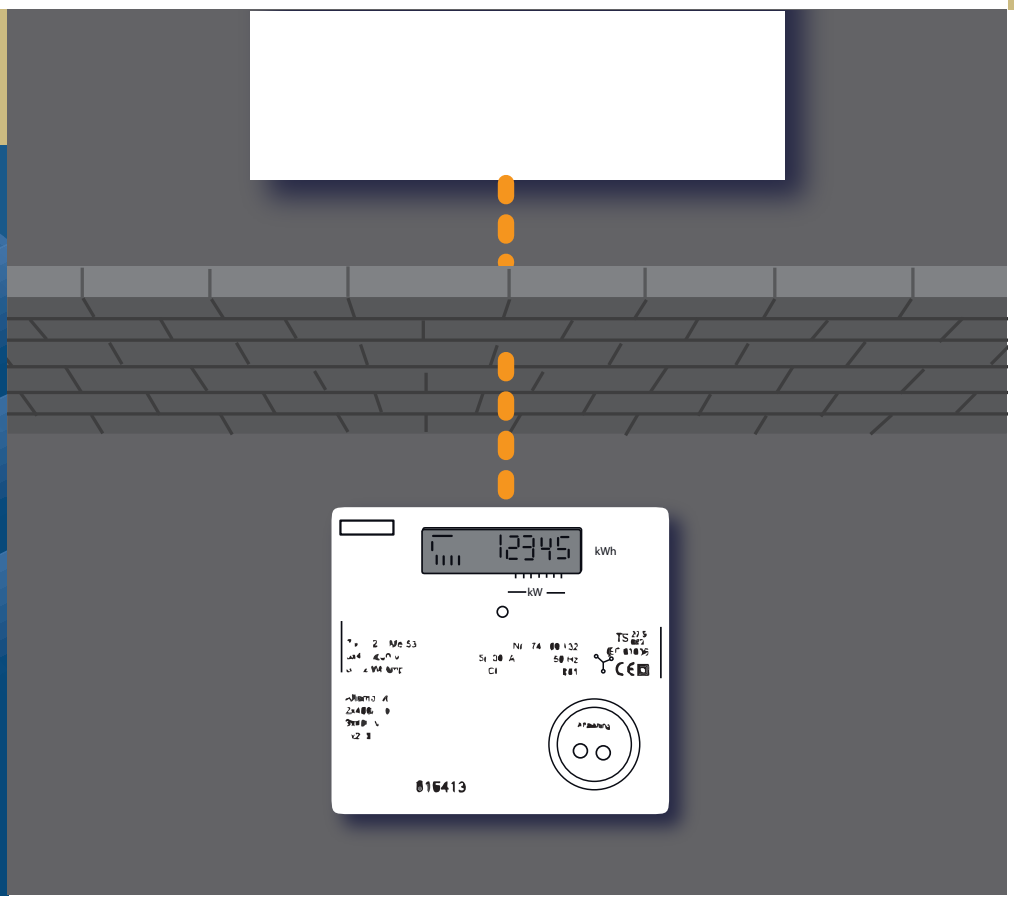
Veileder til sikkerhet i avanserte måle- og styringssystem

Frank Skapalen, NVE
Bjørn Jonassen, Deloitte

7
2012



VEILEDER

Veileder til sikkerhet i avanserte måle- og styringssystem

Norges vassdrags- og energidirektorat
2012

Veileder nr 7/2012

Utgitt av: Norges vassdrags- og energidirektorat

Redaktør:

Forfattere: Frank Skapalen, Bjørn Jonassen (Deloitte)

Trykk: NVEs hustrykkeri
Opplag: Kun på nett
Forsidefoto:
ISSN 1501-0678

Sammendrag: Dette dokumentet er en veileder for hvordan kravene i § 4-2 g (om sikkerhet i AMS) i Forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester kan oppfylles.

Emneord: Avanserte måle- og styringssystem, informasjonssikkerhet, IKT-sikkerhet.

Norges vassdrags- og energidirektorat
Middelthunsgate 29
Postboks 5091 Majorstua
0301 OSLO

Telefon: 22 95 95 95
Telefaks: 22 95 90 00
Internett: www.nve.no

September 2012

Innhold

Forord

Nettselskapene i Norge er nå i ferd med å prosjektere, bestille og etter hvert starte utrullingen av nye, avanserte strømmålere (AMS) til alle målepunktene i Norge. Utrullingen skal være sluttført innen 1.1.2017.

AMS-løsningene vil bli et komplekst system med en omfattende infrastruktur for overføring av kunde- og målerdata, styring av hovedterminaler, styring av forbruk mm. Infrastrukturen vil ha knutepunkter for overføring til databaser som igjen skal håndtere og behandle målerdata.

SINTEF har på oppdrag av NVE utarbeidet en overordnet risikovurdering av AMS. I utredningen pekes det på en rekke kritiske risikoer – både for selve AMS-løsningen og i gitte tilfeller også for kraftforsyningen

Veilederen er delvis basert på utredningen fra SINTEF, og er i hovedsak veiledende for hvordan selskapene skal kunne oppfylle kravet i § 4-2 g) i "Forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester."

Veilederen er utarbeidet gjennom et samarbeid mellom seksjon for kraftmarked og seksjon for beredskap i NVE. Deloitte har bidratt med fagkompetanse.

Oslo, september 2012

Marit L. Fondal
Avdelingsdirektør

seksjonssjef
seksjon for beredskap

seksjonssjef
seksjon for kraftmarked

1 Innledning

Funksjon og drift av AMS er regulert av *FOR 1999.03.11 nr 0301:(OED) Forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester (MAF).* Hovedhensikten med AMS er å opprette direkte kommunikasjon mellom kundenes strømmålere og nettselskapet for oversendelse av målerdata for automatisk avlesning av målerne. Nettselskapene får ansvaret for å innføre og drifte AMS-systemet i sitt forsyningsområde.

I tillegg til egne tjenester skal nettselskapene legge til rette for at ulike tilleggstjenester kan tilknyttes AMS i fremtiden. For å sikre dette foreslår NVE at nettselskapet skal gi andre tjenesteleverandører mulighet til å kommunisere over AMS, og NVE vil kreve at kommunikasjonsløsningene for AMS baseres på standard kommunikasjonsprotokoller, som for eksempel IP.

Forskriften pålegger nettselskapene å sikre sine system, inkludert kommunikasjonsløsninger, mot uautorisert tilgang. Dette gjelder også i forhold til kravet om å gjøre kommunikasjonsløsningen tilgjengelig for tredjepart. Kravet til sikkerhet er overordnet og gir ingen detaljerte føringer utover at selskapene har ansvaret for sikkerheten.

