukes nøkler. Hvordan den første registreringen foregår når det gjelder utveksling av nøkler, er ikke beskrevet i arbeidsgruppene til Open Meter. Slik jeg har forstått det skal det ligge en offentlig nøkkel (Public Key) i et dataregister i måleren når den installeres. Nettselskapet har en privat nøkkel (Private Key) og ved en asymmetrisk nøkkelutveksling blir en symmetrisk nøkkel utvekslet. Open Meter ønsker å bruke symmetriske nøkler i styring og utveksling av måledata. Denne er basert på krypteringsalgoritmen AES-128 og regnes som svært sterk. Fremtidige nøkler vil bruke AES-128 som krypteringsinnpakning, en såkalt AES-128-key-wrap. Disse krypteringsalgoritmene (kun denne ene er anbefalt foreløpig) vil sannsynligvis implementeres i programvare, fordi de ikke er tidskritiske, slik de er i for eksempel mobiltelefoni. Det er satt av 4 bit til informasjon om hvilken krypteringsalgoritme som skal brukes, det vil si at det er satt av plass til 16 (2^4) forskjellige krypteringsalgoritmer. (Se også kapittel 2.2.3.2, Sikkerhetskontekst).

Det er lite sannsynlig at forbrukeren kan få tak i den første offentlige nøkkelen, siden vedkommende ikke har tilgang til smartmåleren under montering og nøkkelutveksling inntreffer så fort måleren er montert i AMS-systemet. Det er likevel en liten sjanse for at montøren kan hente ut denne informasjonen og bruke denne nøkkelen i et såkalt maskeradeangrep på systemet. Et maskeradeangrep innebærer at montøren setter opp en datamaskin som oppfører seg som smartmåleren og lar AMS-systemet tro dette er en smartmåler. På dette viset kan AMS manipuleres ved å gi feilaktige måleravlesninger.

For å kunne gjøre dette må nøkkelen være tilgjengelig på en eller annen måte for montøren. Det vil være mulig siden testutstyret må kunne kommunisere med AMS-nettverket. Dette setter organisatoriske krav til oppbevaring av testutstyr og håndtering av innsidetrussel. Stjålet testutstyr må ikke få konsekvenser for sikkerheten i AMS. Dette innebærer at det må finnes rutiner for ny nøkkeloppgradering når slikt skjer.

Når det gjelder generering av nye nøkler og distribusjon, vil dette skje i nettselskapets datasystem. Denne rapporten går i liten grad inn på dette systemet.

Måten Open Meter har lagt opp nøkkeloppgradering og valg av algoritme, virker svært god. En mulig svakhet er ved initiering av første nøkkel.

3.1.1.2 Strømbackup

Open Meter slår fast at det eneste måleinstrumentet som alltid har tilgang til strøm, er smartmåleren. Andre eksterne målere som vann, varme og gass, vil være batteridrevne og dette vil vanskeliggjør momentan måleravlesning fra disse. Det er ønskelig med en svært lang batterilevetid (> 15 år) og disse målerne vil da gå i en slags dvaletilstand for å spare strøm mellom tidsbestemte avlesninger.

Open Meter nevner ikke noe minimumskrav om batterier i smartmåleren, noe som bør være påkrevet. (Tabell 2-3 viser løsninger med batteri som frivillig, OM-FR-96, OM-FR-97 og OM-FR-98 og strømforsynings-backup er nevnt i Tabell 2-4, OM-TR-2). I Norge har de fleste bygg hovedsikringer som tar all strøm til bygningen. Med PLC og strøm fra nettet, vil AMS-systemet miste muligheten for kommunikasjon med smartmåleren. Hvis smartmåleren da ikke har batteri-backup, vil den ikke kunne registrere forsøk på inntrenging i maskinvaren, eller tilkobling til kommunikasjonsgrensesnittet. Med batteri-backup vil all manipulering med systemet, ved bortfall av strøm, lagres i smartmåleren og sendes til Sentralsystemet når kommunikasjonen gjenopprettes.

3.1.1.3 Eksterne enheter

Smartmåleren har flere grensesnitt, MI1-MI5, for tilkobling av eksternt utstyr.(Figur 3-3). Disse grensesnittene vil, med unntak av MI1, MI2 eller MI3, være blokkert for tilkobling når smartmåleren installeres. Grensesnittene kan kun åpnes for kommunikasjon ved at sentralsystemet åpner for denne muligheten. All kommunikasjon med eksterne enheter skal være kryptert.

Siden alle eksterne enheter må være registrert i sentralsystemet, vil det ikke være mulig å legge til eller fjerne enheter uten at det blir registrert som en hendelse eller alarm.

MI5 brukes for å koble til eksternt brukerutstyr og dette introduserer en mulighet for at forbrukeren kan manipulere systemet. Denne muligheten kan begrenses ved å la dette brukerutstyret kun lese fra smartmåleren. Dette er også foreslått i Open Meter som et frivillig (Optional) anbefaling. (Tabell 2-5, OM-CR-20).

3.1.1.4 Lynnedslag

Strømnettet kan på mange måter betraktes som en stor lynavleder. Lyn og andre påførte spenningstopper vil forplante seg i et stort område. Dette setter høye krav til smartmålerne og særlig kommunikasjonsdelen som har et grensesnitt mot strømnettet (PLC).

Det er to ting som bør avklares i den forbindelse:

1. Er utstyret dimensjonert for spenningstopper?
2. Hva skjer med strømtilførselen til forbrukeren når elektronikken i smartmåleren ødelegges?

Det er lite sannsynlig at det tilbys utstyr på markedet som ikke har et overspenningsvern. Dette bør likevel være noe man sjekker opp før utstyret installeres.

Man kan ikke sikre utstyr mot store spenningstopper som kan oppstå ved lynnedslag i for eksempel en trafostasjon. Nettselskap har hatt gode rutiner for reparasjon ved slike uhell, men må fremover også ta høyde for utskifting av kanskje hundrevis av ødelagte smartmålere. Videre bør det i utgangspunktet være mulig for smartmålerne å levere strøm til forbruker, selv om

kommunikasjonsenheten er ødelagt. Dette vil sannsynligvis koste en del penger for nettselskapet, siden avlesing og kanskje lagring av forbruk er umulig når utstyret er ødelagt. Dette vil da gi nettselskapet et insitament til å utarbeide kriseplaner for å utbedre skadene ute hos forbrukerne hurtig.

Det kan, i enkelte deler av landet, være fornuftig å separere måleren og kommunikasjonsenheten for å gjøre utskifting, test og vedlikehold enklere. Dette åpner for flere grensesnitt i smartmåleren og disse må da ha samme sikkerhet som de allerede foreslåtte grensesnittene.

3.1.1.5 Målerdata

Open Meter har ikke tatt stilling til om data som lagres i smartmålerens registre skal krypteres. All kommunikasjon skal være kryptert og det vil derfor ikke være mulig å kommunisere med måleren uten en krypteringsnøkkel.

Måleren i seg selv er godt beskyttet mot fysisk påvirkning og inngrep. Det skal være detektering for magnetisk påvirkning, åpning av måleren og tilkoblinger mot grensesnittene.

Det er en tenkbar mulighet å få tilgang til elektronikken ved for eksempel boring i dekslet slik at man kan koble seg direkte til registrene. Da vil det være en mulighet for å endre disse målerverdiene og dermed påvirke strømavlesningen. Dette kan man gardere seg mot ved å la også alle registerverdier være kryptert.

3.1.1.6 Struping og stenging av strøm

Stenging av strøm er den mest sensitive og omfattende inngripen overfor en forbruker. Det er svært viktig at nettselskapene utarbeider rutiner for sporbarhet i hvem som iverksatte disse tiltakene.

Struping av strøm kan være nødvendig ved overbelasting i et område. Det settes da et tak på forbruk og strømmen kuttes når dette taket overskrides, men forbrukeren kan selv koble seg til strømnettet igjen ved å koble fra strømkrevende utstyr, slik at man holder seg innenfor avtalt forbruksgrense. (Se også kapittel 3.3.1).

3.1.1.7 Oppsummert Smartmåler

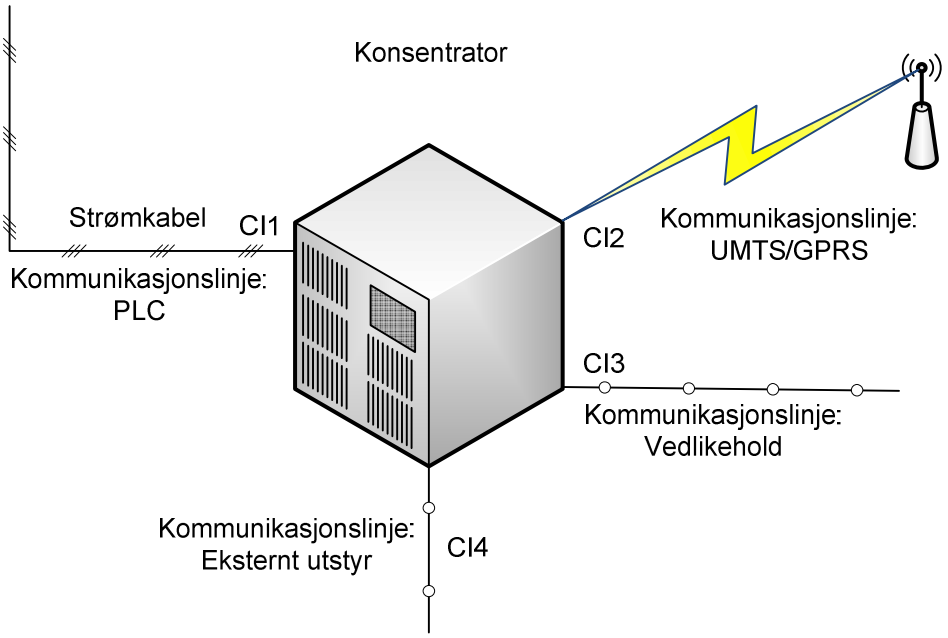
Smartmåleren er fra nettselskapets synspunkt, den enheten som er mest utsatt for manipulering. Denne er fysisk plassert ute hos kundene og nettselskapet har liten oversikt over hva slags midler og metoder som brukes for å manipulere denne. Smartmåleren har omfattende sikkerhetsbarrierer innebygget og vil med enkle mottiltak sikres ytterligere. På bakgrunn av det jeg har skrevet over har jeg utarbeidet en tabell som oppsummerer funnene. (Tabell 3-1).

Tabell 3-1 - Sikkerhetsanalyse av smartmåler

Enhet	Sårbarhet	Sannsynlighet	Konsekvens	Mottiltak
Nøkkel	Kjent nøkkel gir mulighet for kommunikasjon med måler og nettselskap.	LITEN	Man kan manipulere forbruk, stenge strøm o.l. hos forbrukeren.	Nøkkel bør ikke kunne leses ut av en smartmåler/ testutstyr . Vær observant på innsidetrussel
Strømbackup	Uten strømbackup kan smartmåleren manipuleres.	MODERAT	Manipulere målerverdier	Installere batteri-backup i strøm-måleren
Eksterne enheter	Disse kan kommunisere med måleren og påvirke den.	LITEN	Manipulere AMS og målerverdier.	Begrense mulighetene for toveis kommunikasjon gjennom enkelte grensesnitt
Lynnedslag	Kan kutte strømmen til forbrukere.	MODERAT	Det vil ta lenger tid å gjenopprette strømforsyningen	Sørge for at strømmen ikke blir kuttet selv om smart-måleren er defekt
Målerverdier	Kan avleses og endres	LITEN	Manipulere registrene i måleren	Kryptere målerverdier i registrene
Stenge strøm	Kan ramme feil forbruker.	LITEN	Liten-stor: Avhengig av forbrukeren som rammes.	Sørge for gode rutiner ved stenging og struping.

3.1.2 Konsentrator

En konsentrator er som regel fysisk plassert i en transformatorkiosk og kommuniserer og samler inn informasjon fra flere smartmålere. Figur 3-4 viser konsentrator med grensesnitt og de anbefalte kommunikasjonsløsningene fra Open Meter.



Figur 3-4 - Konsentrator og grensesnitt

Grensesnitt CI1 brukes for å kommunisere med smartmålerne og anbefales å være Power Line Communictaion (PLC). CI1 kan gå til tusenvis av smartmålere. (Minimum 3000 endepunkter, se Tabell 2-3, OM-FR-111 og Tabell 2-5 OM-CR-2). CI2 kommuniserer med sentralsystemet og er anbefalt å være trådløst og basert på mobiltelefonistandardene UMTS eller GPRS. Grensesnitt CI3 brukes til test og vedlikehold av systemet. CI4 brukes til eksternt utstyr og kan være for eksempel sensorer og smartmåler. Sensorer kan brukes til å overvåke bygget og området konsentratoren er montert for så å sende alarmer og hendelser til sentralsystemet. En smartmåler kan monteres i transformatorkiosken for å kunne sammenligne levert strøm med forbrukt strøm og på den måten avdekke svindel eller feil i avlesningene.

3.1.2.1 Nøkler

Konsentratoren må ha et register med flere nøkler for å kunne kommunisere med flere smartmålere og sentralsystemet. Alle smartmålere i området bør ha unike nøkler, slik at ikke alle blir kompromittert ved at en nøkkel er kjent. Registeret i konsentratoren bør være kryptert, slik at det ikke er mulig å avdekke nøklene, selv med fysisk tilgang. For øvrig gjelder de samme betraktningene som for nøklene i smartmåleren. (Kapittel 3.1.1.1).

3.1.2.2 Strømbackup

For å kunne registrere hendelser og forsøk på manipulering ved strømbortfall, må også konsentratoren ha en batteriløsning. Dette innebærer at alle hendelser og alarmer lagres i konsentratoren og sendes til sentralsystemet også ved strømbortfall.

3.1.2.3 Eksterne enheter

Konsentratorens grensesnitt vil, på samme måte som i smartmåleren, være utilgjengelige for uønsket kommunikasjon. Det skal derfor ikke være mulig å koble seg til grensesnittene CI3 eller CI4 uten at disse grensesnittene er åpnet for kommunikasjon fra sentralt hold. Siden alle eksterne enheter må være registrert i sentralsystemet, vil det ikke være mulig å legge til eller fjerne enheter uten at det blir registrert som en hendelse eller alarm. All kommunikasjon gjennom grensesnittene er kryptert.

3.1.2.4 Lynnedslag

Transformatorkiosker er eksponert for lyn og andre typer naturødeleggelse. En av forutsetningene i AMS er at alle AMS-enheter skal kunne operere videre hvis en enhet faller fra. Det innebærer at hendelser i konsentratoren ikke skal ramme strømforsyningen hos forbrukerne.

3.1.2.5 Målerdata

Konsentratoren samler inn hundrevis av måledata og sender disse til sentralsystemet. Også her, slik som for smartmåleren, bør man vurdere kryptering av lagrede data, slik at det vanskeliggjør avlesing og manipulering med verdiene i registrene. Gode rutiner i sentralsystemet vil avdekke slike feil, ved å sammenligne med tidligere målinger og ekstrapolere verdiene. Dessuten vil også lastbalansen avdekke en skjevhet mellom forbruk og avgitt kraft, dersom ekstra smartmåler er montert i transformatorstasjonen.

3.1.2.6 Fysisk tilgang

Transformatorstasjoner er ikke under oppsikt og kan derfor være utsatt for hærverk og innbrudd. Konsentratoren har mulighet for tilkobling av eksternt utstyr som kan overvåke stasjonen ved bruk av sensorer som registrerer magnetisk påvirkning, bevegelser i stasjonen og lignende. Selv med fysisk tilgang til konsentratoren vil det være svært vanskelig å manipulere det krypterte nettverket. Det er derfor rimelig å anta at denne type innbrudd først og fremst vil være for å fysisk ødelegge utstyr.

3.1.2.7 Falske alarmer

Enkelte folk tar ut hovedsikringene fra hus og hytter når de skal være lenge bortreist. Dette medfører at kommunikasjonen med smartmålerne som er installert, svikter. I følge de funksjonelle kravene (se Tabell 2-3, OM-FR-131) til konsentratoren, skal den gi beskjed til sentralsystemet når en kommunikasjonslinje svikter (kanal i nettverket mangler).

Dette kan medføre at nettselskapene blir utsatt for mange falske alarmer og en løsning kan være at utkobling og innkobling av hovedsikringer må meldes til nettselskapene. Evt. må nettselskapene kunne forby utkobling av disse.

3.1.2.8 Oppsummert Konsentrator

Konsentratoren er fysisk utsatt for naturskader og uønsket tilgang. Slike situasjoner kan man begrense omfanget av, ved å bruke de mulighetene som ligger i AMS. (Tabell 3-2). Tabellen jeg har laget viser både LITEN, MODERAT og STOR sannsynlighet på enkelte punkter. Med enkle

mottiltak kan disse reduseres, men det er en stor mulighet for at ”Falsk alarm” kan bli et problem, selv med de mottiltak som her er foreslått.

