SINTEF

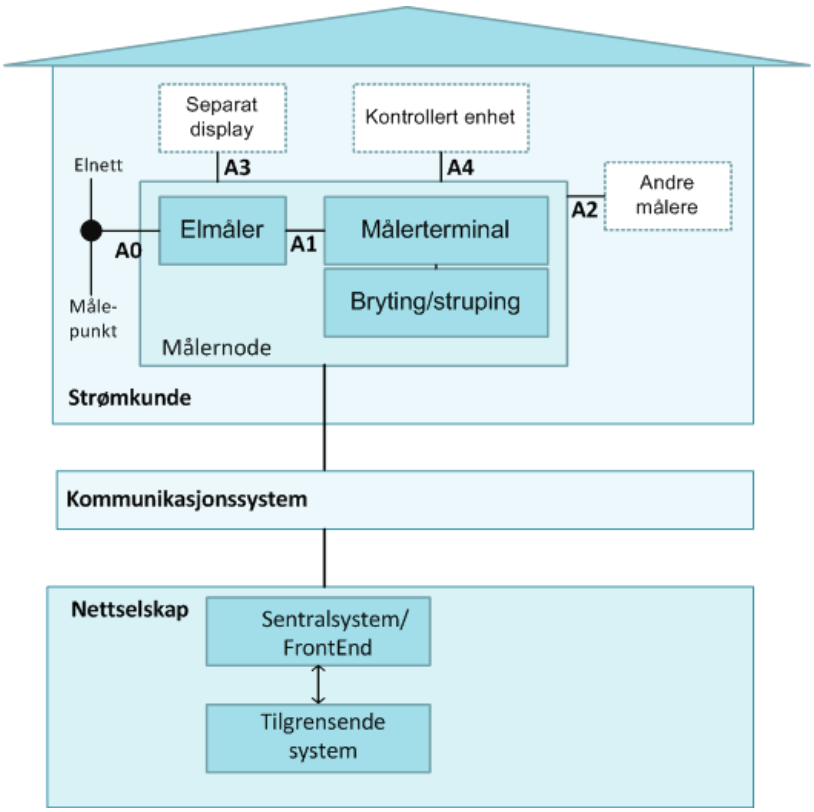
SINTEF A22318 - Åpen

Rapport

Risikovurdering av AMS

Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS

Forfattere
Maria Bartnes Line
Gorm Johansen
Hanne Sæle



SINTEF
2012-02-13

SINTEF IKT
Postadresse:
Postboks 4760 Sluppen
7465 Trondheim
Sentralbord: 73593000
Telefaks: 73592977
postmottak.IKT@sintef.no
www.sintef.no
Foretaksregister:
NO 948 007 029 MVA

Rapport

Risikovurdering av AMS

Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS

EMNEORD:
IKT
Informasjonssikkerhet
AMS

VERSJON
1.0

DATO
2012-02-13

FORFATTERE
Maria Bartnes Line
Gorm Johansen
Hanne Sæle

OPPDRAGSGIVER
Norges vassdrags- og energidirektorat (NVE)

OPPDRAGSGIVERS REF.
Frank Skapalen

PROSJEKTNR
906409

ANTALL SIDER:
44

SAMMENDRAG

Denne rapporten presenterer en overordnet risikovurdering av Avanserte Måle- og Styringssystemer (AMS) knyttet til hvilke konsekvenser det kan ha for kraftforsyningen at AMS utsettes for informasjonssikkerhetsbrudd. Vurderingen er hovedsakelig gjort for AMS basisfunksjoner, som er å registrere måledata hos kunde og overføre disse til nettselskapet, samt bryting/struping av effektuttaket i det enkelte målepunkt.

UTARBEIDET AV
Maria B. Line

SIGNATUR
Maria B. Line

KONTROLLERT AV
Martin Gilje Jaatun

SIGNATUR
Martin G. Jaatun

GODKJENT AV
for Sture Holmstrøm

SIGNATUR
Gerhard Oestedal

RAPPORTNR
SINTEF A22318

ISBN
978-82-14-05280-0

GRADERING
Åpen

GRADERING DENNE SIDE
Åpen

Sammendrag

SINTEF har utført en overordnet risikovurdering av Avanserte Måle- og Styringssystemer (AMS) for Norges vassdrags- og energidirektorat (NVE). Vurderingen omfatter hovedsakelig AMS basisfunksjoner, som er å registrere måledata hos kunde og overføre disse til nettselskapet, samt bryting/struping av effektuttaket i det enkelte målepunkt. Tilgrensende IT-systemer hos nettselskap er vurdert kun i begrenset grad. Fokus i analysen har vært på målepunkt med fast geografisk lokalisering, og mulighet for både forbruk og innmating. Mobile enheter som f.eks. måling av lading av elbiler har ikke vært berørt i analysen.

Det må presiseres at denne rapporten gir en overordnet risikovurdering knyttet til generell AMS-teknologi og infrastruktur. Hvert enkelt nettselskap må selv utarbeide egne risikovurderinger for sine systemer.

I rapporten er det beskrevet en generell AMS infrastruktur med de avgrensningene som er gjort for dette arbeidet. Deretter er det gjort en vurdering ut ifra et informasjonssikkerhetsperspektiv, hvor konfidensialitet, integritet og tilgjengelighet er de viktigste aspektene. Ulike scenarioer og hendelser er presentert og diskutert, og de hendelsene som er vurdert til å ha høyest risiko, har ett eller flere av følgende elementer i seg:

- Uønsket utkobling hos mange kunder
- Programvarefeil
- Sentralsystemet feiler eller brukes i angrepet
- Utro tjener; egen ansatt misbruker kunnskap og/eller legitime tilganger

I tillegg er et scenario med mange målere ute av drift samtidig vurdert til å være kritisk, uten at årsaken trenger å være et målrettet angrep. Dette er fordi konsekvensene vil medføre store kostnader for reparasjon og/eller utskiftning av teknisk utstyr. Ondsinnet programvare vil kunne være årsaken, eller et verktøy i flere av hendelsene, særlig ved angrep som kjøres langveisfra (fjerntilkobling).

Det anbefales at Beredskapsforskriften bør gjelde for AMS, fordi risikovurderingen som er gjort viser at uønskede hendelser med AMS kan få konsekvenser for kraftforsyningen, som er en kritisk samfunnsinfrastruktur. Spesielt er det bryter-/strupefunksjonen som gjør AMS utsatt, med de konsekvensene feil kan ha. Implementeringen av denne funksjonen må vurderes nøye.

Rapporten presenterer i tillegg en rekke anbefalinger knyttet mot utrulling og drift av AMS. Risikovurderinger, omfattende kartlegging og dokumentasjon av systemer, programvareutvikling i henhold til anerkjente standarder og en god organisasjon rundt håndtering av sikkerhetsbrudd er noen av disse anbefalingene. Dessuten må hvert enkelt nettselskap gjøre fornuftige valg knyttet til sammenkoblinger av AMS og driftskontrollsystemene, samt adgangs- og tilgangskontroll til bryter-/strupefunksjonen. Åpne kommunikasjonsprotokoller med nødvendige sikkerhetsmekanismer anbefales framfor proprietære. Outsourcing av AMS-tjenesten er fullt mulig, men det anbefales ikke å outsource selve bryter-/strupefunksjonen. Et samarbeid mellom nettselskaper er imidlertid naturlig å vurdere. Sikkerhetsvurderinger må uansett gjøres tidlig i kravfasen for at løsninger som realiseres, skal kunne implementeres på en god og sikker måte.

SINTEF

Innholdsfortegnelse

1 Bakgrunn

SINTEF IKT og SINTEF Energi AS har fått i oppdrag å utføre en overordnet risikovurdering av Avanserte Måle- og Styringssystemer (AMS) for Norges vassdrags- og energidirektorat (NVE).

Hovedmålsettingen med oppdraget er å:

1. Utarbeide en oversikt over mulige sårbarheter knyttet til komponenter i AMS og den infrastruktur som er nødvendig for et funksjonelt system.
2. Identifisere utfordringer knyttet til direkte og indirekte koblinger mellom styresystemer (driftskontrollsystemer) og AMS.

Risikovurderingen skal avdekke hvilke konsekvenser det kan gi for kraftforsyningen at AMS utsettes for informasjonssikkerhetsbrudd. Vurderingen er hovedsakelig gjort for AMS basisfunksjoner, som er å registrere måledata hos kunde og overføre disse til nettselskapet, samt bryting/struping av effektuttaket i det enkelte målepunkt, mens tilgrensende IT-systemer hos nettselskap er vurdert kun i begrenset grad. Det er fokus på målepunkt med fast geografisk lokalisering, og mulighet for både forbruk og innmating, og ikke mobile enheter som f.eks. måling av lading av elbiler.

Det må presiseres at denne rapporten gir en overordnet risikovurdering knyttet til AMS-teknologi og infrastruktur. Hvert enkelt nettselskap må selv utarbeide egne risikovurderinger for sine systemer.

1.1 Metodikk

Risikovurderingen er gjennomført i henhold til metoden som er dokumentert i Veiledning i risiko- og sårbarhetsanalyse [1]. Først beskrives objektet som skal analyseres. Deretter identifiseres mulige trusler og uønskede hendelser. Så kartlegges sårbarheter i systemene, og disse sees opp imot allerede iverksatte sikkerhetstiltak. Til slutt klassifiseres uønskede hendelser i henhold til sannsynlighet og konsekvens.

I løpet av prosjektperioden har det vært avholdt interne arbeidsmøter i prosjektgruppen, som dekker kompetanseområdene AMS, informasjonssikkerhet og sikkerhets- og styresystemer. I tillegg har vi hatt et heldags arbeidsmøte med deltakere fra NVE, Hafslund Nett og TrønderEnergi AS.

1.2 Om rapporten

Rapporten inneholder først en seksjon om AMS med de avgrensningene som er gjort for denne risikovurderingen. Kritiske komponenter og sårbarheter i AMS, samt mulige hendelser med stort risikopotensiale blir diskutert. Deretter beskrives informasjonssikkerhet; hva som menes med begrepet og hvilke trusler og uønskede hendelser som kan true informasjonssikkerheten til et system, før en vurdering av sikkerheten i åpne vs. proprietære kommunikasjonsprotokoller blir presentert. Kapittel 5 inneholder scenarioer for uønskede hendelser, mens kapittel 6 klassifiserer uønskede hendelser, både scenarioer og hendelser på komponentnivå. Til slutt nevnes noen anbefalinger til bransjen angående utrulling og drift av AMS, samt til NVE for bruk i sine forskrifter og veiledninger for kraftforsyningen i Norge.

2 Avanserte Måle- og Styringssystemer (AMS)

I følge nye forskrifter er det krav om at AMS skal installeres til alle strømkunder i Norge innen 1.1.2017 og 80% skal ha AMS innen 1.1.2016. AMS basisfunksjoner som skal implementeres, er å registrere måledata hos kunde og overføre disse til nettselskapet og bryting/struping av effektuttaket i det enkelte målepunkt.

I følge [2] er det definert følgende funksjonskrav til AMS (§4-2).

AMS skal:

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

I tillegg til detaljert måling av forbruk/innmating på kundenivå og nytteverdier i forhold til bl.a. enklere leverandørskifter, mer korrekt avregning og et mer effektivt kraftmarked, vil fullskala implementering av AMS kunne bidra til økt mengde informasjon vedrørende nettdriften. Det kan for eksempel være registrering av avbrudd, belastning i nettstasjon, jordfeil og/eller registrering av spenningskvalitet [3], men dette er tilleggsfunksjonalitet som ikke er tatt med i AMS-forskriften.

2.1 Systembeskrivelse

I forbindelse med krav om AMS i alle målepunkt, er det flere nettselskap som vurderer muligheten for realisering av nettnytte. Dette er også en relevant problemstilling i forhold til dagens fokus på SmartGrid. Med fullskala AMS og instrumentering av nettstasjoner vil man kunne få en bedre oversikt over status i lavspenningsnettet – helt ned til enkeltkundenivå [3]. Flere alternative kommunikasjonsinfrastrukturer brukes i samband med AMS, og aktualiteten for de ulike alternativene varierer ut fra hvilke(n) løsning(er) nettselskap velger for AMS og framtidens nett.

I dag er det allerede etablert driftskontrollsystem (SCADA[1]) med mulighet for sanntids overvåking og styring av ulike komponenter på høyere spenningsnivå [3]. Hvis man parallelt med utrulling av AMS til alle

[1] SCADA = Supervisory Control and Data Acquisition

strømkunder også installerer teknologi i MV/LV[2]-nettstasjoner for registrering av ulike parametere og overvåking av komponenter, vil man etablere et driftskontrollsystem på lavere spenningsnivå.

Med utgangspunkt i å kunne utarbeide en oversikt over mulige sårbarheter knyttet til komponenter i AMS-systemet og nødvendig infrastruktur, og å identifisere utfordringer knyttet til direkte og indirekte koblinger mellom styresystemer (driftskontrollsystemer) og AMS-systemer, er det i denne rapporten utarbeidet en overordnet oversikt over hvilke komponenter som inngår. Dette er illustrert i figur 2.1.