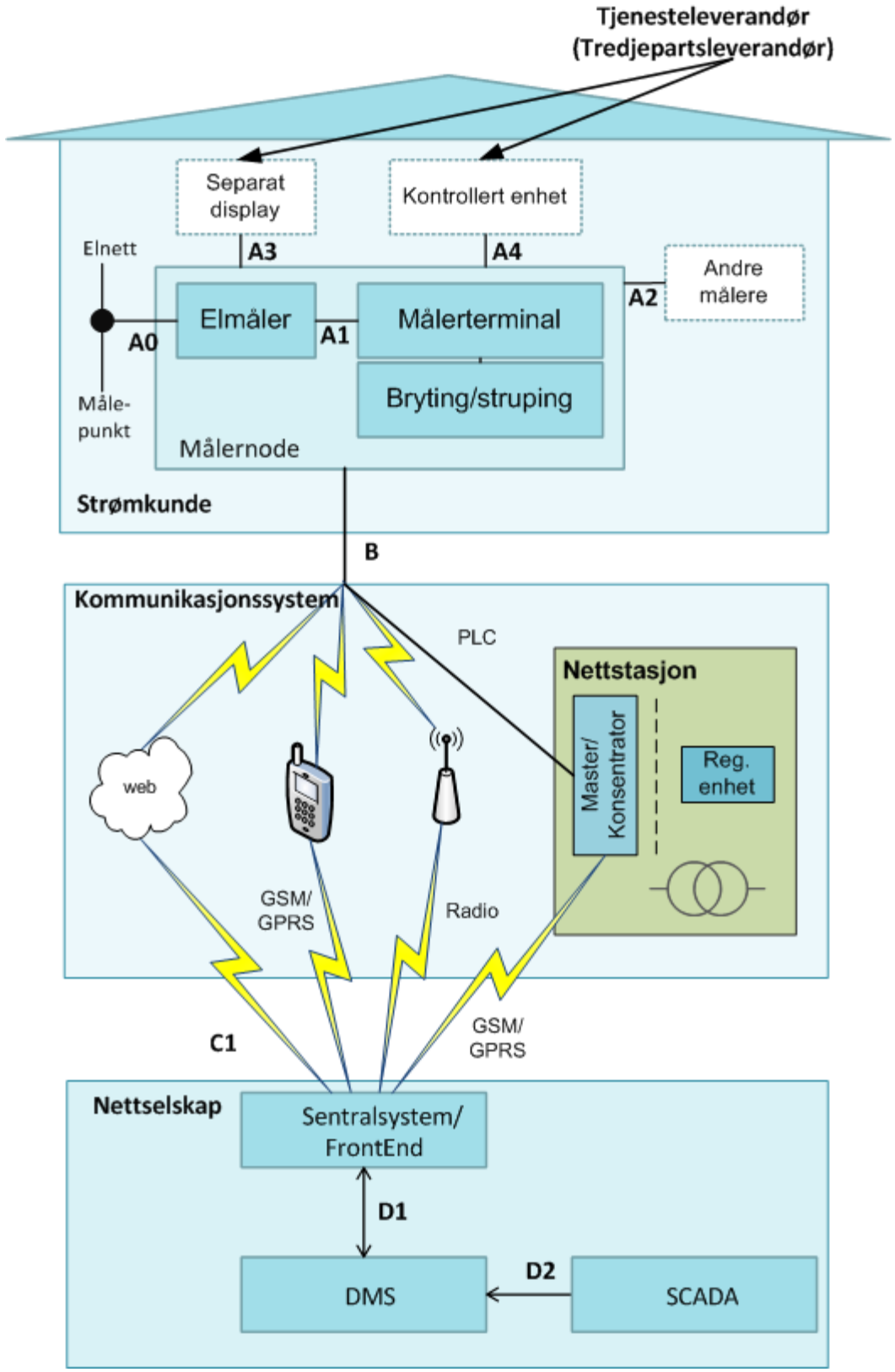
Denne veilederen gir noen eksempler på sikkerhetstiltak som kan implementeres i AMS-løsninger for å kunne bidra til oppfyllelse av forskriftens krav.

2 Veilederens omfang

Veiledningen omfatter innsamlingssystemet (ofte betegnet som ”måleverdikjeden”) – fra målepunktet hos kunden til sentralsystemet hos nettselskap, samt kommunikasjonssystemet.

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.

Figuren under er en skisse basert på hvilke systemer som trenger AMS-data i forbindelse med driften av AMS, og er således ikke en detaljert beskrivelse av IT-strukturen for AMS.



Figur 1 Skisse til AMS-infrastruktur. SINTEF, 2012

2.1 Generelt om ansvaret for informasjonssikkerheten i AMS

Nettselskapet er ansvarlig for informasjonssikkerheten for hele AMS løsningen, også for de delene som eventuelt settes ut til tjenesteleverandør. Hvordan ansvarsforholdet skal være i forbindelse med eventuell felles IKT-løsninger, vil bli behandlet i et eget prosjekt.

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

2.2 Bryte- og strupefunksjonalitet

En viktig funksjon nettselskapene skal implementere er en bryte- og strupefunksjon. En bryterfunksjon innebærer at nettselskapet kan styre lastuttaket i det enkelte målepunkt. Det har vært knyttet stor usikkerhet til kostnader og risiko rundt denne funksjonen – spesielt dersom den brukes til masseutkobling i knapphetssituasjoner.

Sikkerhetsmessig er bryte- og strupefunksjonen vurdert som kritisk. I SINTEF-analysen ble det identifisert mange potensielle risikoer knyttet til flere ulike scenarioer. De største konsekvensene vil man få dersom uautoriserte får tilgang til bryte- og strupefunksjonen, og foretar masseutkobling av målepunkter. En uautorisert masseutkobling vil etter NVEs mening kunne sidestilles med uautorisert tilgang til netteselskapenes driftskontrollsystem.

De sikkerhetsmessige utfordringene ved å implementere et system for bryterfunksjonalitet med muligheter for masseutkobling vil svært store for nettselskapene. NVE er derfor av den oppfatningen at nytten av en slik funksjonalitet ikke er stor nok til å forsvare et eksplisitt krav om å innføre slik funksjonalitet, og vil som minimum kun kreve én-til-én kobling ved benyttelse av bryte- og strupefunksjonalitet. Det vil likevel være opp til selskapene selv å vurdere hvorvidt de ønsker å etablere funksjonalitet som tillater masseutkoblinger.

I veilederen er det da også tatt høyde for at man velger bryte - og strupefunksjonalitet med muligheter for masseutkoblinger.

2.3 Felles IKT-tjenester

Statnett har på oppdrag fra NVE utredet behovet for felles IKT løsninger for å sikre et effektivt sluttbrukermarked for kraft.