Tabell 3-2 - Sikkerhetsanalyse av Konsentrator

Enhet	Sårbarhet	Sannsynlighet	Konsekvens	Mottiltak
Nøkkel	Kjent nøkkel gir mulighet for kommunikasjon med måler og nettselskap.	LITEN	Man kan manipulere forbruk, stenge strøm o.l. hos forbrukeren.	Nøkkel bør ikke kunne leses ut av en konsentrator/ testutstyr . Tiltak mot innsidetrussel
Strømbackup	Uten strømbackup kan konsentratoren og omgivelsene manipuleres.	MODERAT	Manipulere målerverdier	Installere batteri-backup i konsentratoren.
Eksterne enheter	Disse kan kommunisere med måleren og påvirke den.	LITEN	Manipulere AMS og målerverdier.	Begrense mulighetene for toveis kommunikasjon gjennom enkelte grensesnitt
Lynnedslag	Mister kommunikasjon med forbrukere.	MODERAT	Små konsekvenser da AMS skal kunne operere uavhengig av konsentrator	Beskytte mot natur-ødeleggelser.
Målerverdier	Kan avlese og endre verdien til flere målere.	LITEN	Manipulere registrene i måleren	Kryptere målerverdier i registrene
Fysisk tilgang	Får tilgang til konsentrator	LITEN	Hærverk/ ødeleggelse.	Sørge for overvåking av stasjonen.
Falsk alarm	Fjerning av hovedsikringer kan utløse falske alarmer.	STOR	Uoversiktlighet og forstyrrelser i styringssystemet	Forby langvarig utkobling av hovedsikringer, evt. meldeplikt.

3.1.3 Programvare

Programvaren som brukes i AMS er godt beskyttet og det er et krav (Tabell 2-3, OM-FR-56) at den skal være dokumentert av produsenten. Videre er det lagt inn mekanismer for selvsjekk (OM-FR-64) og feil ved installasjonen (OM-FR-65 og OM-FR-66). Den innebygde sikkerheten i distribusjon og igangsetting er tilfredsstillende fordi det er innebygde rutiner for å sikre integriteten i programvaren.

Nettselskapene bør ha rutiner for kjøring av systemsjekk med jevne mellomrom. Dette vil sannsynligvis bli en automatisk integrert del av AMS styresystem, dvs. programvaren som kjører AMS.

3.1.4 Kommunikasjonslinjer

Kommunikasjonslinjene er stort sett tilgjengelige for avlytting, fysisk påvirkning og angrep. Det er to medier som er anbefalt av Open Meter for kommunikasjon, nemlig trådløst og PLC.

All kommunikasjon mellom alle enheter foregår med avanserte krypteringsalgoritmer og avlytting er bare mulig dersom man har tilgang til nøklene. Trådløst utstyr er sårbart for jamming, slik at Sentralsystemet mister kontakten med resten av AMS-nettverket. Jamming innebærer å bruke en støysender som umuliggjør kommunikasjon med utstyret som rammes. I Tabell 3-3 oppsummerer jeg sikkerhetsaspektene i forbindelse med kommunikasjonslinjene.

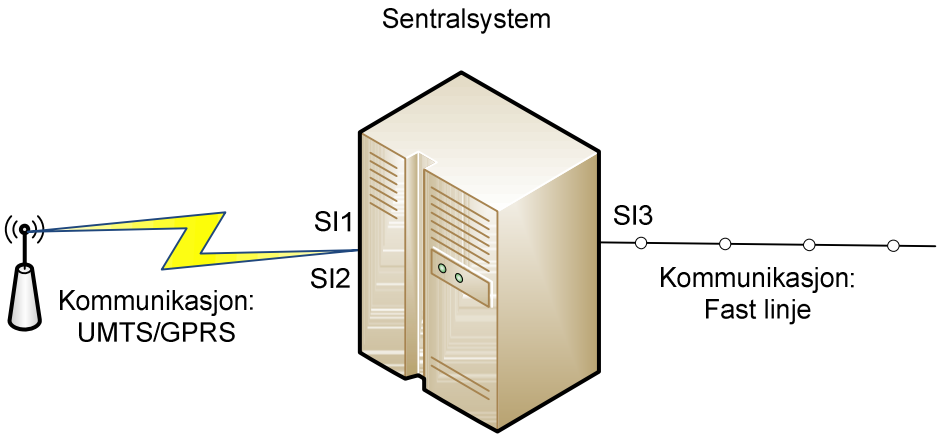
Tabell 3-3 - Sikkerhetsanalyse av kommunikasjon

Enhet	Sårbarhet	Sannsynlighet	Konsekvens	Mottiltak
Kommunikasjons-innhold	Lese meldinger	LITEN	Brudd på integritet og konfidensialitet	Sikker oppbevaring av nøkler
PLC	Fysisk ødeleggelse	LITEN	Brudd på tilgjengelighet	Sikre linjene mot først og fremst naturødeleggelser
Trådløst	Jamming	LITEN	Brudd på tilgjengelighet	Gjøre utstyret i stand til å identifisere støy.

3.1.5 Sentralsystem

Sentralsystemet styrer alle enheter i et AMS-nettverk. Sentralsystemet kommuniserer trådløst med smartmålerne via grensesnitt SI1 eller SI2. SI1 går til konsentrator, som igjen avleser og kommuniserer med smartmålerne. SI2 brukes når smartmålere ikke er tilkoblet konsentrator, men er direkte koblet til Sentralsystemet.

SI3 er kommunikasjonsgrensesnittet mot nettselskapet datasystem. Som regel er Sentralsystemet lokalisert i samme bygg som nettselskapets datasystem og har dermed samme grad av beskyttelse mot fysisk manipulering som dette.



Figur 3-5 - Sentralsystem og grensesnitt

Sentralsystemet er ikke utsatt for samme type risiko som det desentraliserte utstyret. Her er det rutiner, tilganger og redundans som er viktig og må fokuseres på. Dette er klassiske sikkerhetskrav som nettselskapene bruker på sine egne datasystemer og som denne rapporten ikke går videre innpå.

Trusler mot Sentralsystemet, direkte og indirekte, har jeg oppsummert i Tabell 3-4.

Tabell 3-4 – Direkte og indirekte trusler mot Sentralsystemet

	Tilgjengelighet	**Konfidensialitet**	**Integritet**
Maskinvare	Utstyr fjernes eller ødelegges og er dermed ikke tilgjengelige i AMS-systemet.		
Programvare	Program fjernes og nekter brukere tilgang	Uautorisert kopi av programvaren lages.	Et program modifiseres for å gjøre en uønsket handling.
Data	Filer fjernes slik at autoriste brukere stenges ute.	Uautorisert lesing av data. Statistisk analyse av data.	Filer modifiseres eller nye filer lages
Kommunikasjonslinje	Data blir ødelagt eller fjernet. Kommunikasjonslinjene gjøres utilgjengelige	Data blir lest. Datatransporten blir kartlagt.	Data blir modifisert, forsinket, lagret eller duplisert. Falske data lages.

3.2 Systemsikkerhet og personvern

Politiets sikkerhetstjeneste har i en publisert trusselvurdering for 2011 [31] fastslått at IKT er særlig utsatt for internasjonal etterretningsvirksomhet. Slike operasjoner kan også komme i skjermede nettverk og skjermede nettverk er særlig utsatt for utro tjenere. Videre heter det:

Sentrale deler av infrastrukturen i Norge, som for eksempel strømforsyningen, styres digitalt. I flere år har det vært kjent at enkelte stater arbeider med å utvikle en evne til å ramme andre lands infrastruktur gjennom datanettverksoperasjoner.

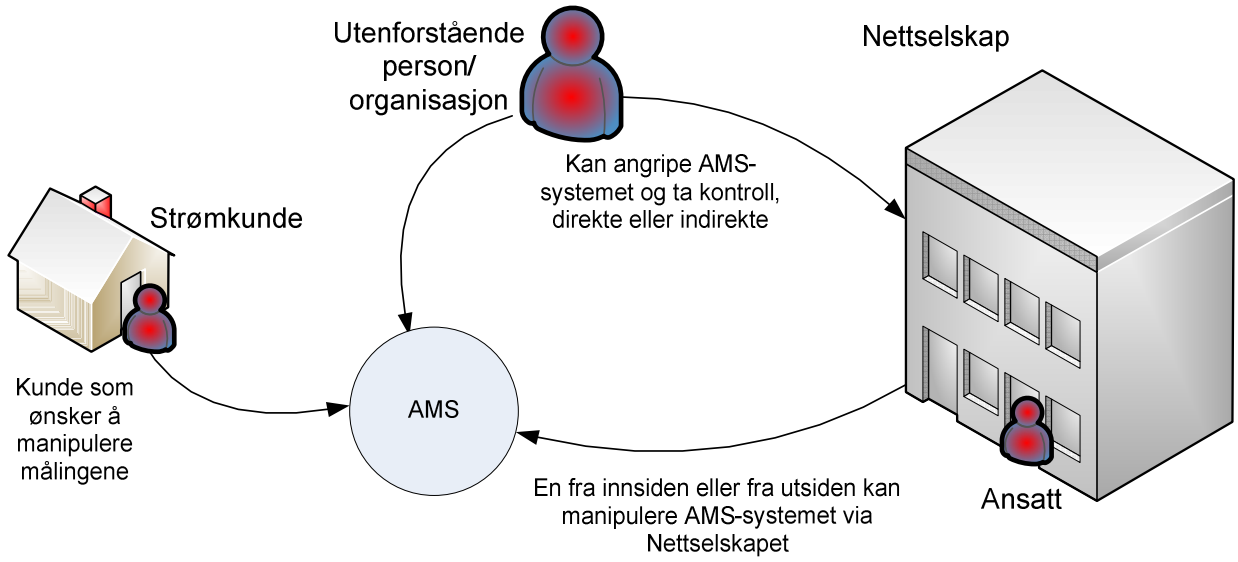
De regner ikke sannsynligheten for et direkte angrep mot strømforsyningen i Norge som særlig stor, men ser at det finnes betydelig og økende marked for kjøp og salg av gradert informasjon.

Personvernet står sterkt i Norge, men visse sider ved innføring av AMS er uavklarte. Det er datatilsynet som håndhever personvernet i Norge gjennom personopplysningsloven. For nettselskapene gjelder at det er virksomhetens leder som står ansvarlig for at regelverket overholdes også i avtaler med tredjepart det utveksles informasjon med.

3.2.1 Systemsikkerhet

Systemsikkerhet i denne sammenheng omfatter problemstillinger som innføring av AMS reiser og er ikke relatert til maskinvaren eller programvaren som sådan. Dette er en holistisk, kvalitativ analyse av AMS, abstrahert fra detaljer, men fokuserer på aktører.

AMS medfører en økt mengde data om forbrukere og fjernstyring av infrastrukturen. Dette gjør forbrukere, nettselskap og samfunnet som helhet mer sårbart fordi strømnettet og kundedata kan manipuleres med av folk både på innsiden og utsiden av systemet.



Figur 3-6 – Konseptuell oversikt over trusler mot AMS

Figur 3-6 viser en oversikt over trusler mot AMS der utenforstående person/organisasjon også kan være en tilbyder av tilleggstjenester. En tilbyder av tilleggstjenester vil, som nettselskapet, også være utsatt for utvendige og innvendige trusler og gjør det totale trusselbilde enda mer uoversiktlig og komplisert. De forskjellige aktørene vil ha forskjellige motiver for å angripe AMS.

3.2.1.1 Strømkunde

En uærlig strømkunde vil først og fremst være opptatt av å manipulere strømmåleren for å redusere strømregningen. Den innebygde, foreslåtte sikkerheten i AMS-systemet, vil gjøre det svært vanskelig å manipulere smartmåleren. Se kapittel 3.1.1.

3.2.1.2 Utenforstående

Utenforstående aktører er i denne sammenhengen:

- Enkeltpersoner
- Organisasjoner og stater
- Tjenestetilbydere

Alle disse er en trussel mot AMS direkte eller indirekte (se Figur 3-6), via nettselskapets eller tredjeparts datasystem.

Utenforstående vil ikke være interessert i manipulering av måledata, men kan ha interesse av å bruke disse til formål utenfor strømkundens og/eller nettselskapets kontroll og inngåtte avtaler. Dette kan for eksempel være å manipulere smartmåleren til å stenge strømmen for å styre strømnettets infrastruktur og destabilisere visse områder.

Enkeltpersoner kan deles i to kategorier:

1) Hackere: De ser en personlig utfordring i å manipulere nettverket.
2) Inntrengere: Personer som har en agenda rettet mot andre personer eller samfunn.

Hackere vil bruke de teknologiske mulighetene som ligger i nettverket for å kunne overta styringen. Inntrengere, eller personer med agenda vil ta alle midler i bruk, også utpressing, kjøp av tjenester og forsøk på å manipulere seg inn i nettverket. Ved samfunnsmessige/politiske motiver vil det være et ønske om å ramme infrastrukturen til flest mulig mennesker for å skape utrygghet og kaos i et samfunn. Økonomiske motiver kan være en generell strømovervåking av svært mange bygg for å kunne avgjøre hvilke som står tomme og dermed er tilgjengelige for uønsket besøk.

Organisasjoner og stater vil bruke de samme fremgangsmåtene som personer med agenda. De vil naturlig nok også ha flere ressurser og kan lettere få innpass og utført operasjoner mot AMS fordi de har:

- Økonomiske ressurser: Det er mulig å betale ”markedsverdien” for utro tjenere i et nettselskap som kan manipulere på oppdrag, eller oppgi brukernavn og passord. (Se under kapittel 3.2.1.3).
- Teknologiske ressurser: Organisasjoner og stater har gjerne tilgang til og mulighet for å utvikle teknologi som er dedikert en bestemt oppgave, for eksempel maskinvare for kryptering.
- Menneskelige ressurser: Det er mulig å ansette mange personer som bare jobber mot begrensede systemer, som også kanskje har jobbet med å utvikle maskinvare og programvare til bruk i AMS.

- Tilgangsressurser: Organisasjoner og stater kan under dekke av "Interesse for AMS i Norge" bli tilbudt besøk og få fysisk tilgang til nettselskap med AMS. Her kan minneenheter og annen elektronikk monteres på maskinvare (nettverk, tastatur og lignende) som kan sende informasjon ut av bygget.

Det er ingen tvil om at det finnes slike aktører, også i Norge, som er interessert i å bruke store ressurser på samfunnsundergravende virksomhet.

Tjenestetilbydere kan i første rekke være villige til å selge informasjon om sin kundegruppe videre til aktører som ønsker å selge profilerte produkter. En slik lekkasje av personinformasjon vil være vanskelig å avdekke, men dette er først og fremst en trussel mot personvernet. (Se kapittel 3.2.2). Tjenestetilbydere skal først og fremst ha tilgang til måledata og kunne styre hjemmenettverk (HAN) på oppdrag fra kunder. (Måten NVE mener dette skal gjøres på i Norge er kontroversielt og amerikanske NIST advarer mot dette, se kapittel 3.2.1.4).

3.2.1.3 Ansatt - Innsidetrussel

Den største trusselen mot AMS er innsidetrusselen. Det vil si at betrodde medarbeidere under press eller mot økonomiske ytelser velger å motarbeide systemet på oppdrag fra en utenforstående. Betrodde medarbeidere er i denne sammenheng egne ansatte, tidligere ansatte, konsulenter, utstyrsleverandører, programvareleverandører o.s.v. Dette gjør det vanskelig å definere hvem som er på innsiden og dermed ta forholdsregler mot disse truslene.

Norge er på europatoppen når det gjelder økokriminalitet [12] og i *… 60 % av de bedriftene som har erfart økonomisk kriminalitet, har dette vært begått av personer innenfor virksomheten.*

Innsidetrussel er erkjent å være et økende problem og det er også ofte vanskelig å finne personen(e) som står bak innbrudd i datasystemene. Dette skyldes at rollefordelingen i datasystemet ikke er tilstrekkelig kartlagt og at oversikten over tilganger er dårlig organisert. I Norge er det dessuten en juridisk formildende omstendighet hvis ansatte eller andre får tilgang til informasjon som er dårlig sikret i utgangspunktet [12].

Selv om det er erkjent at innsidetrusselen er en av de største truslene mot datasystemer er det lite forskning på dette området. Amerikanske Department of Homeland Security (DHS) ga i 2008 ut en rapport [32] "*The Insider Threat to Critical Infrastructures Study",* som konkluderer med det samme som også Norsk Sikkerhetsmyndighet (NSM) hevder:

Finding: the NIAC identified that many CIKR (Critical Infrastructure & Key Resource) operators lack an appropriate awareness of the threat insiders pose to their operations. Education and awareness presents the biggest potential return for policy by motivating CIKR operators and focusing their efforts to address the insider threat. Appropriate awareness will help to shape the insider threat policies and programs needed to address the unique insider risk profile of each CIKR operator.

Et annet aspekt ved innsidetrussel er at når den først er oppdaget er skaden allerede skjedd. Videre er det liten vilje til å innrømme utad at man har et sikkerhetsproblem og dette medfører at utro medarbeidere sjeldent blir anmeldt.