Figuren omhandler innsamlingssystemet (ofte betegnet som ”måleverdikjeden”) – fra målepunktet hos kunden til sentralsystemet hos nettselskap. I figuren er ulike alternativer til kommunikasjonssystem tegnet inn. I forbindelse med strømnettkommunikasjon (PLC) fra kunde til nettstasjon, benyttes en master/konsentrator i nettstasjon. Denne enheten samler inn data fra alle underliggende målere og overfører dette samlet inn til sentralsystemet hos nettselskapet. I forbindelse med radiokommunikasjon kan man også bruke master/konsentrator for å samle inn måledata fra tilknyttede målere.

I følge [2] er det presisert at det ikke stilles krav til at andre enn nettselskapet skal ha fysisk tilgang til kommunikasjonsløsningen i AMS. Tjenesteleverandører får dermed adgang til AMS infrastruktur ved at nettselskapet formidler informasjon mellom tredjepartsleverandør og sluttbruker. Alternativt kan tjenesteleverandører kommunisere direkte med eksternt utstyr hos kunden (f.eks. separat display eller kontrollert enhet), som er tilkoblet målerens standardiserte grensesnitt.

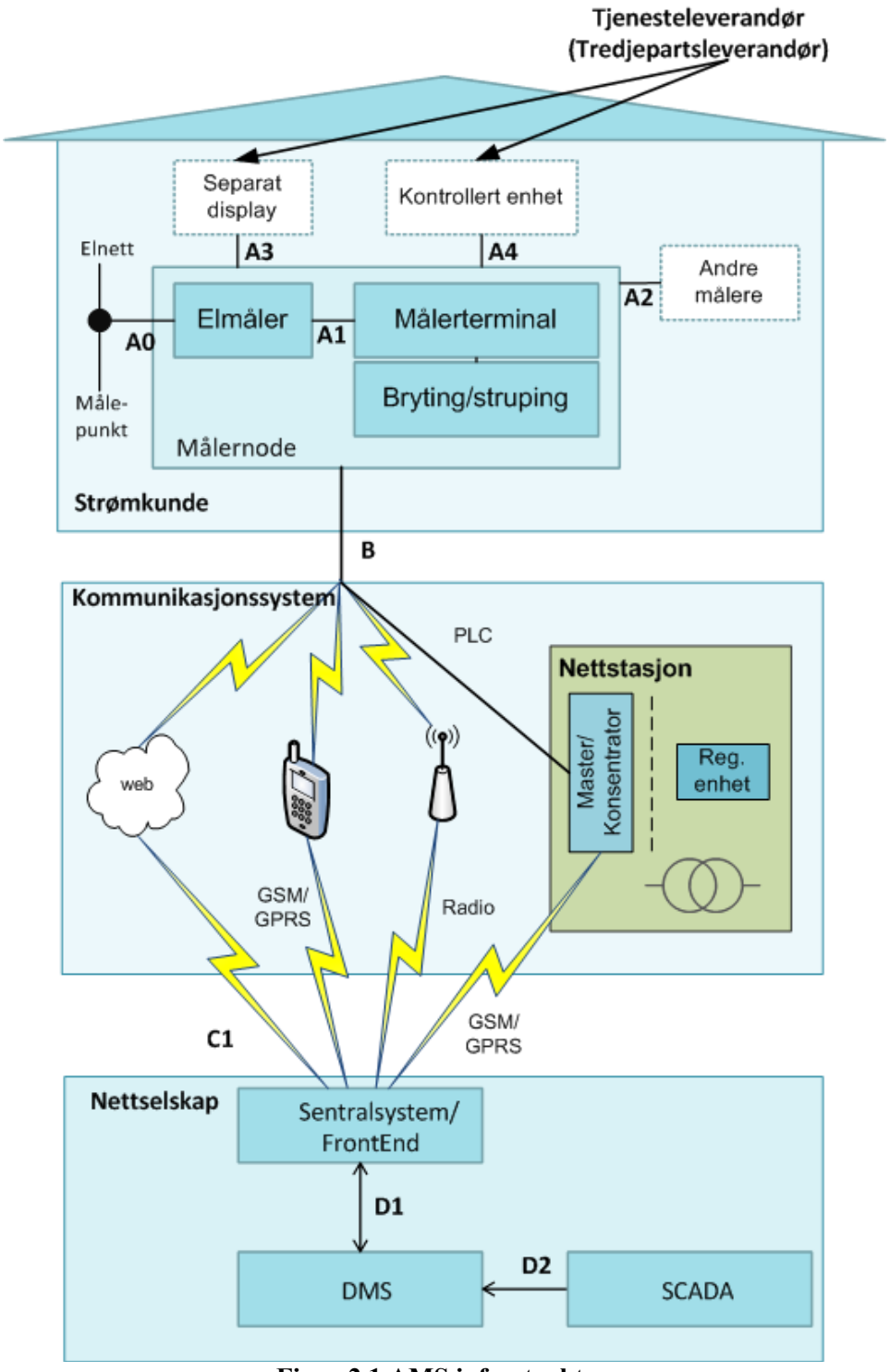
Det er flere alternativer å velge mellom når det gjelder kommunikasjonsløsninger, og per i dag eksisterer det allerede en rekke kommunikasjonsløsninger inn til kundene. Et viktig spørsmål er om man skal benytte eksisterende signalveier som kunden allerede har betalt for gjennom lokale internettilbydere, eller om AMS-signalene skal gå gjennom egne fysiske medium [4]. Det er iallfall viktig å unngå at kunden kan fjerne tilkoblingen mellom egen måler/målerterminal og kommunikasjonssystemet.

Noen eksempler på interne IT-systemer hos nettselskap er også tegnet inn. Dette gjelder IT-systemer knyttet til nettdrift (DMS[3] og SCADA). Det er ikke tatt med IT-systemer knyttet til avregning og fakturering av kundene.

Figuren er en skisse ut fra hvilke systemer som trenger AMS-data i forbindelse med nettdrift. Den er ikke ment som en detaljert beskrivelse av IT-struktur hos nettselskap.

I dette arbeidet er måler og strømforsyning vurdert som to forskjellige enheter. Dette innebærer at måler kan feile og at kunden fortsatt har tilgang til strøm (dvs. strømforbruk registreres ikke). Tilsvarende kan strømforsyningen feile mens måleren fremdeles fungerer (dvs. måler registrerer null strømforbruk).

[2] MV/LV er nettstasjoner mellom "Medium Voltage" og "Low Voltage". På norsk omtales MV som høyspenningsdistribusjon og inkluderer 6, 11 og 22 kV. LV angis som lavspenningsdistribusjon med spenningsnivåene 230 og 400 V.
[3] DMS = Distribution Management System. Driftssystem for lavspenningsnettet.



Figur 2.1 AMS infrastruktur

I figur 2.1 har komponentene fra målepunktet hos kunde til sentralsystemet hos nettselskapet samme struktur som beskrevet i [5]. Bruksområder/funksjonalitet for de ulike komponentene, konsekvens ved feil og grense-snittene mellom de ulike komponentene, er beskrevet i tabell 2.1 og tabell 2.2.

Tabell 2.1 Komponenter i AMS infrastruktur og tilgrensende systemer, og mulige konsekvenser hvis komponent svikter

Komponent	Funksjonalitet	Lokalisering				Mulig konsekvens hvis komponent svikter
		Kunde	Nett-stasjon	Komm. system	Nett-selskap	
Målepunkt	Punkt i kraftsystemet der måleverdier og hendelser registreres. Elmåler er tilkoblet målepunktet [5].	X				*Ingen strømforsyning til kunde, men måler fungerer. Ikke relevant å vurdere i forbindelse med informasjonssikkerhet.*
Elmåler	Registrerer elektrisitet i målepunkt hos kunde. Overfører måleverdier til målerterminal [5]. Inngår i målernode.	X				Ingenting registreres i målepunkt. Feilregistrering i målepunkt.
Målerterminal (inkl. Bryting/ struping)	Mottar måleverdier fra elmåler og viderebehandler dem som måledata. Inneholder kommunikasjonsmodul for elektronisk dataoverføring. Måleverdier lagres i en spesifisert periode, til de er bekreftet mottatt av sentralsystemet [5]. Inngår i målernode.	X				Ingen registrerte måledata eller hendelser kan videreføres til kommunikasjonssystemet. Feil behandling av registrerte måledata. Feil behandling av bryter-/strupefunksjonalitet.
Bryting/struping	Funksjonalitet for å kunne bryte og/eller begrense effektuttaket i målepunktet [1]. Inngår i målernode.	X				Ikke mulighet for å bryte/strupe effektuttak i målepunktet. Hvis feil medfører at bryter/struping er aktivert, vil effektuttak i målepunktet ikke være mulig (eller evt. være begrenset). Feil på strupefunksjon kan gjøre at man struper mer/mindre enn planlagt.
Målernode	Består av Elmåler, Målerterminal og funksjonalitet for bryting/struping [5]. (En samlebetegnelse siden teknisk løsning hos den enkelte kunde kan variere.)	X				*Samlebetegnelse – ikke relevant å vurdere her*
Separat display (Ikke pålagt i hht. Forskrift [2])	Display tilkoblet målernode. Display skal kunne presentere informasjon om bl.a. energibruk, kraftpriser, nettariffer og totalkostnader av forbruket [6].	X				Kunden får ikke informasjon om forbruk og priser. Kunden får feil informasjon om forbruk og priser.

Komponent	Funksjonalitet	Lokalisering				Mulig konsekvens hvis komponent svikter
		Kunde	Nett-stasjon	Komm. system	Nett-selskap	
Kontrollert enhet (Ikke pålagt i hht. Forskrift [2])	Utstyr som inngår i betjening av kundens lokale anlegg [5], f.eks. styring av enkeltbelastninger.	X				Styringsfunksjonalitet i kundens lokale anlegg fungerer ikke, bl.a. ved at ut-/innkobling ikke er mulig. Uvedkommende får tilgang til styrefunksjonalitet.
Andre målere (Ikke pålagt i hht. Forskrift [2])	Omfatter måleutstyr for gass, fjernvarme, vann etc. og evt. også leveringskvalitet o.l. [5]	X				Ingen registrering av måledata fra annet måleutstyr. Feilregistrering i målepunkt.
Master/ Konsentrator (Inngår i kommunikasjons-system)	Komponent som kan inngå i kommunikasjonssystemet til AMS. Kan brukes for innsamling av måledata fra tilknyttede kunder (f.eks. via strømnettkommunikasjon (PLC) eller radio), og videresende samlet måledata via et trådløst kommunikasjonsmedium. Kan tilkobles registreringsenheter i nettstasjon.	(X)	X			Ikke mulig å samle inn måledata og hendelser fra tilknyttede kunder. Ikke mulig å samle inn registrerte parametere og overvåking av komponenter i nettstasjon. Måledata sendes til feil mottaker.
Registreringsenhet i nettstasjon (Ikke pålagt i hht. Forskrift [2])	Registrering av parametere og/eller overvåking av komponenter i nettstasjon, f.eks. kortslutningsindikator, jordfeil og nullpunktssikring. Tilkoblet eget eller AMS kommunikasjonssystem.		X			Ikke mulig å registrere parametere og overvåke komponenter i nettstasjon. Feilregistreringer i målepunkt.
Kommunikasjons system	Ulike kommunikasjonsmedier kan brukes i forbindelse med AMS og vil variere ut fra hvilke(n) løsning(er) nettselskap velger.			X		Ingen eller feil overføring av data fra målernode hos kunde eller master/konsentrator til sentralsystemet. Måledata sendes til feil mottaker.
Sentralsystem/ FrontEnd	Det sentrale datasystemet i innsamlingssystemet. Samler inn måledata og hendelser fra alle målere og registreringsenheter i AMS. sender informasjon videre til ulike IT-systemer hos nettselskap.				X	Ikke mulig å samle inn registrerte måledata og hendelser fra kommunikasjonssystemet. Feil behandling av data.

Komponent	Funksjonalitet	Lokalisering				Mulig konsekvens hvis komponent svikter
		Kunde	Nett-stasjon	Komm. system	Nett-selskap	
Driftssystem distribusjonsnett (DMS) (Ikke pålagt i hht. Forskrift [2])	Driftssystem for distribusjonsnettet [3].				X	Ikke mulig å overvåke lavspennings distribusjonsnett. Får ingen eller feil informasjon om status for ulike komponenter.
Driftskontroll-system (SCADA) (Ikke pålagt i hht. Forskrift [2])	Driftskontrollsystem for vern-, styring og overvåking av ulike komponenter i kraftsystemet, med mulighet for sanntids overvåking og styring av ulike komponenter på høyere spenningsnivå [3].				X	Ikke mulig å overvåke kraftsystemet. Får ingen eller feil informasjon om status for ulike komponenter. (Regulert av forskrift om beredskap i kraftforsyningen [11].)

