NTNU
Det skapende universitet

Vurdering av informasjonssikkerheten ved innføring av AMS innen kraftdistribusjon

Petter Andreas Strøm

Master i kommunikasjonsteknologi
Oppgaven levert: Januar 2012
Hovedveileder: Svein Johan Knapskog, ITEM

Norges teknisk-naturvitenskapelige universitet

NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET
FAKULTET FOR INFORMASJONSTEKNOLOGI, MATEMATIKK
OG ELEKTROTEKNIKK

OPPGAVEBESKRIVELSE

Studentens navn: Petter Andreas Strøm

Tittel: Vurdering av informasjonssikkerheten ved innføring av AMS innen kraftdistribusjon

Beskrivelse:

Norges Vassdrags- og Energidirektorat (NVE) har stilt krav om at alle norske nettselskaper, innen 1.1.2017, skal ha installert Avanserte Måle- og Styringssystemer (AMS) for strøm ved alle sine målepunkter. AMS utgjør store signal- og datamengder som etterhvert vil kreve robust toveis datakommunikasjon mellom mange ledd i nettet. Flere kommunikasjonskanaler er aktuelle å benytte for slik transmisjon; fiber, ADSL, GPRS, lokale radioløsninger og Power Line Communication (PLC). Energiforsyningen er en kritisk del av infrastrukturen i det norske samfunnet og måledata og styringssignaler sendt mellom nodene i et slikt system er svært sensitive og kan misbrukes om uvedkommende får tilgang.

I NVEs endelige forskrifttekst for AMS, Juni 2011, §4-2 punkt g, beskrives krav til informasjonssikkerhet ved målere og datakommunikasjon innen AMS som "sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner". Gjennom oppgaven skal studenten sette seg inn i arkitekturer for AMS, identifisere sårbarheter i slike kommunikasjonssystemer, vurdere mulige konsekvenser av misbruk av data og komme med forslag til utbedringer og løsninger for bedre informasjonssikkerhet. Om tiden tillater det; gjennomføre et simulert angrep på en av sårbarhetene som er funnet.

Frist for innlevering: 29 Januar, 2012
Institutt: Institutt for telematikk, ITEM
Hovedveileder: Svein Johan Knapskog

Trondheim, 6. September, 2011

Svein Johan Knapskog, NTNU/ITEM

Sammendrag

Etter krav fra Norges Vassdrags- og Energidirektorat (NVE) er alle norske nettselskaper innen kraftbransjen pålagt å installere Avanserte Måle- og Styringssystemer (AMS) for alle sine målepunkter innen 1.januar 2017. AMS er en integrering av IKT i kraftforsyningen som muliggjør toveis kommunikasjon for å effektivisere avregning, bytte av kraftleverandør samt danne fundament for det framtidige dynamisk smart strømnett.

I et hvert distribuert kommunikasjonssystem må informasjonssikkerheten håndteres etter vurdert risiko et slikt system innfører. Etter vurderinger av NVEs funksjonskrav ble følgende områder for informasjonssikkerhet i AMS definert; sikring av fysisk utstyr, sikkerhet i hardware, sikkerhet i software, sikring av kommunikasjonsteknologi, organisatorisk informasjonssikkerhet. Fundamentalt for distribuerte systemer er sikker datakommunikasjon og det eksisterer mange typer angrep mot AMS om kommunikasjonsnettverket ikke er tilstrekkelig sikret. Vurderingene av konsekvenser ved suksessfulle angrep viser at avhengighet mellom funksjoner, spesielt styringssignaler og konfigurasjonskommandoer, generelt fører til økt kompleksitet og gir større konsekvenser enn angrep mot målerverdier. Ved enkelte tilfeller av suksessfulle angrep mot styringssignaler i AMS-nettverket, vurderes konsekvensene til å være samfunnmessige da det kan resultere i kaskadeeffekter og ustabilitet for hele kraftnettet.

I denne oppgaven blir det presentert en sikkerhetsarkitektur for kommunikasjon mellom sluttbruker og nettselskap som kan tilstrekkelig nivå av sikkerhet relativt til konsekvensene av angrep. Arkitekturen er basert på forsvar i dybden og implementerer to lag med sikre ende-til-ende forbindelser basert på DLMS/COSEM og IP/IPsec.

English summary

After demands from NVE all Norwegian grid companies are required to install AMI by January 1st 2017. AMI is a digital communication systems that enables two-way communication between end user and the grid company to increase the efficiency of billing, the process of changing power supplier and create a fundament for a future dynamic smart power grid.

Through evaluation of NVEs functional requirements, the following areas for information security for AMI is defined; physical security of equipment, secure hardware design, secure software design, securing of communication technology, administrative and organizational security. Fundamentally for all distributed systems is secure data transfer and there exist many ways to attack an AMI if the network is not adequately secured. The assessment of consequences by successful attacks shows the dependence between functions must be minimized and attacks towards traffic that initiates processes for the receiver, especially control signals and configuration commands, generally leads to increased complexity and gives larger consequences then attacks towards measurement data. For cases of attacks against control signals, it is considered that consequences can result in cascade effects and instability of the entire Norwegian power grid.

This report present a security architecture for the AMI network, between the end user and the grid company, which achieve the goal to realize an acceptable level of security relative to the consequences of various attacks. The architecture is based on the defense in the depth and implements two layers of end-to-end security through a communication profile based on DLMS/COSEM and IP/IPsec.

Forord

Denne masteroppgaven avslutter min 5-årige mastergrad i kommunikasjonsteknologi, ved Institutt for Telematikk (ITEM), fakultet for informasjonsteknologi, matematikk og elektroteknikk (IME) , ved Norges teknisk-naturvitenskapelige universitet (NTNU). Oppgavebeskrivelsen ble utformet i samarbeid med flere i industrien samt tilhørende forskningsinstanser. Oppgaven ble veiledet av Professor Svein J. Knapskog, ITEM, og gjennomført i tidsperioden 6.september 2011 til 29.januar 2011.

Jeg vil takke alle som har bidratt til at denne oppgaven var mulig, deres tilbakemeldinger og interessante diskusjoner.

Svein J. Knapskog, NTNU
Maria B. Line, SINTEF
Ståle Gullbrekken, NTE
Jan Berntzen, Tieto
Hanne Sæle, SINTEF
Jan Hovden, NTNU
Eirik Albrechtsen, SINTEF
Einar Flydal

Til slutt vil jeg også takke min nærmeste familie og venner for å ha støttet meg gjennom alle årene på NTNU

Trondheim, 29. Januar 2012

Petter Andreas Strøm

Innhold

Figurer

Tabeller

Akronymer

3GPP 3rd Generation Partnership Project

6LoWPAN IPv6 over Low power WPAN

AAA Authentication, Authorization, Accounting

ACSE The Association Control Service Element

AES Advanced Encryption Standard

AH Authenitcation Header

AH Authentication Header

AKA Authentication and Key Agreement

AMI Advanced Metering Infrastructure

AMR Automatic Meter Reading

AMS Avanserte Måle- og Styringssystemer

APDU Application Protocol Data Unit

AuC Authentication Center

BG Border Gateway

BPL Broadband over Power Lines

BSC Base Station Controller

BTS Base Transceiver Station

CBC Cipher Block Chaining

CBC-MAC CBC Message Authentication Code

CCM Counter with CBC-MAC

CDMA Code Division Multiple Access

CEN Comité Européen de Normalisation / Committee for Standardization

CERT/CC Computer Emergency Response Team Coordination Center

CIA Confidentiality, Integrity and Availability

COSEM Companion Specification for Energy Metering

CRC Cyclic Redundancy Check

DES Digital Encryption Standard

DLMS Device Language Message Specification

DoS Denial of Service

DPWS Devices Profile for Web Services

EAP Extensible Authentication Protocol

EDGE Enhanced Data-rates for Global Evolution

ESP Encapsulation Security Payload

ETSI European Telecommunications Standards Institute

FDMA Frequency Division Multiple Access

FSK Frequency Shift Keying

GEA GPRS Encryption Algorithm

GGSN Gateway GPRS Support Node

GMSK Gaussian Minimum-Shift Keying

GPRS General Packet Radio Service

GSM Global System for Mobile Communication

GSM Global System for Mobile Communication

GTP GPRS Tunneling Protocol

HAN Home Area Network

HF High Frequency

HLR Home Location Register

HLS High Level Security

HSS Home Subscription Server

HTTP Hypertext Transfer Protocol

IDS Intrusion Detection Systems

IDPS Intrusion Detection and Prevention Systems

IEC International Electrotechnical Commission

IETF Internet Engineering Task Force

IKE Internet Key Exchange

IKT Informasjons- og Kommunikasjonsteknologi

IMSI International Mobile Subscriber Identity

IP Internet Protocol

IPS Intrusion Prevention Systems

IPsec IP security

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

IR Infrared

ISAKMP Internet Security Association and Key Management Protocol

IT Informasjons Teknologi

KBO Kraftforsyningens beredskapsorganisasjon

LBP 6LoWPAN Bootstrapping Protocol

LLS Low Level Security

LR-WPAN Low Rate WPAN

M-Bus Meter Bus

MAC Media Access Control

MAP Mobile Application Part

MGW Media Gateway

MPDU MAC Protocol Data Unit

NAT Network Address Translation

NIST National Institute of Standards and Technology

NVE Norges Vassdrags- og Energidirektorat

OASIS Organization for the Advancement of Structured Information Standards

OBIS Object Identification System

OED Olje- og Energidepartementet

OFDM Orthogonal Frequency Division Multiplexing

OSI Open Systems Interconnection

PAN Personal Area Network

PCU Packet Control Unit

PIN Personal Identification Number

PLC Power Line Communication

PRIME Powerline Intelligent Metering Evolution

PSK Phase Shift Keying

PSTN Public Switched Telephone Network

QAM Quadrature Amplitude Modulation

RF Radio Frequency

RFC Request For Comment

RNC Radio Network Controller

ROS Risiko og Sårbarhet

SA Security Associations

SCADA Supervisory Control And Data Acquisition

SGSN Serving GPRS Support Node

SIM Subscriber Identity Module

SML Smart Message Language

SOA Service-Oriented Architecture

SOAP Simple Object Access Protocol

SPD Security Policy Database

SRD Short Range Device

SSL Secure Sockets Layer

SS7 Signaling System no 7

TCP Transmission Control Protocol

TDMA Time Division Multiple Access

TLLI Temporary Logical Link Identity

TLS Transport Layer Security

TMSI Temporary Mobile Subscriber Identity

TP Twisted Pair

TTP Trusted Third Party

UDP User Datagram Protocol

UE User Equipment

UEA UMTS Encryption Algorithm

UIA UMTS Integrity Algorithm

UMTS Universal Mobile Telecommunications System

VPN Virtual Private Network

W3C World Wide Web Consortium

WAN Wide Area Network

WPAN Wireless Personal Area Network

WSDL Web Services Description Language

W-CDMA Wideband Code Division Multiple Access

xDSL x Digital Subscriber Line

XML Extensible Markup Language

Definisjoner og begreper

AMS-kanalen
Kommunikasjonsstien i nettverket mellom den smarte måleren og sentralsystemet hos nettselskapet

AMS-nettverket
Alle komponenter i et AMS. Inklusive målernoder, konsentratorer og sentralsystem

Kommunikasjonskanal
Se AMS-kanalen

Kommunikasjonsnett
Nasjonal infrastruktur for telekommunikasjon. E.g. GPRS, UMTS, Fiber

Kommunikasjonsprofil
Lagvis sammensettning av protokoller for kommunikasjon i nettverk

Kommunikasjonssystem
Alle komponenter i AMS-kanalen

Målernode
I denne oppgaven tilsvarer dette en smartmåler eller en sluttbruker

Nettselskap
I denne oppgaven: sentralsystemet og alle tilhørende systemer på nettselskapsiden av AMS

Nettverksnode i AMS
Komponent i AMS-nettverket

Nyttelast
Innholdet i en protokollmelding unntatt headerinformasjon

Sluttbruker
Abonnent koblet inn i kraftnettet

Styringssignaler
Meldinger sendt over AMS-kanal som styrer krafttilførselen for mottakeren

Protokollstakk
Se kommunikasjonsprofil

Underliggende protokoll
: Protokollag som ligger under protokollaget i protokollstakken snakket om i den gitte sammenheng

Kapittel 1

Introduksjon

1.1 Motivasjon

3. september 1999 nedsatte Regjeringen Bondevik et tverrpolitisk sammensatt utvalg, Sårbarhetsutvalget. Utvalget hadde fikk i oppgave å "utrede samfunnets sårbarhet med sikte på å styrke samfunnets sikkerhet og beredskap". På grunnlag av utvalgets arbeid ble utredningen "Et sårbart sammfunn" publisert 4.juli 2000 hvor det ettertrykkelig ble presisert at dagens samfunn er mer sårbart enn tidligere. Økt kompleksitet og tettere koblinger fører til at svikt i noen få avgjørende samfunnsfunksjoner kan føre til at store deler av samfunnet får omfattende problemer. Utredningen viser videre at det i økende grad eksisterer avhengigheter mellom kraftforsyning og informasjons- og kommunikasjonssystemer som omtales som "bæresøylene" i et moderne samfunn. Sårbarhetsutvalgets arbeid ble basert på samfunnets tilstand mot slutten av 90-årene. På denne tiden var de sterkeste koblingene mellom kraftforsyning og IKT-systemer bruk av kontroll- og styringssytemer for effektivisering og sentralisert styring og drift av kraftproduksjon. Utredningen påpekte også at framtidige utfordringer ville være økning i elektroniske trusler og økt kompleksitet og angrepsoverflate gjennom økt bruk av IKT innen kraftproduksjon og distribusjon.

Grunnet effektivisering har kontroll- og stryringssystemer, også kalt SCADA, blitt tatt i bruk innen produksjon- og distribusjonsindustrien for olje, gass, elektrisk kraft og vann. Innføringen av SCADA i disse høyrisikosystemene har vist seg å medføre stor risiko da IKT-løsningene benyttet var umodne og hadde mange svakheter med tanke på informasjossikkerhet. Som en effekt av nye muligheter for elektroniske angrep og eksiterende sårbarheter har SCADA systemer i økende grad blitt et mål for elektroniske trusler. Med hensyn til store konsekvenser med mulig samfunnsmessig risiko har også dette vært aktuelle mål for internasjonale trusler og terrorister.

Etter krav fra NVE har alle nettselskaper blitt pålagt å installere AMS for alle sine sluttbrukere innen 1.1.2017. Hensikten med innføringen av AMS er å effektivisere kraftdistribusjon ved bruk av IKT for automatisk måleravlesning og styringsfunksjoner for krafttilførsel hos sluttbrukere. I likhet med SCADA styrker innføringen av AMS koblingene mellom krafttilførsel og telekommunikasjonssystemer. Basert på Sårbarhetsutvalgets vurderinger vil innføringen av elektroniske målere for alle sluttbrukere føre til en drastisk økning i sårbarheten for samfunnet ved større angrepsoverflate, mer kompleksitet og sterkere gjensidig avhengighet mellom de to mest vitale infrastrukturene i samfunnet. Ettersom det i Norge er nettselskapenes ansvar å sikre kommunikasjonen i sine AMS, vil de bli satt i en ny situasjon hvor de blir pålagt tverrfaglige utfordringer gjennom integreringen av IKT i kraftnettet. Det er derfor essensielt å kartlegge de sikkerhetsmessige tiltakene som må iverksettes for å håndtere den innførte risikoen.

1.2 Mål for oppgaven

Målene for denne oppgaven er:

- Vurdere innført risiko gjennom analyse av sårbarheter og konsekvenser ved angrep mot IKT i AMS.
- Kartlegge forskjellige områder for informasjonssikkerhet ved AMS samt hvilke deler av arkitekturen som er mest sårbare med tanke på angrep

- Få oversikt over hvilke krav til informasjonssikkerhet som er satt samt å definere et akseptabelt nivå av informasjonssikkerhet i AMS.
- Komme med forslag til tiltak som kan oppfylle et akseptabelt nivå av informasjonssikkerhet.

1.3 Avgrensninger

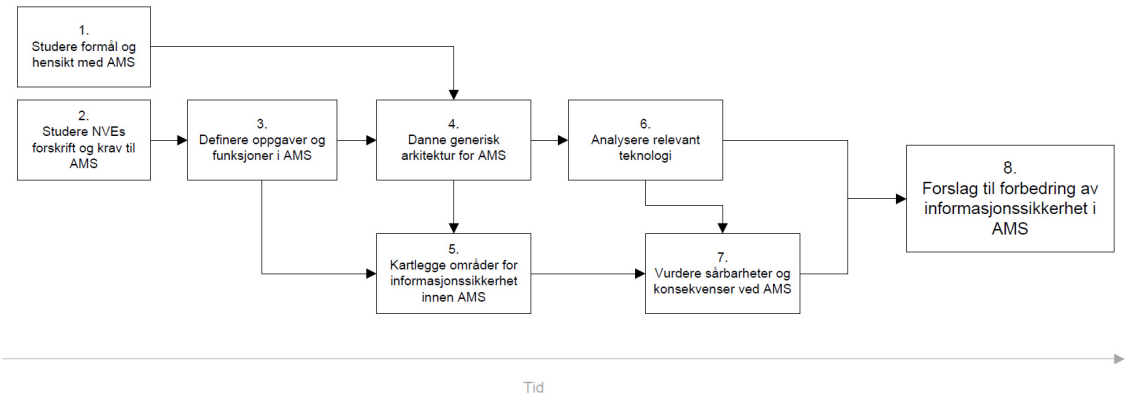
Innføringen av AMS i kraftforsyningen gir mange utfordringer med hensyn til informasjonssikkerhet. AMS blir vurdert ut ifra bruk i Norge. Dette med tanke på nasjonale krav til funksjonalitet, lovverk, tilgjengelig teknologi etc. Selv om denne oppgaven kun presenterer arbeid vedrørende innføringen av AMS i kraftforsyning vil enkelte diskusjoner også være relevante om for AMS benyttet til andre formål, e.g. gass, vann, varme. Oppgaven gir en introduksjon til forskjellige områder for informasjonssikkerhet innen AMS, men kun sikkerhet i kommunikasjonsløsninger blir presentert i dybde grunnet tidsbegrensninger. Videre vil denne rapporten kun presentert arbeid vedrørende kommunikasjonsnettverket som benyttes mellom sluttbrukere og sentralsystemene hos nettselskapene. Denne avgrensningen har flere årsaker. Først og fremst er AMS ennå et relativt nytt tema i Norge og en teknologi under utvikling. Få valg av teknologi og standarder er ennå endelige og hvordan et reelt framtidig scenario vil se ut er vanskelig å predikere for videre studier. Uavhengig av hvilke standarder og teknologier som blir valgt i framtiden vil AMS være avhengig av toveis kommunikasjonsløsninger mellom sluttbrukere og nettselskaper. For det andre vil arkitektur og konfigurasjoner på systemene som benyttes mest sannsynlig varierer fra nettselskap til nettselskap og det vil være en komplisert oppgave å se på dette overordnet og gi en relevant analyse. Derfor vil ikke systemer på nettselskapetssiden av AMS bli studert i denne oppgaven. For det tredje er ikke tilleggsutstyr og systemer på sluttbrukersiden en del av et AMS. Detaljer rundt informasjonssikkerhet på sluttbrukersiden av AMS, e.g. hjemmenettverk, vil derfor ikke bli studert.

