



Risikovurdering av AMS

Frank Skapalen

Seksjon for beredskap, energiavdelingen

NVEs BfK-seminar 11. januar 2012

Rekkefølge

- Formål med AMS, funksjoner
- Hva vi har jobbet med i risikovurderingen
- Scenarier og risikoområder
- Bryte- strupefunksjonalitet
- anbefalinger

Formålet med AMS

- Effektivisere avregningen
- Enklere og raskere for sluttbruker å se virkningen av energieffektivisering eller leverandørskifte
- Mer effektive energioppfølgingsystemer (tredjepart)
- Øke effektiviteten i kraftmarkedet
- Nyttig verktøy i ekstraordinære situasjoner
- Mer effektiv overvåking av kraftnettet – distribusjonsnett
- Distribuert, lokal produksjon i kraftsystemet (Plusskunder)

Funksjonskrav i AMS

- Registrere måleverdier – maks hvert 60. min, ned til hvert 15. min.
- Mulighet for momentan avlesning
- Benytte allment tilgjengelige kommunikasjonsprotokoller
- Bryter- strupefunksjonalitet
- Tilrettelegge for tredjepartstjenester
- Tilrettelegging for bruk av kommunikasjonsstruktur i AMS for tredjepart dersom kapasitet
- Avlesning av andre målere
- Tilrettelegge for fleksibel utvidelse av funksjonalitet

4

Eksisterende sikkerhetskrav

- Krav i forskriften
 - MAF: § 4-2 h) (AMS skal)...*gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner.*

Høringsdokument: 1/2011:

- Krav om risikovurdering
- Kryptering eller lukket datanettverk

Hva vi har jobbet med i risikovurderingen

Hovedmålsetninger

- Få oversikt over mulige sårbarheter knyttet til komponenter i AMS og infrastrukturen som er nødvendig for et funksjonelt system.
- Identifisere utfordringer knyttet til direkte og indirekte koblinger mellom driftskontrollsystem og AMS.