Tabell 2.2 Grensesnitt i AMS infrastruktur og tilgrensende system

Grense-snitt	Komponenter		Beskrivelse av hva som overføres
A0	Målepunkt	Elmåler	Registrerte måledata og hendelser. Registrering av forbruk/produksjon hvert 60. minutt (evt. 15. minutt) [2]
A1	Elmåler	Målerterminal	Registrert måledata og hendelser, for lagring i en begrenset periode.
A2	Målernode	Andre målere	Registrert måledata for gass, fjernvarme, vann o.l.
A3	Målernode	Separat display	Forbruksinformasjon, prisinformasjon og evt. meldinger. Sanntidsinformasjon.
A4	Målernode	Kontrollert enhet	Styringssignaler, prisinformasjon
B	Målernode	Kommunikasjonssystem (inkl. Master)	Registrerte måledata og hendelser, for lagring i en begrenset periode (til mottak er bekreftet av sentralsystem)
C1	Kommunikasjonssystem (inkl. Master)	Sentralsystem	Registrerte måledata og hendelser, for lagring i en begrenset periode (til mottak er bekreftet av sentralsystem)
D1	Sentralsystem	DMS	Registrerte måledata og hendelser fra kunder og nettstasjon
D2	DMS	SCADA	SCADA oversender nettinformasjon til DMS

2.2 Bruksområde AMS

I dette kapitlet er det gitt en overordnet beskrivelse av basisfunksjonene for AMS (måling og bryting/struping), relatert til ansvarsforhold og bruksområder. AMS vil benyttes både i forbindelse med måling og avregning av forbruk og produksjon både ut fra nett- og markedsmessige forhold, samt styring/bryting av forbruk i forbindelse med kundebehandling og nettdrift.

I forbindelse med vurdering av hva som skal reguleres i forskrift ang. AMS, er det i [6] fokusert på muligheten for å effektivisere avregningen og tilrettelegge for et effektivt kraftmarked. Dette gjelder hovedsakelig bruk av AMS for måling og avregning. AMS infrastruktur kan i tillegg integreres med framtidige driftskontrollsystemer i distribusjonsnettet.

2.2.1 Måledata for avregning av effektuttak/innmating

I følge forskrift om måling og avregning (§3-1 [7]) er det nettselskapene som er ansvarlige for alle målere og måleverdier i sitt nettområde. De har imidlertid mulighet til å outsource denne aktiviteten til en tredjepart og f.eks. etablere en avtale om kjøp av måleverdier. Flere nettselskap praktiserer allerede dette i forhold til innsamling av måleverdier til bruk for avregning av forbruket til kundene i nettområdet.

Outsourcing knyttet til oppgaver for måling og avregning må ikke være mer omfattende enn at nettselskapene fremdeles tilfredsstiller krav som er satt gjennom Kompetanseforskriften [8]. Krav til tjenestekvalitet og tilsvarende bør være godt dokumentert i gode avtaler, slik det også gjøres ved outsourcing av andre tjenester. Outsourcing må ikke forveksles med tredjepartstilgang, som i denne rapporten er sett på som aktører som tilbyr tjenester ved siden av AMS.

Følgende vurderinger bør gjøres før outsourcing av AMS (som andre typer tjenester):

- Man må vite hvor (geografisk og til hvem) dataene overføres og lagres, hvem som har tilgang
- Sikkerhetsnivået i løsningen, ifbm overføring, lagring, prosessering, tilbakeføring og sletting
- Regulerer kontrakten forutsetninger, kvalitetssikring, leveringsfase og avvikling, samt mekanismer for fleksibilitet og skalerbarhet?
- Oppetidsgarantier og kompensasjonsordninger ved eventuelle brudd på disse
- Hvordan håndteres og kommuniseres sikkerhetsbrudd
- Muligheter for insourcing etter en stund, eller migrering til annen tilbyder

I [9] er det anbefalt at det etableres felles IKT-løsninger i det norske kraftmarkedet. Det gjelder felles måleverdidatabase og sentrale behandlingsfunksjoner for å administrere ajourføring av informasjonsinnhold, tilgang til database og målernettverk, samt bearbeiding av felles data. Dette vil være en overgang fra dagens ordning (for kunder over 100.000 kWh/år), hvor det enkelte nettselskap samler inn måledata og lagrer disse i en egen måleverdidatabase. En felles måleverdidatabase kan muligens oppfattes som en bransjekoordinert outsourcing av flere oppgaver relatert til måledata.

Med en felles måleverdidatabase vil risikoen for manipulasjon av data bli redusert, bl.a. pga. muligheten for felles sikkerhetsmekanismer [9].

Selv om det anbefales at måledata skal lagres sentralt, vil nettselskapene ha behov for bruk av AMS-data i forbindelse med nettdrift. Det enkelte nettselskap må selv avgjøre hvor mye data de lagrer lokalt [9].

2.2.2 Implementering av bryter-/strupefunksjonalitet

I følge forskrift for AMS er det krav om at det i alle målepunkt (unntatt trafomålte anlegg) skal være mulig å bryte og begrense effektuttaket. Det er ikke spesifisert hvordan nettselskap skal gjennomføre dette, men NVE har i [2] vurdert bryting/struping som følgende:

"...NVE ønsker å vurdere nærmere den sikkerhetsmessige siden ved kravet om å bryte eller strupe effektuttaket i hvert enkelt målepunkt, samt hvilke kriterier som må oppfylles for at nettselskapene skal kunne utføre struping av enkelt målere eller grupper av målere. I gitte tilfeller vil denne funksjonen omfattes av "Forskrift om beredskap i kraftforsyningen", dersom selskapene for eksempel integrerer AMS i sine driftskontrollsystem. Dette vil da bli et viktig punkt ved for eksempel tilsyn av selskapenes driftskontrollsystem..."

En bryter-/strupefunksjonalitet implementert i alle målepunkt kan ha ulike bruksområder, og den bør kunne brukes mot ett målepunkt, en gruppe målepunkt eller alle målepunkt [5]. Eksempler på bruksområder kan være:

- ***Opphør av abonnement ved flytting (kundehåndtering)***
  - Kundesenteret kan bryte effektuttaket i et målepunkt når en kunde melder om flytting. Anlegget kan tilsvarende kobles inn igjen når ny kunde flytter inn. Av sikkerhetshensyn bør det vurderes om det skal installeres en sikkerhetsbryter som i tillegg må opereres manuelt av kunde, for å spenningssette anlegget [3].

- ***Utkobling av målepunkt eller struping av effektuttak ved manglende betaling (kundehåndtering)***
  - For kunder som inngår i kategorien "dårlige betalere", kan kundesenteret bruke bryterfunksjonen for å koble ut målepunktet til betaling er mottatt. Alternativt kan strupefunksjonen benyttes, slik at kunden får strøm til et visst basisforbruk – inntil strømregningen er betalt. Strupefunksjonaliteten vil bidra til at kunden har mulighet for bl.a. litt strøm til oppvarming (spesielt viktig i vinterhalvåret).

- ***Hurtigere gjenoppretting etter feil (nettdrift)***
  - AMS infrastruktur kan benyttes for hurtigere gjenoppretting av strømforsyningen etter en feilsituasjon. Avhengig av hvilken styringsteknologi som er installert, kan den brukes til hurtigere lokalisering av feil og omkoblinger i distribusjonsnettet. Dette er funksjonalitet som er relevant å kontrollere/overvåke fra en driftssentral.

- ***Effektbegrensning i høylastperioder (nettdrift)***
  - Enkeltbelastninger hos kunder (f.eks. varmtvannsbereder hos husholdningskunder) kan kobles ut i 1-2 timer morgen og evt. ettermiddag for å redusere belastningen på nettet. Alternativt kan maksimalgrensen for effektuttak reduseres i definerte høylastperioder. Dette kan enten settes opp som en forhåndsprogrammert jobb som kjøres til faste tider, eller evt. kontrolleres samlet fra f.eks. driftssentral når effektbegrensning/utkobling av enkelt-belastninger er nødvendig.

- ***Utkobling av målepunkt i forbindelse med planlagt utkobling (f.eks. ved vedlikehold av nett) (nettdrift)***
  - I en driftssituasjon kan bryterfunksjonen hos kundene og evt. i nettstasjon, brukes i forbindelse med planlagt utkobling, f.eks. ved behov for vedlikehold av nett. Dette kan være et alternativ til utkobling lokalt (f.eks. i MV/LV nettstasjon), men lokal utkobling er likevel mest sannsynlig for å sikre at sikkerhetsrutiner følges. Hvis bryter-/strupefunksjonen i AMS brukes til dette, er det sannsynligvis mest aktuelt at en driftssentral gjennomfører slike utkoblinger.

- ***Utkobling eller struping av forbruk i en beredskapssituasjon (rasjonering)***
    - I en beredskapssituasjon ved behov for rasjonering, kan utkobling eller strupefunksjonen brukes for å redusere det totale uttaket til alle kundene i et gitt område. Dette er direkte driftsrelatert, og det er derfor mest aktuelt at en driftssentral (evt. KBO[4]) håndterer dette.

Eksemplene over er ikke ment som en fullstendig oversikt, men de viser at det er relevant å bruke bryter-/strupefunksjon i forbindelse med flere av nettselskapets oppgaver (her: kundehåndtering, nettdrift og rasjonering). De ulike bruksområdene vil ha forskjellig konsekvens for kraftsystemet, dvs. utkobling av en kunde i forbindelse med flytting eller dårlig betaler vil gjelde enkelte kunder, effektbegrensning i høylastperioder kan gjelde flere kunder, mens struping av effektuttak i forbindelse med en rasjoneringssituasjon vil kunne gjelde mange kunder.

Ulike forhold vedrørende tilgang til bryter-/strupefunksjonaliteten bør vurderes ut fra hvilke konsekvenser feil bruk av bryter-/strupefunksjon kan ha for kraftsystemet.

Flere nettselskap har allerede outsourcet måledatainnsamlingen og har etablert avtaler om kjøp av måleverdier. For bryter-/strupefunksjonen er det aktuelt med samarbeid mellom flere nettselskap for fremtidens driftskontroll, men det er ikke like aktuelt med generell outsourcing, bl.a. pga pålegg relatert til nettdrift og driftssikkerhet.

Ved koordinering av driftskontrollsystemer vil flere kunder inngå i samme system, og konsekvensen ved innbrudd/feil vil dermed bli større, noe også risikovurderinger for AMS må ta høyde for.

[4] KBO = Kraftforsyningens beredskapsorganisasjon

Viktige forhold knyttet til bryter-/strupefunksjon er bl.a.:

- Hvordan skal bryter-/strupefunksjonalitet implementeres og hvem skal ha tilgang til hva? F.eks. kan en person på kundeservice få tilgang kun til bryting/struping av en eller flere kunder, mens en person fra driftssentralen kan få tilgang til bryting/struping til flere kunder i et større område.
- Fra hvilke(t) system sendes styresignaler fra? (f.eks. driftssentral eller kontor hos kundeservice?)
- Når skal bryter-/strupefunksjonen benyttes? (Beredskapssituasjon eller kun normal drift?)
- Hvilken stilling skal bryter gå til dersom AMS svikter? I de fleste tilfeller vil fornuftig oppførsel være at bryter vedvarer å være i samme stilling som før AMS sviktet.
- Hvilken konsekvens vil det ha for kraftsystemet hvis ikke bryter-/strupefunksjon fungerer? (ikke kobler ut/senker grense for effektuttak, eller ikke kobler inn/øker grense for effektuttak?)
- Hvilken konsekvens vil det ha for kraftsystemet hvis eksterne får tilgang til bryter-/strupefunksjonaliteten i AMS?
- Vurdere om deler av forbruket til en kunde skal fritas fra bryter-/strupefunksjonalitet? Det innebærer bl.a. å vurdere motstridende forhold som å begrense hvor mye som kan kobles ut hos en kunde, og dermed begrense konsekvensen ved at en fremmedaktør klarer å koble ut forbruk hos flere kunder, samtidig som at bryter-/strupefunksjonen ikke skal kunne overstyres av en kunde i en rasjoneringssituasjon.

I følge [2] er nettselskapene pålagt å gjennomføre risiko- og sårbarhetsanalyser når de skal etablere sine AMS-løsninger, og implementeringen av bryter-/strupefunksjonen er et viktig element å inkludere i slike analyser.

3 Informasjonssikkerhet

I dette kapittelet gis det en introduksjon til informasjonssikkerhet; hva som menes med begrepet, ulike beslektede begreper, samt en oversikt over hva slags typer uønskede hendelser som ligger innenfor dette domenet.