Denne rapporten skal ikke foreslå løsninger mot innsidetrusselen, men påpeke at det er et økende problem, der NSM burde utarbeide rutiner sammen med aktuelle aktører for å forhindre eller vanskeliggjøre innsidetrusler mot infrastrukturen.

3.2.1.4 Tjenestetilbydere og tredjeparts tilgang til AMS-nettverket

Tilbydere av tilleggstjenester kan først og fremst være en trussel mot personvernet. Alle foretak i Norge som oppbevarer personopplysninger må ha konsesjon av Datatilsynet. Det er likevel noen uavklarte problemstillinger til dette, bl.a. at det kan være utenlandske tjenestetilbydere. Skal juridiksjonen gjelde der disse er lokaliert, der databasen er lokalisert eller i det landet kundegruppen bor? Det må anses å være en viss fare for lekkasje av personvernopplysninger i slike selskap.

Dersom tjenestetilbyder skal ha anledning til å bruke AMS-nettverket til styring av HAN, dukker det opp ytterligere trusler mot AMS.

I høringsnotatet [13] fra NVE ønsker man å legge til rette for at tredjepart skal kunne kommunisere i AMS-nettverket:

Det er usikkert hvilke behov som vil oppstå for å bruke kommunikasjonsløsningen i AMS til tilleggstjenester. Likevel er det viktig å fastslå at nettselskapet skal legge til rette for at ulike former for tilleggstjenester kan tilknyttes AMS i fremtiden uavhengig at hvilke behov som måtte oppstå. For å sikre at AMS legger til rette for bruk av tilleggstjenester vil vi derfor foreslå at nettselskapet skal gi andre tjenesteleverandører adgang til å kommunisere over AMS.

[…] Kraftleverandører og leverandører av andre energitjenester skal derfor kunne benytte kommunikasjonsløsningen i AMS til å sende og motta informasjon og styringssignaler til og fra eksterne enheter hos sluttbrukeren.

Disse tilgangstjenestene skal altså bruke infrastrukturen i AMS til å kommunisere med smartmålere og styre HAN-system eller gi informasjon på display hos forbrukerne. Dette er også foreslått som en mulighet i en rapport ”Utveksling av informasjon ved innføring av AMS” [33], som er laget på oppdrag fra NVE:

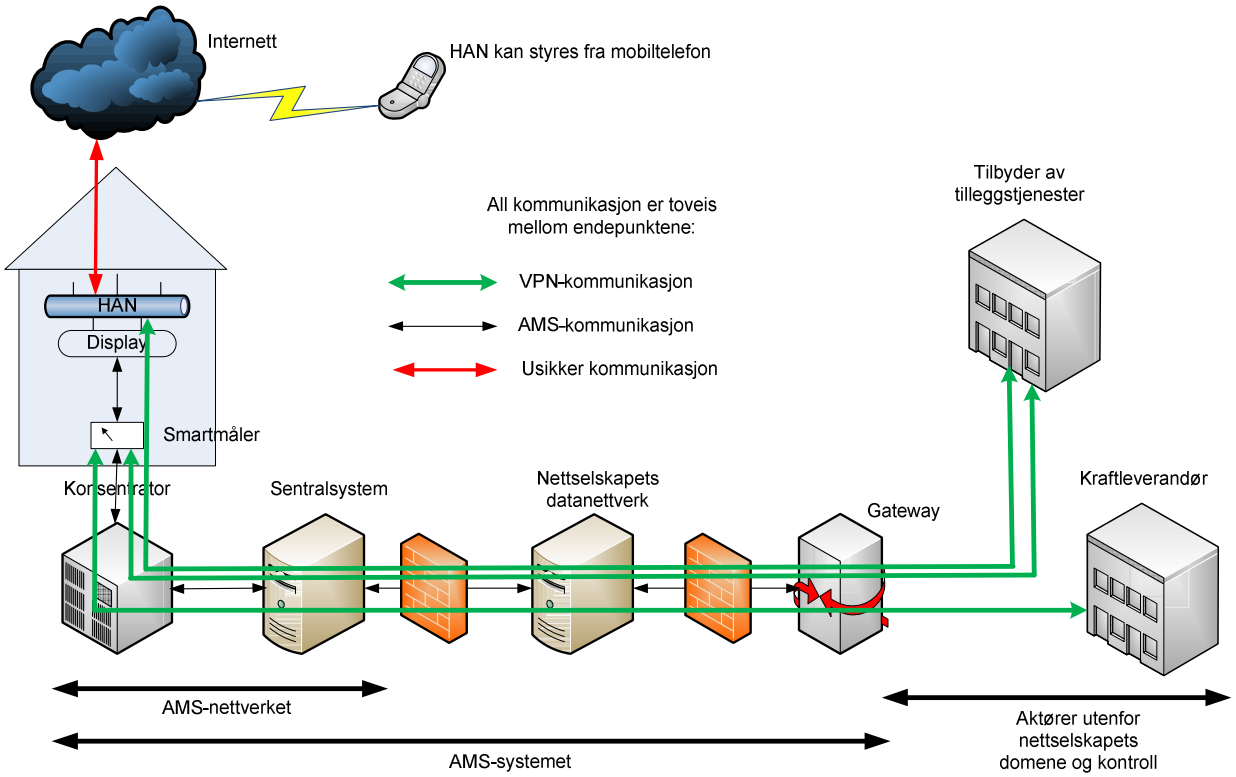
Tilsvarende, hvis løsningen(e) som velges i Norge gir mulighet for styring via målersystemet, bl.a. for at også netteier eller regionalnetteier og systemoperatør (i samarbeid med netteier) skal kunne styre, må det åpnes for at slik styring også kan utføres av tredjepart via nettselskapenes datasystemer. Det må vurderes om det skal stilles spesielle krav til tredjepart mht. slik tilgang til styring, og ansvarsforholdene mht. eventuelle feil som oppstår må avklares. En slik løsning vil ikke være til hinder for at tredjepart kan etablere egne løsninger via andre kanaler (bredbånd eller lignende).

Rapporten ”AMS-Tilleggstjenester, tredjeparts adgang” [34] ser for seg at man i hovedsak skal bruke Internett for tilleggstjenester, men at det kan være nødvendig at AMS-nettverket skal kunne brukes til styring og andre tjenester.

Figur 3-7 viser kommunikasjonen i et AMS-nettverk som brukes av tre forskjellige aktører: Nettselskapet (som ikke er tegnet inn med egen bygning), kraftleverandøren og en leverandør av tilleggstjenester. Det går tydelig fram av figuren at en åpning av AMS-systemet for andre aktører legger beslag på betydelig båndbredde i infrastrukturen. Dette er slik NVE foreslår tilgangene skal være, i sitt høringsutkast [13] fra februar 2011.

HAN og Display er i figuren koblet sammen med toveis kommunikasjon. Dersom tredjepart skal ha tilgang til HAN via AMS-nettverket, må kommunikasjonslinjen her være toveis.

Ved hjelp av tilkobling til Internett skal forbrukeren kunne fjernstyre HAN ved bruk av PC og/eller mobiltelefon. Dette for å kunne varme opp bygningen (eller andre behov) før ankomst. Forbindelsen mellom Internett og HAN er derfor vurdert som "Usikker kommunikasjon", siden den er satt opp av forbrukere som ikke nødvendigvis besitter kunnskap om IKT og sikkerhet. Det innebærer at tredjepart, som styrer HAN via AMS-nettverket, er særlig utsatt for angrep.



Figur 3-7 - Oversikt over kommunikasjonsløsning foreslått av NVE

Problemstillinger knyttet til den foreslåtte løsningen fra NVE er følgende:

- Båndbredde: Det er allerede lav båndbredde i det anbefalte systemet. Med den anbefalte PLC-kommunikasjonen er hastigheten mellom 21,4 kbps og 128,6 kbps. [35] Det forskes på å lage styringssystemer og IDS så enkle som mulig for å ikke bruke unødig båndbredde. Med flere aktører i nettet stjeles båndbredde fra AMS-nøkkelfunksjoner.

- Tilgang: Det blir flere aktører, flere å holde rede på, mer kompliserte brannmurer i systemet, hele nettverket blir mer uoversiktlig. For øvrig virker det urimelig at flere aktører; nettselskap, kraftleverandør og tredjepart, skal lese den samme informasjonen i smartmålerne.

- Sårbarhet: Det er lite sannsynlig at noen kan overta styringen av AMS gjennom tredjeparts tilgangsmuligheter, fordi kommunikasjonen sannsynligvis vil være direkte mellom forbruker og tredjepart. Dette kan gjøres ved at AMS-nettverket fungerer som en VPN-forbindelse. En slik kommunikasjon gjennom AMS-nettverket åpner for Flooding- og DDoS-angrep (se kapittel 2.3.2.3) som medfører at nettselskapet mister styringen over AMS. Faren for dette øker dramatisk når man bruker AMS-nettverket til kommunikasjon med HAN. Slike angrep kan igangsettes av aktører innen tredjeparts datanettverk, hackere som får tilgang til dette, hackere som via Internett får tilgang til HAN hos forbruker og av forbrukeren selv.

Fra kapittel 3.4.1 i NVEs høringsnotat [19] heter det videre:

Siden AMS-kommunikasjonen settes opp av nettselskapet med særlig fokus på sikkerhet og leveringskvalitet, vil AMS være en sikrere og mer tilgjengelig kommunikasjonsløsning enn Internett. Videre er det et sentralt poeng at kommunikasjonsløsningen som er satt opp for å bære AMS-data vil ha tilstrekkelig kapasitet til å bære tjenester som utføres av andre tjenesteleverandører. Krav om tilgang for tjenesteleverandører vil derfor ikke medføre ekstra installasjonskostnader i noen særlig grad.

Det er to betydelige innsigelser mot dette:

1. AMS-kommunikasjonen er i utgangspunktet svært sikker. Ved å innføre tredjeparts tilgang til smartmåleren gjennom dette systemet reduseres denne sikkerheten. Den reduseres ytterligere ved å la tredjepart styre HAN via AMS-nettverket.

2. Kommunikasjonskravet som er foreslått av Open Meter har svært lav båndbredde, der minstekravet er 2400 bps. (Tabell 2-5, OM-CR-3), og høyeste datahastighet i anbefalt løsning (Tabell 2-9, MI1-CI1) er 128,6 kbps. Andre aktører i AMS-nettverket vil begrense styringsfunksjonene i AMS-systemet direkte og indirekte. Dermed faller premisset om at "*kommunikasjonsløsningen […] har tilstrekkelig kapasitet*" ut.

I dokumentet D1.2, "Report on regularity requirements" [36] slår Open Meter fast at autorisert tredjepart skal ha garantert tilgang til måledata, men dette betyr ikke nødvendigvis tilgang til AMS-nettverket, slik det er formulert.

NVE ønsker i sitt høringsutkast adgang for tredjepart i AMS-nettverket og at tredjepart også skal kunne styre et HAN gjennom AMS. Dette vil kanskje[3] ikke være tilfelle i USA, der NIST i dokumentet "AMI Security Profile" [37], advarer mot en slik løsning:

The HAN is not controlled or owned by the utility, and should be treated as a hostile network by the AMI meter. Because of this, we recommend that AMI components should not request or accept information from HAN components. We recommend that AMI components should only push traffic to the home area network.

En slik push-funksjon (enveis kommunikasjon) er foreslått av Open Meter som en frivillig (Optional) implementering i kommunikasjonskravene, Tabell 2-5, OM-CR-20.

HAN vil typisk være tilknyttet Internett fordi mange vil fjernstyre elektriske enheter i hus og hytter, mens de er underveis. Det kan dreie seg om oppvarming av rom, sette på varmtvannsbereder o.s.v. Dette vil da typisk gjøres på en mobiltelefon som er koblet til HAN via Internett. Fra NIST-rapporten:

At this time components and systems connected to the Internet constitute a substantial increase in risk for the core functionality of the AMI system. Connections to the Internet and other public networks is discouraged for AMI systems.

[3] AMI Security Task Force (AMI-SEC-TF), som hovedsakelig jobber på oppdrag av energiverk, ser et bedriftspotensial i å åpne for tredjeparts kommunikasjon til HAN gjennom AMI [38]. Her foreslås også eHelse som en kandidat til en slik kommunikasjonsløsning. Det er derfor sterke krefter, også i USA, som ønsker å åpne AMS-nettverket for tilgang fra tredjepart.

Hvorvidt tredjeparts nettverk inngår i karakteristikken "other public networks" er ikke så lett å avgjøre. Det vil være svært vanskelig å kvalitetssikre nettverkene til selskap som tilbyr tilleggstjenester, ikke minst fordi slike nettverk kan være lokalisert i andre land.

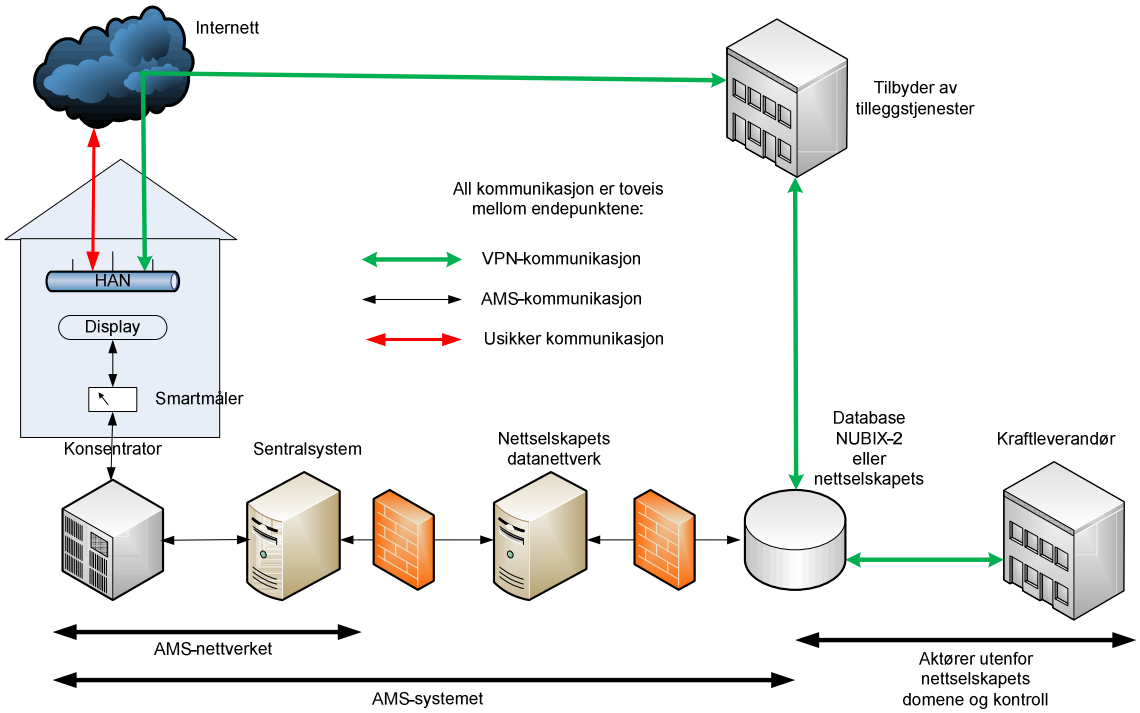
I Norge er 90 % av befolkningen tilknyttet Internett og 83 % har bredbåndstilknytning [39]. Dette innebærer at det allerede er klar en infrastruktur for fjernstyring av HAN via tredjepart.