Grunnet tidsbegrensninger og lite tilgjengelig informasjon vedrørende bruk av mesh-basert AMS i Norge, ble ikke slik teknologi studert i denne oppgaven. Til tross vil mange diskusjoner om sikker overføring av informasjon i AMS nettverk være relevante også for mesh-baserte nettverk. Vurderinger av kostnad ved sikring av IKT-systemer i AMS er heller ikke presentert i denne oppgaven.

1.4 Metodikk

Framdriftsplanen for denne oppgaven er vist i figur 1.1. Boksene i figuren, videre kalt *steg*, viser overordnede arbeidsprosesser mens pilene mellom viser relasjoner og informasjonsflyt mellom arbeidsprosessene.

- Første steg var å sette seg inn i formål og hensikter med innføring av AMS. Dette ble gjort for å få et overordnet inntrykk av hvilke oppgaver og funksjoner et slikt system kunne utføre.
- I steg to ble NVEs forskrift og krav til AMS studert, spesielt til funksjonalitet og informasjonssikkerhet. Av disse kravene og forskriftene kunne det defineres et sett



Figur 1.1: Arbeidsprosess

funksjoner og oppgaver AMS skulle kunne utføre for å oppfylle sine hovedmål, steg tre.

- På grunnlag av steg en og steg tre ble en generisk arkitektur for AMS dannet. Dette ble gjort for å få et innblikk i hvilke systemkomponenter som utgjør et AMS, hvilke komponenter som utfører forskjellige oppgaver, samt deres relasjoner til hverandre.

- Med utgangspunkt i den generiske arkitekturen og definerte oppgaver og funksjoner ble forskjellige områder for informasjonssikkerhet innen AMS kartlagt og studert, steg fem.

- Basert på den generiske arkitekturen ble forskjellige teknologier brukt innen AMS studert, steg seks. Med oversikt over de forskjellige områdene for informasjonssikkerhet, samt analyse av teknologier brukt i AMS, ble sårbarheter og konsekvenser ved eventuelle angrep vurdert, steg 7.

- I steg åtte ble et forslag til forbedring av informasjonssikkerheten i AMS presentert basert på alle de foregående stegene.

I arbeidet med denne oppgaven ble informasjon innhentet på flere vis. For IKT relatert informasjon ble kompetanse og kunnskap fra tidligere studier og fag benyttet i tillegg til innhenting av annen relevant informasjon. For annen informasjon og spesifikke detaljer relatert til AMS ble nødvendig informasjon innhentet fra følgende kilder:

Internett

Faglitteratur Faglitteratur både for IKT og kraftsektoren

Intervjuer/møter/samtaler Kontakter[1] i AMS industrien eller relatert forskning

Seminarer Relevante foredrag og seminarer innen AMS og smarte strømnett.

[1]Se forord i denne oppgaven

1.5 Utfordringer

Avanserte måle- og styringssystemer har eksistert i flere år og større utrullinger finnes flere land. Implementasjoner eksisterer også i Norge, men fortsatt i relativt liten skala og med begrenset funksjonalitet i forhold til hva NVE nå har satt krav om. Ettersom feltet ennå er nytt her til lands var det få empiriske data og erfaringer tilgjengelig relatert til bruk av slike systemer i praksis. Da det ikke eksisterer noen universell liste over oppgaver et AMS system skal utføre, var en utfordring å finne hvilke funksjoner og data som skulle være aktuelle for eventuelle angrep.

Det eksisterer mange standarder og protokoller for kommunikasjon innen AMS. Ettersom det ennå er vanskelig å si hvilke standarder som kommer til å bli dominerende for bruk i Norge, måtte mange standarder studeres og vurderes. En delmengde av standarder og protokoller ble derfor valgt ut på grunnlag av vurderinger gjort av flere i industrien. Flere av standarder og protokoller er lisensbaserte eller er proprietære. Av den grunn var mange dokumenter og spesifikasjoner utilgjengelige for videre studier. Arbeidet presentert i denne rapporten er derfor i enkelte tilfeller basert på informasjon innhentet fra andre kilder. I disse tilfeller er dette presisert gjennom referanser.

1.6 Dokument struktur

Resterende deler av denne oppgaven består av:

Kapittel 2: Avanserte Måle- og Styringssystemer Kapittelet gir en introduksjon til avanserte måle- og styringssystemer. Det presenteres en introduksjon til *smarte strømnett* og relevans til AMS. Norske krav til AMS presenteres og det gis en oversikt over det norske kraftsystemet.

Kapittel 3: Informasjonssikkerhet innen AMS Kapittelet gir en introduksjon til informasjonssikkerhet og motivasjon for feltets relevans innen AMS. Til slutt presenteres forskjellige områder for informasjonssikkerhet innen AMS.

Kapittel 4: Vurdering av trusler mot AMS-kanalen Kapittelet presenterer forskjellige typer trafikk som sendes gjennom AMS-kanalen. Deretter studeres interessenter, trusler og angrep mot de forskjellige trafikktypene.

Kapittel 5: AMS Kommunikasjonsarkitektur Det presenteres generisk arkitektur for AMS-kanalen. Deretter presenteres forskjellige kommunikasjonsprotokoller benyttet mellom komponentene i den generiske arkitekturen.

Kapittel 6: Analyse og vurdering av informasjonssikkerhet for AMS-kanalen En tolkning av NVEs krav til informasjonssikkerhet i AMS-kanalen legges fram. Deretter presenteres vurderinger av sårbarheter, konsekvenser ved angrep, sikkerhetstjenester for AMS-kanalen. Til slutt blir enkelte utfordringer ved informasjonssikkerhet i AMS-kanalen lagt fram.

Kapittel 7: Forslag til sikkerhetsarkitektur for AMS-kanalen Kapitelet legger fram et forslag til sikker overføring av data i AMS-kanalen. Det presenteres forutsetninger

og karakteristikk for løsningen. Deretter presenteres valgte kommunikasjonsteknologier basert på analyse i kapittel 5 og 6. Kapittelet slutter med en vurdering av løsningen.

Konklusjon: Oppsummerer og diskuterer hovedpoeng fra alle kapitler, samt presenterer en konklusjon for oppgaven. Dette kapittelet gir også en oversikt over videre arbeid.

Tillegg 1 Dette vedlegget viser en oversikt over forskjellige grunn-og detaljkrav for AMS. Listen er basert på en kravspesifikasjon for AMS utviklet av SINTEF [74].

Tillegg 2 Dette vedlegget gir en oversikt over protokoller og standarder innen AMS, AMR og AMI. Hentet fra OPENmeter sine dokumenter, [62].

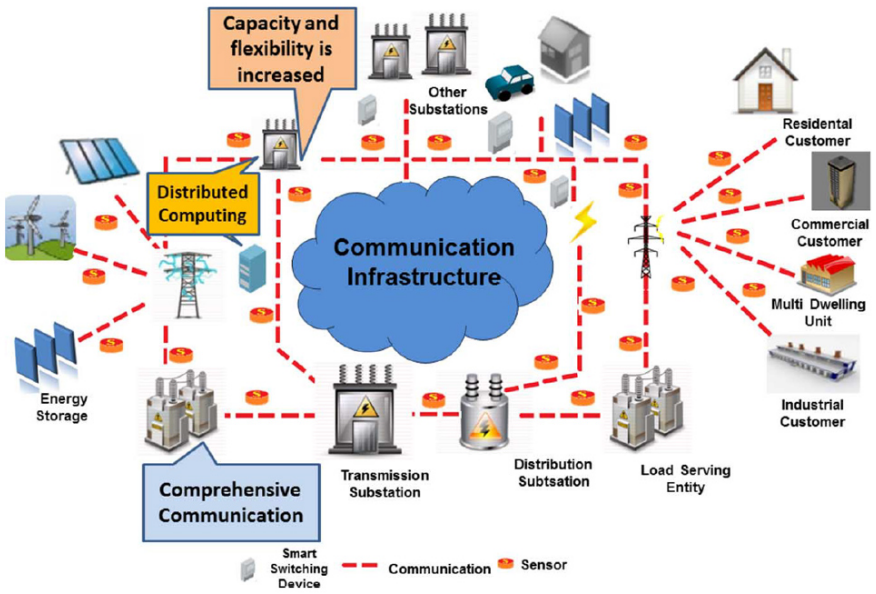
1.7 Terminologi

Denne oppgaven ble skrevet på norsk grunnet dens sterke relasjon til det norske kraftsystemet. Grunnet tverrfagligheten mellom IKT og kraftforsyning var faguttrykk en utfordring da mange utrykk relatert til IKT som oftest er definert og stammer fra det engelske språk. I den sammenheng ble det i de fleste tilfeller benyttet engelske faguttrykk fra IKT for å unngå tvetydighet i oversettelsene til norsk.

I enkelte tilfeller defineres det uttrykk ved å benytte *kursiv*.

Kapittel 2

Avanserte Måle- og Styringssystemer



Figur 2.1: Et smart strømnett ved integrering av telekommunikasjon i kraftnettet [32]

2.1 Smarte strømnett og AMS

Fokuset på *smarte strømnett* har i de siste tiår eksplodert. Mye av motivasjonen for dette er det enorme potensialet som ligger i integrering av fornybar energi samt optimalisering av det eksisterende kraftnettet. Et *smart* strømmnett er i realiteten en integrering av telekommunikasjon i kraftnettet. Et slikt komplett nett muliggjør innsamling og analyse av nær sanntidsdata for overføring, fordeling og forbruk av kraft. Basert på de innsamlede data kan det smarte strømnettet kalkulere og forutse hvordan kraftprodusenter og kraftkonsumenter på best mulig måte kan administrere produksjon og forbruk. Tilgang til nær sanntidsinformasjon om nettets tilstand tillater alle parter å administrere hele kraftnettet som et integrert system. Dette integrerte systemet kan dermed aktivt registrere og reagerer på forandringer i forbruk, produksjon, kvalitet og kostnad, på tvers av alle lokasjoner og nettkomponenter.

Det *smarte nettet* skal benytte en rekke tjenester for å optimalisere distribusjon, produksjon og forbruk av energi. Mange energibærere vil kunne tilføre kraft inn i nettet som fører til robusthet og stabilitet i perioder med lite produksjon av kraft eller i ekstraordinære situasjoner hvor produksjon bortfaller. E.g. skal el-bilers energi kunne føres tilbake til kraftnettet om det lokale forbruket er større enn lokal produksjon og på denne måten opprettholde stabilitet. Lokal produksjon fra mange mindre kraftproduserende enheter, kalt *virtuelle kraftverk*, skal også samlet bidra til å forsyne nettet med tilstrekkelig mengde kraft. Dette realiseres ved å installere e.g. solcellepaneler, vindmøller etc. ved bygg og installasjoner. Det smarte nettet skal også muliggjøre utnyttelsen av fornybar energi i større skala [8]. En felles karakteristikk ved mange fornybare resurser, e.g. solar- og vindenergi, er at tilgjengeligheten varierer og kan ikke kontrolleres. Variasjon i produksjon av vindkraft kan variere fra null til maksimal produksjon på kun 15 minutter, noe som

kan gi variasjoner i flere Gigawatt produsert effekt avhengig av installert kapasitet [42]. Initiativ for satsning på fornybare resurser er iverksatt og vil gi utfordringer med hensyn til varierende produksjon. Et felles mål for de europeiske landene innebærer at samtlige land innen år 2020 skal ha en økning av andelen fornybar energiproduksjon til 20%, senke energiforbruket med 20% og redusere drivgassutslippene med 20%. På forbrukersiden skal det smarte nettet bistå med funksjonalitet for bedre administrering av forbruk samt redusering av forbrukstopper, også kalt *fleksibelt forbruk*. Forbrukstopper vil si tider hvor forbruket er størst og setter høye krav til produksjon og overføringskomponenter i kraftnettet. Ved sentralisert administrering av ut- og innkobling av laster kan forbruket bedre tilpasses produksjonen og forbrukstopper forhindres ved å flytte forbruk til tider med mindre totalt kraftforbruk i nettet. Det smarte strømnettet benytter på denne måten nær-sanntids målinger og reaktive tiltak for å håndtere variasjoner i forbruk og produksjon på en mer dynamisk måte .

Et komplett smart strømnett vil skape et økosystem av sammenkoblede og kommuniserende enheter gjennom funksjoner og tjenester som optimaliserer energiproduksjon, distribusjon og forbruk. Et slikt nett vil utgjøre mange millioner av kommuniserende sensorer og kontrollere e.g. elektriske kraftmålere, transformatorerstasjoner og knutepunkter i kraftnettet, kraftverk og generatorer, sentre for lagring og prosessering av data, kommuniserende elektriske enheter i hjemmet for sluttbrukere, systemer for tredjeparts tjenester etc. Alle enhetene har i hensikt å enten registrer og observere tilstander i nettet, eventuelt å prosessere eller reagere på de observerte tilstandene. Alle disse komponentene kreves å kunne kommunisere transparent for å kollektivt kunne utføre tjenester basert på all den tilgjengelige informasjonen. Koblingen mellom sluttbrukere og kraftnettet er det vi i Norge kaller AMS. AMS vil dermed være fundamentet for et framtidig smart strømnett ettersom det er AMS som hovedsakelig vil stå for kommunikasjonen mellom kraftnettet og forbrukerne. AMS benytter digital telekommunikasjon til å muliggjøre toveis kommunikasjon mot sluttbrukerne. Hos sluttbrukerne er det en digital strømmåler, i.e. *smart meter*, som er koblet mot det lokale kraftnettet og kommuniserer med det vi i denne oppgaven kaller *sentralsystemet* hos nettselskapene. På en slik måte vil den smarte strømmåleren være sluttbrukernes koblingspunkt mot det smarte nettet gjennom AMS.

2.2 AMS i Norge

Seksjon 2.1 forklarte sammenhengen mellom AMS og det framtidige smarte strømnettet. Til tross for at et slikt integrert kommunikasjons- og kraftnett blir realisert i full skala vil, innføringen av AMS, også på kort sikt, gi fordeler med hensyn til optimalisering og administrering av kraftnettet og distribusjon av kraft i Norge. For å få gi grunnlag for diskusjonen og hensikten med innføringe av AMS vil det nå bli gitt en introduksjon til hvordan det norske kraftnettet er strukturert, samt formålet og norske krav til AMS.

2.2.1 Formål

Seksjon 2.1 Begrepet AMS ble for første gang innført av NVE i forslag til forskriftstekst *dokument 12* oktober 2008. Inntil da hadde teknologi for kommunikasjon mellom sluttbrukere og kraftnettet blitt omtalt som 'toveiskommunikasjon' eller 2VK / TVK. NVEs

hovedmålsetning med innføringen av AMS i kraftsektoren er [85]:

> (...) å bidra til et mer samfunnsøkonomisk rasjonelt kraftmarked gjennom å legge til rette for:
>
> - Mer effektiv avregning.
> - Mer effektiv leverandørbytteprosess
> - Optimal tilpasning av forbruk og lokal produksjon.

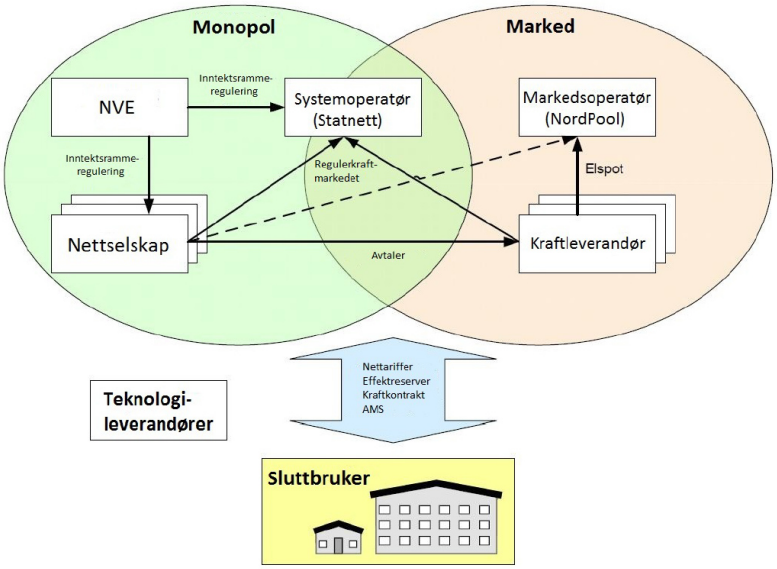
AMS gjennomføres ved at alle eldre kraftmålere blir erstattet med digitale smarte kraftmålere som muliggjør toveis kommunikasjon mellom sluttbrukerne og nettselskapet over et valgt kommunikasjonsmedium. Gjennom slik toveis kommunikasjon kan de smarte strømmålerene ikke bare tilby automatisk innrapportering av faktisk energiforbruk til nettselskapet, men også nødvendig funksjonalitet for å realisere konseptene for det smarte strømnettet beskrevet i seksjon 2.1. Selv om et fullt integrert smart strømnett er mange år fram i tid, vil den økte datamengden nettselskapene får tilgjengelig gjennom AMS også være verdifull for nettselskapene på kort sikt. Dagens distribusjonsnett er gammeldags og uintelligent noe som gjør at nettselskapene ikke til en hver tid har oversikt over nettets tilstand. AMS muliggjør dermed automatisk innrapportering av hendelser og parametre fra nettet som gjør at nettselskapet kan iverksette tiltak om nettilstanden er uten for akseptabelt område, e.g. trenger ikke sluttbrukere lenger å rapportere om bortfall av strøm da dette registreres og rapporteres automatisk til nettselskapet i nær sanntid. Gjennom at nettselskapene ved bruk av AMS automatisk får innrapportert data som forbrukstall samt nettets helse med høyere oppløsning enn tidligere, kan kraftproduksjon og distribusjon optimaliseres noe som vil gi bedre kvalitet på kraftleveransen.

Fra en sluttbrukers perspektiv vil AMS føre til forenklet administrering av kraftleveransen med hensyn til overgangen fra manuell til automatisert innrapportering av forbruk. Som nevnt ovenfor vil også kvaliteten på leveransen mest sannsynlig øke med tanke på økt informasjonsflyt mot nettselskapet om uakseptable forhold i nettet e.g. jordingsfeil, lav eller ingen spenning etc. I tillegg vil høyere tidsoppløsning på forbrukstall gjøre at fakturering av sluttbrukeren bli gjort på grunnlag av eksakt forbruk og kraftpris i forbrukstidspunktet.

AMS vil utgjøre en del av Advanced Metering Infrastructure (AMI). Et AMI vil utgjøre hele verdikjeden inkludert sluttbruker, kommunikasjonssystem, nettselskap samt alle systemene på nettselskapsiden som håndterer, prosesserer og benytter de innsamlede data for å tilby tjenester eller utføre oppgaver. E.g. vil et AMI omfatte alle komponenter fra sluttbrukerens smartmåler, som melder inn forbrukstall til nettselskapet, som videreformidler disse data til tredjeparts faktureringssystemer. AMS må ikke forveksles med Automatic Meter Reading (AMR). AMR er systemer som kun implementerer funksjonalitet for avlesning eller innrapportering av forbrukstall. AMR tilbyr dermed kun en delmengde av funksjonaliteten et AMS, hvor sentralisert styring ikke er støttet.