I rapporten anbefales det at det etableres en datahub som skal fungere som markedets kontaktpunkt mot nettselskapene i forhold til måleverdier, leverandørbytter, innflytting, utflytting, oppsigelse samt autorisasjon og informasjonsutveksling i forbindelse med AMS tilleggstjenester.

Etablering av en datahub vil ikke ha innvirkning på hvordan selskapene implementerer sikkerhet i sine AMS-løsninger da de fremdeles vil ha ansvaret for sine lokale løsninger. Derfor er det i denne veileder ikke tatt hensyn til en eventuell utbygging av felles IKT-løsninger, men forutsetter at det vil bli etablert egne sikkerhetskrav til de felles løsningene som ivaretar for eksempel beskyttelse av kundedata.

3 Forskriftenes krav til sikkerhet i AMS

3.1 Måle- og avregningsforskriften

Sikkerheten i AMS er ikke detaljregulert i noen av NVEs forskrifter. I MAF pålegges nettselskapene å sikre sine system, inkludert kommunikasjonsløsninger, mot uautorisert tilgang (MAF§ 4-2 g)). Dette gjelder også i forhold til kravet om å gjøre kommunikasjonsløsningen tilgjengelig for tredjepart. Kravet til sikkerhet er overordnet og gir ingen detaljerte føringer utover at selskapene har ansvaret for sikkerheten.

3.2 Beredskapsforskriften

I rapporten som SINTEF utarbeidet på oppdrag fra NVE pekes det på forhold i AMS som kan ha innvirkning på forsyningssikkerheten. I rapporten anbefales det at beredskapsforskriften bør gjelde for AMS, fordi risikovurderingen som er gjort i rapporten viser at uønskede hendelser med AMS kan få konsekvenser for kraftforsyningen.

Fra 1. januar 2013 vil dagens ”Forskrift om beredskap i kraftforsyningen” erstattes av ”Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen”. I den nye forskriften er det derfor tatt med en bestemmelse om sikring av AMS dersom denne blir knyttet sammen med selskapets driftskontrollsystem.

NVE vil i fremtiden vurdere om det er nødvendig å forskriftsfeste mer detaljerte krav til sikkerhet i AMS.

4 Bruk av veilederen

Nedenfor listes alle kontrollmålene for de ulike sikkerhetsområdene, eksempler, hensikt og også supplerende veiledning om nødvendig.

4.1 Hvordan kontrollmålene skal brukes

Kontrollmålene omfattes av flere sikkerhetsområder. For hvert av disse områdene er det gitt ett kontrollmål, samt eksempler på hvordan målkontrollen kan oppnås.

Kontrollmålene er et målbart ”krav” til sikkerhetsområdet. Til kontrollmålet er det gitt eksempler på tiltak, prosedyrer etc for å oppnå kontrollmålet. Disse er kun ment som eksempler og skal gi en pekepinn på hvilke tiltak som bør iverksettes for å bidra til å oppnå kontrollmålet. Nettselskapet står fritt til å velge andre tiltak.

Til slutt er det gitt en begrunnelse, eller hensikt med kontrollmålet, og også supplerende veiledning der det er funnet hensiktsmessig.

Nettselskapet må selv vurdere hvilke sikkerhetsområder som skal prioriteres, gitt AMS-løsningens størrelse, kompleksitet, teknologiske valg etc.

Nettselskapet må kunne begrunne om enkelte sikkerhetsområde utelates. Det er derfor lagt ved (vedlegg 1) en tabellarisk fremstilling av kontrollmålene med eksemplene der selskapet selv kan begrunne hvorfor/hvorfor ikke et kontrollmål er valgt.

5 Sikkerhetsområder og kontrollmål

A. Krav til nettselskapet i henhold til forskrift

A.1 Robust sikkerhetsfunksjonalitet

Kontrollmål

a) Sikkerhetsfunksjonalitet i AMS-løsningen skal ikke påvirkes ved feil i AMS eller feil konfigurasjon av annen funksjonalitet.

b) Funksjonalitet som er deaktivert eller ikke brukt skal ikke påvirke sikkerheten i løsningen.

c) Konfigurasjon og oppsett for kritiske kommandoer, målerdata og annen informasjon i AMS løsningen skal være basert på risiko.

Eksempler for å oppnå kontrollmål

- Utstrakt testing av funksjonalitet i et begrenset testmiljø.
- Konkretiser sikkerhetskrav i konkurransegrunnlag og kontrakt med leverandør
- Foreta regelmessig sikkerhetstesting
- Ha prosess og prosedyrer for regelmessig identifikasjon og feilretting av sikkerhetssvakheter
- Kryptering / signering av kommandoer
- Kryptering av sikkerhetsinformasjon
- Overvåking og varsling av unormal bruk eller trafikk

Hensikt

Dersom det oppstår en feil i et system eller i kommunikasjonsløsningen til AMS, så skal dette ikke påvirke informasjonssikkerheten ved at for eksempel kundedata eller annen informasjon blottlegges.

A.2 Sikkerhet i kommunikasjon i AMS-løsningen

Kontrollmål

a) All kommunikasjon mellom måler og sentralsystem og øvrig utstyr i AMS skal foregå på en sikker måte slik at innsyn, avlytting eller manipulering av signaler og informasjon ikke er mulig.

b) Signalene og informasjonen skal krypteres.

Eksempler for å oppnå kontrollmål

- Krypteringsalgoritmer som benyttes for sikker kommunikasjon skal som minimum være FIPS-godkjent (eller ekvivalent).
- Krypteringsløsningen må støtte PKI (Public Key Infrastructure) nøkkel-kryptografi
- Påloggingsinformasjon som krypteringsnøkler, sikkerhetssertifikat etc skal kunne oppdateres sentralt.
- En isolert kompromittering av kryptografiløsning på en enhet skal ikke kunne føre til kompromittering av andre enheter eller systemer i AMS løsningen.
- En isolert kompromittering på en enhet skal ikke kunne føre til en større hendelse.
- Sertifikatnøkler skal lagres kryptert.
- Det er ikke tilstrekkelig å benytte den innebygde kryperingsløsningen i GSM

Supplerende veiledning

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

Krypteringsløsningen som benyttes i GSM (2G) er såpass lett å knekke at det ansees ikke som en sikker løsning alene for å sikre kommunikasjonen i AMS.

Hensikt

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

A.3 Utsetting av utrulling og/eller drift av AMS-løsningen til tredjepart

Kontrollmål

Sikkerheten i AMS skal ikke påvirkes ved at utrulling eller drift av AMS settes ut til ekstern tjenesteleverandør.

Eksempler for å oppnå kontrollmålet

- Nettselskapet må påse at de selv har tilstrekkelig kompetanse til å sette krav til sikkerhet i AMS gjennom kravspesifikasjonen, og også kunne kontrollere at kravene blir etterlevd i driftssituasjonen.
- Nettselskapet må sette målbare krav til leverandørene.
- Kravene må følges opp regelmessig.