To løsninger utkrystalliserer seg:

1) En sentral database med målerverdier enten hos nettselskapet eller hos Statnett der man har en database som hele tiden var oppdatert med målerverdier med høy nok oppløsning (for eksempel hvert 15. minutt) som tilfredsstiller krav til sanntid og hyppighet. Statnett har en Webtjeneste for oppslag av målepunkt [40], NUBIX, som kraftleverandører bruker for å innhente informasjon om målere hos nettselskap. Dette er ikke en database men et knutepunkt for informasjonsutveksling. I Avenirs rapport [41] foreslås det at NVE oppretter en sentral database, som de kaller NUBIX-2, som kan være et sted der måledata fra alle nettselskap kan være tilgjengelig for kunder, kraftleverandører og tredjeparter:

   En topologi som består i at kraftleverandører utelukkende forholder seg til NUBIX-2 og tilsvarende at nettselskapene gjør det samme vil redusere informasjons-kompleksiteten fra å være multiplikativ i antall aktører på hver side til å være additiv

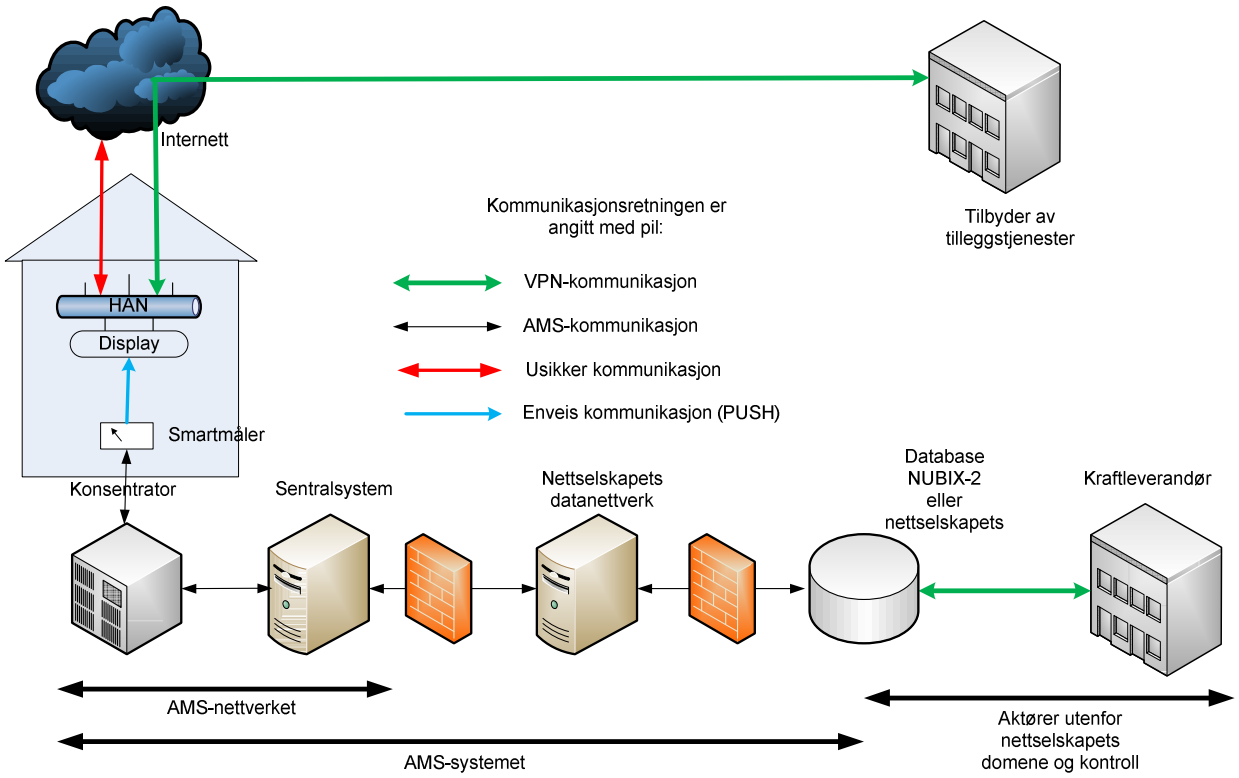
   Figur 3-8 viser denne løsningen, der det ikke er kommunikasjon mellom Display og HAN.



Figur 3-8 - Tredjepart med tilgang til ekstern database og HAN via Internett

2) Tredjepart får tilgang til måledata fra kunden direkte. Målerdata blir produsert av smartmåleren og presentert for HAN/dispaly/tredjepart. (PUSH-funksjon) Det foregår ingen toveis kommunikasjon mellom smartmåleren og dette eksterne utstyret. Avtaler mellom kunder og tjenestetilbydere blir dermed en sak mellom disse to og utenfor nettselskapenes domene. Dette gjør ansvarsforholdene enklere og dermed mer

oversiktlig. AMS-nettverket blir ikke belastet unødig og enklere å kontrollere (sikrere) for nettselskapet. Figur 3-9 viser denne løsningen.



Figur 3-9 - Løsning med tredjepart som bare har tilgang til HAN og Display gjennom Internett.

3.2.1.5 Trusselvurdering, oppsummert

Tabell 3-5 viser en oversikt over truslene beskrevet over. Det er verdt å merke seg at trusselen fra organisasjoner og stater påvirker trusselen fra tjenestetilbydere og ansatte. Organisasjoner og stater har presumptivt store ressurser og kan sette disse inn mot antatt svake punkt i en sikkerhetskontekst.

Tabell 3-5 - Risikovurdering Systemsikkerhet

Trussel fra	Sårbarhet	Sannsyn-lighet	Konsekvens	Mottiltak
Strømkunde	Manipulere med måledata	LITEN	Nettselskap og kraftleverandør taper penger	Hindre tilgang til måledata og se på lastbalansen i området.
Enkeltpersoner	Manipulere samt lese dynamiske strømverdier	LITEN	Innbrudd og annen uønsket effekt hos strømkunder	Bedre den tekniske sikkerheten.
Organisasjoner og stater	Manipulere med infrastrukturen	MODERAT	Destabilisere bygg og områder.	Øke teknisk sikkerhet og være obs på innsidetrussel.
Tjenestetilbyder	Gi informasjon videre	MODERAT	Personvern blir skadelidende	Oppsyn med tredjepart
Tredjepart	Belaste kommunikasjons-kanalen	MODERAT	Nettselskap mister kontroll over AMS nøkkelfunksjoner	Nekte tredjepart tilgang til AMS-nettverket
Ansatt, Innsidetrussel	Trues til å gi/ selge tilgang til AMS	MODERAT	Andre får tilgang til infrastrukturen	Utarbeide gode rutiner mot innsidetrussel.

3.2.2 Personvern

Nettselskap har lang erfaring med å omgås kundesystemer og dermed overholde de krav til personvern som NVE og datatilsynet krever. Selve AMS-systemet, slik det er spesifisert av Open Meter har innebygd gode rutiner for å overholde konfidensialitet, integritet og tilgjengelighet ved bruk av robuste krypteringsalgoritmer. Dataoppbevaringen og transporten fra smartmålerne til nettselskapets datasystem er godt sikret og det er liten grunn til å tro av personopplysninger kan komme på avveie her.

For de fleste nettselskap vil det derfor bli få nye utfordringer knyttet til personvern i forbindelse med etablering av AMS. Likevel er det grunn til å tro at personvernet vil svekkes i forbindelse med innføring av AMS.

Det største problemet ved innføring av AMS er tredjepart og kvalitetssikring av disse, slik at de overholder de norske kravene til personvern. Det vil også være interessant å kartlegge om tredjepart må forholde seg til norsk regelverk, dersom de for eksempel operer fra et annet land. Mye tyder på at EU har sett denne problemstillingen og det pågår nå et arbeid for å harmonisere personvernlovgivningen i EU og Norge. Datatilsynet i Norge er i dialog med EU om disse spørsmålene.

Selv med et forent regelverk innen personvern, vil kontrollmulighetene for å sjekke om tredjepart overholder regelverket svekkes. Også i Norge er dette et problem og Datatilsynet fastslår i en rapport knyttet opp til datalagringsdirektivet [42] at:

Det finnes allerede et strengt regelverk med hensyn til de trafikkdata som teleaktørene lagrer i dag. Kontroller fra tilsynets side viser imidlertid at det er betydelige utfordringer knyttet til selve etterlevelsen av regelverket. Ikke minst gjelder det den allerede eksisterende sletteplikten.

Det sier seg selv at med flere aktører som er i besittelse av sensitive personopplysninger blir kontrollen vanskeligere og mer uoversiktlig. Ikke minst fordi aktørene kan være etablert i et annet land og datasystemene med personopplysningene kan operere fra et tredje land.

I NVEs høringsnotat (se kapittel 2.1.1) er det oppgitt at timeverdier skal lagres i minst 3 måneder og maksimalt 15 måneder. Fra Datatilsynets uttalelse (se kapittel 2.3.4) er det argumentert for at personopplysninger som skal lagres skal knyttes direkte til fakturering. Det vil si at kunder med fastpris ikke skal ha hyppig avlesning av sine målere. Det ser ut at det er en diskrepans mellom NVEs krav og Datatilsynets uttalelser og at kravene til personvern ikke er fullstendig avklart, slik det nå foreligger.

Konklusjonen på personvern er at det er mange uavklarte forhold. Noen av disse går mot tredjepart, slik det er beskrevet over, mens noen går direkte på styre- og overvåkingsmulighetene slik det går frem av kapittel 4.1.

Jeg utarbeider ikke egen tabell i dette delkapitlet, men tar med funnene i en oppsummering for kapittel 3.2.2 og kapittel 3.2.3 i Tabell 3-6.

3.2.3 Driftsrutiner

Enhver virksomhet som operer med samfunnssårbare systemer bør ha en plan for hvordan sikkerheten skal ivaretas i organisasjonen. Politidirektoratet, Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet har gitt ut en meget god veileder [43] som tar opp en del av disse spørsmålene.

Det som fremheves i denne og alle andre publikasjoner angående sikkerhet er at sikkerhet er et lederansvar, men at ledelsen har lite forståelse og interesse for sikkerhet.

Hvis man ser på uttalelser fra Datatilsynet, NSM og utenlandske aktører innen sikkerhet er det videre forbausende ofte mangel på oppfølging for å implementere og vedlikeholde de driftrutinene som bedriftene selv har vedtatt. Regelverket og intensjonene er gode nok, men gjennomføringen blir for dårlig.

NVE ønsker å etablere et eget regelverk for drift av AMS. Det er ikke fastsatt noen tidsfrist på dette prosjektet, men inntil da, er kravet fra NVE at ”*AMS er et stort og omfattende system som også gjør kunder, nettselskaper og samfunnet mer sårbart. Nettselskapene må derfor utarbeide risikovurderinger og gjøre tiltak i henhold til disse vurderingene slik at ikke uautoriserte får tilgang til systemene*”. (Se kapittel 2.1.1).

Det som ofte skjer når statlige organ lager regelverk er at tilsynsrollen blir større og de faktiske tilsynene minker. Ganske enkelt fordi arbeidsmengden i de enkelte direktorater øker. Det er dessverre ingen automatikk i at politikere bevilger mer penger til tilsyn, selv om oppdragsmengden øker. Det arbeides for øvrig med en tverrdepartemental standard for styring av informasjonssikkerhet for statlige virksomheter og tjenesteleverandører. Dette arbeidet har Datatilsynet, i et høringssvar [44], stilt seg positive til.

ISO-27001 [45] er en internasjonal anerkjent standard for å drifte informasjonssystemer. Standardens formål er å tilby en modell for etablering, implementering, operere, overvåke, gjennomgåelse, vedlikeholde og forbedre informasjonssikkerheten.

Denne standarden er også tatt opp i Norsk Standard [46] og publiseres fra dem. Det er flere norske selskap som tilbyr denne sertifiseringen og de er alle akkreditert [47] fra Direktoratet for måleteknikk.

Fordelen med å ha en internasjonal standard som denne implementert i organisasjonen er flere:

- Det er en anerkjent, dynamisk standard for informasjonssikkerhet.
- Det er foretak, godkjente av Direktoratet for måleteknikk, som sertifiserer virksomheten. Disse sørger også for at sertifikatene vedlikeholdes og stiller dermed krav til at virksomheten er oppdatert innen sikkerhetsarbeid.
- Det offentlige slipper en tilsynsordning direkte med virksomhetene som er sertifisert.

Oppsummering i Tabell 3-6

.

3.2.4 Personvern og driftsrutiner, oppsummert

Tabell 3-6 oppsummerer de funnene jeg har gjort i kapittel 3.2.2 og kapittel 3.2.3. Jeg tar også med betraktninger fra kapittel 4.1 i denne tabellen.

Tabell 3-6 - Oppsummering av trusler mot personvern og driftsrutiner

Trussel mot	Sårbarhet	Sannsyn-lighet	Konsekvens	Mottiltak
Personvern	Ansvarsforhold og oppfølging	LITEN	Personvernet svekkes	Avklare ansvarsforhold og følge opp at loven blir etterlevd.
AMS, avdekke svindel (Kap.4.1)	Uten personopp-lysninger er det vanskeligere å finne kunde som stjeler strøm.	LITEN	Strømleverandør og nettselskap taper penger.	Sammenligne forbruk og produksjon og avdekke de som har unormalt lite forbruk.
Samfunnet (Samfunns-sårbarhet)	Manipulere med infrastrukturen	LITEN	Destabilisere bygg og områder.	Ha gode rutiner for drift, som for eksempel ISO-27001

3.3 Personsikkerhet - Liv og helse

AMS vil ha en del funksjoner innebygd som vil bedre kvaliteten på strømmen. Feil med strømkvaliteten vil bli raskt oppdaget og passende tiltak kan iverksettes for å unngå spenningstopper, jordfeil o.s.v. AMS skal også kunne strupe strømmen til et område, dersom det er ønskelig for å unngå overbelastning av nettet. Dette gjøres ved at strømmen kuttes ved en på forhånd fastsatt energimengde. Når strømmen kuttes, må forbrukeren manuelt koble inn strømmen igjen og samtidig sørge for at strømforbruket er under terskelen for nytt avbrudd.

AMS har også innebygd mulighet til å stenge strømmen til bygninger. Dette er regulert i forbrukerkjøpsloven [48] og det er også utarbeidet stengerutiner [49] av Olje- og Energidepartementet (OED) for dette, der det blant annet heter:

Før stenging kan skje, skal nettselskapet sende forbrukeren et skriftlig varsel om stenging. [Og videre at…] *forbrukeren bør ta snarlig kontakt med nettselskapet dersom stenging kan medføre fare for liv, helse eller betydelig tingskade, eller dersom forbrukeren har innsigelser mot grunnlaget for stengingen.*

Det er videre et ønske fra NVE, Open Meter og andre aktører at AMS skal kunne gi jevnere forbruk gjennom døgnets timer, ved at energikrevende utstyr brukes når belastningen på nettet er lavt. Dette skal forbrukeren selv eller andre aktører styre.

En forsert utbygging av AMS kan også forvolde problemer. I følge EUs mandat M/490 [50] skal arbeidet med standardiseringen være ferdig innen utgangen av 2012. Midt-Norge skal ha installert 80 % av sine smartmålere innen utgangen av 2013.

3.3.1 Struping og stenging av strøm

Det jobbes mot å tilby eHelse til pasienter, slik at de kan overvåkes og få behandling i egne hjem, der de før måtte på sykehus. Dette desentraliserte helsetilbudet skal muliggjøres gjennom Internettløsninger. Med en slik svak og sårbar gruppe, som er avhengig av overvåking, kan struping og stenging av strøm få fatale konsekvenser.

Slik stengerutinene er formulert av OED, finnes det en fare for at strømmen kan stenges, selv om det er fare for liv og helse. Kravet om "… *et skriftlig varsel*" er uheldig og man bør vurdere to alternativer:

1) Varsel om struping eller stenging av strøm må bekreftes mottatt av kunden og tilsvaret fra kunden må inneholde opplysninger om det er fare for liv, helse eller betydelig tingskade.
2) Det må foregå et samarbeid mellom nettselskapene og NAV, sykehus eller fastlege om at enkelte smartmålere skal unntas fra stenge- og strupefunksjonalitet. Dette registreres da i nettselskapets datasystem og umuliggjør disse funksjonene. Denne fremgangsmåten kan støte på personvernmessige implikasjoner.

3.3.2 Utjevning av nettbelastning

AMS er tenkt til å bidra med jevnere forbruk, slik at konsumenter av elektrisk kraft bruker kraftkrevende utstyr når strømmen er rimelig. Dette vil da være utstyr som man ikke er tidsavhengig av, for eksempel vaskemaskin, oppvaskmaskin, tørketrommel, lading av batterier

(el-bil og lignende), varmtvann o.s.v. Igangsettelse av slikt utstyr skjer enten via hjemmestyring eller ved at en tjenestetilbyder, med tilgang til forbruk og tariffer, styrer dette i et HAN.

Direktoratet for Sikkerhet og Beredskap (DSB) ser i en rapport [51] med bekymring på en slik utvikling, der det bl.a. slås fast at:

- 40 % av alle branner skyldes enten feil bruk eller feil i elektriske anlegg.
- 4 % av alle branner skyldes elektrisk feil i vaskemaskin, tørketrommel eller oppvask-maskin.

DSB er bekymret for at innføringen av AMS skal resultere i flere branner mens folk sover.

Alt forbruksmateriell som krever mye energi, produserer også mye varme. Det er også større belastninger på husets strømnett og overganger (stikkontakter, sikringer og lignende). Alt dette medfører økt brannfare og særlig i de nordiske land, med utstrakt trehusbebyggelse, vil dette kunne få fatale konsekvenser.

3.3.3 Forsert utbygging av AMS

EU er noe forsinket i sitt arbeide med å standardisere AMS i Europa. Norske nettselskaper ønsker å avvente dette arbeidet, slik at de kan få tilgang til et stort utvalg av standardiserte løsninger for implementeringen av AMS.

Det er derfor en mulighet for at det blir en opphopning av installasjoner mot fristen for ferdigstillelse i 2013 og 2015. (Fristen er den 1. januar etterfølgende år).

Også her advarer DSB i samme rapport [51] som over, med at det vil skje feil. Ikke minst p.g.a. omfanget denne installasjonsprosessen har. Det er allerede registrert brann tilknyttet montering av ny måler og DSB har avdekket mange ”kreative” løsninger som har vært benyttet. De påpeker særlig følgende utfordringer:

- Vær nøye med planlegging og sluttkontroll
- Følg alle krav fra produsent
- Endring av utstyr må gjøres i samarbeid med produsent
- Benytt måler som passer inn i anlegget
- Følg alle krav til EMC som følger FEL og NORM

Slik jeg ser det, vil et forsert arbeidstempo, med mye overtid medføre raske løsninger som ikke alltid er faglig begrunnet. Det bør derfor være et krav til uavhengig inspeksjon i forbindelse med installasjon av smartmålere i bygg, særlig siden tempoet forventes å bli høyt.