Det er ingen eksakte grenser for hvilke komponenter som inngår eller ikke inngår i AMS. Arbeidet presentert i denne rapporten definerer disse grensene ut ifra systemets formål og hovedfunksjonaliteter[1]. Dette utgjør sluttbruker inklusive smarte måler for kraft, sentralsystemet hos nettselskapet og kommunikasjonssystemene mellom måleren og nettselska-

[1] se seksjon 2.2.3



Figur 2.2: Oversikt og relasjonene i det norske kraftnettet [38]

pet. De forskjellige delene av systemet blir presentert i seksjon 2.3 mens dypere analyse av kommunikasjonssystemene blir presentert senere i kapittel 5 og 6.

2.2.2 Kraftsystemet i Norge

Globalt er det stor variasjon i hvordan ulike roller og ansvarsområder er fordelt blant aktørene i et kraftsystemet. I Norge er det mange aktører involvert i produksjon og distribusjon av kraft og det vil nå bli presentert de mest relevante for denne oppgaven og deres relasjoner, figur 2.2. Følgende seksjoner er hentet ut fra tidligere arbeid av undertegnede gjort i sammenheng med prosjektarbeid ved NTNU [43]. Norge fikk i 1990 *Energiloven*[2] [69], som deler ansvar mellom følgende aktører [43]:

2.2.2.1 Myndigheter

Olje- og Energidepartementet (OED) har det overordnede ansvaret i kraftsystemet og energiforsyningen, og skal tilrettelegge for en samordnet og helhetlig energipolitikk i Norge. Enova er et statsforetak under OED som skal fremme miljøvennlig produksjon og bruk av energi.

2.2.2.2 Regulerende myndighet

Det er NVE som har ansvar for de monopolistiske aktivitetene i systemet, det vil si systemoperatøren (Statnett) og nettselskapene. NVE er myndighetenes representant i kraftsystemet, og er ansvarlig for at lover og reguleringer følges, og at fellesskapets interesser blir

[2]Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.

tatt hensyn til. Regulatoren sikrer også at kraftnettet er tilgjengelig for enhver markedsaktør, samt kontrollerer tariffer og inntekter for nettselskapene (nettleie). NVE har også ansvaret for beredskapsplanleggingen, og skal lede landets kraftforsyning under beredskap og i krig.

2.2.2.3 Kraftforsyningens beredskapsorganisasjon

Kraftforsyningens beredskapsorganisasjon (KBO) består av NVE og alle enheter som eier eller har virksomhet innen kraftnettet med tilhørende vassdragsregulering, overføring og distribusjon av elektrisk kraft. Organisasjonen skal kunne løse oppgaver i forbindelse med rasjonering etter energiloven, ved terror- eller sabotasjeaksjoner, i fred ved skade på kraftanlegg som følge av naturgitte forhold og teknisk svikt. KBO skal sørge for å forberede, etablere og opprettholde en struktur som gir alle ledd i kraftforsyningen oppgaver og ansvar for å håndtere ekstraordinære situasjoner.

2.2.2.4 Sluttbruker

Sluttbruker er konsumenten eller kunden som forbruker strøm levert gjennom nettet. Dette kan også forstås som endepunktet som er koblet inn i kraftnettet og hvor et målepunkt registrerer effekten som sluttbrukeren tar ut av nettet. Kraft blir kjøpt basert på kraftkontrakter med kraftleverandøren, samt at nettleie blir betalt til sitt lokale nettselskap.

2.2.2.5 Nettselskaper

Nettselskapene er sluttbrukerens kontaktpunkt til kraftnettet. Disse er ansvarlige for drift og vedlikehold av distribusjonsnettet i sin region og står for investeringer for å koble kunder til nettet, i tillegg til å utvide nettkapasiteten dersom dette er nødvendig. Det er også nettselskapene som har ansvaret for måling og avregning i tillegg til overføring av kraft til sluttbrukere. Ettersom nettselskapene har monopol i sine regioner har sluttbrukere ingen alternativer til valg av nettselskap og er direkte bundet til det lokale nettselskapet.

2.2.2.6 Kraftprodusenter

Kraftprodusenter står for produksjonen av aktiv effekt, og for salg av energien på kraftmarkedet. Det har historisk vært betydelig konkurranse mellom forskjellige produsenter i det norske kraftmarkedet, men i etterkant av dereguleringen i 1990 har antallet fusjoner og oppkjøp tatt seg kraftig opp, og det er i dag Statkraft som er største aktør, med omlag 42% av produksjonskapasiteten [14].

2.2.2.7 Systemoperatøren

Har hovedansvar for overføringssikkerheten i nettet. I Norge er systemoperatøren Statnett, som sørger for time-for-time kraftbalansen, holder tilstrekkelig reservekapasitet i nettet, og sikrer at frekvensvariasjonene i nettet er på et akseptabelt nivå. Statnett drifter også sentralnettet, og og er ansvarlig for å utvikle og drifte det sentrale kraftnettet slik at det til enhver tid møter de kravene samfunnet har til energisektoren.

2.2.2.8 Kraftbørsen

Har ansvar for å motta salgs- og kjøpstilbud av kraft, og for å balansere markedet, og sørger dermed for optimal bruk av energiressursene. I det norske systemet er det den nordiske kraftbørsen Nord Pool ASA som står for både fysisk og finansiell handel. Hovedaktiviteten for børsen er driften av spotmarkedet, som klarerer pris og produksjon for påfølgende døgn, samt finansielle el-kontrakter.

2.2.2.9 Kraftleverandører

Strømleverandørene kjøper strøm via markedet, og videreselger til forbrukere og bedrifter. Historisk har man i Norge kjøpt strøm hos sin lokale tilbyder(da det var monopolistisk produksjon), men ifølge Energiloven skal man nå kunne kjøpe sin elektrisitet fra hvilken som helst strømleverandør, og nettselskapene plikter å levere strømmen uavhengig av hvem som selger denne.

2.2.3 Krav til AMS

Etter krav fra NVE er alle norske nettselskaper innen kraftbransjen pålagt å installere AMS for alle sine målepunkter innen 1.januar 2017. Det er store utgifter knyttet til utrullingen av AMS. Derfor er det viktig at utstyret og investeringene som gjøres oppfyller kravene fra alle de aktørene som er involvert. For systemer på størrelse med AMS er en slik prosess komplisert gjennom å kartlegge alle funksjonskrav, også med hensyn til eventuelle framtidige krav. Selv om det i første omgang settes endelige krav til AMS bør det derfor også tilrettelegges for mulige framtidige utvidelser. Om valg av utstyr viser seg i ettertid og ikke være tilstrekkelig for å utføre alle funksjonene det var tiltenkt, kan konsekvensene bli store ekstrakostnader eller at systemet ikke oppfyller sitt fulle potensialet.

I 2008 la NVE fram et forslag til endringer i *forskrift om måling, avregning og samordnet opptreden ved kraft omsetning og fakturering av nettjenester*. Dette forslaget ble lagt ut for høringer og var starten på en ekstern kartleggingsprosses i sammarbeid med aktører fra kraftindustrien i Norge vedrørende innføring av AMS [85]. I 2009 iverksatte NVE en tilleggshøring på nye forslag til endringer i forskriften basert på tilbakemeldinger fra første høring [86]. Juni 2011 kom en oppsummering av forgående høringsuttalelser og endelig forskriftstekst [87]. Høringene involverte representanter både fra kraftprodusenter, nettselskaper og forbrukere, samt representanter fra installatører og ulike utstyrsleverandører. Norske organisasjoner og initiativer for smarte strømnett samt rådgivningsbedrifter for energibransjen var også involvert. I endelig forskriftstekst statuerer NVE de foreløbige krav og funksjoner som AMS skal oppfylle ved utrullingen fram mot 2017. Det vil nå presenteres hvilke krav til IKT-systemet som stilles. Disse vurderingene er basert på forskrift om måling og avregning[3] [83], endelig forskriftstekst for AMS [87] og andre lover og forskrifter relatert til innføringen av AMS.

[3]Forskrift om måling, avregning og samordnet opptreden ved kraft omsetning og fakturering av nettjenester, 11.Mars 1999 nr 301

2.2.3.1 Funksjonskrav

Denne seksjonen vil presentere generelle Informasjons- og Kommunikasjonsteknologi (IKT)-relaterte funksjoner for AMS og ikke funksjoner knyttet til det elkrafttekniske. I Norge er har AMS to hovedfunksjonaliteter:

- Målefunksjon
- Styrefunksjon

Målefunksjonen utgjør mekanismene som måler forskjellige parametere i nettet og overfører disse data til nettselskap over valgt kommunikasjonssystem, e.g. forbrukstall, jordingsfeil, spenningsavvik etc. Styrefunksjonen er mer komplisert og kan grovt beskrives som muligheten for at nettselskapet skal kunne fjernstyre og konfigurere tilførselen for kraft hos hver sluttbruker. Sentral styring av enkeltlaster hos sluttbrukeren ses også på som en framtidig mulighet men i første omgang vil styring av energitilførsel per målepunkt være mest sentralt. Styring på grunnlag av forbruk og informasjon om priser den smarte strømleseren mottar, ses på en tilleggstjeneste sluttbrukeren kan oppnå gjennom installasjon av eget utstyr lokalt. Funksjonaliteten til slik utstyr beskrives dermed ikke av kravene til AMS.

NVE definerer i forskriftstekst fra 2008 følgende definisjon som vi også vil følge i denne oppgaven [85]:

> En funksjon er å forstå som én av mange enkelthandlinger som AMS-utstyret kan utføre, f.eks. å registrere og lagre energiforbruket.
>
> En oppgave er en tjeneste, et tiltak eller gjøremål som myndigheter har pålagt nettselskaper og andre å utføre, eller som en aktør gjør på eget initiativ. En oppgave kan f.eks. være avregning av en sluttbruker.
>
> Sammenhengen mellom funksjon og oppgave kan uttrykkes slik:
>
> $Oppgave_i = g(funksjon_1, funksjon_2, ..., funksjon_n)$

Av dette ser en at AMS skulle kunne utføre flere *oppgaver* hvor hver oppgave kan involvere én eller flere funksjoner. Videre har NVE delt de ulike oppgavene AMS skal kunne utføre i tre hovedgrupper;

Obligatoriske oppgaver Dette er oppgaver som danner minstekravet til systemet og må kunne gjennomføres fra første dag. Disse oppgavene vil sammen oppfylle hovedmålsettningen til AMS beskrevet i 2.2.1.

Valgfrie oppgaver Oppgaver eller tjenester sluttbrukeren kan kreve å få utført innen rimelig tid. Dette forutsetter da at systemet og utstyret som installeres må kunne tilpasses for å tilby disse oppgavene.

Mulige fremtidige oppgaver Dette er oppgaver som det kan komme pålegg om at AMS skulle kunne utføre i fremtiden. Ettersom det ennå er usikkert hvilke tjenester dette vil dreie seg om, kan det ikke settes krav til utstyr for å støtte slike tjenester fra

første dag eller uten installasjon av ekstra utstyr. Det stilles derimot som et kriteriet at utstyr som installeres ikke skal være absolutte minimumsløsninger, men også bør vurderes med tanke på utstyrets fleksibilitet og mulighet for senere utbyggelser.

Denne rapporten tar hovedsakelig for seg de aspekter som angår de obligatoriske og valgfrie oppgavene AMS skal kunne utføre. Da det ikke finnes noen definert liste over hvilke funksjoner AMS skal benytte vil det i denne oppgaven bli studert de antatte funksjonene AMS vil måtte tilby for å utføre disse oppgavene. Antatte funksjoner og oppgaver for AMS blir presentert i seksjon 4.2. Her følger en oppsummering av IKT-relatert funksjonalitet hentet fra NVEs endelige forskrift til AMS [87, 83].

To-veis kommunikasjon mellom sluttbruker og nettselskap

Om AMS skal nå sitt fulle potensialet i et smart strømnett vil to-veis kommunikasjon være sentralt[4]. NVE stiller krav til at AMS skal kunne formidle forbrukstall, kraftpriser, tariffer, styrings- og jordingsfeilsignaler via AMS-kanalen. Innrapportering av forbruksdata skal overføres til nettselskapet slik at de er tilgjengelige for kraftleverandører og sluttbrukere kl. 09:00 neste dag.

Tredjeparts tilgang

Det stilles ikke krav om at tredjeparts tjenesteleverandører skal ha tilgang til å benytte AMS-kanalen, men det tillates om nettselskapet ønsker dette. Derimot stilles det et krav om at det er nettselskapet som skal formidle informasjonen mellom tredjepart og sluttbruker om AMS-kanalen skal benyttes til slike tjenester. Om et nettselskap velger en slik løsning skal ikke kvaliteten av hovedoppgavene til AMS svekkes om tredjepartstjenester tillates i kanalen. NVE forventer dermed ikke at nettselskapene dimensjonerer kapasiteten utover behov for å oppnå hovedmålene.

Begrense eller bryte effektuttak

Alle målepunkter som installerer AMS skal kunne bryte eller begrense effektuttaket basert på styringssignaler mottatt.

Kommunikasjon med andre målere

Den smarte måleren skal kunne kobles til andre type målere og kommunisere data på vegne av disse gjennom et standard grensesnitt. Dette kan være målere for gass, vann, fjernvarme etc.

Eksternt grensesnitt

Det eksterne grensesnittet mellom smartmåleren og nettselskapet.

Lokalt grensesnitt

Kravene til kraftmåler for AMS definerer at det skal være et lokalt grensesnitt for tilkobling av eksternt utstyr. Dette spesielt med tanke på valgfrie tjenester. Dette kan være tilkobling av display for visning av kraftpriser og kobling imot enhet for styring av lokale laster basert på kraftpriser. Både kabel- og radioløsninger kan benyttes til dette formål. NVE stiller også krav til at nettselskapene tar hensyn til å benytte standardiserte løsninger for tilkobling av slik eksternt utstyr.

[4] se seksjon 2.1

Lagring av data lokalt

Den smarte måleren skal kunne lagre verdier lokalt inntil det er overført til nettselskapet. Det stilles også krav om at lagret data ikke skal gå tapt ved spenningsbrudd. Forbruksdata skal måles med en tidsoppløsning på minimum 15 minutter og maksimum på 60 minutter. Det stilles også krav om at det skal kunne registreres flyt av aktiv og reaktiv effekt i begge retninger.

2.2.3.2 Krav til informasjonssikkerhet

I endelig forskriftstekst, [87], stilles det i § 4-2 punkt g) følgende krav til informasjonssikkerhet:

> g) gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner

Dette er et generelt krav som er rettet til systemet i helhet og dermed samtidig pålagt alle del- og undersystemer. NVE sin kommentar til kravet er følgende [87]:

> Av bokstav g fremgår det at det er nettselskapets ansvar at AMS gir sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner. Dette må gjøres ved at kommunikasjonen i AMS foregår i et lukket nett som er stengt for uvedkommende eller ved at kommunikasjon over offentlige nett krypteres. De tiltak som velges bør være basert på analyser av sikkerhetssituasjonen i selskapet.

Det er også kommentert andre sikkerhetsrelaterte problemstillinger som er mer detaljerte og omfatter mindre AMS funksjoner og deres sårbarheter. Det blir nevnt at [87]:

- "Det er viktig at selskapene sikrer sine AMS-system mot uautorisert tilgang. Nettselskapene må derfor gjøre de tiltak som er nødvendige for å hindre at kundedata kommer på avveie eller at utstyret i AMS-systemet kan slås ut eller manipuleres. Blant annet er det grunn for å tro at en mulig sammensmelting av infrastrukturen for AMS og eksisterende og fremtidige driftskontrollsystemer, vil kunne innebære stor risiko. Derfor må kommunikasjonen mellom målerne og nettselskapene enten foregå i et lukket nett som er stengt for uvedkommende, eller at signalene krypteres dersom kommunikasjonen foregår over offentlig nett."
- "NVEs grunnleggende krav er at kommunikasjonsløsningene skal baseres på åpne standarder, slik at det er mulig med en tredjepartstilgang. Hvis selskapet imidlertid ser at sikkerheten til AMS-systemet blir best ivaretatt ved å benytte en proprietær kommunikasjonsprotokoll, plikter selskapet likevel å gjøre kommunikasjonsløsningen tilgjengelig for tredjepartsleverandører og samtidig oppfylle alle funksjons- og sikkerhetskrav."
- "NVE legger til grunn at alle selskapene gjennomfører grundige risiko- og sårbarhetsanalyser når de skal etablere sine AMS-løsninger. Selskapene må også, vurdere om hele eller deler av AMS-systemet vil omfattes av beredskapsforskriften. Hvilke konkrete løsninger selskapene velger, samt sikring av disse, skal være basert på disse analysene."

- "NVEs grunnleggende krav er at kommunikasjonsløsningene skal baseres på åpne standarder, slik at det er mulig med en tredjepartstilgang. Hvis selskapet imidlertid ser at sikkerheten til AMS-systemet blir best ivaretatt ved å benytte en proprietær kommunikasjonsprotokoll, plikter selskapet likevel å gjøre kommunikasjonsløsningen tilgjengelig for tredjepartsleverandører og samtidig oppfylle alle funksjons- og sikkerhetskrav."
- "Datatilsynet understreker behovet for å gjøre risikovurderinger og etablere tilgangskontroll når andre tjenesteleverandører gis tilgang til kommunikasjonsløsningen."

Denne rapporten vil ta for seg både funksjonskravene og kravene til informasjonssikkerhet for AMS. Kapittel 3 vil gi en innføring i de forskjellige områdene for informasjonssikkerhet innen AMS og kapittel 4, 5, 6 og 7 gjøre et dypere studie av informasjonssikkerhet for kommunikasjonsteknologi benyttet mellom sluttbrukeren og nettselskapet.

2.2.3.3 Dispensasjon for krav

I forskriftshøringene ble det diskutert dispensasjon av funksjonskrav. Dette ble diskutert på grunnlag av at enkelte nettselskaper allerede har innstallert AMS og mener det er urimelig at disse løsningene skal kasseres om de ikke tilfredsstiller alle nye funksjonskrav. NVE statuerer derfor som siste ledd i funksjonskravene følgende [87] :

> Norges vassdrags- og energidirektorat kan etter søknad i særlige tilfeller gi dispensasjon fra enkelte funksjonskrav.

NVEs kommentar er:

> Siste ledd åpner for at det kan gjøres unntak fra enkelte funksjonskrav etter søknad. Eventuelle unntak vil være knyttet til de funksjoner som har liten eller ingen nytte for kunden og at det derfor er samfunnsmessig rasjonelt å innvilge dispensasjon.

2.2.3.4 Beredskapsforskriften

Beredskapsforskriften [84] er pålagt alle enheter underliggende KBO og stiller klare krav til å arbeide systematisk for å forebygge og håndtere ekstraordinære hendelser som kan skade eller kan hindre produksjon, overføring eller fordeling av kraft. Forskriften omfatter både pro- og reaktive tiltak og setter krav til funksjon og overordnete mål framfor detaljer. Krav til organisatoriske aspekter ved drift, risiko- og sårbarhetsanalyse, retningslinjer for informasjonssikkerhet ved bruk av IKT er eksempler på proaktive tiltak. Krav til beredskapsplaner, prosedyrer for gjenoppretting av ressurser og innmelding av hendelser er eksempler på reaktive tiltak. NVE presiserer i 'Veiledning til forskrift om beredskap i kraftforsyningen' at "Risikovurderingene og valg av tiltak ut over minimumskravene, må hele tiden tilpasses endringer i trusselbildet, teknologi og organisasjon." [88]. Beredskapsforskriften er skrevet og tiltenkt kraftforsyningen slik den er organisert og strukturert før utrullingen av AMS. Om beredskapsforskriften skal omfatte AMS er ennå under diskusjon[5].