IKT-systemer blir stadig viktigere innen kritisk infrastruktur. Trenden er at industrielle styringssystemer i økende grad utvikles basert på hyllevare (f.eks. MS Windows) i stedet for rene spesiallagede systemer. Man ser også oftere at slike systemer kobles mot for eksempel administrasjonsnett, som igjen er koblet mot Internett. Den økende bruken av IKT generelt, sammen med økt bruk av hyllevare og økt sammenkobling mot andre nett, øker effektiviteten og mulighetene for samarbeid, og fører til besparelser i både tid og penger knyttet til lokalisering og retting av feil. Samtidig øker sårbarheten når det gjelder typiske IKT-trusler. I mange industrielle miljøer er det ikke tradisjon for å forholde seg til denne typen trusler, og flere bransjer og virksomheter står derfor overfor nye utfordringer framover.

Når det gjelder sikring av IKT-systemer og den informasjonen som ligger i disse systemene snakker man gjerne om sikring av [10]:

- **Konfidensialitet;** det å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang
- **Integritet;** det å sikre at informasjonen og behandlingsmetodene er nøyaktige og fullstendige – innebærer at uvedkommende ikke kan endre informasjon eller systemet som behandler informasjonen
- **Tilgjengelighet;** det å sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov

I en utvidet definisjon av informasjonssikkerhet kan også følgende aspekter inkluderes:

- **Autentisering**; det å få visshet om at en part virkelig er den han/hun utgir seg for å være. Det gjelder både bruker og maskin (jfr. falske minibankautomater)
- **Ikke-benekting**; det å sikre at de som har sendt meldinger ikke kan benekte eller avvise det i etterkant
- **Sporbarhet**; enhver endring av informasjon skal kunne spores; hvem utførte, og når
- **Personvern**; sikre at enkeltindividet kan kontrollere informasjon om en selv og hva denne brukes til.

Når det gjelder drifts- og styringssystemer vil ofte integritet og tilgjengelighet være vel så viktig som konfidensialitet. Man er avhengig av at systemet er tilgjengelig og gjør de oppgavene det er satt til basert på riktig informasjon. Identifiserte sårbarheter knyttet til AMS er i mange tilfeller knyttet opp til avveininger mellom *tilgjengelighet, integritet* og *konfidensialitet*.

I informasjonssikkerhetsarbeidet må man ta hensyn til villede ondsinnede handlinger rettet direkte mot et gitt system, i tillegg til feil og ulykker som kan forårsake sikkerhetsbrudd. På denne måten er ikke informasjonssikkerhet en ren teknisk problemstilling, men i høyeste grad også avhengig av menneskene som opererer systemene, samt organisasjonen som systemene opereres i.

Man vil aldri være i stand til å oppnå 100 % sikkerhet i et system. Det bør heller ikke være noe mål å oppnå så nært opptil 100 % som mulig. Det viktigste, og også det mest utfordrende, er å velge det **rette** nivået av sikkerhet, sett opp mot et akseptabelt nivå av risiko. Sikkerhetsmekanismer kan være kostbare, men det kan også være svært kostbart å **ikke** ha passende sikkerhetsmekanismer på plass. Det kan imidlertid være vanskelig å dokumentere lønnsomheten av en del sikkerhetsmekanismer.

På engelsk skilles det mellom ulike betydninger av ordet sikkerhet, nemlig *safety* og *security*. *Safety* handler typisk om å hindre at et system gjør skade på omgivelsene, altså beskytte liv, helse og miljø, mens *security* handler om å beskytte systemet mot skade fra omgivelsene. I industrielle miljøer er det lang tradisjon for å tenke og håndtere *safety*, mens *security*, hvor også informasjonssikkerhet kommer innunder, innebærer en mer ukjent tankegang. Informasjonssikkerhet handler om å beskytte informasjon. De fleste vil selvsagt være enige om at det er viktig å beskytte liv, helse og miljø, og disse verdiene er akkurat like viktige uansett hvilket system det er snakk om. Hvor viktig det er å beskytte informasjon, avhenger derimot veldig av hva slags type informasjon det er og hva denne brukes til. Men misbruk eller ødeleggelse av enkelte typer informasjon kan ha store konsekvenser for andre verdier, som for eksempel liv, helse eller miljø. De faktiske konsekvensene av brudd på informasjonssikkerheten kan også være vanskelig å forutsi, da det avhenger av intensjonene, kompetansen og kreativiteten til angriper.

Det er også en annen viktig forskjell mellom de ulike sikkerhetstradisjonene. En kritisk komponent vil typisk ha en fail-safe modus, slik at kritiske utganger går til en forhåndsdefinert tilstand dersom enheten feiler eller enheten oppdager en feil. Et system som utsettes for et sikkerhetsbrudd, vil derimot ikke nødvendigvis slutte å virke. Konsekvensen kan like gjerne være at måleverdier er tuklet med, men driften opprettholdes. Derfor kan det være svært vanskelig å avdekke at et sikkerhetsbrudd faktisk har skjedd.

3.1 Ulike betydninger av ordet sikkerhet

I dagligtale brukes gjerne flere ulike begreper for å si noe om IKT-systemer og sikkerhet:

- *Datasikkerhet*; brukes gjerne i dagligtale, og kan bety både nettverkssikkerhet og programvaresikkerhet
- *Cyber-sikkerhet*; brukes om sikkerhet knyttet til Internett og kan sånn sett bety både nettverkssikkerhet og programvaresikkerhet; er mest en mer engelsk variant av begrepet datasikkerhet. Brukes også ofte som *IT-sikkerhet i SCADA-verden*.
- *IT-sikkerhet*; informasjonsteknologi-sikkerhet; også en variant av begrepet datasikkerhet, samtidig brukes dette begrepet mer av profesjonelle, som en kortform av informasjonssikkerhet
- *Programvaresikkerhet*; det at en applikasjon/et program har innebygde sikkerhetsmekanismer og ikke kun baserer seg på å operere i et sikkert miljø
- *Kommunikasjonssikkerhet*; sikkerhet rundt kommunikasjon (ikke begrenset til datakommunikasjon), og mindre fokus på programvaresikkerhet og sikring av informasjon når den ikke kommuniseres/transporteres
- *Nettverkssikkerhet*; sikker overføring av datatrafikk i et kommunikasjonsnett
- *Informasjonssikkerhet*; det mest presise begrepet, som også er tydelig definert i ISO/IEC 27001:2005, som referert til tidligere i dette kapitlet.

Ingen av disse begrepene er feil, men flere av dem er noe upresise. **Informasjonssikkerhet** er det begrepet som er tydeligst definert og som inkluderer meningen av de øvrige begrepene. Vi vil derfor sterkt oppfordre til at NVE bruker dette begrepet i sine krav og veiledninger til bransjen, med den definisjonen som er gitt ovenfor.

3.2 Trusler mot IKT-systemer

Truslene mot IKT-systemene og AMS er delt opp i tre hovedkategorier: *Tilfeldige og utilsiktede feil* som kan skje enten på grunn av svakheter i IKT-systemer, uheldige ansatte eller utenforliggende hendelser, *generelle angrep* som ikke er direkte rettet mot AMS eller tilknyttede systemer, men som kommer som en følge av det generelle trusselbildet mot IKT-systemer, og *målrettede angrep* der angripere benytter IKT-systemer for å skade AMS og/eller tilknyttede systemer spesielt.

Når man vurderer risikoen forbundet med truslene, må man også vurdere i hvilken grad mekanismer for å oppdage og håndtere hendelser eksisterer, og om disse tar for gitt at IT-systemer og kommunikasjonsnettverk fungerer. Det er også viktig å registrere historiske uønskede hendelser knyttet til AMS slik at en kan dra lærdom av disse hendelsene i etterkant og oppdatere eventuelle rutiner og prosedyrer.

3.2.1 Tilfeldige og utilsiktede feil

Lynnedslag, svikt i strømforsyning, brann, disk-krasj, kommunikasjonsfeil og menneskelige feil er typiske eksempler på tilfeldige og utilsiktede feil. På et vis kan slike feil like gjerne omtales som pålitelighetssvikt som sikkerhetsbrudd, men vi har likevel valgt å omtale slike i denne risikovurderingen. For å begrense denne typen risiko, må både tekniske og menneskelige aspekter vurderes. På den tekniske siden kan man sørge for redundans, slik at ikke feil i enkeltkomponenter lammer et større system. På den menneskelige siden må opplæring og bevisstgjøring være kontinuerlige tiltak, og man bør være i stand til å fange opp feil på et tidlig tidspunkt.

3.2.2 Generelle angrep

Det finnes en rekke ulike angrep som retter seg mot IKT-systemer generelt. Et åpenbart eksempel på dette er den enorme mengden med virus og ormer, såkalt ondsinnet programvare/*malign software*/*malware*[5], som finnes på Internett. Det lages og distribueres nye varianter av *malware* hver eneste dag, og de utnytter sårbarheter og svakheter i programvare, operativsystemer og protokoller. Det finnes også verktøy gratis tilgjengelig på nett som kan brukes til å kjøre automatiserte angrep i stor skala, og det kreves ikke nødvendigvis mye kunnskap for å bruke disse verktøyene. Så lenge man har systemer og nettverk som er koblet til Internett på et eller annet vis, kan man rammes av slike angrep, selv om ens egen virksomhet ikke er et uttalt mål for angrepet. *Malware* kommer i form av virus, ormer, trojanere, spionprogrammer, bakdører, tasteloggere, falske antivirusprogrammer m.m., og prinsippet er det samme – det er et dataprogram som

[5] Ofte brukes også begrepet ondsinnet/*malicious*, men det er mer rett å bruke begrepet ondsinnet/*malign*, da programvaren ikke har egen fri vilje.

brukeren ikke har noe kontroll over, og som ofte har uheldige konsekvenser for brukeren og/eller datamaskinen/nettverket.

Målet med angrep kan være mange:

- Tilgang til konfidensiell informasjon
- Samle personopplysninger for salg og bruk til svindel
- Tilgang til prosessorkraft, bruke maskinen som en del av større, målrettet angrep, eller til utsending av spam
- Tastelogging for å samle brukernavn og passord til ulike tjenester på Internett
- Logge en brukers nettaktivitet for å lage en markedsføringsprofil
- Kryptering av filer, for så å kreve penger for dekryptering; utpressing

Bruk av standard hyllevare, kobling mot Internett og tilkobling av bærbare enheter gjør at AMS kan bli utsatt for de generelle IKT-truslene. Eksempler på situasjoner som kan gjelde for AMS er:

- Tjenestenekt (også kalt Denial of Service (DoS)[6]) mot driftssentral. Mister kontakt med kommunikasjonsnettet. Kan skyldes generelt høy aktivitet for virus/ormer.
- Sikkerhetshull i programvare på datamaskiner i styringssystem infiseres av ondsinnet programvare, og de maskinene blir del i et botnet; fjernstyrt av angripere og brukt som verktøy i større, målrettede angrep eller som utsender av spam.

3.2.3 Målrettede angrep

Målrettede angrep kan spenne fra innbrudd/hærverk på utstyr til angrep utenfra via Internett. Noen angrep vil antagelig kreve stor kjennskap til systemene og dermed kun være aktuelle for dedikerte angripere. Det er også mulig å tenke seg angrep på IKT som en del av et større angrep som også inkluderer fysiske angrep. Sannsynligheten for de mest dedikerte angrepene er antakelig liten, men de kan ha store konsekvenser og muligheten bør derfor vurderes. Angripere kan være eksterne eller interne. Eksempler på relevante målrettede angrep:

- Datainnbrudd på målerterminalen hos sluttbruker, der angriper er fysisk til stede. Manipulering av måledata.
- Datainnbrudd på nettstasjoner; angriper oppnår tilgang til kommunikasjonslinjen, gjerne i kombinasjon med DoS-angrep mot driftssentral slik at det er mindre sannsynlighet for å bli oppdaget. Stenge kraftforsyning for et geografisk område.
- Manipulering av driftskontrollsystem, slik at det feilaktig varsles om feil på forsyningslinje.
- Datainnbrudd kombinert med sosial manipulering (eng: *social engineering*) for å innhente informasjon som kan brukes for fysiske angrep
- Avlytting av kommunikasjonslinje, tapping av måledata. Overvåking av sluttbrukere, brudd på personvern.
- Utro tjener, som har innsidetilgang og god kjennskap til enkeltsystemer, kan påvirke måledata, effektuttak, legge inn ondsinnet programvare.

[6] Denial of Service (DoS) (norsk: tjenestenekt-angrep), dvs hindre normal tjeneste på for eksempel en webserver ved å bombardere den med nettverkstrafikk

- Misfornøyde kunder manipulerer måleravlesningen for å betale mindre enn de skal, eller de ønsker å gjøre større skade på virksomhetens systemer
- Uvedkommende tar kontroll over strupefunksjon hos enkelt kunder; skrur av varme når beboere er bortreist om vinteren. Resulterer i fysiske ødeleggelser i bygning.
- Politisk motiverte, som ønsker å ramme samfunnet, ikke enkelt-selskaper. Tar over kontrollen av distribusjonsnettet og mørklegger hele byer.