3.3.4 Personsikkerhet, oppsummering

Tabell 3-7 er en oppsummering av funn i kapittel 3.3. Grunnen til at ”sannsynlighet” er satt til MODERAT, er at funnene er viktige og at mottiltak må vurderes, fordi konsekvensene går på sikkerheten til forbrukerne. Det kan argumenteres med at gruppen som benytter seg av eHelse uansett er utsatt for strømbrudd. Jeg mener likevel at denne gruppen bør unntas fra strupe- og stengefunksjonalitet.

Tabell 3-7 - Oppsummering av aspekter ved personsikkerhet

Trussel	**Sårbarhet**	**Sannsyn-lighet**	**Konsekvens**	**Mottiltak**
Strupe/stenge strøm	Syke forbrukere (eHelse) kan settes i stor fare	MODERAT	Går direkte utover helsen til enkelte kunder.	Avklare bedre strupe- og stengerutiner for utsatt gruppe.
Flytte energi-krevende forbruk til natt.	Fare for brann mens folk sover.	MODERAT	Bygg og liv kan gå tapt.	Ikke flytte forbruk til tider der folk sover.
Forsert utbygging av AMS	Feilinstallasjoner	MODERAT	Dårlige løsninger, større brannfare.	Etablere uavhengig inspeksjon av monteringen.

3.4 Oppsummering av analyse

De fleste funnene som er gjort i kapittel 3, oppsummerer jeg kort i Tabell 3-8, og går igjennom under. En del av disse funnene blir ytterligere problematisert i kapittel 4, der andre sider ved løsningene diskuteres.

Tabell 3-8 - Oppsummering av funn i analysen

Opphav: Problem	Løsning	Henvisning
Smartmåler: Kan manipuleres ved strømbortfall	Bruk batterier	Kap. 3.1.1.2
Smartmåler: Lynnedslag kan ødelegge smartmåleren	Bør kunne levere strøm også om kommunikasjonsenheten skades.	Kap. 3.1.1.4
Smartmåler: Målerdata er ikke kryptert	Kryptere måledata som lagres i registrene	Kap. 3.1.1.5
Smartmåler: Struping og stenging av strøm kan få store konsekvenser.	Enkelte forbrukere bør unntas fra stenging og struping.	Kap 3.1.1.6. Kap. 3.3.1
Konsentrator: Kan manipuleres ved strømbortfall	Bruk batterier	Kap. 3.1.2.2
Konsentrator: Målerdata kan manipuleres	Kryptere måledata i registrene.	Kap. 3.1.2.5
Konsentrator: Hærverk og lignende	Overvåke trafostasjonene.	Kap. 3.1.2.6
Konsentrator: Falske alarmer.	Utarbeide rutiner for hvordan man skal forholde seg til utkoblede hovedsikringer.	Kap. 3.1.2.7
Strømkunde: Manipulerer forbruk	Bruke Open Meters foreslåtte infrastruktur	Kap. 3.2.1.1
Utenforstående: Manipulerer AMS	Kjenne problemstillingen, ha skepsis mot interesse ang. AMS fra utenforstående.	Kap. 3.2.1.2
Innsidetrussel: Manipulere AMS og kunde	Kjenne problemstillingen, ha forebyggende rutiner. ISO-27001.	Kap. 3.2.1.3
Tjenestetilbyder: Selger opplysninger videre.	Avklare ansvarsforhold rundt personvern.	Kap. 3.2.1.4
Tjenestetilbyder/tredjepart bruker båndbredde	Nekte tredjepart adgang til AMS-nettverket.	Kap. 3.2.1.4
Personvern: Hva kan gjøres?	Uavklart	Kap. 3.2.2
Informasjonssikkerhet: Ikke standardisert	Bruk tilgjengelig standard, ISO-27001	Kap. 3.2.3
Personsikkerhet: Trusler mot helse. (eHelse).	Ha kjennskap til brukere med spesielle behov	Kap. 3.3.1
Personsikkerhet: Trusler mot liv (brann)	Ikke bruke fjernstyring av utstyr når man sover.	Kap. 3.3.2
Personsikkerhet: Forsert installasjon	Ha uavhengig inspeksjon av monterte anlegg.	Kap. 3.3.3
AMS: Avdekke svindel	Uavklart	Kap. 4.1

Alle punkter over har jeg beskrevet i tilhørende kapitler, men en litt mer utfyllende beskrivelse til tabellen følger:

Smartmåler: Slik det er satt opp av Open Meter er bruk av batterier et valg. Jeg anbefaler å velge batterier, fordi dette gjør AMS betydelig sikrere, sett fra nettselskapets side. Dersom registerverdier ikke krypteres er det enda mer påkrevet med batteri-backup. Det medfører ekstra omkostninger (batteriskifte) og er ytterligere diskutert i kapittel 4.4.1. For å beskytte selve strømmåleren fra lynnedslag, bør det vurderes å dele smartmåleren i strømmåler og kommunikasjonsenhet. Dette vil sannsynligvis gjøre utskifting av ødelagte enheter billigere og leveransen av strøm til forbruker mer pålitelig. Stenging og struping av strøm kan få store konsekvenser i husholdninger som er tilknyttet eHelse. Det bør utarbeides egne stengerutiner for kunder med særskilte behov.

Konsentrator: Konsentratoren kan også manipuleres med strømbortfall og bør derfor ha batteri-backup. Også her bør man vurdere å kryptere registrene, og ikke bare kommunikasjonen, for å sikre dataintegriteten. Disse enhetene er utsatt for miljømessige påvirkninger, som lyn, vannskade, hærverk og lignende og bør bruke de mulighetene for overvåking som ligger innebygd i AMS-systemet. (Tabell 2-2 OM-GR-12 og OM-GR-17). Falske alarmer kan bli et problem. I Norge er det mange brukere som fjerner hovedsikringene ved lengre tids fravær. Dette vil gi kommunikasjonssvikt (ved bruk av PLC) og rutiner for dette må utarbeides av nettselskapene.

Manipulere AMS: En illojal strømkunde kan ønske å manipulere forbruket for å redusere strømregningen. Slik jeg ser det er mulighetene for dette små, forutsatt at de andre foreslåtte tiltakene er gjort. Utenforstående og innsidere er en større trussel mot AMS. De jobber ofte sammen og har felles interesser. For disse gruppene er det først og fremst viktig å ramme infrastrukturen og dermed skade samfunnet. Infrastrukturen kan rammes ved at utenforstående truer eller belønner folk på innsiden til å jobbe for seg, eller ved at utenforstående overbelaster kommunikasjonen i AMS, slik at styringsfunksjonaliteten blir umuliggjort.

Informasjonssikkerhet: Det er dessverre ingen krav til en enhetlig standard for drift av informasjonssystemer i samfunnskritisk infrastruktur. Denne rapporten har pekt på at særlig nøkkelhåndtering, innsidetrussel og ansvarsforhold (rollefordeling) må avklares. Et slikt system er etablert i ISO-27001 og mange norske firma tilbyr å sertifisere virksomhetene etter denne standarden.

Personvern: Det må avklares om lovverket for personvernet, personopplysningsloven, kan anvendes på tredjepart hvis datalagringen foregår utenfor Norges grenser. Det er også interessant å finne ut om personopplysninger kan brukes i konsentrator for å finne kunder som stjeler strøm. (Se kapittel 4.1).

Personsikkerhet: Problemstillingen rundt innføring av eHelse er tatt opp under **Smartmåler**. I tillegg har DSB uttalt bekymring for økning av brannfare, med fatalt resultat, ved forskyving av strømforbruk til nattestid. En forsert utbygging av AMS kan også øke brannfaren, mener DSB.

4 Diskusjon og innspill

Kompleksiteten og omfanget av programvare og maskinvare som skal installeres og igangsettes i AMS, er så omfattende at en fullstendig sikkerhetsanalyse er umulig. Både hva som kan gå galt og konsekvensene av dette vet man ikke før det er gått noen år og det er høstet erfaringer fra systemet. Det er likevel mulig å avdekke mulige sikkerhetshull og fokusere på de svakhetene som er avdekket i denne rapporten. AMS må også være dynamisk av natur slik at det kan tilpasses nye krav til sikkerhet som følge av et endret trusselbilde.

Det vil derfor være av stor betydning at man følger de anbefalingene fra NIST, Open Meter og NVE om å bruke åpne[4] systemer. Dette sikrer tilgang til maskinvare og programvare fra mange tilbydere og gjør det mindre sannsynlig at man sitter med et utdatert, statisk system.

De resultatene som fremkommer i oppsummeringen, er for oversiktens skyld, også tatt med i kapittel 3.4. (Tabell 3-8).

4.1 Dataintegritet og personvern

Nettselskapene er bekymret for at konsumenter manipulerer med forbruket, slik at data fra målerne ikke er korrekte. Dette kan gjøres på flere måter:

1. Ved å koble seg inn på smartmåleren og endre registerverdiene. Det går frem av kapittel 3 at dette er svært vanskelig, fordi sikkerheten rundt smartmålerne er godt ivaretatt. På den annen side vil eventuelle muligheter og svakheter i disse målerne raskt være tilgjengelig på Internett, slik at mange forbrukere kan tenkes å utforske og benytte seg av, slike mulige svakheter.

2. Ved å koble seg forbi smartmåleren. Enkelte forbrukere besitter kunnskap til å gå inn i sikringsskapet og rett og slett koble ut smartmåleren. Slik AMS er foreslått satt opp av Open Meter, vil slike hendelser avdekkes med en gang. Sentralsystemet vil miste kommunikasjonen med smartmåleren og hendelsen rapporteres til nettselskapets datasystem.

3. Ved å ta ut strøm før smartmåleren. Det finnes eksempler på at det kobles inn lastkrevende utstyr i hovedsikringen. Strømmen som da forbrukes, vil aldri nå smartmåleren.

AMS gir nettselskapene verktøy for å overvåke strømforsyningen på en helt annen måte enn tidligere. Det vil være enklere å kontrollere og sammenligne oppgitt forbruk med produsert kraft.

[4] Det er for øvrig interessant å merke seg at i dagens samfunn etterstrebes åpne, standardiserte systemer, fordi det er antatt at disse er utsatt for omfattende analyser for å finne hull og svakheter. Åpne standarder er derfor å foretrekke fordi de har vist seg robuste mot angrep. Fra rapporten Beskyttelse av Samfunnet, BAS3[25]fra 2001, er det bekymring for bruk av standardiserte systemer:

Kraftleverandørenes IKT-systemer vil i økende grad baseres på standardiserte systemer med kjente sikkerhetshull, som sammenkoples for å oppnå effektive markedsmekanismer.

Den samme skepsisen til åpne systemer finner vi i Sårbarhetsutvalgets[24] rapport fra 2000. Dette er ikke noe særnorsk fenomen. GSM mobiltelefoni ble laget med fokus på Security by Obscurity, dvs. at man ønsket å skjule sikkerhetsmekanismene, her:krypteringsalgoritmen. Da den tilslutt lekket ut på Internett ble svakhetene funnet ganske raskt, og denne første krypteringsalgoritmen regnes nå som utilstrekkelig for GSM. I UMTS brukes åpne, standardiserte algoritmer.

Trafostasjonene kan inneholde en smartmåler, slik at konsentratoren kan sammenligne forbruk og produksjon i sanntid. Det er også mulig å legge inn algoritmer som sjekker den enkeltes forbruk og sammenligner disse med historiske verdier. Dette er sannsynligvis en mer omstendelig prosess, ikke minst fordi forbruk kan endres svært mye over kort tid.

Konklusjonen er at manipulering, slik det er listet opp over, vil være svært vanskelig i AMS. Nettselskapene kan stole på at dataintegriteten er ivaretatt, men det må tas forbehold om at nettselskapene kan bruke de mulighetene AMS gir. Det kan være personvernmessige forhold rundt dette som er problematiske og må avklares. Datatilsynet er i sin "Veileder for bruk av personopplysninger i AMS", (se kapittel 2.3.4) svært klare på at personopplysninger bare kan knyttes opp mot fakturering. Det må derfor søkes på nytt om man ønsker å bruke personopplysninger for å avdekke misbruk av strøm.

Det er mulig det kan trekkes en parallell til måten data blir behandlet på i systemet for automatisk måling av gjennomsnittsfart [52]. Her blir alle personer og biler registrert i systemet, men bare de som overskrider fartsgrensen blir lagret automatisk for så å bli bøtelagt. Alle andre data om lovlige passeringer blir automatisk slettet, slik at de ikke kan hentes frem i ettertid.

Hvorvidt dette er en metode som kan anvendes i AMS kreves det juridisk ekspertise til å avgjøre.

Open Meter har ikke tatt stilling til personvern utover å påpeke at de nasjonale personvernregler i hvert land skal følges. Enkelte ting tyder på at det etter hvert vil bli et harmonisert personvernlovverk i Europa. Datatilsynet har mottatt en henstilling fra EU om å besvare spørsmål knyttet til innføring av AMS i Norge. Datatilsynet slår fast [53]:

Målet med kartleggingen av medlemslandenes retningslinjer for automatiske målesystemer er å utarbeide en felles EU-standard for innføring og bruk av AMS innenfor EU-direktivet for energibesparing. Felles retningslinjer skal sørge for at datasikkerhet, håndtering av måleropplysninger og personvern ivaretas ved innføringen av automatiske målere. EU har også som et mål å bidra til at introduksjonen av slike målere blir enhetlig i alle medlemslandene.

Hvorvidt personvernet vil styrkes eller svekkes av en slik integrasjon, gjenstår å se, men det er sterke krefter som vil muliggjøre alle sider ved AMS, for å fremme sikkerhet og avdekke svindel.

4.2 Tredjeparts tilgang til AMS

Parallelt med denne masteroppgaven har det blitt utarbeidet en rapport "Felles IKT-løsninger i det norske kraftmarkedet" [55] på oppdrag fra NVE. Rapporten konkluderer med at det bør lages:

UTVIDEDE FELLESSYSTEMER med en felles måleverdidatabase og sentrale behandlingsfunksjoner for å administrere ajourføring av informasjonsinnhold, tilgang til database og AMS-nettverk samt bearbeiding av felles data. Det foreslås etablert et sentralt måler-register og en felles måleverdidatabase. I første omgang bør det utvikles noen felles kjernefunksjoner som kvalitetssikring av data, forsvarlige autorisasjons- og autentiseringsregimer og tilrettelegging for statistikkfunksjoner og prognostisering.

NVE stiller seg positive [56] til en løsning med felles IKT-løsning og felles måleverdidatabase for kraftmarkedet. Det er en del juridiske og organisatoriske forhold som må avklares og NVE påpeker at denne løsningen bør kunne gjennomføres med dagens regelverk.

I kapittel 3.2.1.4 gikk jeg gjennom tredjeparts tilgang til AMS-nettverket, der en delkonklusjon var det samme som er sagt her: Nemlig å sentralisere databasene for måleverdier. Mitt fokus er

sikkerhet i AMS og derfor er det enda mer alvorlig at ikke det sentrale punktet jeg tok opp er avklart, nemlig:

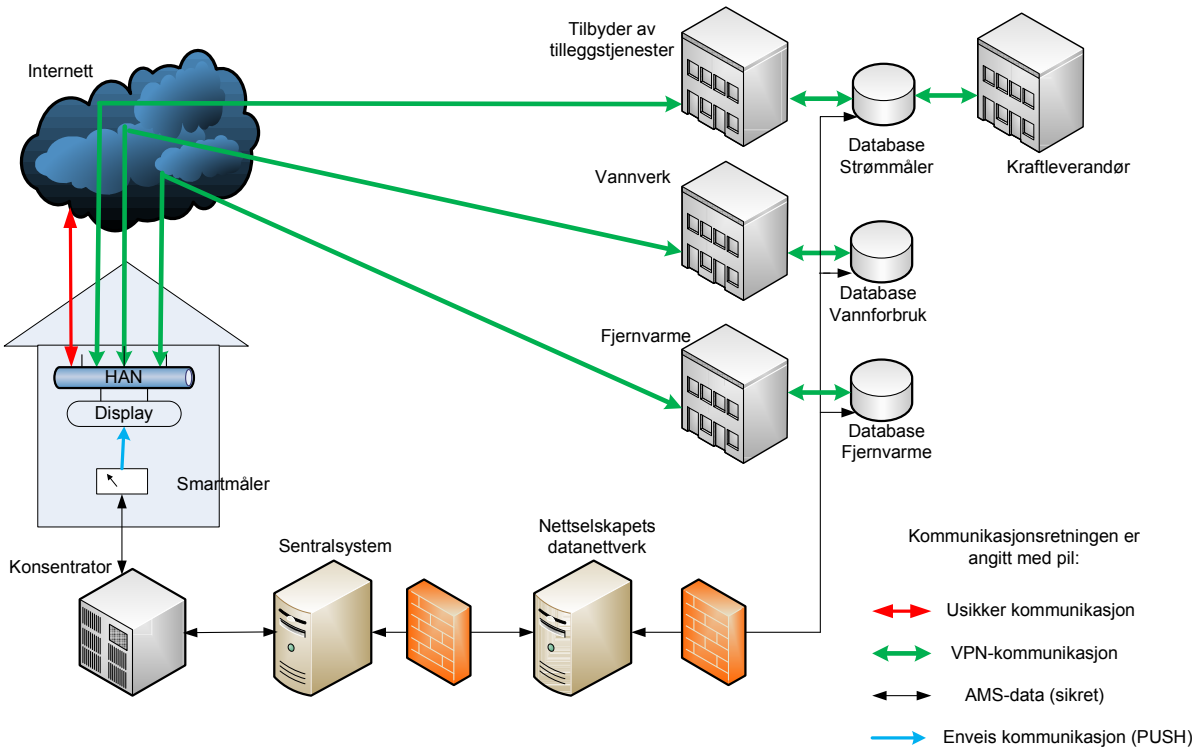
Tredjeparts tilgang til kommunikasjon med HAN gjennom AMS-nettverket.