[5]Samtale med M. Bjartnes Line, SINTEF IKT, 13.desember 2011

2.2.3.5 Personsopplysningsloven

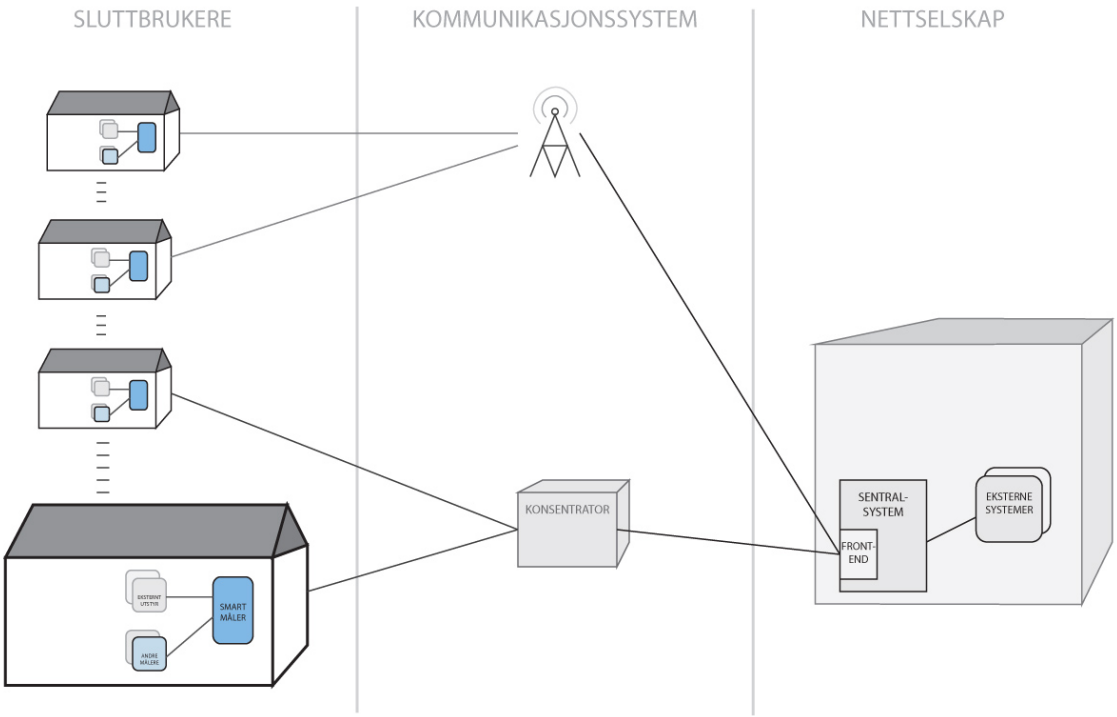
I dag er strømbruk i utgangspunktet knyttet til et målernummer hos sluttbrukeren på en bestemt adresse. Ved innføring av AMS vil den smarte måleren kunne knyttes til en enkeltperson og opplysninger tilgjengelig gjennom AMS kan dermed spores tilbake til en privatperson. I og med at det er nettselskapet som har *behandlingsansvar* for data tilgjengelig gjennom AMS har de også ansvar for å på se at håndtering av disse data er i henhold til personvern og *personopplysningsloven* [68]. Nettselskapene har ansvar for å kunne bekrefte hvilket formål ulike data som samles inn skal brukes til, samt at det må eksistere et rettslig grunnlag for behandling av personopplysninger. I tillegg til at slikt rettslig grunnlag krever samtykke fra sluttbrukeren, har også nettselskapet informasjonsplikt ovenfor sluttbrukerne med tanke på hvilke personvernskonsekvenser ved avtalen om behandling gir. I hovedsak har nettselskapene kun rett til å behandle personopplysninger om strømforbruk og opplysninger nødvendige for å fastsette riktig pris på strømleveransen. Nettselskapene må også sørge for tilfredstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengengelighet ved behandling av personopplysninger. Om nettselskapene skal benytte elektroniske hjelpemidler i behandlingen av personopplysninger må dette meldes til Datatilsynet minst 30 dager før behandlingen trer til. Dersom nettselskapet bruker underleverandører som behandler personopplysninger på vegne av selskapet, regnes leverandøren som en *databehandler* og egne skriftlige avtale må inngås. [22, 21]

2.3 Overordnet arkitektur

Det presenteres nå den overordnede arkitekturen for AMS. I denne rapporten deler vi AMS i tre hoveddeler; sluttbruker, kommunikasjonssystem og nettselskap. Denne seksjonen vil kun gi en oversikt over hvilke deler av systemet som utfører forskjellige oppgaver og hvordan delene er koblet sammen. Disse tre hoveddelene er illustrert i figur 2.3.

2.3.1 Sluttbruker

For enkelhets skyld beskrives en slutt-bruker som ett målepunkt i denne oppgaven. Sluttbrukersiden av AMS vil inkludere alle målepunktene som tilhører og får kraft levert gjennom det lokale nettselskapet. Én sluttbruker kan da ses på som et målepunkt med en tilhørende smart måler for kraft. En sluttbruker kan e.g. være en privat bolig som er koblet til og får levert kraft gjennom sitt lokale nettselskap. Hver elektroniske smart måler har grensesnitt både mot lokale enheter og grensesnitt mot kraftnettet. En smart måler for kraftdistribusjon vil hovedsakelig si en enhet som muliggjør toveis kommunikasjon med nettselskapet for å sende og motta data relatert til kraftleveringen. I tillegg til å ha kapasitet for å prosessere og lagre forbruksdata og styringssignaler, kan den også utføre transmisjon av data for andre enheter koblet til grensesnittene for lokalt utstyr. AMS er ikke unikt for kraftdistribusjon og benyttes også til for eksempel gass- eller vanndistribusjon. I slike flermåleroppsett er det mulighet for at andre målere benytter kommunikasjonsinfrastrukturen for AMS innen kraftdistribusjon ved å koble seg opp til smart måleren. Disse tilfellene vil ikke bli studert nærmere i denne oppgaven da den hovedsakelig ser på AMS innen kraftdistribusjon. Den



Figur 2.3: Overordnet AMS arkitektur

smarte måleren kommuniserer også med eksterne enheter lokalt. Disse grensesnittene kan brukes til tilleggsutstyr som for eksempel styring av lokale laster hos sluttbrukeren og display for visning av forbruksdata. Kommunikasjonen mot kraftnettet skjer hovedsakelig på to forskjellige måter. Enten går kommunikasjonen via dedikerte kanaler mot en nærliggende enhet, kalt konsentrator som står for videre kommunikasjon ut i nettet. For det andre alternativet brukes allerede eksisterende kanaler mellom sluttbruker og nettselskap, e.g. mobilnett som vist i figur 2.3.

2.3.2 Kommunikasjonssystem

I nettet mellom sluttbrukeren og nettselskapet skjer kommunikasjonen enten over dedikerte kanaler eller over allerede eksisterende kanaler, som vist i figur 5.2. For begge løsninger er både kabelbaserte og trådløse løsninger aktuelt. Kommunikasjonsstien går direkte mot nettselskapet eller alternativt indirekte gjennom bruk av konsentrator. En konsentrator er en enhet som oftest sitter i transformatorer nære målepunktet som samler opp data fra flere målepunkter og sender de inn til nettselskapet samlet. Konsentratorløsninger blir brukt om man benytter kraftnettet som kommunikasjonsmedie mellom smartmåleren og nettselskap. Denne løsningen er vanlig hvor mange målepunkter er geografisk tett samlet og hvor man vil minimere trafikk over en kanal mot nettselskapet, oftest over eksisterende nett enten med lav kapasitet eller hvor økning i trafikk utgjør økte utgifter. Kommunikasjonssystemet vil på denne måten utgjøre alt av kommunikasjonsnettverk mellom de smarte målerne hos sluttbrukerne helt til nettselskapenes systemer. Dette kommunikasjonsnettverket kaller vi

i denne oppgaven *AMS-kanalen*, da dette utgjør kanalen for kommunikasjon mellom smart måleren og nettselskapet. Analyse av AMS-kanalen blir presentert i kapittel 4, 5, 6 og 7.

2.3.3 Nettselskap

Som forklart kommuniserer nettselskapet med sluttbrukere på flere måter, enten gjennom dedikerte løsninger eller gjennom eksisterende kommunikasjonsnett. På nettselskapsiden er flere systemer som er involvert. All kommunikasjon mellom kommunikasjonssystemet og systemene på nettselskapsiden håndteres av det som kalles et *sentralsystem*. Et slikt sentralsystem har grensesnitt både mot kommunikasjonssystemet og andre systemer på nettselskapsiden. Grensesnittet mot kommunikasjonssystemet heter *frontend*-systemer[6]. Frontend-systemene er ofte leverandørspesifikke og står for tolking og oversetting av dataformater, samt prosessering av rådata. Dette tillater at systemene på nettselskapsiden ikke trenger å ta hensyn til hvilke teknologier og dataformater som benyttes i AMS-kanalen, men kun å være kompatibelt med grensesnittet mot sentralsystemet.

Det er sentralsystemet som håndterer og videresender all informasjon og data relatert til smart måleren, i tillegg til konfigurasjoner og oppsett av alle systemkomponentene. I de fleste tilfeller utfører sentralsystemet oppgaver på oppdrag mottatt via meldinger og kommandoer fra eksterne systemer, samt returnerer resultater mottatt fra AMS-kanalen tilbake til de eksterne systemene. I noen tilfeller kan sentralsystemet delegere deler av sine oppgaver til konsentratorer i nettet for å minimere kommunikasjon i nettet. I slike oppsett vil konsentratoren motta, reagere og utføre oppgaver på vegne av sentralsystemet. Sentralsystemet har grensesnitt ut mot eksterne kommersielle systemer. Dette er faktureringssystemer, systemer for lagring av måleverdier, systemer for nettverksovervåkning, systemer for vedlikehold og kontroll av nettverkskomponenter i kraftnettet etc. Sentralsystemet utfører oppgaven med å knytte disse systemene sammen med kraftnettkomponentene og har en form for styrefunksjon ved å koordinere og delegere de riktige oppgaver til riktige komponenter ute i nettet. På denne måten trenger ikke de kommersielle systemene å tilrettelegge eller ha kjennskap til selve kommunikasjonen i nettet utover mot sentralsystemet. Selv om de eksterne systemene på nettselskapsiden ikke nødvendig vis er eid og driftet av nettselskapet forholder vi oss til en slik modell når det gjelder nettverket bak sentralsystemet. Dette er kun for å forenkle modellen, til tross for at de forskjellige systemene og tjenestene på denne siden kan være distribuert til mange forskjellige aktører.

[6] også kalt *headend*

Kapittel 3

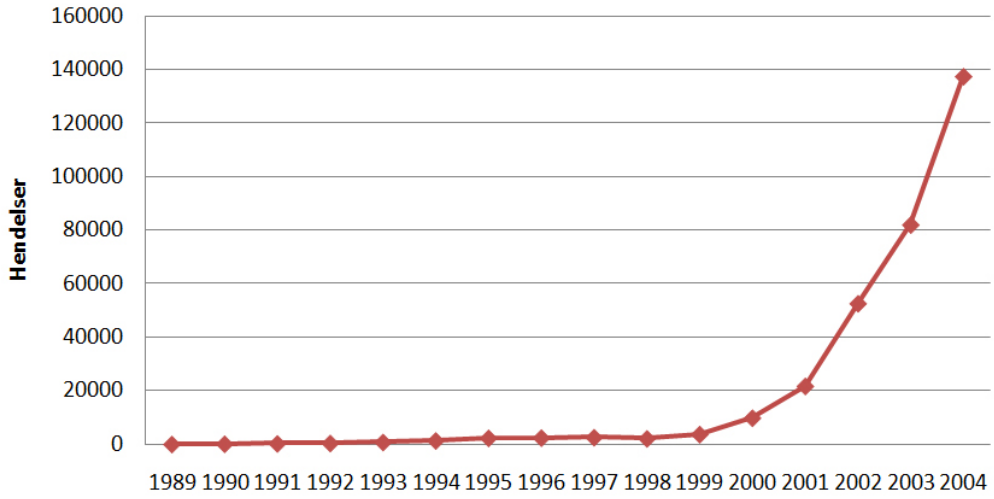
Informasjonssikkerhet innen AMS

Studiene av krav til AMS i forrige kapittel viser at informasjonssikkerheten i AMS håndteres i forhold til flere aktører. Det vil i dette kapittelet bli presentert en introduksjon til arbeid for informasjonssikkerhet før områdene relatert til AMS blir introdusert.

3.1 Introduksjon til informasjonssikkerhet

Da de første digitale datamaskinene ble tatt i bruk var ikke informasjonssikkerhet et relevant tema, da slike maskiner oftest var isolerte enheter med god fysisk sikring i kontorkomplekser etc. Den teknologiske utviklingen av disse maskinene førte raskt til at Informasjons Teknologi (IT) stadig ble benyttet i nye kontekster da maskinene ble fysisk mindre, rimeligere og kraftigere med tanke på prosesseringskraft og lagringsplass. Økt bruk av IT førte videre til dannelsen av lokale datanettverk som senere ble koblet sammen og er forgjengeren til det vi i dag ser på som Internett. Det var med denne utviklingen av telekommunikasjon, i tråd med at datasystemene ble mer fysisk eksponert, som ga initiativ og viste nødvendigheten med mer fokus på informasjonssikkerhet. Som et resultat ble den første Request For Comment (RFC) vedrørende økt sikkerhet i arkitekturen for Internett RFC1636 publisert i 1994. Som en indikator på økningen av trusler mot IKT systemer kan man benytte statistikk over rapporterte informasjonssikkerhetshendelser. Computer Emergency Response Team Coordination Center (CERT/CC) fører slik statistikk på aspekter relatert til informasjonssikkerhet og figur 3.1 viser utviklingen av rapporterte ondartede Internettrelaterte hendelser fra 1988 til 2004. Disse tallene er basert på hendelser som Denial of Service (DoS)-angrep, avlytting og IP-spoofing. Da tallene er basert kun på innrapporterte tilfeller, antas de virkelige tallene å være mye større men relativt til økningen vist i denne statistikken. CERT/CC sluttet å publisere tall over slike hendelser etter 2004. Årsaken til dette er den økende bruken av automatiserte angrepsverktøy som har gjort slike angrep såpass frekvent og normalt at nytteverdien for slike statistiske tall har sunket [16]. Antall angrep og relaterte hendelser har vokst i samsvar med økt trafikk og nye bruksområder for Internett samt økt kompleksitet av protokoller og applikasjoner [82]. Samtidig baserer flere og flere systemer seg på kommunikasjon over Internett hvor mange hviler på sikkerheten i nett og nettprotokollene mens enkelte implementerer sikre ende-til-ende forbindelser for å minimere sjansen for angrep. Naturen av forskjellige angrep på informasjonssystemer har også gjennomgått en utvikling. Tidlige angrep baserte seg på å utnytte enkle hull i programvare og protokoller i applikasjonslaget, mens man i dag finner sofistikerte komplekse angrep som baserer seg på designsvakheter på tvers av flere protokollag samtidig, fra fysisk kretsdesign til applikasjonslag. I tillegg til disse teknologiske designmessige aspektene har det i de senere år blitt økt fokus på det administrative og organisatoriske rundt håndtering av slike informasjonssystemer, også kalt *social engineering*-angrep. Ikke alle trusler trenger å være fra eksterne angrep. Også autoriserte brukere av systemer kan være trusler mot informasjonssikkerheten da de e.g. kan utnytte rettigheter til ondartede hensikter, eller eventuelt ha gitt rettigheter til uautoriserte brukere ved på ett eller annet vis ha delt hemmelige systempassord.

Slik har utfordringene innen informasjonssikkerhet gått fra stort sett å være basert på sikring av fysisk tilgang, til å bli et komplekst tverrfagelig felt som inkluderer de fleste ledd fra produksjon av systemkomponenter til prosedyrer for håndtering av informasjonssystemene samt administrative prinsipper. Ettersom innføringen av AMS vil være en inte-



Figur 3.1: Innrapporterte ondartede Internettrelaterte hendelser fra 1988 til 2004, CERT/CC [16]

grering av et distribuert informasjonssystem i det eksisterende kraftnettet bør derfor alle disse aspektene inkluderes i en vurdering av informasjonssikkerheten av AMS.

3.1.1 Begreper innen informasjonssikkerhet

Det er ingen universelle definisjoner for begreper innen informasjonssikkerhet. Denne seksjonen definerer derfor disse begrepene for å unngå tvetydighet samt å gi leseren en konkret beskrivelse av hvordan begrepene er benyttet i denne oppgaven. Definisjonene er basert på beskrivelsene av Stallings [82], som videre er basert på RFC 2828 [78].

3.1.1.1 Sikkerhet, sikkerhetstjenester og sikkerhetsmekanismer

Ordet *sikkerhet* er i det norske språk kontekstavhengig og kan ha flere betydning i forskjellige sammenhenger. I denne rapporten bruker vi ordet om sikring mot tilsiktede hendelser, e.g. kriminalitet, spionasje, sabotasje, terrorisme. En *sikkerhetsmekanisme* er en prosess som er designet til å detektere, forhindre, eller gjenopprette et system til opprinnelig tilstand med hensyn til sikkerhetsangrep. Sikkerhetsmekanismer i IT systemer kan være kryptering, digitale signaturer, autentiseringsprotokoller etc. En *sikkerhetstjeneste* benytter en eller flere sikkerhetsmekanismer for å skape en tjeneste for informasjonssikkerhet. Om sikkerhetsmekanismer benyttes korrekt kan man da oppnå sikkerhetstjenester som konfidensialitet, integritet, autentisering, aksesskontroll etc. *Ikke-fornektelse* er enkelte ganger sett på som en sikkerhetstjeneste. Ikke-fornektelse vil si en tjeneste som hindrer en bruker å nekte utførelsen av en oppgave. Ettersom dette er en tjeneste ofte tilbudt internt i systemer, ikke kommunikasjonskanaler, diskuteres ikke denne tjenesten ettersom den anses å bli tatt hånd om av endesystemene i AMS og ikke i AMS-kanalen alene.

Integritet

Stallings beskriver *autentisering* som en egen sikkerhetstjeneste som tar hånd om ektheten for mottaker og avsender. I vår definisjon av integritet inkluderer vi autentisering av sender, mottaker og ekthet av datastrøm. I enkelte tilfeller hvor autentisering av avsender/mottaker gjøres separat fra integritetssjekk av meldingsinnhold, vil de forskjellige tjenestene bli diskutert hver for seg.

Integritet er å kunne garantere at data mottatt er eksakt lik data sendt av en autorisert sender. Dette betyr at mottatte data ikke skal være utsatt for uautoriserte modifikasjoner. Dette begrepet inkluderer forfalsket data, sletting av data og duplikatmeldinger. Integritet går på ekthet av data, at data sendt ikke er fullstendig eller delvis modifisert, at avsender og mottaker ikke er autentiske, og at flyten av meldinger ikke er endret.