- Nettselskapet må ha innsyn og forståelse av sikkerhetstiltakene som etableres og risikoen tjenesteutsettingen medfører.
- Nettselskapet må ha realistisk mulighet til å trekke tilbake avtalen ved avtalebrudd, uakseptabel risiko eller endringer i regulering.
- Tjenesteutsettingen må ikke påvirke risiko for kraftforsyningen negativt.

Hensikt

Denne målkontrollen er basert på kravene i kompetanseforskriftens § 3 som går på både evne til å ivareta nettforvaltningsoppgaver og oppgaver innenfor måling og avregning. En viktig del av nettforvaltning er sikkerhet og beredskap.

Supplerende veiledning

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

Nettselskapet skal også kunne gis mulighet til å avtalefeste NVEs rett til revisjon av leverandøren. Revisjon av leverandøren skal kunne gjennomføres uten hinder.

B. Overordnet sikkerhetsarbeid rundt AMS

B.1. Etablering og oppfølging av sikkerhetskrav

Kontrollmål

a) Nettselskapets ledelse skal utarbeide og godkjenne overordnede sikkerhetskrav til AMS-løsningen. Disse skal dekke alle prosesser og systemer som påvirker AMS og eventuelt kraftforsyningen. Kravene skal være målbare og dokumenteres.

b) Nettselskapet ledelse skal etablere et system for å følge opp og forbedre sikkerhetskravene for AMS.

Eksempler for å oppnå kontrollmålet

- Nettselskapets ledelse dokumenterer sitt engasjement for å få utarbeidet sikkerhetskravene og oppfølgingen av dem.
- Nettselskapet skal sørge for å ha nødvendig tilgang på kompetanse på eget sikkerhetsarbeid knyttet til AMS.
- Nettselskapet skal utpeke en informasjonssikkerhetsansvarlig for AMS. Denne personen skal gis nødvendig myndighet, ansvar og opplæring samt få avsatt tilstrekkelige tid og ressurser slik at funksjonen kan ivaretas på en tilfredsstillende måte.
- Det må gjennomføres tilstrekkelig opplæring på informasjonssikkerhet for alle nettselskapets egne og innleide ressurser.

- Kravene skal baseres på risiko- og sårbarhetsanalyse og være tilstrekkelige for å oppnå et akseptabelt risikonivå.
- Sikkerhetskravene skal gjennomgås minimum årlig for å klarlegge om kravene er hensiktsmessig i forhold til nettselskapets behov, etterlevelse av forskriftskrav og om kravene er tilstrekkelige.

Hensikt

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

Supplerende veiledning

Dette kontrollmålet ligger tett opptil kravet om overordnede sikkerhetskrav i henhold til BfK og organiseringen knyttet til beskyttelse av driftskontrollsystem.

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

B.2 Risiko- og sårbarhetsanalyse

Kontrollmål

Det skal gjennomføres risiko- og sårbarhetsanalyse av AMS med den hensikt å identifisere risiko forbundet med drift og sikkerhet av AMS.

Eksempler for å oppnå kontrollmålet

- I analysen skal alle forhold vurderes som for eksempel kan hindre korrekt avregning, hindre tilfredsstillende funksjonalitet, sette informasjonssikkerheten i fare eller hindre funksjonalitet i kraftforsyningen.
- Det skal fastsettes akseptabelt risikonivå som risikoene i risiko- og sårbarhetsanalysen skal vurderes mot. Der hvor risikonivå er høyere enn akseptabelt risiko skal tiltak etableres slik at akseptabelt risikonivå oppnås. Nivå på sikkerhetstiltak skal være tilpasset risiko.
- Dersom større tiltak er nødvendig for å oppnå akseptabelt risikonivå, skal tilstrekkelige midlertidige kompenserende tiltak iverksettes inntil permanente tiltak er på plass.
- Risiko- og sårbarhetsanalysene skal utføres og gjennomgås årlig og ved endringer i løsninger eller i trusselsituasjon som påvirker drift og sikkerhet i AMS.

Hensikt

Risiko- og sårbarhetsanalysene skal gi nettselskapet styringsgrunnlag for å etablere hensiktsmessige sikkerhetstiltak og for å verifisere at risikoen er akseptabel.

ROS-analysen skal ha som hensikt å identifisere årsaker til at uønskede hendelser i AMS-løsningen, sannsynligheten det er for at hendelsen inntreffer, samt hvilke konsekvenser hendelsen kan utløse. Videre skal analysen vurdere sannsynlighets- og /eller konsekvensreduserende tiltak.

Supplerende veiledning

Det er gjennomført flere analyser og risikovurderinger og veiledning om kan bidra til å få på plass en metodikk for gjennomføring av ROS-analyser;

- Overordnet risiko- og sårbarhetsanalyse for innføringen av AMS, Energi Norge/Proactima 2012.

- Risikovurdering av AMS, SINTEF 2012

- Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen, NVE Veileder nr 2 2010)

B.3 Oppdatert dokumentasjon av AMS-løsningen

Kontrollmål

Det skal til enhver tid foreligge fullstendig og oppdatert dokumentasjon av AMS-løsningens komponenter og konfigurasjoner.

Eksempler for å oppnå kontrollmålet

- Alle sikkerhetsrutiner og sikkerhetstiltak skal være dokumentert.
- Dokumentasjonen bør være systematisert og sporbar, og det skal klart fremkomme gyldighet, eierskap og endringshistorikk.
- Dokumentasjonen skal være beskrevet og komplett på en slik måte at enhver (både internt og evt leverandør) effektivt kan utføre vedlikehold eller feilretting.
- Dokumentasjonen skal oppbevares separat fra AMS-løsningen
- Utførte kontrolltiltak skal være dokumenterte og etterprøvbare.

Hensikt

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

Supplerende veiledning

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

B.4 Sikkerhetsavtaler

Kontrollmål

Nettselskapet skal inngå sikkerhetsavtaler med alle leverandører eller enkeltpersoner som ikke er ansatt i nettselskapet dersom de skal utføre enhver form for arbeid på kritiske løsninger eller komponenter i AMS-løsningen.

Eksempler for å oppnå kontrollmålet

- Underskrevne avtaler.

Hensikt

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

C. Kontroll med tilgang til system og utstyr

C.1 Tilgangskontroll - system

Kontrollmål

Nettselskapet skal ha prosedyrer og kriterier for tildeling, endring, sletting og verifikasjon av korrekt tilgang til kundedata samt AMS-funksjonalitet (eks. bryterfunksjonalitet).