Etter hvert vil sannsynligvis vannverk og fjernvarmeanlegg også ha interesse av tilgang til måledata fra AMS. Disse kan også være interessert i fjernstyring av vanningsanlegg og varme gjennom AMS-nettverket. En slik ytterligere belastning av båndbredde og redusert sikkerhet er ikke ønskelig.

Open Meter har skissert en mulighet til å umuliggjøre dette, nemlig ved at smartmåleren bare kan ha enveis grensesnitt mot forbrukerens utstyr (Tabell 2-5, OM-CR-20). Målerdata blir kun presentert for forbrukeren gjennom grensesnitt MI5, men kommunikasjon med smartmåleren utover det, blir ikke mulig. Hvis slike smartmålere installeres, er det ikke mulig å bruke AMS-nettverket til kommunikasjon med HAN.

Figur 4-1 viser et forslag til hvordan AMS, etter mitt syn, bør implementeres, der det er tatt hensyn til de mulighetene som ligger i Open Meters anbefalinger.

Det er i utgangspunktet ikke kritisk at tilbyder av tilleggstjenester, vannverk og fjernvarmeanlegg har tilgang til dedikerte databaser, siden de slik det fremgår av figuren, er direkte tilkoblet kunden via Internett og har dermed tilgang til kundens display med sanntids måleverdier. Dessverre åpner dette også for en mulighet for at kunden kan manipulere display, siden det ikke er toveis kommunikasjon med smartmåleren og dermed ingen alarmer eller varsler som kan kommuniseres til AMS-nettverket. Det er derfor å anbefale at nettselskapene presenterer alle målerverdier fra et AMS-system i dedikerte databaser tilgjengelige for kunder og tredjepart.



Figur 4-1 - Løsning med desentraliserte databaser og ingen tredjepartstilgang i AMS-nettverket

Det er programvaren som åpner for kommunikasjon med andre enheter, men det må være muliggjort gjennom maskinvaren. Det er derfor mulig på et evt. senere tidspunkt, å endre kommunikasjonen mellom smartmåler og Display fra å være toveis, til å bli enveis (PUSH). Dette gjøres da gjennom en oppgradering av programvaren i smartmåleren.

Andre vurderinger rundt tilleggstjenester

I kapittel 3.3.2 fremkommer det bekymringer fra DSB om brannfare ved bruk av fjernstyrte tilleggstjenester. Bruk av effektkrevende utstyr medfører økt brannfare. Det fremkommer også i en rapport fra Fjordkraft [57] at ved å flytte forbruket fra kl. 17 til kl. 04 for vaskemaskin, oppvaskmaskin og tørketrommel, blir samlet besparelse pr. år kr. 45,- (1500 kWh, 2009).

Uten mer bevisste prisstrategier vil neppe forbruket endres så mye, som bransjen og NVE legger opp til og det spørs om markedet for leverandører av tilleggstjenester overhode eksisterer.

Etter hvert som flere hus tar i bruk smart teknologi for fjernstyring av huset, vil også styresystemer som kan forholde seg til informasjon fra smartmåleren være tilgjengelig. Det er grunn til å tro at prisen på slikt utstyr vil bli svært lav om noen år, siden markedet i Europa blir på flere millioner enheter.

Det er for øvrig grunn til å stille seg spørrende til hvordan utjevning av belastningen i nettet skal foregå. Vil prisen kunden får fra kraftleverandøren være historisk, i sanntid eller neste tidsepoke? Følgende problemstillinger knytter seg til de tre scenarioene:

- Historisk prising: Hvis prisen for kraft var rimeligst kl. 04 foregående natt vil automatiske distribuerte systemer (d.v.s. tredjepart eller utstyr tilknyttet smarte hus), sette på mye utstyr til samme tid påfølgende natt og prisen på kraft vil øke. Besparelsen blir med andre ord minimal.
- Prising i sanntid. Det blir vanskeligere å fjernstyre ressurskrevende utstyr, fordi man må forholde seg til terskelverdier, som kanskje ikke inntreffer.
- Fremtidig pris: Dersom man vet prisen gjennom alle timer i det neste døgnet, vil ressurskrevende utstyr bli koblet inn på gunstigste tidspunkt. Kraftleverandørene kan bruke en slik prissetting og differensiere prisene til de forskjellige forbrukerne gjennom døgnet og dermed unngå forbrukstopper. Men det er usikkert om en fremtidig pris vil være riktig estimert, siden prisen på elektrisk kraft er gjenstand for tilbud og etterspørsel.

Summerer man opp brannfare og muligheter for besparelse slik det er nevnt over, er det stor sannsynlighet for at forbrukere vil avstå fra fjernstyring av elektrisk utstyr mens de sover.

4.3 Frist for igangsetting av AMS

Det har vært satt flere årstall for ferdig utrulling av AMS i Norge. Olje- og Energidirektoratet har fastslått at 80 % av forbrukerne i midt-Norge skal ha smartmålere installert innen 2013 og 80 % av forbrukerne i landet for øvrig, innen 2015.

De første standardene fra EU er tilgjengelig på slutten av 2012 [50], og da har nettselskapene i midt-Norge et år på å nå målsettingen. I følge en artikkel i Teknisk Ukeblad [58] mener administrerende direktør for Energi Norge, Oluf Ulseth at "*Vi opplever 2013 som ekstremt ambisiøst. 2013 var et veldig annet signal enn bransjen har fått så langt*"

Konkurransetilsynet ga den 6. mai 2011 tilsvar [59] på høringsutkastet fra NVE der de bl.a. skriver:

Konkurransetilsynet etterlyser en nærmere analyse av den samfunnsøkonomiske lønnsomheten ved innføring av AMS i minst 80 prosent av målepunktene i Midt-Norge allerede innen 1. januar 2014. Konkurransetilsynet vil foreslå at det utføres en nytte- og kostnadsvurdering vedrørende en slik tidlig implementering.

Det bør vurderes om man i Norge skal avvente EUs standardiseringsarbeid og bruke den opprinnelige planen om installasjon av AMS innen 1. januar 2018, i stedet for den fremskyndte planen fra Olje- og Energidirektoratet. Se også kapittel 3.3.3.

4.4 Drift av AMS

Fra kapittel 3.2.3 er det anbefalt å bruke et allerede innarbeidet system for informasjonssikkerhet, ISO-27001. Dette kapittelet vil påpeke enkelte sider ved AMS som uansett driftssystem krever særskilte tiltak og rutiner.

4.4.1 Batteri-backup

Det er i kapittel 3 foreslått at alle utplasserte enheter i AMS-nettverket bør ha ekstra batterier som driver enhetene ved strømbortfall. I Tabell 2-4, OM-TR-2 over tekniske krav, er det foreslått at strømmåler og konsentrator skal ha batteri-backup. Dette er et såkalt avansert krav og dermed ikke et av minimumskravene til AMS-nettverket. Dette vil medføre økte vedlikeholdskostnader for nettselskapene og går på bekostning av kravet om å velge utstyr som reduserer vedlikeholdet. (Tabell 2-2, OM-GR-21)

Man må vurdere om dataintegriteten er nok ivaretatt uten strøm-backup. Denne rapporten anbefaler likevel strøm-backup fordi de enkelte komponenter vil være bedre beskyttet mot fysisk påvirkning, siden hendelser som skjer mot utstyret kan lagres når nettverket er nede.

Nettselskapene må, ved implementering av batteri-backup, utarbeide rutiner for utskifting av batterier. Dette må også gjøres i forbindelse med eksterne målere (vann, varme etc.) som er batteridrevne i utgangspunktet.

4.4.2 Ytre påvirkninger

I kapittel 3 er det påpekt at naturødeleggelser og lynnedslag kan skade systemet og at slike hendelser må få begrenset omfang for resten av systemet.

I boka Security Engineering [54] er det omtalt installasjon av kredittstrømmålere, d.v.s. elektroniske målere der det forhåndsbetales for strømforbruket. Dette gjøres på flere måter, men vanligvis er det en nøkkel som kjøpes og denne er knyttet til en bestemt måler. Denne installeres (via et kort) i måleren og måleren vil da levere strøm inntil kreditten er oppbrukt. Det var ingen toveis kommunikasjon, men det fantes statisk balanse innebygget i system, slik at man i etterkant kunne få en oversikt over om levert strøm samsvarte noenlunde med kreditert strøm. Ved lynnedslag gikk svært mange målere i stykker og kundene klagde over dette og måtte da oppgi til kraftleverandøren og nettselskapet hvor mye strøm de hadde forbrukt. (Siden det ikke var toveis kommunikasjon måtte selskapene stole på kundens opplysninger når de utstedte et nytt strømkredittkort ved slike uhell). Etter hvert ble det en forståelse for at det var de ”heldige” som

fikk lynnedslag, fordi de kunne jukse med kreditten. Dette utviklet seg til at folk begynte å bruke husets strømkabler direkte på strømmåleren for å simulere lyn mot denne. Gjennom denne metoden viste det seg at det var mulig å få maksimal kreditt hvis en spesiell del av kretsen i måleren ble ødelagt. Etter hvert fant man også ut at et spenningsfall fra 220 Volt til 180 V ga måleren maksimal kreditt. Dette resulterte i at barn i området kastet kjettinger på høyspentlinjer (11 kV) for å få spenningsfall over et stort område, som da fikk maksimal kreditt.

Det denne historien bl.a. viser er at kunder kan gå til dramatiske skritt for å "lure" systemet. Når en svakhet er avdekket sprer denne løsningen seg svært fort og særlig i vår tid, der Internett gjør informasjon bredt tilgjengelig på kort tid. Det er umulig å kunne helgardere seg mot den oppfinnsomhet og intensitet som noen oppviser for å knekke et system.

Videre kan lyn få andre utilsiktede konsekvenser som det kan ta tid å lokalisere og oppdage: Styresignaler ut i AMS-nettverket kan bli korrupte og uønskede effekter inntreffer, som for eksempel stenging av strøm. Avlesningsverdier kan bli ødelagt eller endret slik at kunder eller nettselskap får feil i avregningen.

Det finnes en del systemer for selvtest i AMS-enhetene. Det er viktig å bruke disse mulighetene med jevne mellomrom for å verifisere at utstyret er intakt.

Enkelte har kalt det nye smarte nettet (integrert strømnett og AMS) for *verdens største lynavleder, med en mikroprosessor i alle endepunkt*. Det er stor mulighet for at hundrevis av smartmålere og/eller kommunikasjonsenheter kan ødelegges i et lynnedslag. Nettselskapene må ta høyde for dette i fremtiden.

4.4.3 Nøkler

Krypteringsalgoritmen og nøkkellengden som er valgt av Open Meter er svært god. Dette vil gjøre det vanskelig å få tilgang til data og styresignaler innen AMS-systemet. Med tilgang til nøkler ligger derimot systemet åpent for manipulering.

Distribusjon, oppbevaring og generering av nøkler er derfor svært kritisk innen nettverket. Denne rapporten kan ikke gå inn på disse prosessene i nevneverdig grad, siden dette ofte blir ivaretatt av proprietære systemer.

Det er likevel viktig at nettselskapene har utarbeidet gode rutiner for tilganger til nøklene og for kompromitterende hendelser. Nøkler kan komme på avveie ved at utstyr blir stjålet, kassert eller ved at uautoriserte, utenfor eller innenfor, får tilgang til dem.

4.4.4 Tilgang og rollefordeling

Det bør utarbeides rutiner i nettselskapene for å avklare ansvarsforholdene i alle ledd i forbindelse med innføring av AMS. Dette er særlig viktig for de operatørene som skal stå for styringsfunksjonaliteten og nøkkelhåndtering. Systemet må klart kunne identifisere hvem som igangsatte prosesser i nettverket. (Se også Tabell 2-2 OM-GR-1, OM-GR-17 og Tabell 2-3 OM-FR-145). Det kan også vurderes om det bør være to personer for å utøve særlige kritiske operasjoner, som stenging og lignende. Den ene personen (fakturaavdeling eller lignende) kan initiere prosessen og den andre (driftsoperatør) kan utføre operasjonen. Dette vil gjøre sporbarhet og ansvarsforhold oversiktlig og begrense feil.

4.4.5 Oppsummering

Innsidetrussel er tatt opp i kapittel 3.2.1.3, men er tatt med i Tabell 4-1 for å samle viktige driftsrutiner i en oversiktlig tabell.

Tabell 4-1 - Fokus på viktige sider ved driftsrutinene

Hva	Hvorfor	Hvordan
Batteri-backup	Sikrer smartmåler og konsentrator mot manipulering ved kommunikasjonssvikt.	Utarbeide driftsrutiner for batteribytte
Ytre påvirkning	Beskytte utstyr mot skade og være oppmerksom på at utstyret er utsatt.	Utarbeide driftsrutiner for utskifting av desentralisert utstyr (smartmåler, konsentrator) og kjøring av selvsjekk på utstyret.
Nøkler	Nøkler på avveie bryter med integritet, konfidensialitet og autentisitet.	Utarbeide driftsrutiner for oppbevaring og distribusjon av nøkler. Avklare rollefordeling.
Tilgang	Systemet må gjennom logg kunne fremvise hvem som har tilgang og tidspunkt.	Avklare rollefordeling og tilganger innen nettselskapet.
Innsidetrussel	Innsidetrussel er kanskje den største trusselen mot manipulering av AMS.	Være observant på problemstillingen og utarbeide rutiner for håndtering.

4.5 Oppsummering av diskusjon og innspill

Dette kapitlet har tatt enkelte funn fra kapittel 3 opp til diskusjon. Jeg har i denne diskusjonen prøvd å holde et videre perspektiv, men dette har ikke endret hovedinnholdet i antagelsene og funnene fra kapittel 3, som derfor blir stående. Jeg har også laget en betenkning (kapittel 4.3) om at det finnes argumenter for den opprinnelige datoen (01.01.2018) for ferdigstillelse av AMS.

Tabell 4-1 inneholder i hovedsak funn fra forskjellige delkapitler i kapittel 3. En del av disse er diskutert videre i kapittel 4.4 og samlet i en tabell for oversiktens skyld.

5 Konklusjon

Norske nettselskap står foran betydelige investeringer i årene fremover når det gjelder Automatiske måle- og styringssystemer, omtalt som AMS. Dette setter store krav til sikkerhet, ikke minst fordi strømnettet er en viktig del av samfunnets infrastruktur og dermed et utsatt og yndet mål for sabotasje.

AMS er utsatt for manipulering av forbrukere, utvendige aktører og utro tjenere innen nettselskapene. Som et desentralisert nettverk, der mange komponenter er utenfor nettselskapenes oppsyn, er det også utsatt for fysisk påvirkning, som hærverk, lyn og andre naturskader.

AMS samler inn opplysninger om forbrukere og kan dermed avdekke forbruksmønster. All informasjon om forbrukere kan misbrukes og dette setter store krav til personvern.

Det er tatt utgangspunkt i NVEs høringsnotat og Open Meters publiserte dokumenter for å få en oversikt over AMS. Ut i fra disse dokumentene har det reist seg problemstillinger som går på sikkerhet og personvern.

Rapporten har hatt fokus på tre problemområder:

- Systemsikkerhet eller overordnet sikkerhet: Avdekke svakheter i operasjon og organisasjon av systemet.
- Sikkerhet i AMS: Avdekke svakheter i AMS-nettverket på komponentnivå.
- Personvern: Avdekke svakheter i personvernet.

Min innstats, med bakgrunn i publikasjonene fra NVE og Open Meter, har vært å identifisere og analysere problemområdene for å kunne foreslå tiltak.

Systemsikkerhet – Overordnet sikkerhet

NVE foreslår at tredjepart skal ha adgang til AMS-nettverket og kunne styre forbrukerelektronikk (HAN) gjennom dette. Denne rapporten anbefaler ikke en slik løsning og foreslår:

1. Nettselskapene har en ekstern database som produserer måledata med en hyppighet som tilfredsstiller kravene fra tredjepart.
2. Tredjepart styrer HAN via Internett og ikke via AMS-nettverket.