Konfidensialitet

Konfidensialitet beskytter data mot passive angrep som uautorisert innsyn, overvåkning etc. Når en garanterer konfidensialitet vil ingen informasjon om kommunikasjon mellom sender og mottaker være tilgjengelig gjennom passive angrep.

Tilgjengelighet

Tilgjengelighet er sikkerhet for at et system, eller en systemtjeneste, er tilgjengelig og mulig å benytte ved etterspørsel fra autoriserte brukere, i henhold til systemets krav til ytelse. Tilgjengelighet vil derfor si sikring mot uautoriserte handlinger som svekker tilgjengeligheten eller ytelsen ved en tjeneste for autoriserte brukere.

3.1.1.2 Angrep

Vi henter definisjonen av et *angrep* fra RFC 2828, *Internet Security Glossary* [78]:

> An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

3.1.1.3 Trussel

Vi henter definisjonen av en *trussel* fra RFC 2828 [78].

> A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. (...) That is, a threat is a possible danger that might exploit a vulnerability.

3.1.1.4 Sårbarhet

Vi henter definisjonen av en *sårbarhet* fra RFC 2828 [78].

> A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy. (...) If the attacks needed to exploit a vulnerability are very difficult to carry out, then the vulnerability may be tolerable. If the perceived benefit to an attacker is small, then even an easily exploited vulnerability may be tolerable.

3.1.1.5 Konsekvens

En *konsekvens* vil si de direkte og indirekte følgene av et angrep. Et angrep trenger ikke å være suksessfullt for å få konsekvenser, også angrep som blir hindret underveis kan få følger og konsekvenser.

3.2 Motivasjon for informasjonssikkerhet i AMS

3. september 1999 nedsatte Regjeringen Bondevik et tverrpolitisk sammensatt utvalg under ledelse av Kåre Willoch; *Sårbarhetsutvalget*. Utvalget fikk i oppgave å "utrede samfunnets sårbarhet med sikte på å styrke samfunnets sikkerhet og beredskap". På grunnlag av utvalgets arbeid ble utredningen 'NOU 2000:24 - Et sårbart sammfunn' publisert 4.juli 2000. I denne utredningen presiseres samfunnets avhengighet til nasjonal kritisk infrastruktur, hvorav avhengigheten til infrastruktur for telekommunikasjon og kraftforsyning var størst og blir kalt "bæresøylene" i et moderne samfunn. Utredningen presiserte også at det eksisterte gjensidig avhengighet mellom disse infrastrukturene. I sammendraget av utredningen skrives det under seksjon '1.2 Sårbarheten og de fremtidige utfordringene' følgende [75]:

> Dagens samfunn er mer sårbart enn før. En svikt i noen få avgjørende samfunnsfunksjoner kan føre til at store deler av samfunnet får omfattende problemer. Svikt i telekommunikasjon og kraftforsyning kan virke spesielt lammende på samfunnet. Forhold som bidrar til at vi står overfor nye sårbarhet- og sikkerhetsutfordringer er blant annet:
>
> - De teknologiske endringene.
> - Den økende kompleksiteten i samfunnet.
> - Det økende kostnads- og effektiviseringspresset.
> - Reduksjonene i bemanningen i mange virksomheter.
> - Utsettingen av offentlige tjenester til kommersielle virksomheter.
>
> Sikkerhetsutfordringene er betydelig forandret i forhold til bare for noen få år siden. Når det gjelder bevisste handlinger (for eksempel sabotasje eller terrorisme), er trusselbildet preget av en forskyvning fra det manuelle mot det elektroniske. De store endringene i bruken av informasjons- og kommunikasjonsteknologi endrer betydningen av landegrensene i sikkerhets- og beredskapssammenheng.

Utredningen utdyper også den økende bruken av IKT systemer i kraftsektoren. Denne koblingen ble sett på som så viktig for samfunnets sikkerhet at et eget kapittel ble dedikert til å diskutere nye sårbarheter dette medførte[1]. Spesielt ble det påpekt at sårbarheten ved bruk av kontroll- og styringssystemer, også kalt Supervisory Control And Data Acquisition (SCADA), innen kraftproduksjon samt at angrep mot slike IKT systemer i enkelte tilfeller kan få samfunnsmessige konsekvenser. Bruk av SCADA systemer i kraftbransjen blir benyttet effektivsere driften ved å innføre løsninger som muliggjør sentralisert styring av e.g. kraftproduksjon ved hjelp av IKT. Selv om arbeidet presentert i utredningen ikke var basert på innføring av AMS, er mange av vurderingene sentrale. Karakteristikken for

[1] *J. Hovden*, samtale, 10.november 2011, Gløshaugen, Trondheim

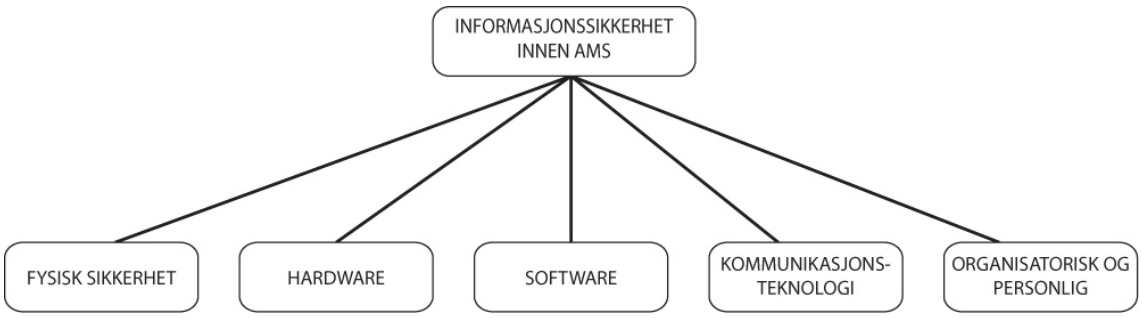
AMS og SCADA må anses å være meget lik med tanke på sårbarheter og avhengighet mellom kraftforsyning og IKT. I likhet med SCADA benytter også AMS IKT for å oppnå effektivisering i form av automatisert og sentralisert styring og administrasjon av kraftforsyning til sluttbrukere. En kan si at innføringen av AMS vil føre til sterkere koblinger mellom IKT og kraftforsyningen, samt at angrepsoverflaten for begge infrastrukturene øker drastisk. Sårbarhetsutvalget skriver [75]:

> IKT-systemene er kommersielle systemer med åpen arkitektur basert på internasjonale standarder, og gjør systemene mer sårbare både overfor angrep fra innsiden og angrep utenfra. Et stort antall datamaskiner knyttes sammen i nett ved å benytte både offentlige teletjenester og kraftforsyningens eget telenett. Angrep utenfra er mulig fordi en i dagens kraftforsyning har behov for å knytte IKT-systemer og nettverk sammen, det vil si mer utstrakt bruk av åpne nett. Dette innebærer i prinsippet at det er en sammenkobling av driftssystemene for kraftforsyningen og verden for øvrig. Man blir ofte nødt til å inngå kompromisser mellom funksjonalitet og sikkerhet. Det finnes få relevante krav til aktørene som sikrer et tilstrekkelig sikkerhetsnivå.
>
> Fra produksjonsverkene går den elektriske energien via overføringsnett og distribusjonsnett ut til den enkelte abonnent. I takt med økende effektivisering er IKT-avhengigheten i driften av overføringsnettene økende, og dermed også potensielt IKT-sårbarheten.

Sitatet påpeker nødvendigheten med å sikre funksjonaliteten for AMS samt sårbarheten som innføres ved å benytte åpne nett for kommunikasjon i slike distribuerte systemer. Omfang og type av angrep mot kontroll- og styringssystemer i kraftbransjen varierer men utredningen utdyper viktigheten ved integritet av kommunikasjon samt risikoen ved uautorisert tilgang til styrings- og konfigureringsfunksjonalitet. Utredningen presiserer også kompleksiteten ved automatisering av utstyr og prosesser for styring, samt integriteten av datagrunnlag for slik automasjon.

AMS er fundamentet for framtidens *smarte strømnett* og AMS vil i framtiden bli benyttet i mange nye sammenhenger for å realisere oppgaver innen energi- og kraftsektoren. Man vet derfor ikke hvilke krav til informasjonssikkerhet et framtidig scenario vil sette. Derimot kan man ta utgangspunkt i dagens situasjon og gjøre systemet fleksibelt for utvidelser slik at framtidige krav og behov kan oppfylles. I 2010 publiserte National Institute of Standards and Technology (NIST) rapporten 'NISTIR 7628:Guidelines for Smart Grid Cyber Security' [40]. Her beskriver NIST at det ikke er et spørsmål *om* komponenter og enheter av et smart strømnett vil bli utsatt for IKT-angrep, men kun et spørsmål om *når*. Dette begrunnes med økende angrepsoverflate, økende trusselbilde samt teknologisk utvikling og økt produksjon av spesialdesignede verktøy for IKT-angrep. M/411 er et mandat fra Europakommisjonen med formål å standardisere kommunikasjon og funksjonalitet for smartmålere i Europa. OPENmeter er en organisasjon dannet i sammenheng med M/441, med mål om å spesifisere et sett med standarder for AMS. OPENmeter skriver følgende om informasjonssikkerhet i AMS [60] :

> Cyber-security is a well known issue in classical IT systems. For some years, there has been a growing interest in cyber-security concerning industrial systems which are more complex, independent and interconnected.



Figur 3.2: Områder for informasjonssikkerhet innen AMS

> Authorities put a special emphasize on Critical Infrastructure Protection and Industrial Automation Control Systems, especially infrastructure supporting energy, transport, telecommunications, and water. At the moment, collaboration between European countries is being organized, and special directives about security of vital infrastructures are likely to be enforced.

Av denne seksjonen ser en at innføring av AMS innfører en sammfunnsmessig risiko med hensyn til økt angrepsoverflate for kritisk infrastruktur. I sammenheng med et stadig økende trusselbilde og framtidig bruk av AMS i det smarte strømnettet, bør arbeid for sikring av systemet samt tilhørende funksjoner prioriteres.

3.3 Forskjellige områder for informasjonssikkerhet innen AMS

Denne seksjonen vil gi en innføring i hvilke forskjellige områder for informasjonssikkerhet som må håndteres i sammenheng med innføringen av AMS. For hvert område skisseres grovt sentrale problemstillinger og enkelte eksempler på trusler og utfordringer. Det presenteres i denne seksjonen kun en innføring til de forskjellige områdene mens resterende kapitler av denne oppgaven presenterer en dypere analyse av informasjonssikkerhet for AMS-kanalen. De følgende områdene vil nå bli presentert, vist i figur 3.2: fysisk sikkerhet, hardware, software og kommunikasjonsteknologi og administrativt/organisatorisk domenet.

3.3.1 Fysisk sikkerhet

Område for fysisk sikkerhet omfatter aspekter om hvorvidt systemelementene er tilstrekkelig fysisk sikret i.e. utilgjenglig for uvedkommende og uautoriserte brukere. Koblinger mellom systemelementene ses også på som en komponent av nettverket og er oftest de komponentene som er mest eksponert. For distribuerte systemer som utnytter datanettverk mellom systemkomponentene er denne problemstillingen essensiell da komponenter kan være eksponert for fysiske angrep. Fysiske angrep er e.g. tyveri av komponenter for å ekstrahere data, fysisk modifikasjoner av utstyr for uautorisert tilgang til kommunikasjonsnettet og fysisk destruksjon av utstyr.

Relatert til AMS

Fysisk sikring av alle komponenter i et nettverk er sentralt. I AMS gjelder dette alle komponentene på både sluttbruker, kommunikasjonssystem og nettselskap, vist i figur 2.3. På nettselskapsiden av systemet er som oftest de fleste komponentene sikret fysisk ved at de er installert i komplekser med tilstrekkelig sikring og aksesskontroll. Dette gjelder derimot ikke alltid for komponenter hos sluttbrukere og i kommunikasjonssystemet. I Norge er stort sett alle kraftmålere montert innendørs i bygninger med en form for sikring eller adgangskontroll, i motsetning til i andre land hvor strømmålere er montert på utsiden av bygg med hensyn til manuell avlesning utført av kraftselskapene. For kommunikasjonssystemet er grad av fysisk eksponering avhenging av hvordan kommunikasjon med mellom sluttbruker og nettselskapet skjer; direkte til nettselskapet eller indirekte via konsentrator, trådløs eller kabelbasert, driftet av tredjepart eller av nettselskapet selv. Konsentratorer er ofte lokalisert på steder kun med passiv sikring i form av ubemannede transformator stasjoner etc. Uansett hvilke løsninger som benyttes er det kommunikasjonssystemet i AMS som er mest fysisk eksponert. Koblingen mellom sluttbrukere og nettselskapet varierer men strekker seg som oftest over store geografiske områder, gjennom kommunikasjonsnett med varierende fysisk sikring.

3.3.2 Hardware

Området for hardware omhandler design av utstyr på komponentnivå. Seksjon 3.1 fortalte at nye angrepsmetoder utnytter alle svakheter ved IT systemer, uansett lagnivå. Grundige studier av nye systemer kartlegger alle svakheter ved systemkomponentene samt deres relasjoner. En type av slike studier kalles *reverse engineering*. For å utnytte kunnskap om svakheter på hardware design til et angrep krever det oftest fysisk tilgang til komponentene det gjelder.

Relatert til AMS

I likhet med domenet for fysisk sikring gjelder også sikker design av hardware for alle komponentene for sluttbruker, kommunikasjonssystem og nettselskap. Sikker hardware dreier seg om hvor moden teknologien som benyttes er med tanke på sikkerhet, samt hvor eksponert de aktuelle komponentene er for fysiske angripere. For komponenter og systemer på nettselskapsiden benyttes ofte tradisjonelt utstyr for datasentre. Slikt utstyr er ofte godt etablert i industrien med god modenhet og god fysisk sikring. Det vil si at om disse komponentene har designmessige svakheter vil det være vanskelig for en angriper å utnytte disse svakhetene da den fysiske tilgangen til utstyret vil være begrenset. For kommunikasjonssystemet vil økt fysisk eksponering føre til økt sannsynlighet for å utnytte svakheter i hardware. For de smarte målerne og tilkoblet eksternt utstyr er teknologien ennå ung og mange nye komponenter designes fortløpende i trinn med økt etterspørsel. Mangel på entydige standarder og krav i bransjen gjør at mange forskjellige design utvikles uten at sikkerheten vurderes godt nok. Det finnes allerede flere rapporter på at slike designmessige svakheter i hardware kan utnyttes til angrep som har konsekvenser for informasjonssikkerheten. [95, 23]. Ettersom tilgjengeligheten til slikt utstyr er veldig god, da målerne er lokalisert hos sluttbrukerne, kan en anta at slike angrep er sannsynlige.

3.3.3 Software

Sikkerhetshull i ny programvare forekommer ofte. En sentral forskjellen mellom designfeil i software og hardware er at feil i hardwarekomponter er permanente mens feil og sårbarheter i software som oftest kan håndteres gjennom oppdatering av firmware eller patcher. Derfor er det viktig å minimere designmessige feil fra hardware, ettersom eventuelle svakheter i software kan håndteres av softwareoppdateringer. Det må også presiseres at i motsetning til fysiske angrep på hardware, som oftest er visuelle, kan hull i software og på logiske nivå ikke være merkbare uten dypere analyse av programkode.

Relatert til AMS

Som for fysisk sikkerhet og for sikker design av hardware, gjelder også sikker design og implementasjon av software, alle komponentene i AMS. I liket med design av hardware, vil også nivået av modenhet i softwaredesign varierer mellom de forskjellige delene av AMS. Man kan anta at svakheter i sikkerhet vil forekomme for software i alle komponenter i AMS, spesielt i de større datasystemene hos nettselskapet. Selv om tradisjonelle sikkerhetsmekanismer for datasentre kan benyttes i enkelte sammenhenger vil AMS kreve at nettselskapene tar i bruk mange nye systemer for å håndtere kommunikasjonen med sluttbrukerne. I mange tilfeller vil nye systemer måtte utvikles og tilpasses. Slike systemer vil være svært omfattende og komplekse som fører til utfordringer med hensyn til sikkerheten. Kompleksitet gjennom integrasjon av mange forskjellige funksjoner og eksterne systemer fører til sikkerhetsutfordringer. Et slikt system involverer mange aktører og grensesnitt mot deres systemer som må sikres. Sikker design av software for de smarte målerne vil være en utfordring. Produksjonskostnadene for målere skal være lav, som videre går utover funksjonalitet og kapasitet. Målerne vil mest sannsynlig ha strenge rammer for kapasitet i form av prosseseringskraft, lagringskapasitet etc. som igjen setter begrensninger for hvilke oppdatering av software som er mulige. Ettersom muligheten for softwareoppdateringer er essensielt for informasjonssikkerheten bør kapasiteten og ytelsen av hardwarekomponentene ikke dimensjoneres for lavt slik at det settes for strenge rammer for mulige oppdateringer.

3.3.4 Kommunikasjonsteknologi

Domene for kommunikasjonsteknologi kan deles opp i tre underdeler; sluttbruker, kommunikasjonssystem og nettselskap. Ettersom resterende kapitler av denne oppgaven omhandler kommunikasjon i AMS henvises det til de respektive kapitlene for nærmere diskusjon.

Sluttbruker Kommunikasjon mellom enheter hos sluttbrukeren av AMS, også kalt Home Area Network (HAN). Dette involverer kommunikasjon med lokale enheter og er til dels inkludert i et AMS. Et helt den smarte måleren skal kunne kommunisere med lokalt utstyr og andre målere, og det er kommunikasjonen mot disse komponentene som må sikres gjennom AMS. Nettverket bak disse komponentene er ikke en del av AMS og diskuteres dermed ikke i denne oppgaven.

Kommunikasjonssystem Kommunikasjon mellom den smarte måleren og sentralsystemet, også kalt AMS-kanalen. En analyse av informasjonssikkerheten i AMS-kanalen blir presentert i kapittel 4 og 6 og vil ikke bli beskrevet i denne seksjonen.

Nettselskap Kommunikasjon mellom systemer og aktører bak sentralsystemet hos nettselskapet. Ettersom sammensetningen av systemer og aktører bak sentralsystemet ikke er entydig og vil varierer fra nettselskap til nettselskap beskrives ikke slik kommunikasjon nærmere i denne seksjonen. Det henvises til resterende kapitler av denne oppgaven, da prinsipper for sikker kommunikasjon vil være lik og mange løsninger også kan være aktuelle for kommunikasjon bak nettselskapet.

3.3.5 Organisatorisk og personlig

Et av de største paradigmeskiftene innen informasjonssikkerhet er oppfattelsen av at informasjonssikkerhet ikke er et utelukkende teknisk problem, men en utfordring som også omfatter det personlige, organisatoriske i tillegg til den tekniske sikkerheten. Tett knyttet til brukeradferd er også organisasjons kultur og fokus på informasjonssikkerhet, hvor brukere og ansatte ikke bare er passive observanter men aktive deltakere for å oppnå informasjonssikkerhet [94].