Eksempler for å oppnå kontrollmålet

- Ha prosedyrer som sikrer at kun autoriserte personer kan få tilgang til, endre, slette eller utlevere målerdata eller annen sensitiv kundeinformasjon. Prosedyrene skal inkludere både intern og ekstern tilgang.
- Nettselskapet skal foreta tilstrekkelig bakgrunnssjekk av personell som skal ha tilgang til å håndtere sensitive systemer og informasjon. Med tilstrekkelig menes for eksempel som minimum vandelsattest (hvis mulig), kredittsjekk og referansesjekk.
- Tilgang skal administreres på basis av forhåndsdefinerte roller og tilgangsnivåer.
- Tilganger skal tildeles, endres, fjernes og revideres basert på tjenestelig behov.
- Ha prosedyrer og tekniske løsninger som skal sikre at kritiske operasjoner ikke kan kunne utføres av én person alene.

- Ha prosedyrer som sikrer at maskinvare som inneholder sensitiv informasjon skal avhendes på en sikker måte.
- Ha tekniske løsninger for å oppdage uautorisert endring i målerdata eller personopplysninger
- Ha tekniske løsninger for å forhindre uautorisert utlevering av målerdata eller personopplysninger
- Ha tekniske løsninger for å loggføre dersom det utføres endringer i allerede registrerte målerdata
- Ha tekniske løsninger for å loggføre dersom målerdata eller annen kundeinformasjon utleveres til autorisert tredjepart.

Hensikt

Systematisk tilgangskontroll er helt nødvendig for å ha kontroll på hvem som har tilgang, og hva de har tilgang til. Dette gjør det lettere for nettselskapet å avdekke eventuell uautorisert tilgang.

C.2 Identifisering og autorisasjon av enheter

Kontrollmål

Det skal implementeres mekanismer for å autentisere og autorisere enheter i AMS før det opprettes forbindelse mellom enheten og resten av AMS. Ved bruk av WLAN, NAN eller HAN eller GSM bør ekstra sterk autentisering foretas.

Eksempler for å oppnå kontrollmål

- Det skal ikke tillates tilkobling av enheter uten at disse er autorisert og autentisert
- Hver enhet i AMS skal tildeles et unikt sikkerhetssertifikat som kontrolleres før det sendes/mottas data fra enheten.
- Der man ikke får kontrollert eller verifisert enheten, skal enheten nektes tilgang til nettverket.
- Sikkerhetssertifikatet skal benyttes for å autorisere enheter i AMS

Hensikt

AMS utsettes for stor sårbarhet dersom man ikke positivt kan foreta en sikker identifisering av hver enkelt enhet som er tilkoblet AMS. Svært mange av enhetene i AMS vil måtte plasseres på steder der nettselskapet har begrenset kontroll med utstyret. Dette gjelder i særdeleshet måleren og annet utstyr som blir plassert nær kundene. Derfor bør enhetene underlegges strenge sikkerhetskontroller før de kommer i kontakt med AMS-løsningen.

C.3 Identifisering og autorisering av eksternt utstyr

Kontrollmål

Håndholdte enheter (feltutstyr) må være autorisert og skal autentiseres av AMS - løsningen. Bruker skal være autorisert og autentisert.

Eksempler for å oppnå kontrollmål

- Det skal ikke tillates tilkobling av eksternt utstyr uten at disse er autorisert og autentisert
- Hver enkelt enhet skal utstyres med et sikkerhetssertifikat som kontrolleres ved oppkobling mot enheter i AMS.
- Det skal sperres for at eksternt utstyr benyttes til annet enn oppgave mot AMS.
- Autoriseringsprosessene skal være formaliserte i form av instrukser/prosedyrer.
- Det skal være mulig å fjerne/endre autorisering av håndholdte enheter sentralt.

Hensikt

Påkobling av eksternt utstyr kan utgjøre en potensiell stor risiko mot AMS dersom de ikke er underlagt streng autorisasjons- og brukskontroll.

C.4 Kontroll med integriteten til programvare

Kontrollmål

Det skal etableres et system for overvåking og avdekking av uautoriserte endringer av programvare og informasjon.

Eksempler for å oppnå kontrollmålet

- Utføre integritetsskanning av AMS-løsningen
- Integriteten på programvare må sjekkes ved oppstart, oppdatering og eksekvering.
- Enheten skal være sikret fysisk og logisk mot uautorisert oppdatering og endring av programvare
- Endringer av programvare skal være testet og godkjent
- Implementering av automatiske verktøy som varsler ved integritetsavvik.
- Enhetene i AMS skal kunne verifisere at alle spørringer og kommandoer er gyldige, har rett format og er foretatt fra autentisert og autorisert kilde.
- Sikkerhetssertifikatet skal benyttes for verifikasjon av kommandoeksekvering

Hensikt

Systemkomponenter som har gjennomgått uventede eller uautoriserte endringer har trolig blitt kompromittert eller korrupte. Slike hendelser må oppdages, rapporteres, vurderes og eventuelt korrigeres av kompetent personell.

Supplerende veiledning

Man må påse at bruken av automatiske verktøy for integritetskontroll må ikke ha negativ innvirkning på AMS-løsningens operative funksjon. Dette kontrollmålet kan ses i sammenheng med kontrollmål for sikker kommunikasjon.

C.5 Elektronisk beskyttelse mot ondsinnet programvare og inntrengning

Kontrollmål

Det skal etableres et system for overvåking og beskyttelse av programvaren i AMS med hensikten å oppdage og stanse ondsinnet programvare.

Eksempler for å oppnå kontrollmål

- Virusbeskyttelse eller tilsvarende
- Beskyttelse mot målrettede og tilfeldige angrep
- Implementering av ”Intrusion detection system” eller ”Intrusion protection system”
- Brannmurbeskyttelse
- Logisk eller fysisk segmentering/soneinndeling av ulike deler av nettverk etc.

Hensikt

Ondsinnet programvare eller inntrengning kan forstyrre eller ødelegge AMS i den grad at informasjonssikkerheten blir kompromittert.

C.6 Oppbevaring av sikkerhetssertifikater og krypteringsnøkler

Kontrollmål

a) Nettselskapet skal utarbeide retningslinjer for sikker oppbevaring av sikkerhetssertifikater og krypteringsnøkler som benyttes i AMS.

b) Enheten skal lagre påloggingsinformasjon, sikkerhetssertifikater og annen sikkerhetsinformasjon sikkert.

Eksempler på aktivitet for å oppnå kontrollmål

Ingen

Hensikt

Ved kompromittering av krypteringsnøkler og sikkerhetssertifikater utsettes AMS-løsningen for stor risiko.