Ved å la flere aktører få bruke AMS-nettverket reduseres båndbredden i systemet og det kan gå utover funksjonaliteten og dermed sikkerheten i AMS. Flere aktører medfører også mindre oversikt over tilgang, fordi det blir flere å holde rede på.

Forbrukerelektronikken som skal styres gjennom AMS er gjerne koblet sammen i et HAN, som igjen er tilkoblet Internett. Dette gir en direkte åpning mellom Internett og tredjeparts datasystem gjennom AMS-nettverket. Tredjeparts datasystem er dermed eksponert for flooding og DDoS, noe som vil føre til overbelasting av AMS-nettverket og det vil dermed ikke kunne styres av nettselskapene. Fra et sikkerhetssynspunkt vil det være svært viktig å nekte tredjepart all adgang, direkte og indirekte, til AMS-nettverket. (Se Figur 4-1).

AMS skal muliggjøre en jevnere belastning av strømnettet ved at forbrukere kobler inn strømkrevende utstyr når strømmen er rimelig. Dette vil da typisk skje på natten, når folk sover. DSB advarer mot en slik utvikling, siden strømkrevende utstyr produserer mye varme og

brannfaren øker. Dette utgjør en fare for liv og helse. Mye tyder på at man ikke får den utjevnende belastningen av strømnettet som er ønsket, nettopp fordi det vil gå på bekostning av personsikkerheten.

Litt frem i tid vil eHelse være en realitet i mange hjem. Stenging eller struping av strøm hos personer som benytter dette tilbudet, kan få store konsekvenser. Man bør vurdere muligheter for å fange opp denne gruppen i nettselskapets datasystem, slik at visse bygg/personer er unntatt fra strupe- og stengefunksjonalitet.

Den største trusselen mot AMS-systemet er trusselen innenfra. Sentrale medarbeidere i nettselskapet kan bli satt under press eller lokkes økonomisk, slik at utenforstående får tilgang til systemet. Innsidetrusselen er reell også i Norge, men er vanskelig å avdekke. Det er også gjort forholdsvis lite forskning på dette. Det er viktig at nettselskapene erkjenner denne trusselen og utarbeider rutiner som søker å minimere den og også holder seg oppdatert på ny forskning innen dette feltet.

Selve kommunikasjonen i AMS, slik det er foreslått av Open Meter, er godt beskyttet mot avlytting og manipulering. Meldinger over nettverket krypteres med en såkalt AES krypteringsalgoritme med 128 bit nøkler. Dette forutsetter imidlertid at nettselskapene har innarbeidet gode og sikre rutiner for bruk og oppbevaring av nøkler i eget datasystem. Det er derfor viktig at håndtering av nøkler blir en sentral del av systemsikkerheten innad i bedriften.

NVE har planer om å utarbeide rutiner for drift av AMS. Disse bør være prioritert fremover, slik at dette kommer på plass før AMS implementeres. Det kan være en god idé å kreve ISO-27001-godkjennelse av nettselskap, siden dette er en etablert internasjonal standardisering av sikkerhet i et informasjonssystem, og som etterses og vedlikeholdes av private, statlig akkrediterte, operatører.

Sikkerhet i AMS

Open Meter har mange minimumskrav i sine anbefalinger. I tillegg kommer avanserte og frivillige krav. Ved å implementere enkelte av de to sistnevnte kan sikkerheten i AMS-nettverket økes ytterligere.

Denne rapporten anbefaler å bruke batteri-backup i konsentrator og smartmåler, slik at disse enhetene ikke kan manipuleres med når strømnettet er nede, eller sikringer er fjernet. Dette øker sikkerheten for AMS-nettverket, men medfører også økte vedlikeholdskostnader for nettselskapene.

Det anbefales også at alle måledata er kryptert i registrene slik at de ikke kan hentes ut av smartmålere og konsentratorer, ved kassering av utstyr eller ved en tilgangsmetode.

Nettselskap i Norge må vurdere tiltak i forbindelse med fjerning av hovedsikringer i bygg. Enkelte hus- og hytteeiere tar ut hovedsikringer ved langvarig reisevirksomhet og lignende. Fjerning av hovedsikringer vil øyeblikkelig gi en logisk alarm i AMS-systemet. Rapporten har forelått å forby fjerning eller ha meldeplikt ved utkobling.

Det bør vurderes om smartmåleren skal bestå av to adskilte komponenter: Strømmåler og kommunikasjonsenhet. Enkelte områder i Norge er svært utsatt for lynnedslag og et lynnedslag i eller nær en trafostasjon kan sette hundrevis av smartmålere ut av funksjon. Med separate komponenter er det sannsynligvis større sjanse for at selve strømleveransen til bygningen ikke blir berørt av en defekt kommunikasjonsenhet.

Personvern

AMS i seg selv gir ikke problemer med personvern, siden data er kryptert i nettverket og dermed er beskyttet mot avlytting og misbruk. Det er likevel en del uavklarte forhold som må vurderes:

- NVE ønsker datalagring utover det Datatilsynet har godkjent frem til nå. (15 måneder).
- I utgangspunktet kan ikke personopplysninger brukes til annet enn fakturering. Det innebærer at nettselskapene ikke uten videre kan bruke måledata knyttet til personopplysninger for å avdekke for høyt strømuttak i forhold til rapportert forbruk, i et område.
- Hvordan ha oppsyn med tredjepart? Tredjepart kan være lokalisert i et annet land og ha kundedatabasen i et tredje land.

Dette er juridiske spørsmål som må finne sin løsning i det juridiske miljø. Denne rapporten kan ikke foreslå noen løsning på personvernmessige problemstillinger, men påpeke problemområder.

Fremtidig arbeid

Det kunne være interessant å gå nærmere inn på den operative drift av AMS og spesifisere drifts- og vedlikeholdsrutiner. NVE skal etter hvert komme med et slikt forslag og dette kunne dannet utgangspunkt for et slikt arbeid.

Det er også uavklarte forhold rundt personvern og mulighetene AMS kan gi. I fremtiden er det sannsynlig at personvern i forbindelse med AMS blir løftet opp på et felles europeisk nivå. Dette kunne danne utgangspunkt for å se om personvernet for norske forbrukere blir styrket eller svekket og på hvilken måte.

De siste dagene (18. mai til 23 mai, 2011) har det blitt avdekket et par alvorlige sikkerhets-hendelser mot sensitiv norsk infrastruktur. Forsvaret har blitt tappet for informasjon [60] og mobilnettet i store deler av Norge har blitt slått ut [61]. En sårbarhetsanalyse av samfunnet, med fokus på energimarkedet og AMS, ville være interessant.

Referanseliste

[1] Devoteam, Telecom, hjemmeside: http://no2.devoteam.com/index.php

[2] Helsedirektoratet: eHelse, En oversikt: http://www.helsedirektoratet.no/omdirektoratet/avdelingar/ehelse_49911

[3] NVE , Hjemmeside: http://www.nve.no/

[4] SGIP GB HAN, "Smart Energy Profile 1.x", 2011: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/HANTF/SGIP_GB_HAN_TF_SEP1.x_Recommendation-1-21-11.doc

[5] European Commission, "The EU climate and energy package": http://ec.europa.eu/clima/policies/brief/eu/package_en.htm

[6] Christian Haugen ,Masteroppgave: "Vurdering av kommunikasjonsalternativer for informasjonsutveksling med AMS mellom smarte hus og et smart kraftnett" , 2010. http://www.sintef.no/project/M-AMS/Ferdige%20dokumenter/Masteroppgave_Kommunikasjonsalternativer%20AMS.pdf

[7] NVEs referanseside om AMS: http://www.nve.no/no/Kraftmarked/Sluttbrukermarkedet/AMS/

[8] NIST, Smartgrid hjemmeside: http://www.nist.gov/smartgrid/

[9] W. Stallings & L. Brown, "Computer Security – Principles and Practice", Pearson, 2008.

[10] C. Brenton & C. Hunt, "Network Security", 2. Ed., SYBEX, 2003.

[11] A. Calder & S. Watkins, "IT Governance – A Managers Guide to Data Security and ISO 27001/ISO 27002", 4. Ed., Kogan Page, 2008.

[12] T. Daler, R. Gulbrandsen, T.A. Høie, T Sjølstad, "Håndbok I datasikkerhet – Informasjonsteknologi og risikostyring", 2. utg. Tapir Akademisk Forlag, 2006.

[13] NVE, "Høringsnotat 1-2011": http://www.nve.no/PageFiles/808/AMS%20h%c3%b8ringsnotat%20endelig%20versjon%20(2).pdf?epslanguage=no

[14] Open Meter, hjemmeside: http://www.openmeter.com/

[15] Olje-og Energidirektoratet, "pressemelding nr. 4/11", 2011: http://www.regjeringen.no/nb/dep/oed/pressesenter/pressemeldinger/2011/tar-krafttak-for-automatisk-strommaling-.html?id=630569

[16] NVE, "AMS,Forslag til endringer i forskrift 11. mars 1999 nr. 301. Tilleggshøring", 2009: http://www.nve.no/PageFiles/808/AMS%20siste%20versjon.pdf?epslanguage=no

[17] EU, Standardiseringsmandatet M/441: http://www.openmeter.com/documents/m441en.pdf

[18] CEER , Hjemmeside: http://www.energy-regulators.eu/portal/page/portal/EER_HOME

[19] Open Meter Deliverables: Arbeidsdokumenter som beskriver AMI: http://www.openmeter.com/?q=node/11

[20] Open Meter, WP-1, Deliverable 1-1: http://www.openmeter.com/files/deliverables/Open%20Meter_D1%201_Requirements_v1.0_20090701.pdf

[21] Internet Engineering Task Force, IETF: http://www.ietf.org/

[22] IETF, RFC 2828, Begreper brukt i datasikkerhet: http://www.ietf.org/rfc/rfc2828.txt

[23] IETF, RFC-3565, Bruk av AES-algoritmen, : http://www.ietf.org/rfc/rfc3565.txt

[24] Sårbarhetsutvalget, "Et sårbart samfunn", 2000: http://www.regjeringen.no/Rpub/NOU/20002000/024/PDFA/NOU200020000024000DDDPDFA.pdf

[25] Forsvarets forskningsinstitutt, "En sårbar kraftforsyning", 2001: http://www.nve.no/PageFiles/850/Sluttrapport.pdf?epslanguage=no

[26] Departementets definisjon på personvern: http://www.regjeringen.no/nb/dep/fad/tema/personvern/hva-er-personvern.html?id=448290

[27] Datatilsynet, "AMS og personvern": http://www.datatilsynet.no/templates/Page____3644.aspx

[28] Datatilsynet, "Veiledere i internkontroll": http://www.datatilsynet.no/templates/article____1716.aspx

[29] Nasjonal Sikkerhetsmyndighet: "Temahefte 1/2006". https://www.nsm.stat.no/Documents/Temahefter/Sårbarheter%20og%20trusler%20mot%20informasjonssystemer.pdf

[30] Berthier, Sanders, Khurana: IDS for Advanced Metering Infrastructure, University of Illinois: https://www.perform.csl.illinois.edu/Papers/USAN_papers/10BER01.pdf

[31] Trusselvurdering fra Politiets Sikkerhetstjeneste: http://www.pst.politiet.no/Filer/utgivelser/trusselvurderinger/NTV2011_web.pdf

[32] Department of Homeland Security, "Insider threat to critical infrastructure study", 2008: http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf

[33] Pöyry A/S, "Utveksling av informasjon ved innføring av AMS", 2010, http://www.nve.no/pagefiles/808/r-2010-04econ_utveksling%20av%20informasjon%20ved%20innf%c3%b8ring%20av%20ams.pdf?epslanguage=no

[34] Thema Consulting Group & Devoteam daVinci, "AMS tilleggstjenester, Tredjeparts adgang", 2011: http://www.nve.no/PageFiles/808/Thema_110202_AMS-tilleggstjenester.pdf?epslanguage=no

[35] Prime Technology, "Spec White Paper": http://www.prime-alliance.org/portals/0/specs/MAC_Spec_white_paper_1_0_080721.pdf

[36] Open meter, D1.2, “Report on regulatory requirements”: http://www.openmeter.com/files/deliverables/Open_Meter_D1.2_Regulation_v1.1_20090717.pdf

[37] NIST comments, Open Smart Grid , “AMI Security Profile v046”: http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/AMI%20Security%20Profile%20(ASAP-SG)/AMI%20Security%20Profile%20Comment%20Files/AMI%20Security%20Profile%20-%20v0_46%20-%20NIST%20Comments.doc

[38] AMI-SEC-TF, “AMI System Security Requirements”,(Appendix B6), 2008: http://www.smartgridipedia.org/images/2/2e/AMI_System_Security_Requirements_-_v1_01_-_Final.pdf

[39] Statistisk Sentralbyrå, SSB, “IKT-bruk i husholdningene”, 2. kvartal 2010: http://www.ssb.no/emner/10/03/ikthus/index.html

[40] Statnett, ”NUBIX – Webtjeneste for oppslag av målepunktID”: http://www.ediel.no/EdielPortal/showdocument.aspx?doc=NO/nubix.htm

[41] Avenir A/S, ”Nettselskapets rolle i det fremtidige norske kraftmarked med AMS-infrastruktur”, 2010: http://www.nve.no/PageFiles/9739/Nettselskapenes%20rolle%20med%20AMS%20-%20Notat%20fra%20Avenir.pdf

[42] Datatilsynet, ”Datalagringsdirektivet (DLD) og Personvern”: http://www.datatilsynet.no/templates/Page____3820.aspx

[43] Politiets sikkerhetstjeneste, ”Veiledning for sikkerhet og beredskap”, 2011: http://www.pst.politiet.no/Filer/utgivelser/Utgivelser/terror_sikkerhetsveileder.pdf

[44] Datatilsynet, ”Høringssvar - Utredning om standarder for styring av informasjonssikkerhe”t: http://www.datatilsynet.no/templates/Page____3855.aspx

[45] ISO-27001: http://www.27000.org/iso-27001.htm

[46] Norsk Standard, portal for kjøp av standarder: http://www.standard.no/no/

[47] Norsk akkreditering: Oversikt over godkjente virksomheter for sertifisering: http://www.akkreditert.no/no/

[48] Lovdata, Forbrukerkjøpsloven: http://www.lovdata.no/all/hl-20020621-034.html

[49] Olje- og energidepartementet, ”Stengerutine”r: http://www.regjeringen.no/nb/dep/oed/tema/strom/stengerutiner.html?id=444365

[50] European Commission, ”Smart Grid Mandate M/490 EN”, 2011: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf

[51] Direktoratet for Sikkerhet og Beredskap: ”AMS, En fare for el-sikkerheten”: http://www.standard.no/Global/PDF/Elektro-NEK/Lavspenning/Seksjon6-4-Grav-AMS-Elsikkerhet.pdf

[52] Statens Vegvesen, ”Nå starter automatisk måling av gjennomsnittsfart”, 2009: http://www.vegvesen.no/Om+Statens+vegvesen/Media/Nyhetsarkiv/Lokalt/Region+%C3%98st/Oppland/N%C3%A5+starter+automatisk+m%C3%A5ling+av+snittfart.107603.cms

[53] Personvern i EU: http://www.datatilsynet.no/templates/Page____3766.aspx

[54] R. Anderson, “Security Engineering, A Guide to Building Dependable Distributed Systems”, Wiley, 2001.

[55] Thema, Devoteam DaVinci, ”Felles IKT-løsninger i det norske kraftmarkedet”, April 2011: http://www.nve.no/Global/Publikasjoner/Publikasjoner%202011/Diverse%202011/Felles%20%20IKT-l%c3%b8sninger%20i%20det%20norske%20kraftmakedet.pdf

[56] NVE, ”Felles IKT-løsning”: http://www.nve.no/no/Nyhetsarkiv-/Nyheter/Felles-IKT-losning-i-kraftmarkedet/

[57] S.Gjessing, ”Nytte og muligheter for kraftleverandørene”, Fjordkraft, 2009: http://www.nve.no/Global/Seminar%20og%20foredrag/Energidagene%202009/Sesjon%204/20091015%20AMS%20Energidagene.pdf

[58] Teknisk Ukeblad, Artikkel om strømmåling i midt-Norge: http://www.tu.no/energi/article274499.ece

[59] Konkurransetilsynet, ”Svar på NVEs høringsutkast, 06.05.2011”: http://www.konkurransetilsynet.no/ImageVault/Images/id_4979/ImageVaultHandler.aspx

[60] Forsvaret, ”Målrettet dataangrep på forsvaret”, 18.05.2011: http://forsvaret.no/aktuelt/publisert/pressemeldinger/Sider/Malrettet-dataangrep-pa-Forsvaret.aspx

[61] Nrk, Reportasje om mobilnettet, 23.05.2011: http://www.nrk.no/nyheter/distrikt/hedmark_og_oppland/1.7644863

[62] Europeisk komite for elektroteknisk standardisering: http://www.cenelec.eu/

[63] DLMS/COSEM: http://www.dlms.com/index2.php

[64] PRIME-PLC: http://www.prime-alliance.org/

[65] Lovdata, ”Forskrift om avregning” (Se tillegg D for utskrift av §7-1): http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-19990311-0301.html

Vedlegg

Vedlegg A - Ordliste og forkortelser

Algoritmer:
Små delprogram som gjør en oppgave.