Det må presiseres hvordan relevans organisatorisk informasjonssikkerhet har til de fundamentale sikkerhetsmekanismer for et informasjonssystem. Når en ser på alle sikkerhetstiltakene for et system, gjør de forskjellige mekanismene hver sin oppgave for å forsikre at uautoriserte brukere ikke får tilgang til systemets informasjon og funksjoner. Disse funksjonene baserer seg videre på at autoriserte brukerne håndterer systemet på riktig måte slik at nivået av sikkerhet blir ivaretatt. Derfor behøves det faste prinsipper og retningslinjer for hvordan brukere skal opptre for at riktig nivå av sikkerhet skal oppnås. Hovedpunktene for organisatorisk og personlig sikkerhet som bør håndteres er:

System aksess Beskrivelse og rettigheter for brukere av systemet. Videre inkluderer systemaksess også identifisering og autentisering av brukere, autorisering og redegjørelse for brukeres handlinger i systemet.

Prosedyrer Prosedyrer beskriver hva som skal gjennomføres og rapporteres ved forskjellige hendelser. For informasjonssystemer kan dette være prosedyrer for håndtering av adgangskort, frekvent utskifting av brukerpassord, innrapportering av brudd på sikkerhets reglement, dataangrep etc. De definerte prosedyrene skal beskrive i detalj hva som bør gjennomføres og iverksettes for slike hendelser. Da det ikke er mulig å skape en liste over alle scenarioer som kan oppstå bør det også være anbefalinger om prosedyrer for uventede situasjoner med kontaktpersoner for hvert ansvarsområde.

Prinsipper og retningslinjer Alle systemer skal ha et sett grunnregler og prinsipper som definerer nivået av informasjonssikkerhet for systemet. Disse prinsippene bør konkret definere hvilke rammer som er satt for bruk av systemets funksjoner og data. Prinsipper og retningslinjer kan varierer i natur og kan omhandle alt fra tilkobling av utstyr til lagring og distribusjon av data.

God brukeradferd For et system, er til sluttbrukernes handlinger som avgjør nivået for informasjonssikkerhet som oppnås. I et system som teknisk sett er sikret er det opp til brukerne å følge de retningslinjene og reglene som er satt for bruken av systemet. En barriere eller mekanisme for å forhindre et hendelsesforløp er nytteløs om en bruker velger å unngå disse tiltakene. På denne måten, er god brukeradferd og

holdninger den viktigste komponenten i sikkerhetssammenheng. God brukeradferd oppnås om brukerne har god forståelse av risikoen knyttet til bruk av systemet, hvilke sikkerhetsmekanismer som er implementert samt deres hensikt. Om dette gjøres på rett måte kan riktig brukeradferd bli det mest effektive virkemiddelet for å oppnå god informasjonssikkerhet [94].

Relatert til AMS

Punktene nevnt med relevans for dette domenet er generelt for alle informasjonssystemer. Unikt for AMS er antall eksterne aktører knyttet til AMS, spesielt i nettverket bak nettselskapet, beskrevet i seksjon 2.3.3. For hver aktør som utnytter systemet varierer rettigheter til funksjoner og tilgjengelig informasjon. Utfordringen for organisatorisk sikkerhet blir da å koordinere de nevnte punktene på tvers av alle disse aktørene på en slik måte at det ikke går utover informasjonssikkerheten og kravene satt til AMS. En annen utfordring er omstruktureringene i kraftmarkedet som skjer med innføringen av AMS. Nettselskapene står nå ansvarlig for informasjon som sendes gjennom kommunikasjonssystemet og at denne kommunikasjonen sikres. På en slik måte må nettselskapene forholde seg til informasjonssikkerhet på et annet vis enn tidligere. Det finnes standarder som beskriver organisatorisk sikkerhet. ISO/IEC 27000 er en standard som gir anbefalinger på håndtering av informasjonssikkerhet på det organisatoriske plan som passer for virksomheter i alle størrelser [26].

Kapittel 4

Vurdering av trusler mot AMS-kanalen

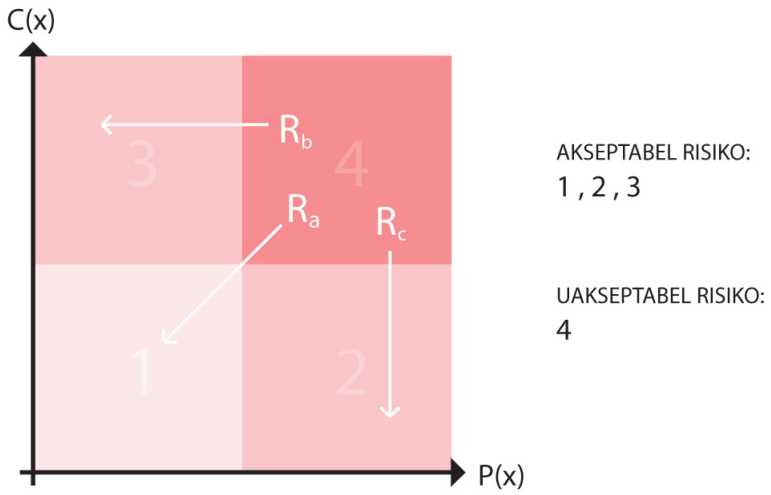
Det fundamentale for sikkerhet i et distribuert system som AMS er sikker kommunikasjon mellom systemkomponentene. Det vil i resterende kapitler av denne oppgaven presenteres en vurdering av sikkerheten for AMS-kanalen, samt til slutt et forslag til løsning i kapittel 7. Når en skal vurdere informasjonssikkerheten for AMS-kanalen må en kartlegge hvilke oppgaver systemet er designet til å gjøre og hvilke data som kommer til å bli sendt mellom komponentene i systemet. Når en har en oversikt over hvilke oppgaver som skal kunne utføres kan en anta hvilken type trafikk som vil bli generert av de forskjellige funksjonene som benyttes til å utføre de forskjellige oppgavene. Med en oversikt over hvilken trafikk som blir sendt gjennom AMS-kanalen kan en videre anta hvem som har interesse av disse data, samt hvilke måter de kan innhentes.

4.1 Vurdering av nivå av informasjonssikkerhet for AMS-kanalen

I et AMS er det AMS-kanalene mot de forskjellige målepunktene som er distribuert og har størst angrepsoverflate. Om informasjonssikkerheten for AMS-kanalene ikke er over et akseptabelt nivå vil angrep mot kommunikasjonen i en AMS-kanal kunne føre til sårbarheter for hele AMS. Hva som er akseptabelt nivå av sikkerhet må settes i forhold til hvor stor *risiko* som knyttes til systemet. Risiko R ved hendelse x er ofte definert som et produkt av sannsynlighet P for at en hendelse x inntreffer og konsekvensene K om hendelse x inntreffer.

$$R(x) = P(x) \times C(x)$$

For AMS-kanalen må risikoen ved innføring av et slikt system vurderes gjennom å undersøke hvor stor sannsynlighet for at forskjellige angrep inntreffer samt hvilke konsekvenser som er forbundet til angrepene. Akseptabelt nivå av sikkerhet trenger ikke å være et nivå hvor systemet er sikret mot absolutt alle angrep og uheldige situasjoner. En kan derimot håndtere situasjoner der risikoen er uakseptabelt høy ved å iverksette tiltak som reduserer sannsynligheten eller konsekvensene til et akseptabelt nivå. For AMS kan man dermed ikke se for seg at et slik distribuert kommunikasjonssystem skal kunne håndtere og være helt sikkert mot alle mulige angrep og uheldige situasjoner. Hvordan man kan oppnå et akseptabelt nivå av sikkerhet i AMS-kanalen illustreres i figur 4.1. Figuren viser et diagram over risiko for tre forskjellige hendelser/angrep R_a, R_b og R_c. Figuren viser også hvordan områder av diagrammet som indikerer akseptabel og ikke akseptabel risiko. Et akseptabelt nivå for informasjonssikkerhet i AMS-kanalen må være en tilstand hvor hendelser med uakseptabelt høy sannsynlighet og konsekvenser, R_a, er håndtert. For angrep hvor det ikke er mulig å redusere de store konsekvensene bør tiltak for å redusere sannsynligheten iverksettes, R_b. For angrep hvor det er vanskelig å redusere sannsynlighet bør tiltak for å redusere konsekvensene iverksettes, R_c. Ved slike tiltak ser vi ut ifra figuren at alle hendelser/angrep er innenfor hva vi kan se på som akseptert risiko. Akseptabelt nivå av informasjonssikkerhet vil dermed være et nivå hvor sikkerhetsmekanismer brukes til størst mulig grad å få risiko ved alle hendelser/angrep til et akseptabelt nivå.



Figur 4.1: Akseptabelt nivå av informasjonssikkerhet i AMS-kanalen

4.2 Funksjoner og oppgaver utført av AMS

Eksakt hvilke oppgaver AMS skal kunne utføre vil varierer fra system til system og være avhengig av de enkelte implementasjonene. For å skape et overordnet og generalisert sett av oppgaver ble det brukt en kravspesifikasjon for AMS utviklet og skrevet av Graabak og Sæle ved SINTEF Energi [74]. Denne kravspesifikasjonen er utarbeidet med NVEs krav til AMS, [87], som utgangspunkt og er ment som en veiledning for nettselskaper som skal installere AMS. Graabak og Sæle definerer forskjellige kategorier av krav. I alt defineres 13 *grunnkrav* og 153 *detaljkrav*. Grunnkravene, krav 0.1 til 0.13, er spesifikasjoner som oppfyller NVEs krav til AMS. De 153 resterende er mer spesifiserte krav som totalt oppfyller de 13 grunnkravene men også definerer en rekke valgfrie og anbefalte oppgaver og funksjoner for AMS. For hvert av de 13 grunnkravene henvises det til de mest relaterte kravene blant de 153 mer detaljerte kravene. Det er grunnkravene og disse mest relaterte detaljkravene ble brukt som utgangspunkt for arbeidet presentert i denne oppgaven, se tabell 4.1.

I tillegg til disse ble det også valgt å inkludere enkelte detaljkrav som ikke er direkte relatert til noen av grunnkravene, se tabell 4.2. Dette er krav som ble ansett til å være kritiske og absolutt nødvendige for AMS. Dette vil være krav som med stor sannsynlighet vil bli implementert for alle AMS. Disse kravene ble også inkludert grunnet at de har stor relevans til evaluering av informasjonssikkerheten i systemet. Det blir nå gitt en kort begrunnelse for hvorfor disse kravene ble inkludert.

Krav 130 For et distribuert system som AMS er det nødvendig å kunne endre parametre og konfigurasjoner i nettverksnodene uten å være nødt til å oppsøke målenoden fysisk. Dette gjelder spesielt i tilfeller der parametre eller konfigurasjoner skal endres for en større gruppe målenoder samtidig.

Krav 131 En må anta at all programvare inneholder feil eller av andre grunner må oppdateres etter første innstallasjon. Dette kan både være sikkerhetsmessige oppdate-

Grunnkrav	**Detaljkrav**
0.1	1, 3, 4
0.2	123
0.3	6, 7, 123
0.4	8, 125
0.5	41, 42, 43, 44, 45, 71
0.6	48, 49, 50, 56
0.7	93, 126, 127, 128, 129
0.8	67, 68
0.9	10, 11, 12
0.10	8, 9, 10
0.11	8, 9, 10
0.12	54, 55, 56
0.13	55, 56

Tabell 4.1: Grunnkrav og tilhørende detaljkrav [74]

Detaljkrav	**Navn**
130	Fjernstryring av parametre
131	Oppgradering av programvare i Målerterminal og Kommunikasjons-system

Tabell 4.2: Andre detaljkrav inkludert [74]

ringer, oppretting funksjonsfeil eller utvidelser av funksjonalitet. Dette gjelder også for AMS og mulighet for programvareoppdateringer vil være nødvendige.

Tillegg A i denne oppgaven gir en oversikt over grunnkravene, de respektive detaljkravene samt de andre detaljkravene som ble inkludert. Oversikten i tillegg A viser hvilken trafikk hvert krav vil generere og tilhørende karakteristikk. Seksjon 4.3 presenterer hvilken trafikk som genereres av de oppgavene som ble inkludert, og kan antas å bli sendt over AMS-kanalen.

4.3 Trafikk i AMS-kanalen

Trafikken i AMS-kanalen kan skilles på type trafikk og hvilken data som sendes. Selv om all trafikk observeres som data i form av bits i overføringsmediet, ble det valgt å skille på hvilke prosesser som iverksettes hos mottakeren. Med oppgavene definert i kravspesifikasjonen som grunnlag ble trafikken klassifisert ut ifra om data som sendes inneholder kommandoer og automatisk iverksetter prosesser hos mottakeren. Det må presiseres at når det snakkes om alle smartmålerne, betyr dette alle smartmålerne for ett nettselskap. De følgende trafikklassene ble definert og blir presentert i seksjonene som følger:

- Målerverdier
- Konfigureringskommandoer
- Styringssignaler
- Hendelser og alarmer
- Trafikk til/fra lokalt tilleggsutstyr
- Annen trafikk

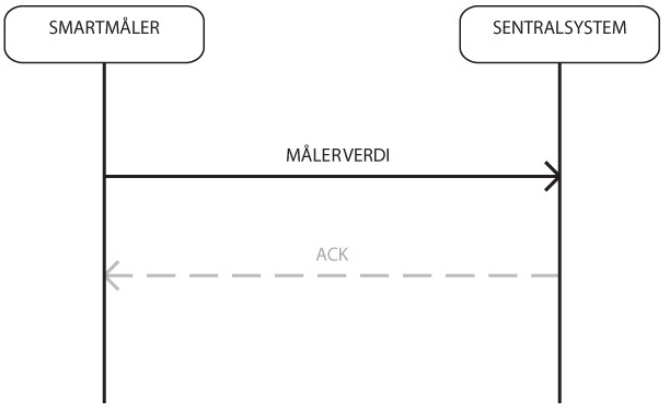
4.3.1 Målerverdier

Målerverdier er den enkleste formen av trafikk i AMS-kanalen. Målerverdier lagres kun av mottaker uten å iverksette noen form for prosess. E.g. innrapportering av kraftforbruk. Selv om målerverdier iverksetter former for interne prosesser[1] anses ikke dette som kommandoer. Figur 4.2 viser et sekvensdiagram for sending av målerverdi. En `MÅLERVERDI` kan kun bli sendt fra smartmåleren til sentralsystemet. For å bekrefte mottak kan sentralsystemet sende `ACK` tilbake til smartmåleren.

4.3.2 Hendelser og alarmer

Når det skjer en tilstandsendring ved smartmåleren eller i nettet vil notifikasjoner om endringen sendes fra smartmåleren eller til sentralsystemet. Dette klassifiseres som hendelser eller alarmer. Listen under viser eksempler på hendelser og alarmer. Figur 4.3 viser sekvensdiagram for sending av hendelse/alarm. Når en `TILSTANDSENDRING` skjer ved

[1] lagring, prosessering etc.



Figur 4.2: Sekvensdiagram for målerverdier

smartmåleren, sendes en `HENDELSE/ALARM` til sentralsystemet. Sentralsystemet kan da enten kun registrere mottaket eller iverksette prosess. For å bekrefte mottak kan sentralsystemet sende `ACK` tilbake til smartmåleren.

1. Hendelse

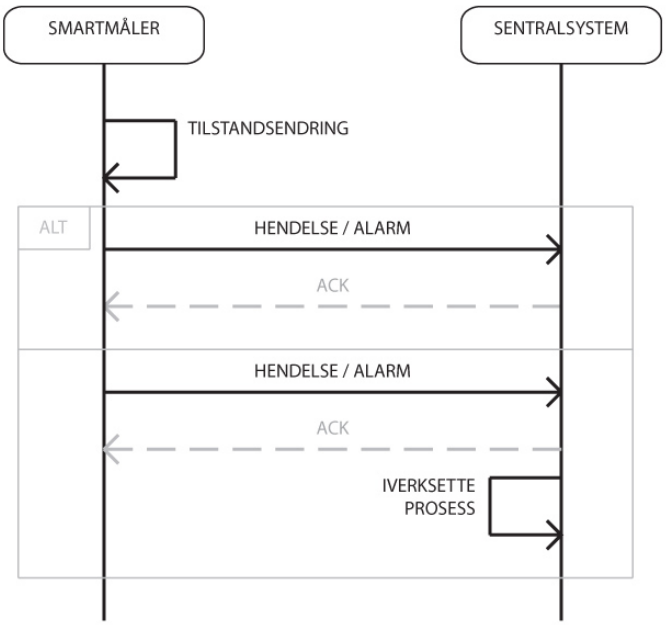
   a) Jordfeil
   b) Anlegg uten spenning
   c) Lysbuedeteksjon
   d) Dør åpen i nettstasjon
   e) Vann i nettstasjon
   f) Høy temperatur i komponent i kraftsystemet
   g) Manglende olje i komponent i kraftsystemet

2. Alarm

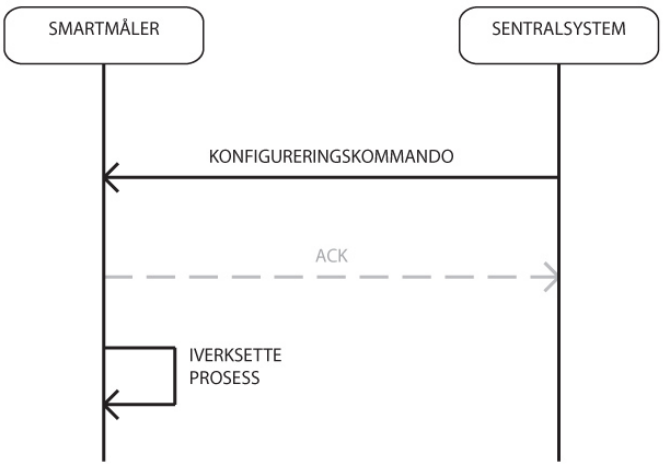
   a) Datamanipulering
   b) Innbruddsforsøk

4.3.3 Konfigureringskommandoer

Konfigureringskommandoer endrer parametre eller konfigurasjoner i smartmåleren for mottakeren. Konfigureringskommandoer kan sendes fra sentralsystemet til én, en gruppe eller alle smartmålerene samtidig. Figur 4.4 viser et sekvensdiagram for sending av konfigureringskommando til én smartmåler. En `KONFIGURASJONSKOMMANDO` sendes fra sentralsystemet til smartmåleren. For å bekrefte mottak kan smartmåleren sende `ACK` tilbake til sentralsystemet. Deretter iverksetter smartmåleren en prosess for å konfigurere seg i henhold til den mottatte meldingen. Listen under viser en oversikt over forskjellige konfigurasjonskommandoer.



Figur 4.3: Sekvensdiagram for hendelser/alarmer



Figur 4.4: Sekvensdiagram for konfigureringskommand

1. Parametre

   a) Intervall for registrering av måleverdier

   b) Parametre for maks effektuttak

2. Programvareoppdateringer

   a) Firmwareoppdateringer

   b) Programwareoppdateringer / patcher

4.3.4 Styringssignaler

Styringssignaler vil si kommandoer som initierer en prosess som endrer tilstanden for kraft-tilførselen hos mottakeren. Her skilles det på to forskjellige styringssignaler; signaler for åpning og lukking av tilførsel, signal for iverksetting av maks effektutak. Sistnevnte må kommenteres. Effekt P er definert som $P = W/t$ hvor W er arbeid og t tid. I kraftbransjen brukes wattimer, Wh[2] om effekt. Kravene til AMS om å kunne bryte og begrense effektuttaket i det enkelte målepunktet, er å begrense hvor mye W et målepunkt kan ta ut av nettet. Effekt i dette tilfellet vil dermed være øyeblikksforbruket for det enkelte målepunktet. I.e. om man ser effekt som uttrykk av strøm I og spenning U, $P = I \cdot U$, kan dette gjøres ved å redusere den elektriske inntakssikringen til et målepunkt. En slik elektrisk sikring begrenser hvor mye strøm I som kan gå gjennom sikringen og er målt i ampere, A.