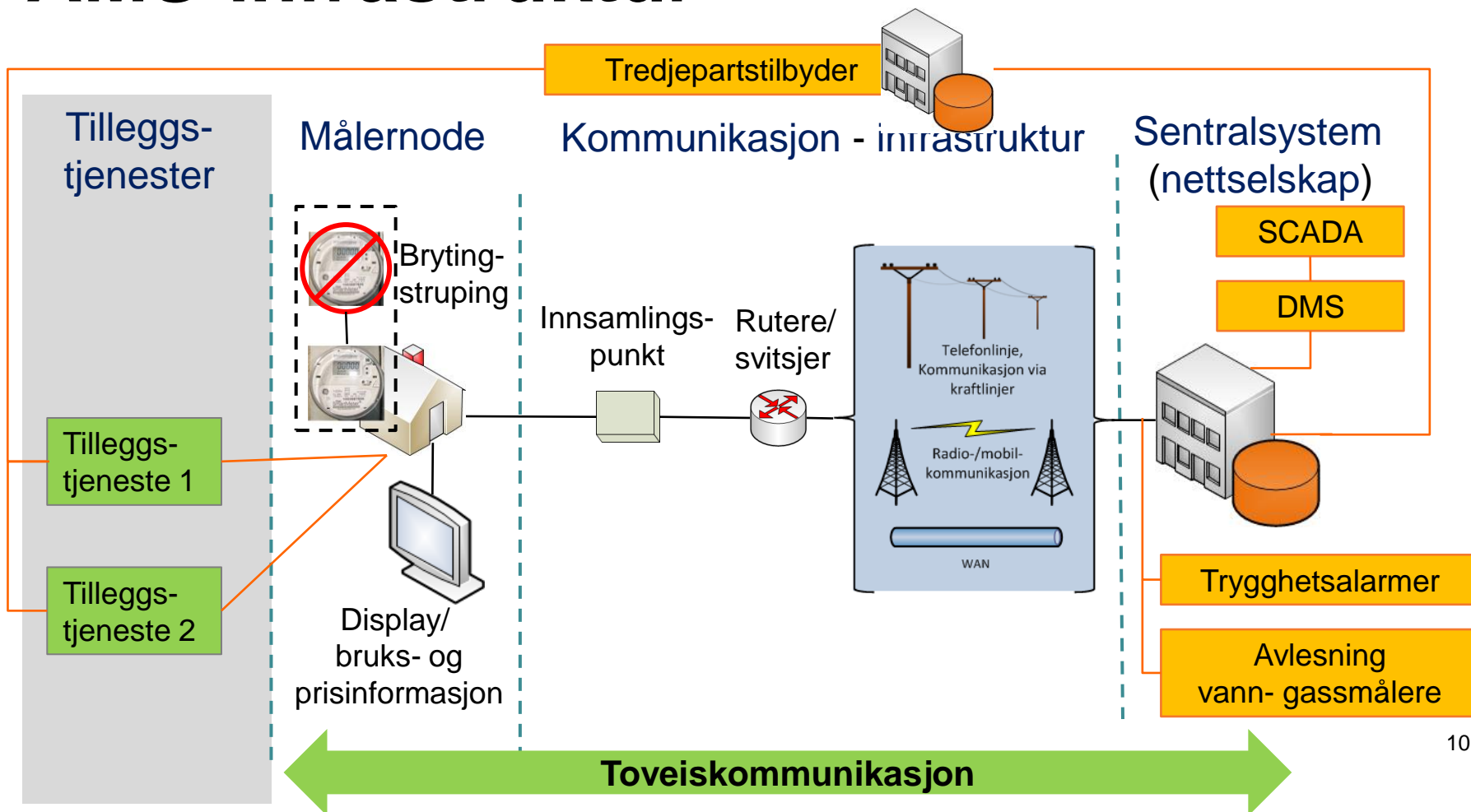
Fra måler til sentralsystem

- Måleverdikjeden – fra målepunktet hos kunden til sentralsystemet hos nettselskap
- Måler og strømforsyning er vurdert som to forskjellige enheter
 - Måler kan feile og kunden har fortsatt strøm (strømforbruk registreres ikke)
 - Strømforsyning kan feile og måler fungerer (måler registrerer null strømforbruk)

Dette har vi vurdert

- Måleverdikjeden – fra målepunktet hos kunden til sentralsystemet hos nettselskap
- Måler og strømforsyning er vurdert som to forskjellige enheter
 - Måler kan feile og kunden har fortsatt strøm (strømforbruk registreres ikke)
 - Strømforsyning kan feile og måler fungerer (måler registrerer null strømforbruk)