I kapittel 5 utdypes flere av disse eksemplene i scenario-beskrivelser. Personverntrusler er imidlertid ikke nærmere beskrevet, da disse ikke kan sies å ha en direkte påvirkning på kraftforsyningen. De er derfor utelatt videre i denne risikovurderingen, etter avtale med oppdragsgiver.

3.3 Håndtering av sikkerhetsbrudd

Hendelseshåndtering bør være en proaktiv prosess som innebærer både forebyggende arbeid, håndtering av det som måtte inntreffe, og et skikkelig etterarbeid, inkludert læring og erfaringsdeling. Etterarbeidet bør deretter brukes aktivt i risikostyringsprosessen og i det generelle sikkerhetsarbeidet internt, for eksempel når det gjelder opplæring og styrking av sikkerhetsbevissthet hos de ansatte.

I driftskontrollmiljøer hvor man har gode prosesser rundt håndtering av typiske safety-hendelser, bør man forsøke å samkjøre dette med håndtering av security-hendelser og på den måten få en helhetlig tilnærming til arbeidet med forebygging, rapportering og oppfølging.

Såkalte *near misses* – nesten-hendelser – bør registreres på lik linje med faktiske hendelser. Dette er nyttig for å øke antallet hendelser som utgjør grunnlaget for det forebyggende arbeidet man gjør, som å teste egne rutiner og lære av det som skjer.

God håndtering av uønskede hendelser bidrar til reduksjon av konsekvenser og kostnader som følger av sikkerhetsbrudd.

4 Sikker kommunikasjon

Det finnes et utall av standard og de facto standard protokoller. Ulike protokoller benyttes for AMS i dag, og det pågår et standardiseringsarbeid. Denne rapporten lister ikke opp ulike alternativer, men gir en generell vurdering av åpne vs. proprietære protokoller og hvordan data kan sikres. Tabell 4.1 illustrerer noen fordeler og ulemper med proprietære vs åpne protokoller.

Tabell 4.1 Proprietær vs åpen protokoll

Fordel	Proprietær	Åpen	Kommentar
Tilpasset det aktuelle behov	x		En proprietær protokoll kan tilpasses det aktuelle behov og gi fordeler i form av kortere telegram (datagram) og optimal responstid.
Kompatibilitet med annet utstyr		x	Kostnader og risiko forbundet med å få ulikt utstyr til å snakke sammen er ofte betydelige. Ikke bare ved oppstart, men gjennom produktets levetid.
"Life cycle cost" og kostnad for forbruker		x	Produkter basert på åpne standarder er ofte rimeligere både i innkjøp og vedlikehold eller utskifting pga. konkurrerende produkter.
Alternative leverandører		x	Risiko reduseres ved at man ikke er prisgitt en leverandør.
Utbyggbarhet og innovasjon		x	Standard løsninger gjør det mer attraktivt for andre leverandører å utvikle nye produkter og tjenester.
Informasjonssikkerhet	(x)	(x)	Sikkerheten ligger ikke i om en protokoll er proprietær eller ikke. Informasjonssikkerhet må ivaretas av sikkerhetsmekanismer i protokollen.

Som det fremgår av tabellen har åpne protokoller mange fordeler fremfor proprietære. Når det gjelder informasjonssikkerhet er de imidlertid nokså likestilt. En proprietær protokoll er normalt vanskeligere å angripe fordi den i utgangspunktet ikke er kjent. Vha. logging eller utro tjenere kan imidlertid innholdet avsløres, og data kan avlyttes eller manipuleres. *En proprietær protokoll må derfor beskyttes på lik linje med en åpen protokoll.*

4.1 Hvordan beskytte data

Mulige feil som kan oppstå når data skal sendes fra A til B er:

- Telegram kommer aldri frem
- Repetisjon av telegram (typisk som følge av programvarefeil)
- Falske telegram (telegram fra andre kilder enn forutsatt)
- Feil rekkefølge på telegram (dette kan være kritisk f.eks. dersom enheter skal slås av eller på)
- Korrupte data (telegrammet kommer frem med feil innhold)
- Tidsforsinkelse (telegrammet kommer senere enn forutsatt)

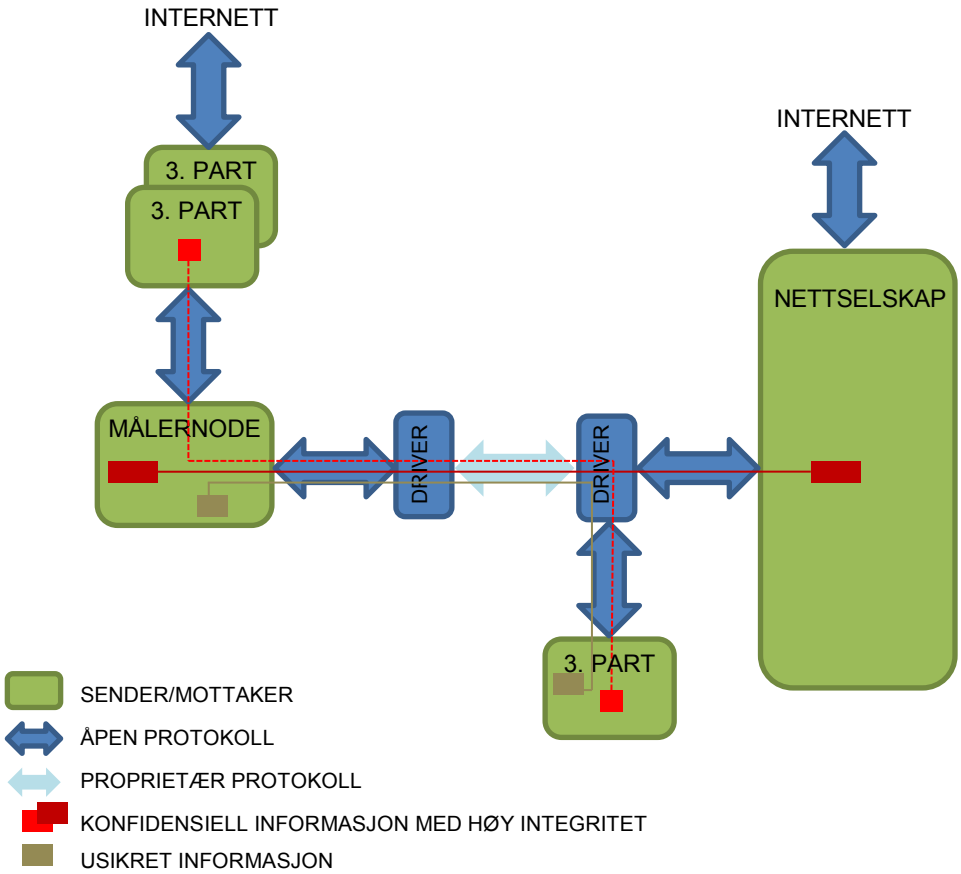
I tillegg må data beskyttes mot avlytting. For at mottaker av data skal kunne oppdage at en av de ovenstående feil har oppstått, og for å hindre avlytting, må telegrammene være beskyttet med disse sikkerhetsmekanismene:

- Kryptering (koding av data vha kodenøkler hos sender og mottaker)
- Tidsstempel (telegrammet inneholder tidspunkt for sending av data)
- Fortløpende teller (alle telegram bør inneholde en teller som inkrementeres hver gang data sendes)
- Sjekksum (med en god sjekksumalgoritme kan ødelagte data oppdages med stor sannsynlighet)

Sammen vil disse sikkerhetsmekanismene gi sikker kommunikasjon fra ende til ende *uavhengig av kommunikasjonskanalens kvalitet*. Data kan ikke manipuleres eller avlyttes medmindre krypteringsnøklene kommer på avveie. Data kan bli ødelagt eller bli borte, men mottaker vil oppdage dette og kunne gi alarm eller be om data på nytt. (Ødelagte data oppdages vha. sjekksum, data som blir borte oppdages vha. fortløpende teller.)

Et eksempel på sikker kommunikasjon er vist i figur 4.1. Denne illustrerer hvordan informasjon kan overføres sikkert fra ende til ende gjennom ulike kommunikasjonskanaler. Usikret informasjon kan overføres gjennom de samme kanaler eller via internett. I figuren er det illustrert bruk av både proprietære og åpne protokoller. Dette er ikke nødvendigvis en anbefalt løsning, men er teknisk mulig å implementere vha. drivere[7] eller oversettere uten at dette påvirker informasjonssikkerheten negativt.

[7] En driver kan konvertere signalet og oversette mellom protokoller med ulike fysiske lag, f.eks RS232 til USB.



Figur 4.1 Sikker kommunikasjon i AMS

Dersom målernoden i figuren tillates å motta usikret informasjon, innebærer dette økt risiko for at sikkerhetshull i målernodens programvare blir utnyttet (se f.eks. Tabell 6.1 Id 8).

Der de nevnte sikkerhetsmekanismer ikke kan benyttes, f.eks ved kritiske analoge målinger, må fysisk sikring benyttes. Dette gjelder typisk forbindelsen A0 mellom målepunkt og elmåler (se Figur 2.1). Dersom elmåler er intelligent og grensesnittet A1 mellom elmåler og målerterminal er en dataprotokoll, f.eks. trådløs, må tilsvarende sikkerhetsmekanismer implementeres i elmåleren.

4.2 Kvitteringsmeldinger

Med ovennevnte sikkerhetsmekanismer vil mottaker merke at data blir borte eller er ødelagt, men avsender av data kan ikke vite om data blir korrekt mottatt medmindre den får en kvittering tilbake. Hvorvidt kvittering skal benyttes eller ikke, bør vurderes for ulike telegramtyper. For syklisk sending av AMS måledata fra målernoden trenger ikke mottaker å sende kvittering, da det allerede er krav om at mottaker skal kunne etterspørre data fra gitte tidsrom. Bruk av kvitteringsmeldinger for sykliske data kan faktisk ha negative konsekvenser i form av vranglås-situasjoner ved svakheter i kommunikasjonskanalen. Ved sending av strupe/bryte-telegram vil det derimot være fornuftig å kreve at målernoden sender kvittering tilbake.

5 Scenarioer for uønskede hendelser

I det følgende beskrives noen scenarioer som kan oppstå som følge av innføring av AMS og toveis-kommunikasjon i kraftnettet fra kunde til nettselskap, og evt. via nettstasjon. Dette er ikke en uttømmende liste av scenarioer og uønskede hendelser, men eksempler som dekker ulike aspekter ved AMS. Når systemer er koblet sammen og mot Internett, vil det være angripers fantasi, kompetanse og motivasjon som setter grenser, og det er nærmest umulig å beskrive alle mulige situasjoner.

Malware (virus, ormer, o.l) vil kunne være årsaken til flere av hendelsene, eller verktøyet som brukes i flere av tilfellene, særlig ved angrep som kjøres langveisfra (fjerntilkobling).

De ulike scenarioene er beskrevet ut fra hva som er mulige hendelser, konsekvenser og tiltak. De er oppsummert med en tilhørende vurdering av konsekvens og sannsynlighet i kapittel 6.2.

5.1 Stort antall AMS ute av drift samtidig

Dette scenarioet omhandler ikke målrettede angrep. Det forutsettes dessuten at bryterfunksjonaliteten ikke er aktivert, dvs. effektuttak i målepunktet er verken begrenset eller koblet ut.

Mulige hendelser:

- Lynnedslag.
- Programvareoppdatering feiler.
- *Malware* har kommet inn på komponenter i kommunikasjonssystemet for AMS.
- Ved bytte av kommunikasjonsleverandør hos mange kunder i samme geografiske område på en gang.
- Vedlikehold på kommunikasjonsnettet fører til brudd på linjen.

Mulige konsekvenser:

Selv om målerne er ute av drift, vil strømforsyningen likevel kunne fungere som normalt. Dersom målerne fungerer, og det er kun kommunikasjonslinjen som er nede, vil måledata bli registrert som de skal og sendt til nettselskapet når linjen er oppe igjen. Dersom målerne er ute av drift, vil måledata ikke bli registrert. Dette er ikke kritisk, men uheldig, spesielt dersom det skjer i tunglast-perioder, hvor nettselskapene er ekstra interessert i å få registrert forbruk for planlegging. Hvis nettselskapet har registrering av belastning i trafoer på høyere spenningsnivå, har de tilgang til aggregerte data som kan brukes i driften – inntil måledata fra enkeltkunder blir tilgjengelig igjen.

For kraftproduksjon tilknyttet distribusjonsnettet kan konsekvensen være at avregning blir feil. Hvis måledata registreres i sanntid og brukes i en driftssituasjon, vil de som drifter kraftnettet kunne miste oversikt, og for mye kraft kan bli ført ut på nettet.

Dessuten:

- Ved oppstart etter feil på kommunikasjonsnettet skal mange målere sende mye data samtidig – fare for overbelastning i kommunikasjonsnettet.
- AMS-utstyr kan ha blitt ødelagt, noe som medfører store kostnader knyttet til reparasjon/utskiftning.