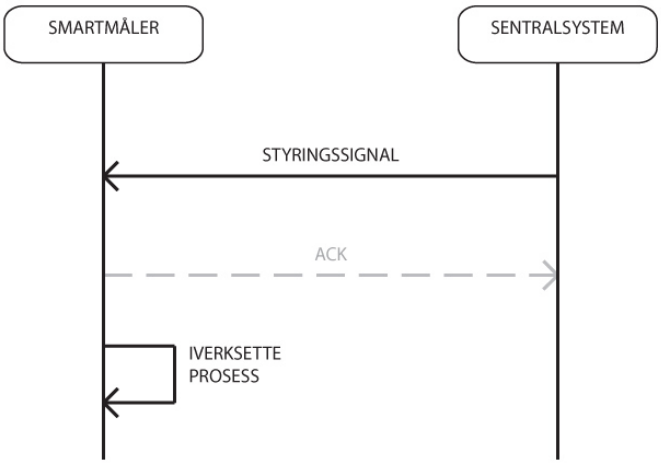
Kravet om begrensning og brytning av effektuttak sier at tilførselen av kraft skal brytes om effektuttaket overskrider den definerte maksgrensen. Denne maksgrensen settes og justeres sentralisert gjennom konfigurasjonskommandoer fra sentralsystemet. I vårt arbeid defineres derfor signal som iverksetter funksjonalitet for maks effektuttak som et styringssignal. Men det må presiseres at en konfigurasjonskommando som setter maksgrensen til en urimelig høy eller lav verdi også vil kunne benyttes som en bryter for å respektivt åpne eller lukke effektuttaket for målepunktet. Dette forutsetter at funksjonalitet for struping/-bryting av effektuttak ved en definert maksgrense er iverksatt.

Styringssignaler for åpning og lukking av tilførsel kan sendes til én eller en gruppe smartmålere samtidig. Signal for iverksetting av maks effektuttak kan sendes til én, en gruppe eller alle smart målerne samtidig. Figur 4.5 viser et sekvensdiagram for sending av et styringssignal til én smartmåler. Sentralsystemet sender `STYRINGSSIGNAL` til smartmåleren. For å bekrefte mottak kan smartmåleren sende `ACK` tilbake til sentralsystemet. Deretter iverksetter smartmåleren en prosess i henhold til mottatt styringssignal.

4.3.5 Trafikk til/fra lokalt tilleggsutstyr

Kravene til AMS spesifiserer ikke annet lokalt tilleggsutstyr enn display for visning av forbruksdata. Trafikk i sammenheng med lokalt tilleggsutstyr kan sendes begge veier over AMS-kanalen. Figur 4.6 viser et sekvensdiagram for sending av meldinger til og fra lokalt

[2] avhenigig av størrelsesorden benyttes kW (kilowatt, 10^3), MW (megawatt, 10^6), GW (gigawatt, 10^9), TW (terawatt, $10^(12)$)



Figur 4.5: Sekvensdiagram for styringssignaler

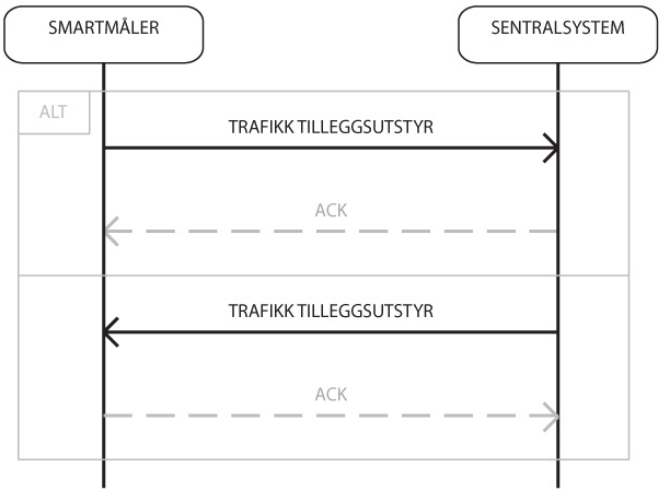
tilleggsutstyr. For å bekrefte mottak kan både smartmåleren og sentralsystemet sende `ACK` tilbake til avsenderen.

4.3.6 Annen trafikk

Det er ennå uvisst hvorvidt AMS-kanalen kommer til å bli benyttet til kommunikasjon for tjenester levert av tredjepart. Selv om NVE ikke stiller krav til at AMS-kanalen skal benyttes og dimensjoneres for slike tjenester, se 2.2.3.1, bør slike eventuelle framtidige utvidelser vurderes. Denne oppgaven presenterer ikke noe arbeid relatert til tredjeparts tjenester i AMS-kanalen og derfor blir ikke denne trafikklassen spesifisert nærmere.

4.4 Trusler mot AMS-kanalen

Denne seksjonen vil gi et bilde av hva som utgjør trusler mot AMS-kanalen. All informasjon tilgjengelig i et AMS er basert på data sendt over AMS-kanalen og trafikklassene presentert i forrige seksjon. En trussel mot AMS-kanalen vil dermed være alle som kan ha nytte av å tilegne seg adgang til trafikken. I denne sammenheng skilles det på trusler og angrep innen AMS. Når det snakkes om en trussel mot AMS vil det si noen som er motiverte for å gjøre angrep. Et angrep er da tiltaket trusselen utøver mot AMS, se seksjon 4.5. Informasjon og data fra AMS systemer kan være verdifulle for mange instanser, ikke bare aktørene innen den kraftsektoren. McNabb lister opp forskjellige aktører som kan nyttegjøre informasjon tilgjengelig gjennom AMS. Dette er ikke kun forbruksdata, men også informasjon og statistisk over aktivitet i AMS-kanalen [57]. Tabell 4.3 forteller ikke hvordan slik data er innhentet, men gir en indikator på aktører som kan være motivert for å tilegne seg slik informasjon, både på lovlig og ulovlig vis. Sett bort ifra kriminelle, er det få av disse aktørene som kan nyttegjøre eller har stor verdi av informasjon innhentet på ulovlig vis. Dette vil i de fleste sammenhenger være lovbrudd, og kan ikke brukes i forretningsmessige sammenhenger. Derimot viser tabellen at det er en rekke aktører som



Figur 4.6: Sekvensdiagram for trafikk til/fra tilleggsutstyr

kan ha nytte av informasjon sendt i AMS-kanalen. Av de nevnte utgjør kriminelle den mest sannsynlige aktøren som vil kunne nyttegjøre seg av informasjon innhentet, også på ulovlig vis.

LeMay et al. har i sin rapport, [37], laget en oversikt over trusler mot AMS, se tabell 4.4. Oversikten viser at det er variasjon i motivasjonen for de forskjellige truslene, samt at tilgjengelige resurser for de enkelte varierer. E.g. kan det antas at nysgjerrige lyttere ikke har store ressurser og kompetanse tilgjengelig for angrep mot AMS. For aktive angripere som terrorister og kriminelle kan ressursene være større, samt at sterk motivasjon kan føre til innhenting av spesialkompetanse for gjennomføring av angrep. Oversikten viser også at det vil eksistere motivasjon for aktører innen AMS for å utnytte sin rolle eller tilgang til AMS-systemer. Tabell 4.4 og 4.3 viser at det er både mange interessenter for AMS-data samt at det er mange forskjellig motivasjoner og mål for å utføre angrep mot AMS. Variasjonen i de forskjellige truslene viser at tiltak for å sikre AMS-kanalen må gjennomføres, både for angrep fra aktive angripere som terrorister og illegale operasjoner fra uetiske aktører.

4.5 Klassifisering av angrep mot AMS-kanalen

AMS står ovenfor mange av de samme utfordringene til informasjonssikkerhet som andre distribuerte systemer. Et komplett AMS er distribuert over store fysiske områder og flere av nettkomponentene er uten tilsyn hvor grad av fysisk sikring varierer. Kommunikasjonsnettverket må antas å være heterogent ettersom tilgangen på kommunikasjonssløsninger vil variere mellom lokasjoner i nettet. Denne seksjonen gir en introduksjon til grunnleggende angrep mot datanettverk. Kapittel 6 diskuterer disse angrepene i sammenheng med AMS samt de særegne utfordringene og konsekvensene det får for informasjonssikkerheten.

Kavitha og Sridharan publiserte i 2010 en rapport på sårbarheter i trådløse sensornettverk hvor de ga en klassifisering av forskjellige angrep på datanettverk [81]. Deres definisjon

Interessenter	**Eksempler på bruksområdet**
Nettselskap	Faktureringsgrunnlag, stryring av tilførsel etc.
Rådgivningsselskaper innen energibruk	Utarbeide energibesparende tiltak
Forsikringsselskaper	Informasjon om unormalt forbruk
Andre forretninger og innovasjon	Bruk av data til å utvikle nye produkter og markeder
Rettslige instanser	Identifisere mistenkelig og ulovlig aktiviteter; politi, myndigheter etc.
Rettstvister og rettsaker	Bruk av data som bevis
Eiere av eiendom	Oppfølging av leiekontrakter
Private etterforskere	Monitorering av spesielle hendelser
Presse	Tilegne sensitiv informasjon om profilerte og ikke profilerte personer
Kreditorer	Tilegne informasjon som kan indikere betalingsevne etc. Kredittsjekk
Kriminelle	Identifisere optimal tid for innbrudd basert på overvåkning av aktivitet

Tabell 4.3: Interessenter for AMS-data [57]

Trussel	**Eksempel**
Nysgjerrige avlyttere	Avlytting av nabo eller spesifikke målere uten videre motivasjon
Motiverte avlyttere	Avlytting motivert for videre angrep eller agenda. E.g. overvåking av aktivitet før innbrudd
Uetiske kunder	Autentiske kunder som prøver å stjele strøm eller manipulere faktureringsgrunnlaget for å redusere utgifter
Uetiske tjenesteaktører innen AMS	Systemaktører innen AMS som utnytter informasjonen de besitter til ondsinnede formål
Aktive angripere	Aktive angripere e.g. terrorister og kriminelle med store ressurser og sterk motivasjon for ondsinnede angrep mot AMS
Publisitets angriper	"Hackere" som utøver ondsinnede handlinger mot AMS for egen tilfredstillelse

Tabell 4.4: Trusler mot AMS-kanalen [37]

på trådløse sensornettverk[3] var "a large network of resource-constrained sensor nodes with multiple preset functions, such as sensing and processing (...) the major elements of a WSN are the sensor nodes and the base station.". Til tross for at alle koblingene mellom komponentene i et AMS-nettverk ikke nødvendigvis er trådløse, er egenskapene ved disse to nettverkene like nok til at samme klassifisering av angrep kan bli brukt for AMS. Listen under er hentet fra Kavitha og Sridhara og viser de fire hovedklassene for angrep [81]. De neste seksjonene presenterer en kort gjennomgang av disse fire angrepsklassene samt deres relevans til AMS.

1. Based On the Capability of the Attacker
   a) Outsider versus insider (Node Compromise) attacks
   b) Passive versus active attacks
   c) Mote-class versus laptop-class attacks
2. Attacks on Information in Transit
   a) Interruption
   b) Interception
   c) Modification
   d) Fabrication
   e) Replaying existing messages
3. Host Based Vs Network Based
   a) Host-based attacks
   b) Network-based attacks
4. Based On Protocol Stack
   a) Physical Layer
   b) Data Link layer
   c) Network layer
   d) Transport layer
   e) Application layer

4.5.1 Angrep basert på angriperens muligheter

a) Avgjør hvilke muligheter en angriper har som en del av nettverket eller utenforstående. Dette inkluderer også når en angriper benytter angrep for å bli en del av nettverket.

b) Passive angrep innebærer kun avlytting og monitorering av aktivitet i nettverket. Aktive angrep involverer alle former for modifisering av data eller innføring av falsk trafikk.

c) Avgjør kapasiteten for utstyret benyttet av angriperen. For AMS vil dette være en utfordring med tanke på varierende kapasitet for komponenter i AMS-nettverket, e.g. smartmålerene.

[3]Wireless Sensor Network (WSN)

4.5.2 Angrep på trafikk i transitt

a) Et slikt angrep forstyrrer eller stanser trafikk sendt over AMS-kanalen for å nå sitt mål. Dette angrepet er basis for DoS-angrep.

b) Innebærer uautorisert avlytting av trafikk sendt mellom komponentene i nettet.

c) Slike angrep innebærer at angriperen gjør modifiseringer av trafikk sendt i AMS-kanalen.

d) Angriperen sender falsk trafikk inn i AMS-kanalen.

e) En angriper lagrer autentiske meldinger sendt over AMS-kanalen for å sende de på nytt senere.

4.5.3 Angrep på nettverkskomponenter eller nettverksangrep

a) Involverer å gå til angrep på komponentene i nettet.

b) Angriperen utnytter alle egenskapene for datanettverket for å tilegne seg urettferdige fordeler i nettverket. I.e. angriperens oppførsel skaper avvik fra den tiltenkte funksjonen for nettverksprotokollene.

4.5.4 Angrep basert på protokollag

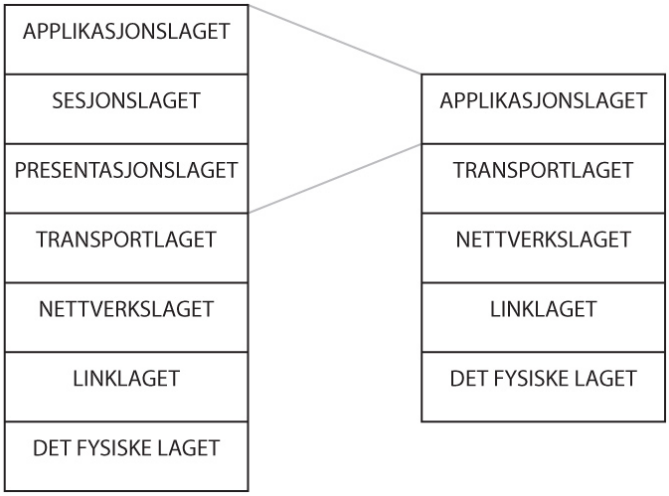
Aktuelle angrep mot AMS-kanalen kan skje i alle protokollag benyttet for kommunikasjon mellom komponentene i AMS-nettverket. En typisk lagdeling av nettverksprotokoller er vist i listen under, se seksjon 5.1 for nærmere beskrivelse.

- Applikasjonslaget
- Transportlaget
- Nettverkslaget
- Datalinklaget
- Det fysiske laget

Kavitha og Sridharan presenterer en liste over angrep basert på protokollag i trådløse sensornettverk [81]. Ettersom enkelte av nettverkene studert i deres rapport er mesh-baserte, er ikke angrepene for hvert protokollag direkte overførbare til typen AMS studert i denne oppgaven. Mesh-baserte sensornettverk benytter i.e. andre nettverksprotokoller enn slik AMS er studert i denne oppgaven. Angrep mot forskjellige protokollag av AMS blir diskutert nærmere i kapittel 6.

Kapittel 5

AMS Kommunikasjonsarkitektur



Figur 5.1: Orginal OSI modell og den kollapsede modellen

I dette kapittelet presenteres kommunikasjonen mellom de forskjellige enhetene i den overordnete arkitekturen lagt fram i seksjon 2.3. For hver kobling vil det presenteres aktuelle protokoller og teknologier som blir benyttet. Dette vil gi grunnlaget for analyse og diskusjon i kommende kapitler. Når det i denne rapporten refereres til *AMS-kanalen* henvises det til stien kommunikasjonen mellom sentralsystemet og den smarte måleren følger. *AMS-nettverket* vil videre si nettverket som dannes av alle AMS-kanalene og de respektive smartemålerne som er styrt av ét sentralsystem.

Et nettverk kan beskrives som et sett med elementer, kalt *noder*, og deres koblinger til hverandre, kalt *linker*. I denne oppgaven vil det benyttes denne formuleringen om datanettverket i AMS. Enhetene[1] som kommuniserer kalles noder, og koblingene mellom de kalles linker. Linkene utgjør forskjellige kommunikasjonsprotokoller over forskjellige medier. Open Systems Interconnection (OSI)-modellen blir benyttet som utgangspunkt, hvor det blir presentert relevante protokoller i de forskjellige lagene. OSI modellen som ble lagt fram av den internasjonale standardiseringsorganisasjonen ISO er originalt syv lag , men ofte blir de tre øverste lagene (sesjonslaget, presentasjonslaget og applikasjonslaget) sett på som ett lag, altså applikasjonslaget. Om ikke annet er spesifisert benyttes den kollapsede versjon av OSI modellen i denne oppgaven, se figur 5.1. En komplett oversikt over alle kommunikasjonsprotokollene på de forskjellige nivå for en link kalles en *protokollstakk*. Det overordnede prinsippet for en slik lagdelt protokollstakk er at hvert lag tilbyr en rekke tjenester for det overliggende laget. Ved å kunne varierer bruken av forskjellige protokoller, som tilbyr et sett tjenester, vil en kunne sette sammen en tilpasset protokollstakk med ønskede egenskaper. For de forskjellige nettverkslinkene i AMS er det mange alternative protokoller på alle lag av protokollstakken. Noen alternativer blir presentert i seksjon 5.2.

[1] konsentrator, den smarte måleren, sentralsystemet etc.

5.1 Generisk arkitektur for AMS-kanalen

Denne seksjonen vil presentere karakteristikk for de forskjellige nodene og linkene samt i den generiske arkitekturen for AMS-kanalen, se figur 5.2. I resterende seksjoner av dette kapitlet vil det presenteres aktuelle kommunikasjonsprotokoller for linkene i den generiske arkitekturen.

5.1.1 Noder/nettelementer i AMS

Smartmåler

Funksjonaliteten for smarte målere varierer etter leverandør, type og modell. Hvilken måler som blir benyttet i det enkelte tilfellet avhenger blant annet av kommunikasjonsteknologi tilgjengelig, fysiske begrensninger ved målepunkt og valg av løsning valgt av nettselskapet AMS. Det ingen entydige spesifikasjoner for hva som utgjør en smart måler eller hvilken funksjonalitet de bør støtte. Minstekravene til funksjonalitet for målere i Norge defineres av NVEs forskrift [87] og er oppsummert i seksjon 2.2.3.1. Utover disse kravene er det opp til nettselskapene selv å spesifisere funksjonaliteten og hvilken type måler de vil installere for sine målepunkter.