AMS-infrastruktur

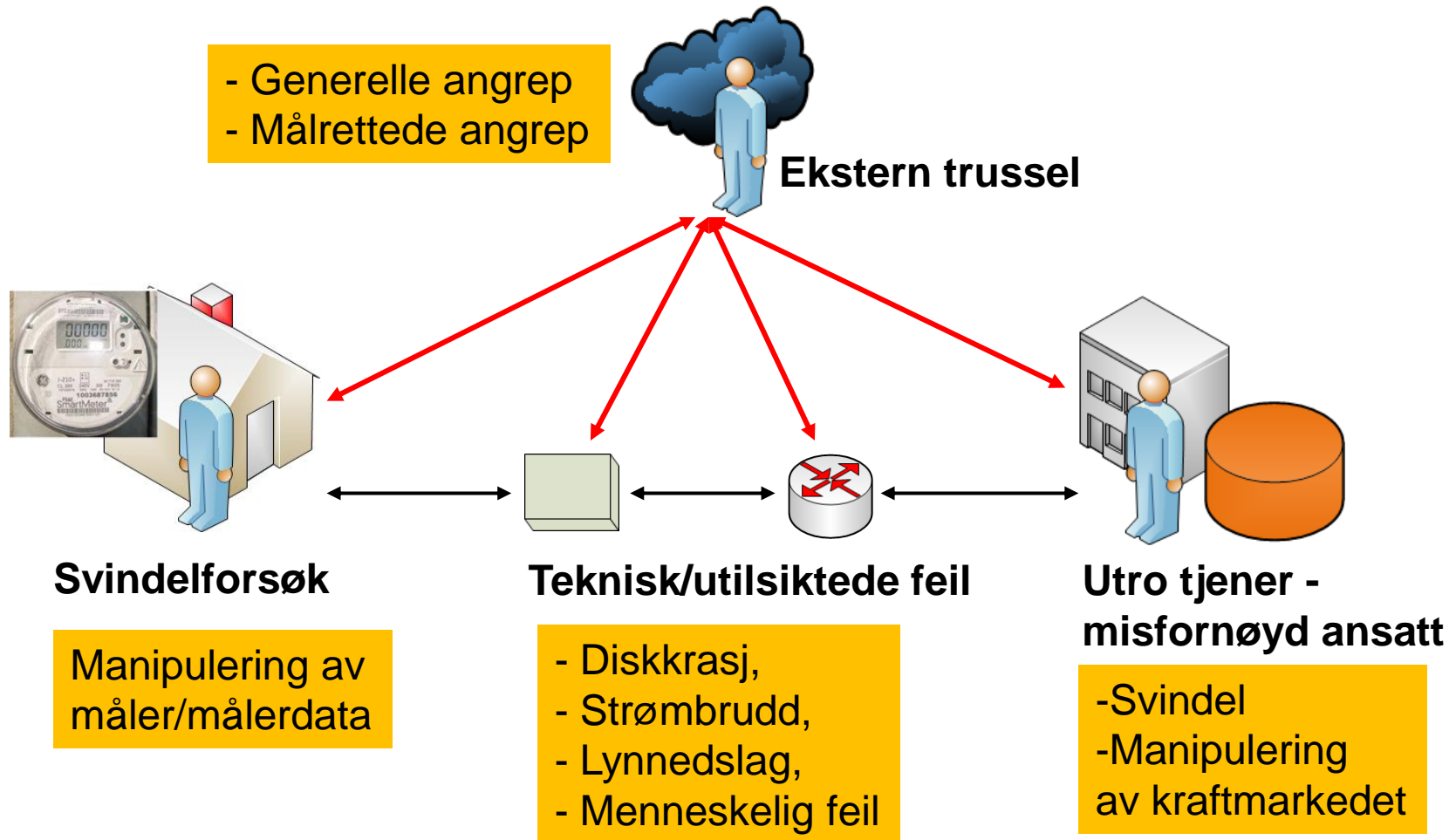


Scenarier og risikoområder

11



Hvilke trusler snakker vi om?



12

Uønskede hendelser - scenarier

- Stort antall AMS ute av drift samtidig (ikke målrettet angrep)
 - Måler og strømforsyning er adskilt; kan ha strøm selv om måleren er nede
 - Ikke kritisk, men uheldig i tunglast-perioder
 - Kan bety store reparasjonskostnader
- Kunde manipulerer måledata
 - Egne eller andres; endrer forbruk eller flytter forbruk til rimeligere tidspunkt
 - Feilfakturering og feil datagrunnlag for å beregne nettap. Kan avdekkes med balansemåling

13

Uønskede hendelser - scenarioer

- Interne trusler – utro tjener
 - Legitime tilganger misbrukes. Koordinerte, målrettede angrep kan oppnå hva som helst.
 - Logging, opplæring, bevisstgjøring, need-to-know, kvalitetssikring er fornuftige tiltak.
- Målrettet angrep på kraftforsyningen i et spesifikt geografisk område
 - Datainnbrudd i nettstasjoner, hackerverktøy langveisfra, samarbeid mellom ekstern og intern
 - Bryte strømforsyning, fysiske ødeleggelser, manipulering av måledata
 - Kryptering av signaler er en god barriere

14

Bryter- /strupefunksjonalitet

15



Noregs vassdrags- og energidirektorat

16.01.2012

Bryter-/strupefunksjonalitet (1)