D. Overvåking og håndtering av hendelser

D.1 Kontroll med sårbarheter i programvare

Kontrollmål

a) Nettselskapet skal ha prosesser for å fange opp eventuelle kjente programvaremessige sårbarheter i sitt AMS-miljø.

b) Dersom man blir kjent eller varslet om sårbarheter, skal disse evalueres og eventuelt håndteres umiddelbart.

Eksempler for å oppnå kontrollmål

- Avtaler om varsling fra leverandør(ene) eller andre relevante samarbeidspartnere dersom det oppdages sårbarheter i sine system.
- Regelmessig sårbarhetsscanning av enheter og infrastruktur.
- Interne prosedyrer for hvordan slik informasjon skal behandles og sårbarheter håndteres.
- Prosedyrer som sørger for at sikkerhetsoppdateringer blir utført så raskt som praktisk mulig på en sikker måte.

Hensikt

Dersom sårbarheter som ikke blir vurdert eller håndtert, kan systemet utsettes for inntrenging gjennom sårbarheten.

Supplerende veiledning

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

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

D.2 Logging og overvåking

Kontrollmål

Nettselskapet skal ha satt opp løsning og rutiner for sikkerhetslogging i den totale AMS-løsningen.

Eksempler på aktivitet for å oppnå kontrollmål

- Alle nettverkskomponenter, AMS enheter, operativsystemer, databaser, applikasjoner med videre skal settes opp med rett loggnivå for sikkerhet.
- Endringer, feil, normal og unormal aktivitet og sikkerhetshendelser skal logges.
- Loggene skal sikres og overvåkes sentralt for å fange opp eventuelle uønskede sikkerhetshendelser.
- Logger skal kunne lagres lokalt dersom kommunikasjon mot sentralsystem ikke er tilgjengelig. Lokal logg må være av tilstrekkelig omfang stor for å kunne håndtere forventet maksimal nedetid på kommunikasjonsløsning.
- Lokale og sentrale logger skal sikres mot uautoriserte endringer.

Hensikten med kontrollmålet

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

D.3 Avviks- og hendelseshåndtering

Kontrollmål

Nettselskapet skal etablere en dokumentert prosess for avviks- og hendelsesregistrering og -håndtering.

Eksempler for å oppnå kontrollmål

- Alle avvik skal følges opp.
- Prosessen skal inneholde retningslinjer for hvordan avvik skal behandles. De kan for eksempel være;
    - klassifisering av hendelser,
    - roller og ansvar
    - plan for håndtering og avklaring
    - eskalering
    - terskel for varsling til NVE
- Avvik som det ikke gjøres noe med, skal godkjennes
- Alle avvik fra egne og eksterne krav skal dokumenteres.
- Alle avvik som ikke er lukket skal følges opp til de lukkes.

Hensikt

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

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

D.4 Katastrofehåndtering og –øvelser

Kontrollmål

a) Nettselskapet skal ha beredskapsplaner og forberedte løsninger for å sikre beredskap, kontinuitet og evne til å håndtere katastrofer knyttet til informasjonssikkerhet og AMS.

b) Det skal jevnlig gjennomføres øvelser for å håndtere omfattende sikkerhetshendelser og -katastrofer.

Eksempler for å oppnå kontrollmål

- Beredskapsplanene og løsningene skal evalueres regelmessig og i forbindelse med evaluering av øvelser.
- Planene for og resultatene fra øvelsene skal dokumenteres. Avdekkes gap eller mangler etter øvelsene, skal det tas hensyn til dette i evalueringen eller oppdateringen av beredskapsplaner.
- Øvelser bør inkludere feilsituasjoner, sikkerhetshendelser i kombinasjon med ekstremvær eller andre relevante hendelser.
- Øvelsene bør inneholde elementer av gjenoppretting etter katastrofer.
- Som et minimum skal det gjennomføres årlige øvelser.

Hensikt

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

D.5 Sikkerhetskopier og gjenoppretting

Kontrollmål

a) Det skal foreligge sikkerhetskopier av all kritisk programvare, konfigurasjoner, dokumentasjon av alle relevante komponenter i AMS-løsningen.

b) Det ska foretas jevnlig sikkerhetskopiering av måledatabasen.

c) Sikkerhetskopiene skal lagres på et sikkert sted et annet fysisk sted enn der.

Eksempler for å oppnå kontrollmål

- Nettselskapet skal med jevne mellomrom teste at gjenoppretting av sikkerhetskopiene fungerer etter hensikten.

Hensikt

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

E. Endrings- og versjonskontroll

E.1 Kontroll med endringer i AMS

Kontrollmål

Nettselskapet skal dokumentere prosedyrer for å planlegge og utføre endringer i AMS-miljøet.

Eksempler for å oppnå kontrollmål

- Alle endringer i AMS-løsningen skal dokumenteres.
- Alle endringer skal testes og godkjennes før de rulles ut.
- Alle endringer skal vurderes i forkant om endringen kan medføre risiko for kritiske AMS-funksjoner eller medføre konsekvenser for kraftforsyningen.
- All ny programvare som innføres i AMS løsningen skal sikres slik at integritet ivaretas.
- Enheter skal kunne verifisere at oppdatering av firmware er autorisert og at firmwaren er umodifisert og godkjent før den oppdateres.

Hensikt

Kontroll med endringer i AMS-løsningen er avgjørende for å ivareta krav om robust sikkerhetsfunksjonalitet og AMS.løsningern fungerer etter sin hensikt også etter endringer.

E.2 Oversikt over versjoner i program- og maskinvare

Kontrollmål

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

Eksempler for å oppnå kontrollmål

- Etablere en form for sentral liste med oversikt over maskinvare, versjoner av programvare som disse benyttes etc.
- Alle endringer i konfigurasjoner og programvare skal logges.
- Fast prosedyre og klare ansvarsforhold for oppdatering av listen ved endringer.
- Automatiske systemer som gir oversikt over programvareversjoner og som kan rulle ut oppdateringer.

Hensikt

AMS vil for mange selskaper bli en stor og kompleks løsning med mange komponenter. Oversikt over programvare og maskinvare er derfor viktig for å forebygge mot unødige sårbarheter som kan utnyttes.

F. Fjerntilgang til AMS-løsningen

F.1 Fjerntilgang til AMS fra tredjepart eller leverandør

Kontrollmål

Det skal etableres prosedyrer for godkjenning, administrering og overvåking av eksterne tilkoblinger for vedlikehold og diagnostiske aktiviteter på alle komponenter i AMI-systemet.

Eksempler for å oppnå kontrollmål

- Det skal ikke opprettes tilkobling til tredjepart eller leverandør uten eksplisitt avtale med selskapet.
- Tredjepart må forpliktes til å etterleve relevante sikkerhetskrav.
- Tredjepart må benytte en sikker løsning for fjerntilgang.
- Fjerntilgang skal kun tillates fra sikre lokasjoner som ikke medfører økt risiko.
- Når ekstern vedlikehold er fullført, skal det fra nettselskapet eller fra AMS-komponenten avslutte alle økter og eksterne tilkoblinger som er opprettet.