Mulige tiltak:

- Elektronikken, selve måleren, må være sikret mot lynnedslag.
- Programvare må kunne oppdateres uten at en tekniker må fysisk inn i huset og stå ved måleren. Selv om dette kan forårsake feil, er det likevel en stor fordel i forbindelse med tetting av sikkerhetshull, innlegging av ny funksjonalitet og feilrettinger.
- Kravet om overføring av måleverdier fra kunde til nettselskap minst en gang i døgnet må kunne omgås ved omfattede feilsituasjoner.
- Lokal kraftproduksjon vil måtte ha lokalt vern som sikrer mot ustabilt nett og overbelastning av kritiske komponenter.
- Også for produsert kraft vil data logges og kan hentes opp i ettertid. Feil avregning for lokale kraftprodusenter kan justeres i ettertid gjennom korreksjonsoppgjør.

5.2 Kunde manipulerer måledata

Mulige hendelser:

- Kunden manipulerer egne måledata slik at de viser mindre forbruk.
- Kunden manipulerer data og "flytter" forbruk fra dyre høylast-perioder til rimeligere lavlast-perioder. Totalt forbruk blir riktig, men avregning og fakturering blir feil.
- Kunden manipulerer egne måledata slik at eget forbruk er redusert og naboens forbruk er økt.

Mulige konsekvenser:

- Nettselskap oversender feil datagrunnlag til kraftleverandør, som dermed fakturerer feil for de involverte kundene. Det som ikke blir avregnet som forbruk til kunde vil inngå i nettap.
- Nettselskap får feil datagrunnlag til å beregne nettap.

Mulige tiltak:

- Balansemåling i nettstasjon kan gjøre det mulig å avdekke slike feil, hvis nettap under aktuell nettstasjon er betydelig større enn normalt. Dette vil være avhengig av hvor mye måledata er manipulert.
- Hvis manipulering av egne data gjøres i målerterminal, vil det imidlertid være uoverensstemmelse mellom registrert målerstand og faktisk målerstand på måler.
- Det bør implementeres funksjonalitet i AMS som skal detektere forsøk på manipulering av data og generere alarm til sentralsystemet [5]. Forsøk på manipulering kan f.eks. være å påvirke elmåler med magnet eller innbrudd på kommunikasjonslinjer.
- Kryptering av måledata vil gjøre manipulering av måledata vanskelig.

5.3 Interne trusler – Utro tjener

Mulige hendelser:

- Person som er autorisert til å få tilgang til bryter-/strupefunksjon misbruker dette.
- Autorisert person gir tilgang til uvedkommende, som dermed kan kontrollere bryter-/strupefunksjonen for enkeltkunder eller større områder.
- Autorisert person endrer koblinger i nettet slik at bryter-/strupefunksjonen virker på feil husstand eller på et større område, slik at nettselskapet handler i god tro, men forårsaker utkoblinger eller effektbegrensninger hos feil kunder.
- En person på innsiden legger inn ondsinnet kode slik at angriper på utsiden får en bakdør inn i systemet for videre styring og kontroll.
- En ansatt oppgir informasjon og utleverer dokumenter knyttet til kontrakter, avtaler, interne rutiner og drift til uvedkommende.
- Ulovlig videreformidling/salg av måledata og/eller personopplysninger.
- Enkeltkunder får hjelp fra en utro tjener til å manipulere måledata, slik at de kan betale mindre enn det de skal.

Mulige konsekvenser:

- Generelt vil utro tjenere kunne misbruke tilganger de allerede har i forbindelse med sitt daglige arbeid. Med utviklingen innenfor AMS og SmartGrid forøvrig, vil systemer henge sammen i større grad enn før, mulighetene for fjerntilkobling vil øke, og på den måten vil flere ansatte få tilgang til funksjoner som har med drift å gjøre.
- Koordinerte, målrettede angrep hvor interne ressurser med detaljert kjennskap til systemer bidrar, kan oppnå nær sagt hva som helst. Dette er et *worst-case scenario*, med store muligheter for omfattende skader for både nettselskapet, kundene og samfunnet.

Mulige tiltak:

- God tilgangskontroll internt, basert på et "need-to-know"-prinsipp, slik at ansatte ikke har tilgang til flere systemer enn de trenger for sitt daglige arbeid. Hver bruker skal ha eget brukernavn og passord, slik at ikke felles admin-brukere kan benyttes til ulovlige handlinger og slik at alle handlinger kan spores.
- Logging, slik at man i etterkant kan gå tilbake og se hva som gikk galt og hvem som utførte handlingen.
- Opplæring og bevisstgjøring av ansatte, slik at de kjenner systemene og forstår trusselbildet, og er i stand til å se konsekvensene av sine egne handlinger.
- Gode rutiner ved ansettelser; sjekk bakgrunn og referanser før nyansettelser. Industrispionasje er en økende aktivitet i Norge, og dette må kraftbransjen også ta innover seg og håndtere.
- Gode kvalitetssikringsrutiner for å avdekke avvik så tidlig som mulig.
- Kryptering og integritetskontroll av datakommunikasjon vil hindre avlytting og begrense mulighetene for manipulering av data, samt avdekke tidlig dersom uautoriserte endringer har blitt utført.

5.4 Målrettet angrep på kraftforsyningen i et spesifikt geografisk område

Mulige hendelser:

- Datainnbrudd i en eller flere MV/LV-nettstasjon(er) (master/konsentrator – ref. Figur 2.1).
- Bruk av bakdører og annet hackerverktøy langveisfra, gjennom Internett, administrativt nett og ut i kommunikasjonsnettet mot enkeltkundene.
- Samarbeid mellom ekstern angriper og utro tjener, som beskrevet i scenarioet over (kap. 5.3); utlevering av informasjon, hjelp til å legge inn ondsinnet kode, osv.
- Vern som er manipulerte og ikke virker.

Mulige konsekvenser:

- Bryte strømforsyning til flere kunder. Koble ut transformator – eller bryte strømforsyning til alle kunder lokalisert under aktuell nettstasjon.
- Uvedkommende tar kontroll over bryterfunksjon hos en eller flere sluttbrukere – skrur av strømmen mens det er -20 ute.
- Fysiske ødeleggelser på komponenter i kraft- og/eller kommunikasjonsnettet
- Fysiske ødeleggelser av AMS hos kunder.
- Manipulerte data som gir feil informasjon om belastning i et område, kan gi overbelastning/lite forbruk. Konsekvens for kraftsystemet kan være et ustabilt system.
- Manipulerte vern fungerer ikke som de skal, bl.a. at de kobler ikke ut i en feilsituasjon.

Mulige tiltak:

- Fysisk adskillelse mellom kritiske nett og komponenter, slik at ikke alt kan nås utenfra.
- God oversikt og dokumentasjon av systemer og nettverkskoblinger, for å unngå at det finnes åpninger som man ikke kjenner til og derfor ikke har sikret.
- Risikovurderinger av alle komponenter og systemer, slik at man oppnår rett sikkerhetsnivå i forhold til økonomiske prioriteringer, og har et bevisst forhold til hvilke risikoer man aksepterer.
- Gode brannmurer, oppdateringsrutiner og antivirusmekanismer.
- Bryter-/strupefunksjonen må ha en fail-safe tilstand. Fail-safe tilstand bør være å opprettholde nåværende tilstand dersom målernoden svikter.

5.5 Uheldige konsekvenser av tredjepartstilgang

Mulige hendelser:

- Separat display med enveis kommunikasjon (i utgangspunktet), med mulighet for toveis, slik at displayet kan utgjøre en innfallsport for angriper inn mot AMS.
- Lavere sikkerhetsnivå på AMS fordi flere skal ha tilgang til måledata fra målernode hos kunde (grensesnitt A3 og A4 i Figur 2.1); personvernet kompromitteres for å tilfredsstille tredjeparts behov.

Dette er eksempler på hendelser som kan gi tredjepart tilgang til AMS-infrastruktur, og dermed også mulighet for f.eks. manipulering av data eller misbruk av bryter-/strupefunksjon.

Mulige konsekvenser:

- Display og annet utstyr som er tilkoblet AMS, brukes som en innfallsport for en angriper, for å manipulere måledata hos en eller flere kunder, eller for å oppnå tilgang til kommunikasjonslinjer videre i nettet mot nettstasjoner og nettselskap.
- Et angrep på tredjepartstjenesten kan ramme AMS, så lenge de benytter samme infrastruktur. Kommunikasjonslinjen kan bli utilgjengelig, slik at måledata ikke kan samles inn, eller bryter-/strupefunksjonen ikke fungerer.

Mulige tiltak:

- Definere tydelig hvilken tjenestekvalitet som er tilgjengelig for tredjepart ut i fra hva AMS behøver, slik at systemet skaleres for AMS og ikke for andre mulige tjenester, noe som også er presisert av NVE[8].
- Designe systemet slik at tredjeparts tilkobling (målernode hos kunde) ikke kan medføre skade.

[8] I [1] har NVE presisert at det ikke stilles krav om at andre enn nettselskapet skal ha fysisk tilgang til kommunikasjonsløsningen i AMS. Adgang for tjenesteleverandører innebærer derimot at nettselskapet skal formidle informasjon mellom tredjepartsleverandør og sluttbruker. NVE vil samtidig understreke at det ikke forventes at AMS-kanalen skal dimensjoneres utover den kapasitet som er nødvendig for å tilfredsstille nettselskapenes og kraftleverandørenes behov for overføring av data.

En grunnleggende forutsetning for kravet om videreformidling av informasjon mellom AMS, tjenesteleverandører og eksternt utstyr tilknyttet lokalt er at kommunikasjonsløsningen skal dimensjoneres etter kravene om innhenting av forbruksdata daglig. Kommunikasjonsløsningen skal kun benyttes når det er ledig kapasitet i AMS og når sikkerhetskravene er oppfylt. Innsamling av måleverdier skal ha prioritet fremfor andre formål.

Det er presisert at det primært er energirelaterte tjenester som anses aktuelle å tilknytte AMS. Dette gjenspeiles i kravet om at AMS skal kunne sende og motta informasjon om forbruk, kraftpriser og tariffer, samt at de skal kunne overføre styrings- og jordfeilsignal.

6 Klassifisering av uønskede hendelser

I det følgende presenteres en rekke uønskede hendelser knyttet til de ulike komponentene i AMS. Gjennom en vurdering av alvorlighet og sannsynlighet, framheves de hendelsene som har størst risikopotensiale, fortrinnsvis sett fra et nettselskaps ståsted. SINTEF har gjort denne vurderingen ut i fra kompetanse, erfaring og innsikt i tekniske systemer. Den må ikke sees på som en endelig fasit, og hvert enkelt nettselskap må i tillegg gjøre sine vurderinger ut i fra egne systemer.

Alvorlighet og sannsynlighet er kategorisert ut i fra en skala 1-5, hvor 1 er lav og 5 er høy. Risiko er produktet av alvorlighet og sannsynlighet. Risiko er presentert som et tall i tabell 6.1 og representert med en farge i en risikomatrise til slutt i kapittelet. Med en usymmetrisk risikomatrise, som vår, vil to hendelser med samme risiko, kunne ha ulik farge i risikomatrisen.

Noen generelle prinsipper er benyttet ved vurdering av alvorlighet og sannsynlighet:

- "Ingen måling" er normalt vurdert som mindre alvorlig enn "feil måling" pga. at hendelsen er lettere å oppdage raskt.
- En "teknisk svikt" er i utgangspunktet vurdert med sannsynlighet 3. Variasjoner opp eller ned vil være avhengig av blant annet systemets kompleksitet.
- Et "målrettet angrep" som vil ramme mange er i utgangspunktet vurdert med sannsynlighet 3. Variasjon opp eller ned vil være avhengig av blant annet antall som rammes og hvor lett det vil være å utføre angrepet. I tillegg til at "antall som rammes" påvirker konsekvens, er det antatt at målrettede angrep vil være mer sannsynlig dersom det rammer mange.

Alvorlighet – forklaring til kategoriene 1-5:

1. lite alvorlig for både nettselskapet og kunden. Ingen måleravlesning, feil info om priser etc.
2. mindre alvorlig for et nettselskap og kunden. Feil måleravlesning hos en kunde, ødelagt utstyr.
3. alvorlig for et nettselskap, kan også være kritisk for en eller flere privatkunder eller virksomheter som ikke er trafomålt. Uønsket utkobling.
4. kritiske konsekvenser for ett nettselskap. Feil måleravlesning eller utkobling hos mange kunder og virksomheter som ikke er trafomålt.
5. svært kritiske konsekvenser for ett eller flere nettselskap samtidig. Målrettet angrep som forårsaker strømbrudd hos mange kunder. For at kraftforsyningen på nasjonalt nivå skal rammes, må flere, eller de store, nettselskapene rammes.