Mulige bruksområder

- Opphør av abonnement ved flytting (kundehåndtering)
- Utkobling av målepunkt eller struping av effektuttak ved manglende betaling (kundehåndtering)
- Hurtigere gjenoppretting etter feil (nettdrift)
- Effektbegrensning i høylastperioder (nettdrift)
- Utkobling av målepunkt i forbindelse med planlagt utkobling (f.eks. ved vedlikehold av nett – nettdrift)
- Utkobling eller struping av forbruk i en beredskapssituasjon (rasjonering)

16

Bryter-/strupefunksjonalitet (2)

Viktige forhold å vurdere:

- Hvordan implementere, og hvem skal ha tilgang til hva?
- Fra hvilket system skal signalene gå fra?
 - Driftssentral eller kundeservice?
- Når skal bryter-/strupefunksjonen benyttes?
 - Beredskapssituasjon, normal drift eller begge deler?
- I hvilken stilling skal bryter gå til dersom AMS svikter?

Bryter-/strupefunksjonalitet (3)

Viktige forhold å vurdere:

- Hvilken konsekvens vil det ha for kraftsystemet hvis ikke bryter-/strupefunksjon fungerer?
- Hvilken konsekvens vil det ha for kraftsystemet hvis eksterne får tilgang til bryter-/strupefunksjonaliteten i AMS?
- Bør dere vurdere om deler av forbruket til en kunde skal fritas fra bryter-/strupefunksjonalitet?

Felles for høyrisiko-hendelsene

- Felles for høyrisiko-områdene;
 - Uønsket utkobling hos mange kunder
 - Programvarefeil
 - Sentralenhet feiler eller brukes i angrepet
 - Utro tjener
- Scenarioet med mange målere ute av drift samtidig er også vurdert til å være kritisk. Dette er pga store kostnader for reparasjon/utskiftning av utstyr.

Anbefalinger

20



Utrulling og drift

- Sikker kommunikasjon
 - Bruk åpne protokoller som støtter kryptering for all kommunikasjon hvor informasjonssikkerhet må ivaretas
 - Tidsstempel, fortløpende teller og sjekksum må implementeres på sendersiden og avvik må håndteres på mottakersiden, evt. fysisk sikring

Utrulling og drift (2)

- Bryter-/strupefunksjonen
 - Faste oppdrag eller i en beredskapssituasjon?
 - Evt. testintervall bør defineres hvis bryter brukes sjelden
 - Implementering bør vurderes nøye
 - Adgang og konsekvens ved teknisk svikt og målrettet angrep bør reduseres
 - Fail-safe bør være slik at konsekvens blir minst mulig ved feil

Utrulling og drift (3)

- Programvareutvikling
 - I henhold til anerkjente standarder
 - Oppdatering fra sentralt hold
- Outsourcing
 - Måleverdiinnsamling kan outsources
 - Bryter-/strupefunksjon kan ikke like lett outsources, men samarbeid mellom flere nettselskap er naturlig

Utrulling og drift (3)

- Kartlegging og dokumentasjon av systemer
 - God og oppdatert dokumentasjon kan redusere sannsynligheten for flere uønskede hendelser
- Risikovurdering
 - Krav om risikovurderinger for IT-systemer bør også gjelde for AMS
 - Sjekkliste

Utrulling og drift (4)

- Adgang og tilgang til AMS
 - Vurdere fysisk adgangs- og tilgangskontroll til bryter-/strupefunksjonen
 - Vurderingene må gjøres hos hvert enkelt nettselskap, og sikringstiltak må implementeres på rett nivå ut i fra valgt løsning

Utrulling og drift (5)

- Sammenkobling av AMS og driftskontrollsystemer
 - AMS-funksjonalitet 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.
 - Etterarbeid bør brukes i risikostyringsprosessen og det generelle sikkerhetsarbeidet.

Anbefalinger krav og regelverk

- Beredskapsforskriften bør gjelde for AMS
 - 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.
- Flere av kravene som er i BfK kapittel 6, bør gjelde også for AMS