Hensikt

I de tilfeller selskaper ønsker å benytte en tredjepart eller leverandør til å bistå med systemvedlikehold, oppgradering av programvare, feilretting eller liknende må dette beskyttes mot uautoriserte tilgang ellers utsettes AMS-løsningen for store sårbarheter og trusler.

G. Fysisk beskyttelse av AMS-løsningen

G.1 Beskyttelse mot fysisk uautorisert tilgang til AMS-utstyr

Kontrollmål

a) Alle rom som inneholder utstyr som er kritisk for AMS skal være egen adgangskontrollert sone.

b) Komponenter i AMS utenfor adgangskontrollerte soner skal beskyttes mot uautorisert fysisk tilgang.

c) Alle forsøk på å få uautorisert tilgang til utstyr i AMS-løsningen eller rom med kritisk AMS-utstyr skal oppdages straks.

Eksempler på aktivitet for å oppnå kontrollmål

- Ved forsøk på uautorisert fysisk adgang skal det sendes et varsel til nettselskapet. Varselet skal logges og inneholde tidspunkt for utløsning av varselet.
- Det skal kunne bevises dersom det har blitt utført uautorisert tilgang, for eksempel ved at det etterlates fysiske merker eller andre typer spor dersom noen bryter opp enheten.
- Kommunikasjonsinstallasjoner og - skap skal beskyttes mot uautorisert fysisk adgang. Ved forsøk på og uautorisert adgang skal varsel sendes til nettselskapet. Nettselskapet skal undersøke og iverksette aktiviteter tidsriktig.
- Varsel om uautorisert fysisk adgang skal følges opp av nettselskapet.

Hensikt

Ved å få fysisk tilgang til komponentene i AMS, spesielt de som er plassert utenfor nettselskapets kontrollerte område, kan man få elektronisk tilgang til AMS og systemene som driver dette.

H. Bryte- og strupefunksjonalitet

H.1 Beskyttelse av bryte- og strupefunksjonalitet

Kontrollmål

System og nettverk som benyttes til styring av bryterfunksjonalitet skal sikres særskilt mot forsøk på uautorisert utførelse av bryte- og strupefunksjonalitet.

Eksempler for å oppnå kontrollmål

- Bryte- og strupefunksjonalitet er kun tillatt utført av nettselskapet selv.

- Det skal utarbeides særskilte prosedyrer for utførelse av denne funksjonen.
- Kun særskilt autoriserte personer skal kunne få tilgang til- og adgang til å utøve strupe- og bryterfunksjonalitet.
- Det skal ikke være mulig for én person alene å autorisere samt utføre bryte- eller strupefunksjonen.
- Det skal etableres automatiske kontroller som vil redusere mulighet for å bryte eller strupe et stort antall punkter som følge av feil eller målrettede angrep.
- Den fysiske lokasjonen til systemene for strupe- og bryterfunksjonalitet skal være en egen adgangskontrollert sone.

Hensikt

Bryte- og strupefunksjonen er kritisk og inngår i mange uønskede hendelser som potensielt kan få store konsekvenser for nettselskapet. For utdypende risikovurdering, se ”Risikovurdering av AMS”, SINTEF 2012.

Supplerende veiledning

Bryte- og strupefunksjonalitet gis også særskilt oppmerksomhet i ny, revidert beredskapsforskrift. Der vil det inngå en bestemmelse om særskilt sikring av funksjonaliteten dersom funksjonen for bryte- og struping av måleren integreres med nettselskapets driftskontrollsystem.

I. Elektromagnetisk interferens (EMI)

I.1 Beskyttelse mot EMI

Kontrollmål

Alle komponentene i AMS-løsningen skal være tilstrekkelig skjermet mot elektromagnetisk interferens (EMI).

Eksempler på aktivitet for å oppnå kontrollmål

- Nettselskapet må vurdere i hvilken grad EMI vil være tilstede i de miljøene komponentene skal utplasseres og sørge for tilstrekkelig beskyttelse.
- Nettselskapet må forsikre seg om at de aktuelle komponentene er testet slik at de ikke påvirker andre komponenter både i og utenfor AMS.
- Særskilt vurdering bør foretas for komponenter som skal plasseres i nærheten av elkraftteknisk utstyr som for eksempel i nettstasjoner.
- Komponentene bør oppfylle kravene til elektromagnetisk kompatibilitet i henhold til for eksempel CISPR, IEC, ISO eller EN-standardene.

Hensikt

EMI kan påvirke og også stanse funksjonalitet i elektriske kretser. Mange komponenter i AMS vil sannsynligvis utplasseres i miljøer som allerede har mye elektromagnetisk stråling i form av mobilsignaler, trådløse rutere, radiosignaler etc.

I enkelte tilfeller kan måleren eller andre komponenter som benyttes i AMS også selv være en kilde til EMI (for eksempel ved bruk av GSM eller annen trådløs overføring av data).

Vedlegg 1: Tabell over kontrollmålene

Tabell over kontrollene.

*) Sett J (ja) eller N(nei) for om selskapet har implementert målkontrollen. Egne kommentarer kan for eksempel være begrunnelse for hvorfor/hvorfor ikke kontrollen har blitt implementert.

Nr	Sikkerhetsområde/kontroller	(J/N*)	Begrunnelse for ekskludering	Beskrivelse av hvordan kontrollen er implementert
A. Krav til nettselskapet i henhold til forskrift omkring sikkerhet i AMS				
A.1	a) Sikkerhetsfunksjonalitet i AMS-løsningen skal ikke påvirkes ved feil i AMS eller feil konfigurasjon av annen funksjonalitet. b) Funksjonalitet som er deaktivert eller ikke brukt skal ikke påvirke sikkerheten i løsningen. c) Konfigurasjon og oppsett for kritiske kommandoer, målerdata og annen informasjon i AMS løsningen skal være basert på risiko.			
A.2	a) All kommunikasjon mellom måler og sentralsystem og øvrig utstyr i AMS skal foregå på en sikker måte slik at innsyn, avlytting eller manipulering av signaler og informasjon ikke er mulig. b) Signalene og informasjonen skal krypteres.			