Sannsynlighet – forklaring av kategoriene 1-5:

1. Lite sannsynlig. Målrettede angrep med liten effekt. Motivasjonen for denne typen angrep ansees som lav hos de som innehar kompetansen til å gjennomføre slike.
2. Noe sannsynlig. Målrettet angrep mot en kunde (se over). Enkel teknologi.
3. Sannsynlig. Målrettede angrep som krever kompetanse for å gjennomføre, vil oftere ramme mange enn kun en kunde, fordi det er mer attraktivt.
4. Meget sannsynlig. Teknisk svikt et eller annet sted i systemet som bryter kommunikasjonen.
5. Svært sannsynlig. Teknisk eller menneskelig feil som ikke har noen betydning for måleravlesning eller bryterfunksjonaliteten. Ingen slike hendelser er vurdert i denne analysen.

6.1 Hendelser knyttet til de ulike AMS-komponentene

Tabell 6.1 Uønskede hendelser knyttet de ulike AMS-komponentene

Id	Komponent	Hendelse	Årsak	Konsekvens	Alvorlighet 1-5 hvor 5 er katastrofalt	Sannsynlighet 1-5 hvor 5 er svært sannsynlig	Risiko	Mulige tiltak
1.	Målepunkt[9]	Manipulering av sensor	Målrettet	Feil eller ingen måleravlesning	2	3	6	Fysisk/Plombering
2.		Sensor feiler	Teknisk svikt	Ingen måleravlesning	1	2[10]	2	Elmåler detekterer svikt og rapporterer
3.	Målernode inkludert - Elmåler - Målerterminal - Bryting/Struping - Alle grensesnitt	Manipulering av elektronikk	Målrettet	Feil eller ingen måleravlesning	2	1	2	Fysisk/Plombering
4.		Manipulering av bryterfunksjon[11] vha elektronikk	Målrettet	Uønsket utkobling	3	1	3	Fysisk/Plombering
5.		Manipulering via grensesnitt på målernode, f.eks. ved falsk programvare	Målrettet	Feil eller ingen måleravlesning hos **en** kunde	2	2	4	Kryptering Robust design [12] Programvare-overvåking[13]

[9] Det forutsettes at sensoren (kobling A0 i systemskissen - Figur 2.1) er en analog tilkobling/måling.
[10] Lav sannsynlighet pga enkelt konstruert sensor
[11] Strupefunksjon kan manipuleres likt med bryterfunksjon, men er mindre kritisk og tas ikke med i tabellen.
[12] Grensesnitt må lages slik at de ikke på noe vis kan påvirke andre funksjoner enn de de er ment å skulle påvirke
[13] Programvare-overvåking kan innebære at det sendes melding til sentral ved alle forsøk på å endre programvare..

Id	Komponent	Hendelse	Årsak	Konsekvens	Alvorlighet 1-5 hvor 5 er katastrofalt	Sannsynlighet 1-5 hvor 5 er svært sannsynlig	Risiko	Mulige tiltak
6.		Manipulering via grensesnitt på målernode	Målrettet	Feil eller ingen måleravlesning hos **mange** kunder	4	3[14]	12	Kryptering Robust design
7.		Manipulering av bryterfunksjon via grensesnitt på målernode	Målrettet	Uønsket utkobling hos **en** kunde	3	2	6	Kryptering Robust design
8.		Manipulering av bryterfunksjon via grensesnitt på målernode	Målrettet	Uønsket utkobling hos **mange** kunder	5	3	15	Kryptering Robust design
9.		Elektronikkomponent (er) feiler	Teknisk svikt	Feil eller ingen måleravlesning	2	3	6	Redundans Selvtest[15]
10.		Elektronikkomponent (er) feiler	Teknisk svikt	Uønsket utkobling	3	3	9	Redundans Selvtest
11.		Elektronikkomponent (er) feiler	Teknisk svikt	Elektrisk utstyr slås av/på slik at utstyret skades.	2	3	6	Redundans Selvtest
12.		Programvarefeil	Teknisk svikt	Feil eller ingen måleravlesning hos mange	4	3	12	Programvare-utvikling ihht anerkjent standard.[16]

[14] Manipulering via grensesnitt er vanskelig, og antas at motivasjonen og dermed sannsynligheten er større for å gjøre dette hos mange enn hos en.
[15] Det forutsettes at selvtest tar fornuftig aksjon, f.eks alarm og avbrudd av struping.
[16] For eksempel IEC 12207 [14]

Id	Komponent	Hendelse	Årsak	Konsekvens	Alvorlighet 1-5 hvor 5 er katastrofalt	Sannsynlighet 1-5 hvor 5 er svært sannsynlig	Risiko	Mulige tiltak
13.		Programvarefeil	Teknisk svikt	Uønsket utkobling hos mange	4	3	12	Programvare-utvikling ihht anerkjent standard.
14.		Tyveri av krypteringsnøkkel	Målrettet	Manipulering av måledata eller bryterfunksjon for en enhet.	2	2	4	Bruk av anerkjente metoder for håndtering av nøkler
15.	Separat display inkludert grensesnitt på målernode	Grensesnitt benyttes til manipulering av egen målernode	Målrettet	Dekket under målernode	-	-	-	
16.		Grensesnitt benyttes til manipulering av forbruk eller prisinformasjon på andres display	Målrettet	Kunder tror de bruker mer eller mindre strøm enn de faktisk gjør. Kunder tror strømmen er dyrere/billigere enn den faktisk er.	1	1	1	Kryptering kan benyttes, men er neppe hensikts-messig. Store avvik kan oppdages på strømregningen.
17.		Elektronikkomponent (er) feiler	Teknisk svikt	Ingen visning eller fryste verdier i display.	1	3	3	Kunden oppdager og rapporterer feil. Designes slik at fryste verdier unngås eller oppdages.
18.	Kontrollert enhet inkludert grensesnitt	Grensesnitt benyttes til manipulering av målernode	Målrettet	Dekket under målernode	-	-	-	

Id	Komponent	Hendelse	Årsak	Konsekvens	Alvorlighet 1-5 hvor 5 er katastrofalt	Sannsynlighet 1-5 hvor 5 er svært sannsynlig	Risiko	Mulige tiltak
19.		Kontrollert enhet ignorerer utkoblingskommando.	Teknisk svikt	Nettselskap oppnår ikke styring av en kontrollert enhet Manglende funksjon hos kunden, varmtvann el.	2	3	6	Manuell overstyring av kunde
20.	Andre målere/ givere	Grensesnitt benyttes til manipulering av målernode	Målrettet	Dekket under målernode	-	-	-	
21.		En eller annen feil i systemet gjør at målesignal ikke kommer til mottaker.	Teknisk svikt	Konsekvens avhenger av funksjonen til tilkoblet utstyr. Kan være svært alvorlig, f.eks. trygghetsalarm, brannalarm.	5	4	20	Her er det verdt å merke seg at til-koblet utstyr fra et sikkerhetsaspekt, kan bli dimensjonerende for krav til infrastruktur hva gjelder både oppe-tid og responstid. (Se fotnote 8)
22.	Master/ Konsentrator	Manipulering av data	Målrettet	Feil eller ingen måleravlesning hos mange kunder	4	3	12	Fysisk sikring Kryptering Robust design
23.		Manipulering av bryterfunksjon	Målrettet	Uønsket utkobling hos mange kunder	5	3	15	Fysisk sikring Kryptering Robust design

Id	Komponent	Hendelse	Årsak	Konsekvens	Alvorlighet 1-5 hvor 5 er katastrofalt	Sannsynlighet 1-5 hvor 5 er svært sannsynlig	Risiko	Mulige tiltak
24.		Elektronikkomponent (er) eller programvare feiler	Teknisk svikt	**Feil** måleravlesning hos mange kunder	4	3[17]	12	Kryptering Sjekksum Balansemåling i nettstasjon
25.		Elektronikkomponent (er) eller programvare feiler	Teknisk svikt	**Ingen** måleravlesning hos mange kunder	2	3	6	Redundans Selvtest Balansemåling i nettstasjon
26.	Registreringsenhet	Manipulering av data eller programvare	Målrettet	Feil data fra registreringsenhet kan medføre utkobling[18] av stasjon og dermed strømbrudd for mange.	4	3	12	Fysisk sikring Kryptering Robust design Programvare-overvåking
27.		Elektronikkomponent (er) eller programvare feiler	Teknisk svikt	Feil data fra registreringsenhet kan medføre utkobling av stasjon og dermed strømbrudd for mange.	4	3	12	Redundans Selvtest

[17] Svært lite sannsynlig (=1) dersom sjekksum benyttes.
[18] Utkobling kan skje fra sentral fordi feil målinger tilsier at utkobling er nødvendig, eller utkobling kan skje pga feil som ville vært oppdaget dersom systemet var intakt.

Id	Komponent	Hendelse	Årsak	Konsekvens	Alvorlighet 1-5 hvor 5 er katastrofalt	Sannsynlighet 1-5 hvor 5 er svært sannsynlig	Risiko	Mulige tiltak
28.	Sentralsystem/ FrontEnd	Manipulering av data	Målrettet	Feil eller ingen måleravlesning hos svært mange kunder med mulige konsekvenser for kraftforsyningen	5	3	15	Fysisk sikring Kontrollfunksjoner[19] Rutiner Balansemåling Kraftfordeling kan gjøres som i dag, uavhengig av AMS
29.		Manipulering av bryterfunksjon	Målrettet	Uønsket utkobling hos alle kunder	5	3	15	Fysisk sikring Kontrollfunksjoner Rutiner
30.		Programvare feiler	Teknisk svikt	Feil eller ingen måleravlesning hos svært mange kunder med mulige konsekvenser for kraftforsyningen	5	3	15	Redundans Kontrollfunksjoner Rutiner Balansemåling Kraftfordeling kan gjøres som i dag, uavhengig av AMS
31.		Tyveri av krypteringsnøkkel	Målrettet	Manipulering av måledata med mulige konsekvenser for kraftforsyningen eller utkoblings-funksjon for alle enheter	5	3	15	Bruk av anerkjente metoder for håndtering av nøkler Kontrollfunksjoner Rutiner Balansemåling Kraftfordeling kan gjøres som i dag, uavhengig av AMS

[19] Typiske kontrollfunksjoner vil være integritetskontroll, logging, autentisering, løsninger for deteksjon og hindring av datainnbrudd (IDS/IPS).

6.2 Konsekvensvurdering av scenarioene

Scenarioene som ble beskrevet i kapittel 5, er oppsummert i nedenstående tabell, sammen med en vurdering av alvorlighet og sannsynlighet. De er plassert inn i risikomatrisen på neste side.

Tabell 6.2 Scenarioer, med tilhørende vurdering av alvorlighet og sannsynlighet

Nr	Scenario	Alvorlighet (1-5, hvor 5 er katastrofalt)	Sannsynlighet (1-5, hvor 5 er svært sannsynlig)	Risiko
S 1	Stort antall AMS ute av drift samtidig	4	3	12
S 2	Kunde manipulerer måledata	2	2	4
S 3	Interne trusler – utro tjener	5	3	15
S 4	Målrettet angrep på kraftforsyningen i et spesifikt geografisk område	5	3	15
S 5	Uheldige konsekvenser av tredjepartstilgang	3	2	6

Risikomatrisen som presenteres i dette kapitlet har en foreslått fargeinndeling. Hvert enkelt nettselskap må selv bestemme sine egne grenser for hva som er akseptabel risiko. Typisk vil man ikke akseptere hendelser i den røde sonen, for slike skal det iverksettes tiltak. For hendelser i gul sone skal risikoreduserende tiltak vurderes, mens grønn sone indikerer at risikoreduserende tiltak ikke er nødvendig.

Risiko beregnes ut ifra sannsynlighet og alvorlighet for en uønsket hendelse. Risiko for uønskede hendelser dokumenteres i risikomatrisen.

Rødt : høy risiko. Hendelser i denne sonen kan ha store konsekvenser.
Gult : middels risiko. Hendelser i denne sonen kan ha uheldige konsekvenser.
Grønt : lav risiko. Hendelser i denne sonen medfører ingen større konsekvenser.

		Alvorlighet				
		Lite farlig	**Noe farlig**	**Alvorlig**	**Kritisk**	**Katastrofalt**
Sannsynlighet	**Svært sannsynlig**					
	Meget sannsynlig					21
	Sannsynlig	17	1, 9, 11, 19,25	10	S1, 6, 12,13,22, 24, 26, 27	S3, S4, 8, 23, 28, 29, 30, 31
	Noe sannsynlig	2	S2, 5, 14	S5, 7		
	Lite sannsynlig	16	3	4		

De hendelsene som er vurdert til å ha høyest risiko, har et eller flere av følgende elementer i seg:

- Uønsket utkobling hos mange kunder
- Programvarefeil
- Sentralsystem feiler eller brukes i angrepet
- Utro tjener

I tillegg er scenarioet med mange målere ute av drift samtidig vurdert til å være kritisk. Årsaken er at konsekvensene vil medføre store kostnader for reparasjon og/eller utskiftning av teknisk utstyr.