AMI:
Advanced Metering Infrastructure: En engelsk (og EU) betegnelse på et system som består av elektroniske målere (for strøm, vann etc.) og en infrastruktur som kommuniserer med disse målerene. Kommunikasjonen er toveis. Betegnelsen AMS-nettverket brukes synonymt i denne rapporten.

AMS:
Automatisk Måle- og Styringssystem. Dette omfatter all maskinvare og programvare som trengs for å lese og regulere smartmålere og annen maskinvare, direkte eller indirekte, tilknyttet disse i et strømnett. Dette omtales i teksten som AMS og AMS-systemet. Det vil typisk bestå av smartmåler, konsentrator, sentralsystem og nettselskapets eget datasystem som styrer AMS-nettverket via Sentralsystemet. (Se Figur 1-2 - Oversikt over). AMS skal hente måledata fra smartmålerne og samtidig overvåke systemet. En del av overvåkingen skal være automatisk, slik at feil blir korrigert i sanntid av systemet. Alle målinger, alarmer og hendelser blir rapportert til nettselskapets datasystem via sentralsystemet.

AMS-enheter:
De enkelte bestanddelene i et AMS-nettverk. Det er Smartmåler, Konsentrator, Sentralsystem og kommunikasjonslinjer.

AMS-Nettverket:
AMS-nettverket er den delen av AMS som er utenfor nettselskapets datasystem. Dette er logisk adskilt fra nettselskapets lokaliteter og denne delen av AMS-systemet omtales som AMI (Advanced Metering Infrastrucure) på engelsk.

AMS-Systemet:
Samme som AMS.

Asymmetriske algoritmer:
Brukes innen kryptografi som betegnelse på et system der man krypterer en tekst med en nøkkel og dechiffrer teksten med en annen nøkkel. Kalles også Diffie-Hellman etter deres arbeid ”New Directions In Chryptography”, 1976.

bps:
Bits pr. sekund. Brukes i datakommunikasjon om overføringshastighet gjennom grensesnitt.

CEER:
Council of European Energy Regulators (CEER) er en uavhengig europeisk samling av nasjonale reguleringsmyndigheter for strøm og gass. NVE er norsk deltager i denne organisasjonen.

CEN:
Comité Européen de Normalisation. Den europeiske standardorganisasjon.

CENELEC:
Comité Européen de Normalisation Électrotechnique. Europeisk Komitè for elektroteknisk standardisering [62].

Display:
En skjerm for fremvisning av målerverdier, tariffer, informasjon o.s.v. fra nettselskap eller kraftleverandør. Koblet til smartmåler med toveis eller enveis kommunikasjon. Bør være åpning for at PC, HAN o.s.v. kan kobles til Display for videre bruk av data.

DLMS/COSEM:
Distribution Line Message Spesification eller Distribution Language Message Spesification. Et generelt konsept for abstrakt modellering av kommunikasjonsstørrelser. COmpanion Specification for Energy Metering lager regler,basert på eksisterende standarder for datautveksling med smartmålere [63].

DSB:
Direktoratet for Sivil Beredskap.

eHelse:
Informasjonsteknologi skal i større utstrekning brukes i helsevesenet. Det vil bli mer utstrakt bruk av telemedisin, slik at en større del av behandlingen og overvåkingen av pasientene kan gjøres i hjemmet.

ETSI:
European Telecommunications Standard Institute. Uavhengig europeisk standardiseringsorganisasjon for telekommunikasjon.

Gateway:
Knutepunkt for datatrafikk som binder sammen to nettverk.

GPRS:
General Packet Radio Service. En utvidelse av GSM-mobiltelfoni som i praksis gir en datahastighet på ca. 40 kbps.

GSM:
Globalt System for Mobilkommunikasjon er det første vellykkede digitale mobilnettet og omtales ofte som et 2. generasjons (2G) mobilnett.

HAN:
Home Area Network er et nettverk som knytter forskjellige digitale enheter sammen i hjemmet eller andre bygninger. Dette kan være styring av for eksempel vaskemaskiner, oppvaskmaskiner, tørketromler, varmtvannsberedere, varmeovner og lys. HAN vil ofte være koblet til Internett slik at man kan fjernstyre hytta eller hjemmet utenfra.

IDS:
Intruder Detection System. Et system for overvåking av et datanettverk, med hensikt å hindre inntrengere i å få tilgang.

Kbps:
Kilobit pr. sekund. Se bps.

Konsentrator:
Maskinvare som vanligvis vil være lokalisert i transformatorstasjoner og så kommuniserer og samler inn måledata fra flere smartmålere om gangen. Disse verdiene blir så sendt

videre til Sentralsystemet. Det er et krav fra **OM** at en konsentrator skal kunne adressere minst 3000 smartmålere.

Kraftleverandør:
De som står for salg av elektrisk kraft.

M/441:
Et europeisk mandat med målsetting om å lage europeiske standarder der målerutstyr kan brukes om hverandre. CEN, CENELEC og ETSI skal utføre mandatet og timeplanen [30] for når standardene skal være klare, er allerede overskredt.

Mbps:
Megabits pr. sekund. Se bps.

Nettselskap:
De som står for distribusjon av elektrisk kraft og er eiere av kraftnettet og AMS.

Nettselskapets datasystem:
Et datasystem som styrer AMS, har kunderegister med forbruk og kundedata knyttet til smartmålerne.

NIST:
National Institute of Standards and Tecnology. Amerikansk standardiseringsorgan som utgir standarder for bruk i industri, regjering og akademia.

OM:
Open Meter.

Open Meter:
Europeisk prosjektgruppe som skal foreslå åpne og tilgjengelige standarder for bruk i AMI. Prosjektet er finansiert av den europeiske kommisjon og samarbeider med den Europeiske Standard Organisasjonen, CEN, CENELEC og ETSI

PLC:
Power Line Communication. Datakommunikasjon over det vanlige strømnettet. Den valgte løsningen (PRIME) fra Open Meter har en datahastighet mellom 24,6-128,4 kbps, avhengig av modulasjonen som velges.

PRIME:
PoweRline Intelligent Metering Evolution er en allianse [64] som har satt fore seg å utvikle en åpen, ikke-proprietær telekommunikasjonsløsning. Den er basert på PLC.

PSTN:
Public Switched Telephone Network. Offentlig telefonnett som er svitsjet (koblet opp direkte mellom to punkter) i motsetning til Internett som sender pakkede data.

Sentralsystemet:
Dette er hovedprosesseringsenheten i AMS-nettverket. Her samles alle måledata inn fra alle konsentratorer (eller direkte fra smartmålerne): Strømforbruk, feilmeldinger, hendelser, alarmer. Dette kan gjøre AMS-nettverket delvis autonomt, slik at det kan overvåke og ta forholdsregler ved feil i AMS-nettverket. Sentralsystemet blir kontrollert av nettselskapets datasystem og rapporterer også målerverdier, hendelser o.s.v. tilbake til dette. Sentralsystemet er logisk adskilt fra nettselskapets datasystem, men er ofte fysisk plassert i samme lokaliteter. Betegnelsene Front End og Central Access Server (CAS) brukes også, men ikke i denne rapporten.

sFTP:
Secure File Transfer Protocol. En protokoll for sikker overføring av filer på et nettverk.

Smarte hus:
Betegnelse på hus som er digitalisert. Det innebærer at elektriske apparater, strømkretser og lyskretser kan fjernstyres. Disse er ofte en del av et HAN-nettverk.

Smart meter:
Se Smartmåler.

Smartmåler:
En måler- og kommunikasjonsenhet som erstatter de gamle elektromekaniske strømmålerne i bygninger. Denne skal blant annet kommunisere forbruk, gi informasjon til forbruker, regulere strømforbruk, avstenge strøm, overvåke strømkvalitet og jordfeil.

SNMPv3:
Simple Network Management Protocol versjon 3. En Internettstandard for å styre enheter på IP-nettverk.

Symmetriske algoritmer:
Brukes innen kryptografi som betegnelse på et system der man krypterer og dechiffrer med samme nøkkel.

Systemsikkerhet:
Sikkerhet på et overordnet nivå knyttet til bl.a. drift, driftsrutiner og trusler fra personer og organisasjoner som ønsker å manipulere AMS-systemet.

Timeverdier:
Verdier (typisk kraftforbruk) som registreres i et AMS-system hver time.

Tjenesteleverandører:
Et firma som leverer tjenester som er relatert til målerverdier i AMS-systemet. Ved hjelp av disse verdiene kan elektrisk utstyr, vanningsanlegg og varme fjernstyres.

UMTS:
Universal Mobile Telecommunications System. Et såkalt 3. generasjons (3G) mobiltelefonnett med dataoverføringshastighet fra 384 kbps til 2 Mbps.

Vedlegg B Avregningsforskriften § 7-1.

Nettselskapene skal tilby andre tjenestetilbydere adgang til AMS på ikke-diskriminerende vilkår. NVE referer til § 7-1 i avregningsforskriften [65] som sier:

§ 7-1. *Nettselskapets nøytralitet og informasjonsplikt*

Nettselskapet skal i enhver sammenheng opptre nøytralt overfor kraftleverandører og sluttbrukere, herunder når det gjelder:

a) informasjon om kraftleverandører og kraftmarkedet,

b) håndtering av leverandørskifter,

c) nyetablering av abonnement,

d) oversendelse av måledata,

e) valg av faktureringsrutiner,

f) avregnings- og faktureringsplikt.

Nettselskapet skal håndtere informasjon på en måte som gjør at enkeltleverandører ikke kan gis konkurransefortrinn.

Nettselskapet skal informere sluttbrukere om relevante forhold knyttet til leverandørskifte, måling og avregning.

Nettselskapet skal på forespørsel oppgi den justerte innmatingsprofilen for siste kalenderår og hvilke kraftleverandører som er balanseansvarlige i nettselskapets kraftnett.

På forespørsel skal nettselskapet stille all pliktig informasjon etter dette kapitlet til disposisjon på et allment brukt elektronisk format, dersom informasjonen er lagret elektronisk.

Nettselskapet plikter å informere sluttbrukere om hvilke kraftleverandører som leverer kraft i deres nettområde. Ved oppstart av leveringspliktig kraftleveranse i medhold av energiloven § 3-3 skal nettselskapet uten ugrunnet opphold informere sluttbrukeren om de vilkår som gjelder for leveringen, samt gi sluttbrukeren informasjon om hvilke kraftleverandører som leverer kraft i området og hvordan en sluttbruker kan skaffe seg en kraftleverandør. Dette skal meddeles skriftlig i form av et oppstartbrev som skal utformes i henhold til mal utarbeidet av Norges vassdrags- og energidirektorat. Nettselskapet skal deretter minimum hver tredje måned gi sluttbruker den informasjon som nevnes i annet punktum, i form av et påminnelsesbrev som skal utformes i henhold til mal utarbeidet av Norges vassdrags- og energidirektorat.

Sluttbrukere som mottar leveringspliktig kraftleveranse skal informeres om endringer i priser og leveringsvilkår senest tre uker før endringen finner sted.

For å legge til rette for en effektiv håndtering av leverandørskifte, anleggsovertagelse og oppstart skal alle nettselskap med distribusjonsnett gjøre relevante kundedata tilgjengelige for en internettbasert søketjeneste administrert av avregningsansvarlig.

0 Endret ved forskrifter 17 des 2001 nr. 1461 (i kraft 1 jan 2002), 12 des 2005 nr. 1473 (i kraft 1 jan 2006), 14 des 2006 nr. 1463 (i kraft 1 jan 2007), 4 juli 2007 nr. 1085 (i kraft 1 jan 2008), 20 des 2010 nr. 1709 (i kraft 1 jan 2011).

Vedlegg C Avregningsforskriften § 4

Forslag til nytt kap. 4 Avanserte måle- og styringssystemer:

§ 4-1. Plikt til å installere AMS

Nettselskap skal i hvert enkelt målepunkt installere AMS.
Nettselskapene har ikke plikt til å installere AMS dersom:
a) forbruket i målepunktet er svært lavt og forutsigbart,
b) installasjon er til vesentlig og dokumenterbar ulempe for sluttbruker.
Dersom nettselskap og sluttbruker er uenig om installasjon av AMS, kan saken fremlegges Norges vassdrags- og energidirektorat til avgjørelse.
Norges vassdrags- og energidirektorat kan dispensere fra nettselskapenes plikt til å Installere AMS i særlig tilfeller.

§ 4-2. Funksjonskrav

AMS skal:
a) lagre måleverdier med en registreringsfrekvens på maksimalt 60 minutter, og kunne stilles om til en registreringsfrekvens på minimum 15 minutter,
b) være innrettet slik at måleverdiene kan innhentes momentant av nettselskapet,
c) kunne tilknyttes og kommunisere med eksternt utstyr gjennom et standardisert basert på Internett-protokoller,
d) kunne tilknyttes og kommunisere med andre typer målere,
e) registrere og lagre data også ved spenningsavbrudd,
f) kunne bryte og begrense effektuttaket i det enkelte målepunkt,
g) kunne sende og motta informasjon om priser, tariffer, totalkostnader og laststyring, samt kunne overføre alarm- og jordfeilsignal,
h) gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner og
i) registrere flyt av aktiv og reaktiv effekt i begge retninger.

§ 4-3. Måleverdier

Måleverdiene skal registreres og lagres i målepunktet inntil måleverdiene er overført til nettselskapet.
Måleverdiene skal overføres til nettselskapet etter at driftsdøgnet er avsluttet.
Måleverdiene skal være tilgjengelig for sluttbruker og eventuelt for kraftleverandør med fullmakt fra sluttbruker innen kl. 09.00 neste dag. Kraftleverandør skal ha tilgang på samlet forbruk per time for alle sine kunder i det aktuelle nettområdet innen kl 09.00 neste dag.

§ 4-4. Distribusjon og presentasjon av informasjon

Måleverdiene, jf. § 4-3, tredje ledd, skal vederlagsfritt gjøres tilgjengelig for sluttbrukeren via Internett.
Nettselskapet skal via Internett også presentere informasjon om forbruk i det enkelte målepunkt. Informasjonen skal presenteres på en slik måte at det er mulig å sammenligne forbruket, priser og kostnader over tid.
Leverandører av energitjenester, herunder kraftleverandører skal ved fullmakt fra kunden vederlagsfritt få tilgang til måleverdiene fra nettselskapet.

§ 4-5. Lagring av måleverdier

Nettselskap skal lagre måleverdier med tidsoppløsning på 60 minutt i minimum 3 måneder og inntil 15 måneder.
Nettselskapet skal lagre måleverdier med tidsoppløsning på en måned for de foregående 3 kalenderår.
Nettselskapet skal lagre måleverdier med tidsoppløsning på ett år for de foregående 3 kalenderår.

§ 4-6. Display

Nettselskapet skal tilby display dersom sluttbruker ønsker dette. Sluttbruker må selv dekke kostnaden for displayet, inklusive kostnadene for kommunikasjonsmodulen mellom display og AMS.
Kraftleverandør skal kunne sende prisinformasjon til displayet. Nettselskapet skal kunne sende tariffinformasjon til displayet.
Displayet skal synliggjøre kraftprisen, nettariffen og totalkostnaden ved det løpende forbruket.

§ 4-7. Krav til installering og rapportering

Nettselskap skal innen 1.1.2017 ha installert AMS i alle målepunkt i sitt konsesjonsområde.
Nettselskap i Nord-Trøndelag, Sør-Trøndelag og Møre- og Romsdal skal ha installert målere i minimum 80 % av sine målepunkter innen 1.1.2014.
Nettselskapene i resten av landet skal ha installert målere i minimum 80 % av sine målepunkter innen 1.1.2016.
Nettselskap skal innen 1.1.2012 levere en plan for innkjøp og installasjon av målere til Norges vassdrags- og energidirektorat.
Dersom nettselskap kan godtgjøre at det er svært utfordrende å etterleve § 4-7 andre ledd kan Norges vassdrags- og energidirektorat gjøre vedtak om dispensasjon.

§ 4-8. Overgangsbestemmelser

Når nettselskap har installert AMS i henhold til § 4-7, skal
a) sluttbruker ha tilgang til måleverdier lokalt,
b) nettselskapet tilby display dersom sluttbruker ønsker dette. Sluttbruker må selv dekke kostnaden for displayet, inklusive kostnadene for kommunikasjonsløsning mellom display og AMS. Kraftleverandør skal kunne sende prisinformasjon til displayet. Nettselskapet skal kunne sende tariffinformasjon til displayet. Displayet skal synliggjøre kraftprisen, nettariffen og totalkostnaden ved det løpende forbruket,
c) nettselskapet vederlagsfritt tilby sluttbrukeren informasjon om sitt forbruk på Internett og
d) nettselskapet skal legge til rette for at sluttbrukerne i Nord-Trøndelag, Sør-Trøndelag og Møre- og Romsdal kan inngå kraftpriskontakter basert på timeverdier.