Nr	Sikkerhetsområde/kontroller	(J/N*)	Begrunnelse for ekskludering	Beskrivelse av hvordan kontrollen er implementert
A.3	Sikkerheten i AMS skal ikke påvirkes ved at utrulling eller drift av AMS settes ut til ekstern tjenesteleverandør.			
B Overordnet sikkerhetsarbeid rundt AMS				
B.1	a) Nettselskapets ledelse skal utarbeide og godkjenne overordnede sikkerhetskrav til AMS-løsningen. Disse skal dekke alle prosesser og systemer som påvirker AMS og eventuelt kraftforsyningen. Kravene skal være målbare og dokumenteres. b) Nettselskapet ledelse skal etablere et system for å følge opp og forbedre sikkerhetskravene for AMS.			
B.2	Det skal gjennomføres risiko- og sårbarhetsanalyse av AMS med den hensikt å identifisere risiko forbundet med prosjektering, utrulling, drift og sikkerhet av AMS.			
B.3	Det skal til enhver tid foreligge fullstendig og oppdatert dokumentasjon av AMS-løsningens komponenter og konfigurasjoner.			
B.4	Nettselskapet skal inngå sikkerhetsavtaler med alle leverandører eller enkeltpersoner som ikke er ansatt i nettselskapet dersom de skal utføre enhver form for arbeid på kritiske løsninger eller komponenter i AMS-løsningen.			

Nr	Sikkerhetsområde/kontroller	(J/N*)	Begrunnelse for ekskludering	Beskrivelse av hvordan kontrollen er implementert
C. Kontroll med tilgang til system og utstyr				
C.1	Nettselskapet skal ha prosedyrer og kriterier for tildeling, endring, sletting og verifikasjon av korrekt tilgang til kundedata samt AMS-funksjonalitet (eks. bryterfunksjonalitet).			
C.2	Det skal implementeres mekanismer for å autentisere og autorisere enheter i AMS før det opprettes forbindelse mellom enheten og resten av AMS. Ved bruk av WLAN, NAN eller HAN eller GSM bør ekstra sterk autentisering foretas.			
C.3	Håndholdte enheter (feltutstyr) må være autorisert og skal autentiseres av AMS - løsningen. Bruker skal være autorisert og autentisert.			
C.4	Det skal etableres et system for overvåking og avdekking av uautoriserte endringer av programvare og informasjon.			
C.5	Det skal etableres et system for over-våking og beskyttelse av programvaren i AMS med hensikten å oppdage og stanse ondsinnet programvare.			

Nr	Sikkerhetsområde/kontroller	(J/N*)	Begrunnelse for ekskludering	Beskrivelse av hvordan kontrollen er implementert
C.6	a) Nettselskapet skal utarbeide retningslinjer for sikker oppbevaring av sikkerhets-sertifikater og krypteringsnøkler som benyttes i AMS. b) Enheten skal lagre påloggingsinformasjon, sikkerhetssertifikater og annen sikkerhetsinformasjon sikkert.			
D. Overvåking og håndtering av hendelser				
D.1	a) Nettselskapet skal ha prosesser for å fange opp eventuelle kjente programvaremessige sårbarheter i sitt AMS-miljø. b) Dersom man blir kjent eller varslet om sårbarheter, skal disse evalueres og eventuelt håndteres umiddelbart.			
D.2	Nettselskapet skal ha satt opp løsning og rutiner for sikkerhetslogging i den totale AMS-løsningen			
D.3	Nettselskapet skal etablere en dokumentert prosess for avviks- og hendelsesregistrering og -håndtering.			

Nr	Sikkerhetsområde/kontroller	(J/N*)	Begrunnelse for ekskludering	Beskrivelse av hvordan kontrollen er implementert
D.4	a) Nettselskapet skal ha beredskapsplaner og forberedte løsninger for å sikre beredskap, kontinuitet og evne til å håndtere katastrofer knyttet til informasjonssikkerhet og AMS. b) Det skal jevnlig gjennomføres øvelser for å håndtere omfattende sikkerhetshendelser og -katastrofer.			
D.5	a) Det skal foreligge sikkerhetskopier av all kritisk programvare, konfigurasjoner, dokumentasjon av alle relevante komponenter i AMS-løsningen. b) Det ska foretas jevnlig sikkerhetskopiering av måledatabasen. c) Sikkerhetskopiene skal lagres på et sikkert sted et annet fysisk sted enn der.			
E. Endrings- og versjonskontroll				
E.1	Nettselskapet skal dokumentere prosedyrer for å planlegge og utføre endringer i AMS-miljøet.			

Nr	Sikkerhetsområde/kontroller	(J/N*)	Begrunnelse for ekskludering	Beskrivelse av hvordan kontrollen er implementert
E.2	Nettselskapet skal ha en oppdatert oversikt over versjoner av all maskinvare, firmware, oppdateringer og programvare som benyttes i AMS løsningen. Oversikten skal oppdateres ved endringer og ved regelmessige gjennomganger.			
F. Fjerntilgang til AMS-løsningen				
F.1	Det skal etableres prosedyrer for godkjenning, administrering og overvåking av eksterne tilkoblinger for vedlikehold og diagnostiske aktiviteter på alle komponenter i AMI-systemet.			
G. Fysisk beskyttelse av AMS-løsningen				
G.1	a) Alle rom som inneholder utstyr som er kritisk for AMS skal være egen adgangskontrollert sone. b) Komponenter i AMS utenfor adgangskontrollerte soner skal beskyttes mot uautorisert fysisk tilgang. c) Alle forsøk på å få uautorisert tilgang til utstyr i AMS-løsningen eller rom med kritisk AMS-utstyr skal oppdages straks.			

Nr	Sikkerhetsområde/kontroller	(J/N*)	Begrunnelse for ekskludering	Beskrivelse av hvordan kontrollen er implementert
H. Bryte- og strupefunksjonalitet				
H.1	System og nettverk som benyttes til styring av bryterfunksjonalitet skal sikres særskilt mot forsøk på uautorisert utførelse av bryte- og strupefunksjonalitet.			
I. Elektromagnetisk interferens (EMI)				
I.1	Alle komponentene i AMS-løsningen skal være tilstrekkelig skjermet mot elektromagnetisk interferens (EMI).			

Denne serien utgis av Norges vassdrags- og energidirektorat (NVE)

Utgitt i Veilederserien i 2012

Nr. 1 Slipp og dokumentasjon av minstevannføring for små vassdragsanlegg med konsesjon (19 s.)

Nr. 2 Cost base for small-scale hydropower plants (< 10 000 kW) (90 s.)

Nr. 3 Cost base for hydropower plants (182 s.)

Nr. 4 Veileder for fyllingsdammer (49 s.)

Nr. 5 Veileder til forskrift om energivurdering av tekniske anlegg og energimerking av bygninger

Nr. 6 Utbetaling ved svært langvarige avbrudd. Veileder til kapittel 9A i kontrollforskriften

Nr. 7 Veileder til sikkerhet i avanserte måle- og styringssystem. Frank Skapalen og Bjørn Jonassen

Norges
vassdrags- og
energidirektorat

Norges vassdrags- og energidirektorat

Middelthunsgate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 09575
Internett: www.nve.no