Risikoreduserende tiltak bringer risiko ned på lavt nivå for samtlige kritiske hendelser. Det må imidlertid være en balanse mellom kostnaden for risikoreduserende tiltak og konsekvenser ved en eventuell hendelse, inkludert både skaden som forårsakes, samt kostnaden for å håndtere hendelsen.

7 Anbefalinger

Dette kapitlet har en todelt struktur; hvor første del gjelder anbefalinger til bransjen angående utrulling og drift av AMS, og andre del er adressert til NVE, som skal videreutvikle krav og regelverk for bransjen.

7.1 Utrulling og drift

Kommunikasjonsprotokoller

Det anbefales at det benyttes åpne protokoller som støtter kryptering for all kommunikasjon hvor informasjonssikkerhet må ivaretas. Tidsstempel, fortløpende teller og sjekksum må implementeres i applikasjonslaget dersom dette ikke er en del av protokollen. Disse mekanismene må være implementert på sendersiden, og avvik må håndteres på mottakersiden. Der slike mekanismer ikke kan benyttes, f.eks ved kritiske analoge målinger, må fysisk sikring gjøres.

Bryter-/strupefunksjonen

Bryter-/strupefunksjonen er en funksjon som kan brukes til faste oppdrag (daglig effektreduksjon i topplastperioder) eller som en beredskapsfunksjon (flytting, dårlige betalere, rasjonering). Hvis bryter-/strupefunksjonen brukes sjelden, bør nettselskapene definere et testintervall for funksjonen for å sikre at den fungerer tilfredsstillende når den aktiveres.

Bryter-/strupefunksjonen er kritisk og inngår i mange uønskede scenarioer, og implementeringen av denne bør vurderes nøye. Det gjelder både forhold hos kunde/i nettstasjon og konsekvens ved evt. feil, og hvordan funksjonaliteten skal implementeres hos nettselskapene. Adgang til bryter-/strupefunksjonaliteten og konsekvensen ved både teknisk svikt og målrettede angrep bør reduseres. Fail-safe status for denne funksjonen bør vurderes slik at konsekvensen blir minst mulig ved feil – både for kunde, kraftsystemet og nettselskapet.

Programvareutvikling

Programvareutvikling i AMS bør skje i henhold til anerkjente standarder. Dokumenterte tester og verifikasjon er spesielt viktig, initielt, og ikke minst ved programvareendringer. Testene må omfatte unntaksscenarioer. Utviklingsprosessen kan ta sikte på å følge Common Criteria [15], uten at det nødvendigvis er kostnadseffektivt å arbeide for en sertifisering.

Funksjonelt er det viktig at programvare kan oppdateres fra sentralt hold. På den måten kan eventuelle sikkerhetshull lett tettes. Maskinvare (prosessor, minne, etc.) må initielt ha reservekapasitet for å understøtte programvareendringer[20].

[20] Eksempelvis inneholder NORSOKs standard for sikkerhetssystemer [13] krav om at gjennomsnittlig prosessorlast ikke skal være over 75%, mens minne skal ha 50% reserve, ved leveranse.

Outsourcing

AMS er en infrastruktur til bruk for måling og bryting/struping. Nettselskapene er ansvarlige for måling og avregning, og allerede i dag er det flere som outsourcer denne aktiviteten. Følgende vurderinger bør gjøres før outsourcing av AMS (som andre typer tjenester):

- Man må vite hvor (geografisk og til hvem) dataene overføres og lagres, hvem som har tilgang
- Sikkerhetsnivået i løsningen, ifbm overføring, lagring, prosessering, tilbakeføring og sletting
- Kontrakt som regulerer forutsetninger, kvalitetssikring, leveringsfase og avvikling, samt mekanismer for fleksibilitet og skalerbarhet
- Oppetidsgarantier og kompensasjonsordninger ved eventuelle brudd på disse
- Håndtering og kommunikasjon av sikkerhetsbrudd
- Muligheter for insourcing etter en stund, eller migrering til annen tilbyder

Ved implementering av en bryter-/strupefunksjon, kan AMS inngå direkte i nettdriften (ref. driftskontrollsystem/SCADA), og denne funksjonaliteten kan ikke like lett outsources, men samarbeid mellom flere nettselskap er naturlig.

Kartlegging og dokumentasjon av systemer

Et viktig tiltak for å redusere sannsynligheten for mange av de uønskede hendelsene som er diskutert i denne rapporten, er å ha god og oppdatert dokumentasjon av AMS-systemet. Dette innebærer å opprette, og vedlikeholde, en oversikt over alle komponenter, systemer og nettverkskoblinger: Hvilke komponenter finnes, hvilke henger sammen, hvor går kommunikasjonslinjen, hva skjer hvis spesifikke komponenter feiler, hvilke komponenter er mest kritisk, hvilke programmer og operativsystemer kjører på hvilke maskiner, hvordan er oppdateringsrutinene på hver enkelt maskin – og ikke minst, hvordan reagerer gamle komponenter på økt kompleksitet og sammenkoblinger med flere typer nye systemer? Dessuten, hvordan håndteres en driftssituasjon med endringer, hvor en ny tilkobling kan velte alle forutsetninger som en gammel risikovurdering var basert på? Dette er en sentral aktivitet i enhver risikovurdering; hvis man ikke vet hvilke systemer man har, så kan man heller ikke velge fornuftige sikkerhetsmekanismer.

Risikovurdering

Risikovurderinger må gjøres tidlig i kravfasen for at løsninger som realiseres, skal kunne implementeres på en god og sikker måte. Deretter må det gjennomføres jevnlige risikovurderinger, slik at alle utvidelser og øvrige endringer blir fanget opp og vurdert ut i fra et sikkerhetsperspektiv. Beredskapsforskriften [11] har allerede krav til at det til enhver tid skal eksistere oppdaterte risikovurderinger for IT-systemer, inkludert driftskontrollsystemer. Dette bør også gjelde AMS, slik at AMS vurderes på lik linje med øvrige IT-systemer og at det tas riktige beslutninger knyttet til sikkerhetsmekanismer.

Tabell 7.1 inneholder en rekke momenter som bør avklares under en risikovurdering og kan brukes som et konkret hjelpemiddel for det enkelte selskap.

Tabell 7.1 Sjekkliste til bruk i en risikovurdering

Organisatorisk	Teknisk
IT-sikkerhetspolicy	Tilgangskontroll
IT-sikkerhetsreglement	Brann
Ansvar og myndigheter	Strømbrudd
Outsourcing	Nettverksarkitektur, sonedeling
IT-sikkerhetsledelse	Passord-policy
Lover og regler	Fysisk sikkerhet
Avtaler (SLA) med underleverandører	Fjernaksess
Holdninger og bevissthet	Patching, sikkerhetsoppdateringer
Dokumentasjon av systemer og koblinger, kritikalitetsvurdering av komponenter	"Svarte svaner" (hendelser med lav sannsynlighet og katastrofale konsekvenser
Standarder	Resiliens, motstandsdyktighet
Revisjon	Sabotasje, terrorisme
Internasjonale forhold, f.eks. lovverk	Redundans

Adgang og tilgang til AMS

Hvert enkelt nettselskap må ta en vurdering rundt fysisk adgangs- og tilgangskontroll til bryter-/strupefunksjonen. Det kan være naturlig å se på denne som en del av SCADA-systemene, samtidig som det kan være praktisk å ha tilgang til den fra kontornettverket, eller sogar fra kundesenteret. Det er såpass store forskjeller mellom ulike nettselskap, at det er vanskelig å lage en generell anbefaling. Vurderingene må derfor gjøres hos hver enkelt, og sikringstiltak må implementeres på rett nivå ut i fra valgt løsning.

Sammenkobling av AMS og driftskontrollsystemer

Tidligere har automatisk måling av forbruk blitt knyttet til måling og avregning, og mulighet for å fakturere kundene for deres faktiske forbruk. Med bryter-/strupefunksjonalitet installert på kundenivå og i MV/LV nettstasjoner vil nettselskapene får oppdatert informasjon om status og driftsforhold i nettet og mulighet for regulering. Tidligere var feil på automatisk måling knyttet til feil avregning, men ved AMS kan feil også bli relatert til selve nettdriften. AMS-funksjonaliteten knyttet til drift og driftskontrollsystemer bør risikovurderes på lik linje med dagens etablerte driftskontrollsystemer (SCADA).

Håndtering av sikkerhetsbrudd

Hendelseshåndtering bør bestå av både forebyggende arbeid, håndtering av det som måtte inntreffe, og et skikkelig etterarbeid, inkludert læring og erfaringsdeling. Etterarbeidet bør deretter brukes aktivt i risikostyringsprosessen og i det generelle sikkerhetsarbeidet internt, for eksempel når det gjelder opplæring og styrking av sikkerhetsbevissthet hos de ansatte.

7.2 Krav og regelverk

Gjeldende krav fra NVE til bransjen er at 80% av alle strømkunder i Norge skal ha AMS innen 1.1.2016 og 100 % skal ha AMS innen 1.1.2017. Det må imidlertid ikke bli slik at tidsfristen blir styrende for tekniske og organisatoriske valg som gjøres for implementasjon. I så fall vil det være en risiko for at de løsningene som blir realisert, ikke er tilfredsstillende i forhold til informasjonssikkerhet og personvern. NVE må vurdere hvordan dette skal håndteres, uten at resultatet bare blir at man flytter fristen og utsetter problemene.

Beredskapsforskriften

Denne rapporten anbefaler at Beredskapsforskriften [11] bør gjelde for AMS, fordi risikovurderingen som er gjort viser at uønskede hendelser med AMS kan ha konsekvenser for kraftforsyningen, som er en kritisk samfunnsinfrastruktur. Spesielt er det bryter-/strupefunksjonen som gjør AMS utsatt, med de konsekvensene feil bruk kan ha.

Kapittel 6 i Beredskapsforskriften omhandler Informasjonssikkerhet, og flere av de kravene som allerede er implementert, bør gjelde også for AMS. I tillegg gir rapporten følgende anbefalinger til mulige endringer i veiledningen til forskriften:

- Pkt. 6.1.1 kan gjerne inneholde et kulepunkt om kartlegging og dokumentasjon av systemer. Dette er ikke spesifikt uttrykt i dag.
- Pkt. 6.1.8 bør inneholde en kildehenvisning til trusselvurderinger fra Politiets sikkerhetstjeneste.
- AMS (med bryter-/strupefunksjonalitet inkludert) bør inngå i §6-4 og klassifiseres på samme måte som driftssentraler, slik at kravene også kan gjelde AMS, for eksempel for fjerntilgang.

Bransjesamarbeid

Forum for informasjonssikkerhet i kraftsektoren kan være rett sted for bransjesamarbeid rundt sikkerhetsutfordringer, både for diskusjon av gode og aktuelle løsninger, og for å arbeide forebyggende mot sikkerhetshendelser.

8 Referanser

[1] "Veiledning i risiko- og sårbarhetsanalyse", Nasjonal sikkerhetsmyndighet, April 2005.

[2] "Avanserte måle- og styringssystemer. Oppsummering av høringsuttalelser og endelig forskrift", NVE-Dokument 7/2011, www.nve.no/ams

[3] "Bruksområder for AMS-data registrert hos kunder og i MV/LV nettstasjoner", H. Sæle, D. E. Nordgård, J. Heggset, SINTEF Energi AS, TR A7095, April 2011, www.sintef.no/m-ams

[4] "Vurdering av kommunikasjonsalternativer for informasjonsutveksling med AMS mellom smarte hus og et smart kraftnett", Christian Haugen, Master i kommunikasjonsteknologi, NTNU, Juni 2010, www.sintef.no/m-ams

[5] "Kravspesifikasjon fullskala utbygging av Avanserte Måle- og Styringssystemer (AMS) (toveiskommunikasjon)", I. Graabak, H. Sæle, SINTEF Energi AS, TR A7138, September 2011

[6] "Avanserte måle- og styringssystemer. Høringsdokument februar 2011", NVE-Dokument 1/2011, www.nve.no/ams

[7] "FOR 1999-03-11 nr 301: Forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester", www.lovdata.no

[8] "FOR 2011-03-10 nr 263: Forskrift om krav til kompetanse mv. hos anleggs- og områdekonsesjonærer (kompetanseforskriften)", www.lovdata.no

[9] "Felles IKT-løsninger i det norske kraftmarkedet", Thema, Devoteam DaVinci, 04.04.2011, www.nve.no/ams

[10] NS 7799:2003 Norsk standard for informasjonssikkerhet – norsk oversettelse av ISO/IEC 27001:2005: Information security management systems

[11] "FOR 2002-12-16 nr. 1606: Forskrift om beredskap i kraftforsyningen", www.lovdata.no

[12] Basic Reference Model, ISO/IEC 7498-1:1994

[13] Safety and Automation Systems (SAS), NORSOK Standard I-002, Rev 2, 2001

[14] Standard for Information Technology, ISO/IEC 12207:1995

[15] The Common Criteria for Information Technology Security Evaluation (CC), www.commoncriteriaportal.org

Teknologi for et bedre samfunn

www.sintef.no