Konsentrator

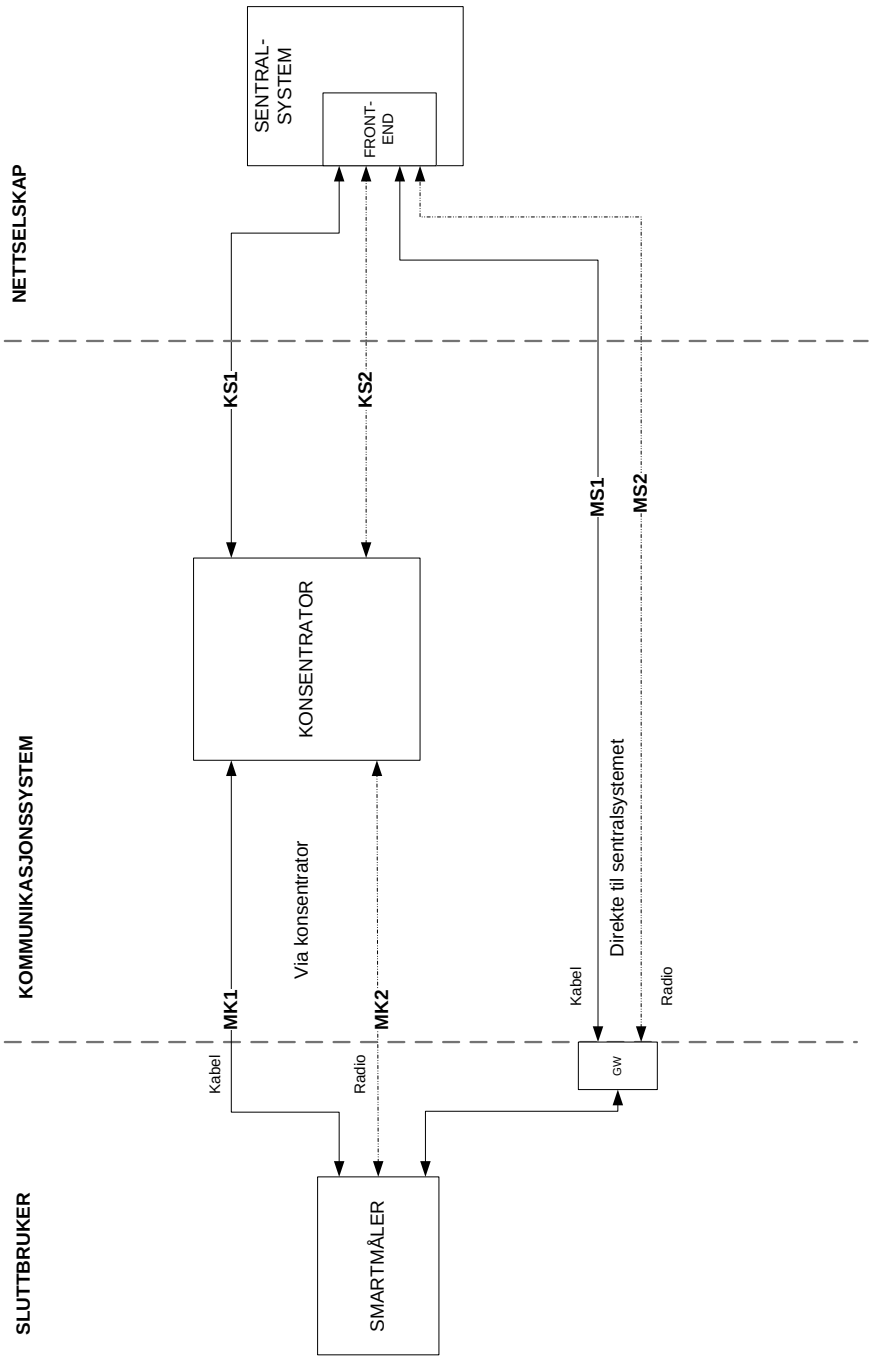
Konsentratoren er et mellomledd mellom den smarte måleren og sentralsystemet som håndterer kommunikasjon begge veier i AMS-kanalen. Konsentratoren er ofte benyttet til å aggregere data fra flere målere og sende de samlet inn til sentralsystemet. I tillegg til *store and forwarding* av tillater også konsentratoren direkte videresending av meldinger for e.g. styringssignaler. Samtidig kan en konsentrator delegeres oppgaver ordinært håndtert av et sentralsysteme for å minimere trafikk i AMS-kanalen.

Løsning via konsentrator blir ofte benyttet for målere hvor Power Line Communication (PLC) blir benyttet som kommunikasjonsmedium mot målepunktet. Dette er grunnet begrensninger for teknologien som overføringskapasitet og skalerbarhet i de forskjellige delene av kraftnettet[2]. Derfor er konsentratorer ofte plassert i transformatorer nære målepunktet som videresender aggregert data over et medium med høyere overføringskapasitet mot sentralsystemet. Antallet målere en konsentrator kommuniserer med varierer og er avhengig av avstand til målerne og kommunikasjonsteknologi benyttet. Konsentratorer plasseres derfor på optimale lokasjoner for å kunne dekke flest målere i sitt område.

Sentralsystem

Sentralsystemet er hjernen for kommunikasjon i AMS-nettverket. Sentralsystemet har grensesnitt mot AMS-kanalen og mot eksterne systemer som håndterer data mottatt/sendt gjennom AMS-kanalen. Grensesnittet mot AMS-kanalen heter *frontend*-system og ble omtalt i seksjon 2.3.3. Ettersom realiseringen av systemene på nettselskapsiden vil varierer fra nettselskap til nettselskap, spesifiseres ikke sentralsystemet nærmere, se seksjon 2.3.3.

[2]Se seksjon 5.3.1



Figur 5.2: Generiske arkitektur for AMS-kanalen

5.1.2 Linker

Ved beskrivelse av linkene tas utgangspunkt i figur 5.2. For linkene skilles det på kommunikasjonsteknologier som benytter kabel og radio. Dette er grunnet deres distinkte forskjell i egenskaper og konsekvenser med tanke på informasjonssikkerhet.

MK: Måler - Konsentrator
Trafikkarakteristikk: Denne linken kobler kun ett målepunkt mot konsentratoren vil kun overføre trafikk med tilknytning det aktuelle målepunktet. Om den smarte måleren benyttes til kommunikasjon av data på vegne av andre typer målere vil også data fra disse målerne gå over denne linken.

MK1: Kabel
Kommunikasjonssti: Kommunikasjon skjer oftest over kabler som er praktisk utilgjengelige for uvedkommende, enten over dedikerte kabler for datakommunikasjon eller datakommunikasjon over kraftkabler. Med praktisk utilgjengelig mener vi at en enten må grave opp kablene eller at kablene går inne i bygg med former for fysisk sikring. Avstanden til konsentrator varierer men kan oftest være tilsvarende avstand som til trafostasjoner.

MK2: Radio
Kommunikasjonssti: Som all annen trådløs kommunikasjon er det vanskelig å avgrense spredningen av radiosignaler. Disse radiosignalene vil derfor være tilgjengelig for alle i en viss omkrets rundt transceiveren, avhengig av forhold som transmisjoneffekt, antennetype etc. Avstanden til konsentratoren varierer også for radioløsninger. Men om en konsentrator kun opererer mot målepunkter over radioløsninger trenger ikke konsentratorer nødvendigvis å være plassert i transformatorstasjoner.

KS: Konsentrator - Sentralsystem
Trafikkarakteristikk: Hva som sendes mellom konsentrator og innsamlingssystemet er avhengig av hvilken retning man studerer. Fra sentralsystemet til konsentratoren sendes data som er tiltenkt en eller flere målere koblet til konsentratoren. Sentralsystemet kan også sende data og meldinger tiltenkt konsentratoren, disse blir da ikke sendt videre. Trafikk sendt mellom konsentratoren og sentralsystemet vil være trafikk til/fra én måler, aggregert trafikk til til/fra flere målere, eller data og signaler generert av konsentratoren.

KS1: Kabel
Kommunikasjonssti: Kabelbaserte løsninger mellom konsentrator og sentralsystem skjer mest sannsynlig over telekommunikasjonsnett. Disse nettene er distribuerte over store avstander. Komponentene i slike nett er ofte praktisk utilgjengelige men komponentene er ofte plassert i ubevoktede lokasjoner. Enkelte nettselskaper innen kraftindustrien har også bygget ut kommunikasjonsnett i sine områder. Kabler og komponenter i disse nettene er derfor ofte lokalisert sammen.

KS2: Radio
Kommunikasjonssti: Radioløsninger benytter oftest radiobaserte kommunikasjonsnett mellom konsentrator og sentralsystem. Arkitekturen for slike nett er oftest at

aksessnettet er tråløst mens stammenettet går over kabelbasert infrastruktur. I slike løsninger vil radiosignalene for linken mot aksessnettet være tilgjengelig for alle i fysisk nærhet av konsentratoren og basestasjonen for aksessnettet. I stammenettet vil tilgjengligheten være begrenset av tilgjengeligheten av kablene og komponentene i stammenettet.

MS: Måler - Sentralsystem
Trafikkarakteristikk: Denne linken vil ha lik karakteristikk som MK linkene.

MS1: Kabel
Kommunikasjonssti: Denne linken vil ha lik kommunikasjonssti som link KS1.

MS2: Radio
Kommunikasjonssti: Denne linken vil ha lik kommunikasjonssti som link KS2.

5.1.3 Bruk av mobilnett i AMS

Når mobilnett benyttes innen AMS vil noden som er knyttet til nettet besitte en mobilterminal. Enten noden er en smartmåler eller er en konsentrator vil den ha en innebygget mobilterminal eventuelt være tilknyttet en ekstern mobiltermial. E.g. i GSM er et SIM-kort entydig for et abonnement og benyttes blant annet til autentisering og identifisering av brukeren mot nettet. På denne måten kan man si at en smartmåler vil være en mobilterminal med et SIM-kort hvor mobilterminalen er entydig for målepunktet og SIM-kortet for sluttbrukeren. Mobilterminalene som benyttes innen AMS vil i motsetning til de fleste andre mobilterminaler i mobilnettet ha en statisk posisjon og i de fleste tilfeller være knyttet til samme Base Transceiver Station (BTS) dens hele levetid. Roaming vil derfor ikke være noe aktuelt for disse mobilterminalene.

5.2 Valg av kommunikasjonsprotokoller for AMS-kanalen

For de forskjellige linkene i den generiske arkitekturen for AMS er det mange alternativer for kommunikasjon på alle lag. Ettersom det er nettselskapene som står ansvarlige for utbyggingen av AMS for sine målepunkter, er valget av løsninger og teknologier for AMS opp til nettselskapene og deres behov. Hvilke kommunikasjonsteknologier som benyttes for AMS-kanalen vil derfor variere mellom nettselskaper og er basert på valgene de forskjellige nettselskapene gjør.

Selv om det ikke stilles krav eller bestemmelser i forhold til valg av kommunikasjonsteknologi ved utrullingen av AMS i Norge, er det gjort flere analyser på hvilke valg som er mest hensiktsmessige. I 2010 gjorde Haugen en vurdering av "Kommunikasjonsalternativer for informasjonsutveksling med AMS mellom smarte hus og et smart kraftnett" [41]. I sin rapport vurderer Haugen en rekke kommunikasjonprotokoller og standarder etter kriterier som robusthet, skalerbarhet, kostnad, grad til framtidssikkerhet og funksjonalitet. Hans vurdering ble gjort opp i mot egnte egenskaper og krav for utrulling av AMS i Norge. Haugen oppsummerer med å anbefalte protokoller og standarder best egnet i forhold til disse kravene samt sine egne vurderingskriterier. I 2010 publiserte Craemer og Deconinck en rapport som vurderte forskjellige standarder tilgjengelig for bruk i AMI [25]. I denne

Teknologi	Grad av standarisering	Robusthet	Skalerbarhet	Kostnad	Grad av fremtidssikkerhet	Funksjonalitet	Total poengsum
LonWorks	4	4	2	2	2	1	15
Fiber	4	4	4	0	4	4	20
xDSL	4	4	3	4	2	2	19
HFC	4	4	3	4	2	2	19
Prime PLC	2	3	4	3	3	3	18
GSM/UMTS/HSPA/LTE	4	3	4	2	0	4	17
SITRED	0	3	3	1	2	2	11
M-Bus	4	3	3	4	2	3	19
SML	1	4	4	4	4	4	21
DLMS/COSEM	3	4	4	4	4	4	23
DPWS	x	x	x	x	x	x	

Figur 5.3: Vurdering av valgte standarder og protokoller [41]

rapporten studerte de standarder, ikke bare for AMS-kanalen men for hele verdikjeden i et AMI, inkludert standarder for kommunikasjon i smarte hjem og komponenter for kobling mot kraftnettet. I deres analyse vurderte de standardene hovedsakelig etter 4 kriterier; åpen eller lukket standard, standardens plassering i OSI samt modularitet og kompatibilitet mot andre protokollag, funksjonalitet og fleksibilitet, standardens modenhet, ytelse og skalerbarhet. I sine rapporter gir OPENmeter en oversikt over forskjellige åpne og offentlige standarder for AMS. De alternative løsningene OPENmeter beskriver i disse dokumentene er basert på allerede eksisterende og aksepterte standarder for AMI, som samtidig anbefales etter initiativets kriterier [60, 61, 65, 64, 66]. Tillegg B gir en oversikt over de forskjellige standarder og protokoller OPENmeter beskriver, samt standardenes bruksområde og egenskaper etc.

Grunnet tidsbegrensninger var en full vurdering av alle tilgjengelige protokoller og standarder ikke mulig innen rammene for denne oppgaven. Det ble derfor valgt ut en delmengde standarder og protokoller for nærmere analyse. Denne delmengden ble valgt ut på grunnlag av analysene i rapportene beskrevet i over. Det overordnede kriteriet for utvelgelsen var at hver standard og protokoll skulle være vurdert til et aktuelt framtidig alternativ av analysene i de respektive rapportene. Vurderingene beskrevet i de tre rapportene, er skrevet av eller har opphav i tre forskjellige fagmiljøer innen AMI. Vurderingene gjort av disse fagmiljøene kan derfor ses på som objektive. Samsvar i resultatene på tvers av disse rapportene må derfor ses på som en god indikator for valg av standarder og protokoller. Figur 5.3 viser de utvalgte standardene og protokollene, samt utvalgte [3] resultater for de standardene og protokollene vurdert av Haugen [41].

Haugen rangerer sine resultater på en skala fra 0 til 4 hvor høyt tall beskriver i hvor stor grad de ulike teknologiene oppfyller vurderingskriteriene. Enkelte resultatene vist i figuren diskuteres i kapittel 6 men det henvises til hans rapport for fullstendig diskusjon [41]. De forskjellige standardene og protokollene aktuelle for AMS-kanalen har forskjellig formål og hensikt og er derfor plassert i forskjellige nivå av protokollstakken. Figur 5.4 viser en oversikt over de forskjellige standardene og protokollene som vurdert i denne

[3] Vurderingskriterie *sikkerhet* er ikke tatt med i denne modellen. Sikkerhetsvurdering av disse protokollene blir presentert i kapittel 6.2 av denne rapporten

Ikke egnet for AMS-kanalen	
Euridis	Ikke framtidsrettet grunnet lav funksjonalitet [41]
IEC 61107 / IEC 62056-21	Ikke framtidsrettet grunnet lav funksjonalitet [41]
IEC 61850	Ikke framtidsrettet da det ikke er en spesifikk standard for bruk i AMS [41]
Mulig aktuelle for AMS-kanalen	
PLC S-FSK	Ikke framtidsrettet grunnet liten båndbredde [61]
ODEL/GS2	Ikke standardisert, ikke et godt alternativ for kommunikasjon mellom nettselskap og sluttbruker [41]

Tabell 5.1: Standarder og protokoller for AMS-kanalen ikke studert i denne oppgaven

oppgaven og hvilke protokollag de definerer. Figur 5.5 viser hvilke linker disse protokollene og standardene mest sannsynlig vil bli brukt.

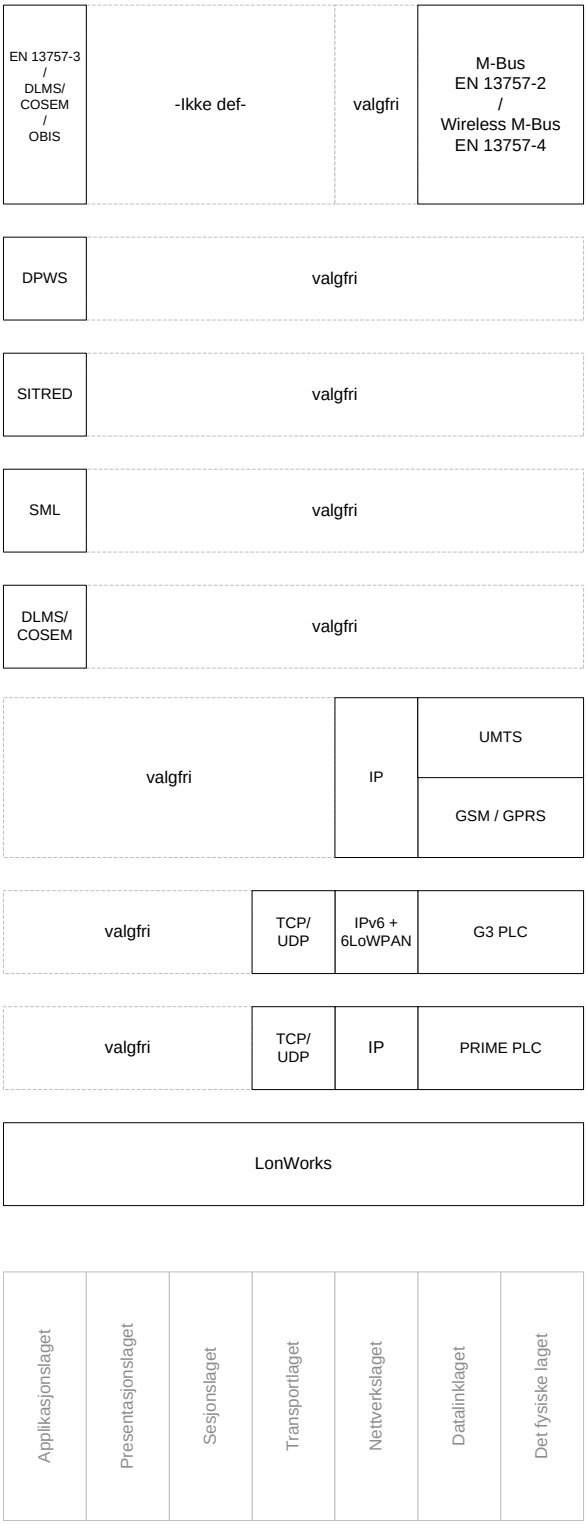
Tabell 5.1 gir en oversikt over noen standarder og protokoller ikke studert i denne oppgaven samt grunn til at de ikke ble studert. De listede standardene og protokollene er kun de som er listet som aktuelle for AMI i følge rapportene nevnt. For en utvidet oversikt over standarder og protokoller for AMI henvises det til de respektive rapportene nevnt over, samt vedlegg B. *Ikke egnet for AMS-kanalen* er protokoller som mangler funksjonalitet eller muligheter for utvidelser. Ofte protokoller beregnet på AMR eller andre deler i AMI. *Kunne vært aktuelle for AMS-kanalen* lister standardene og protokollen som kunne blitt brukt i AMS-kanalen, samt kort begrunnelse til hvorfor de ikke ble studert nærmere.

5.3 Kommunikasjonprotokoller

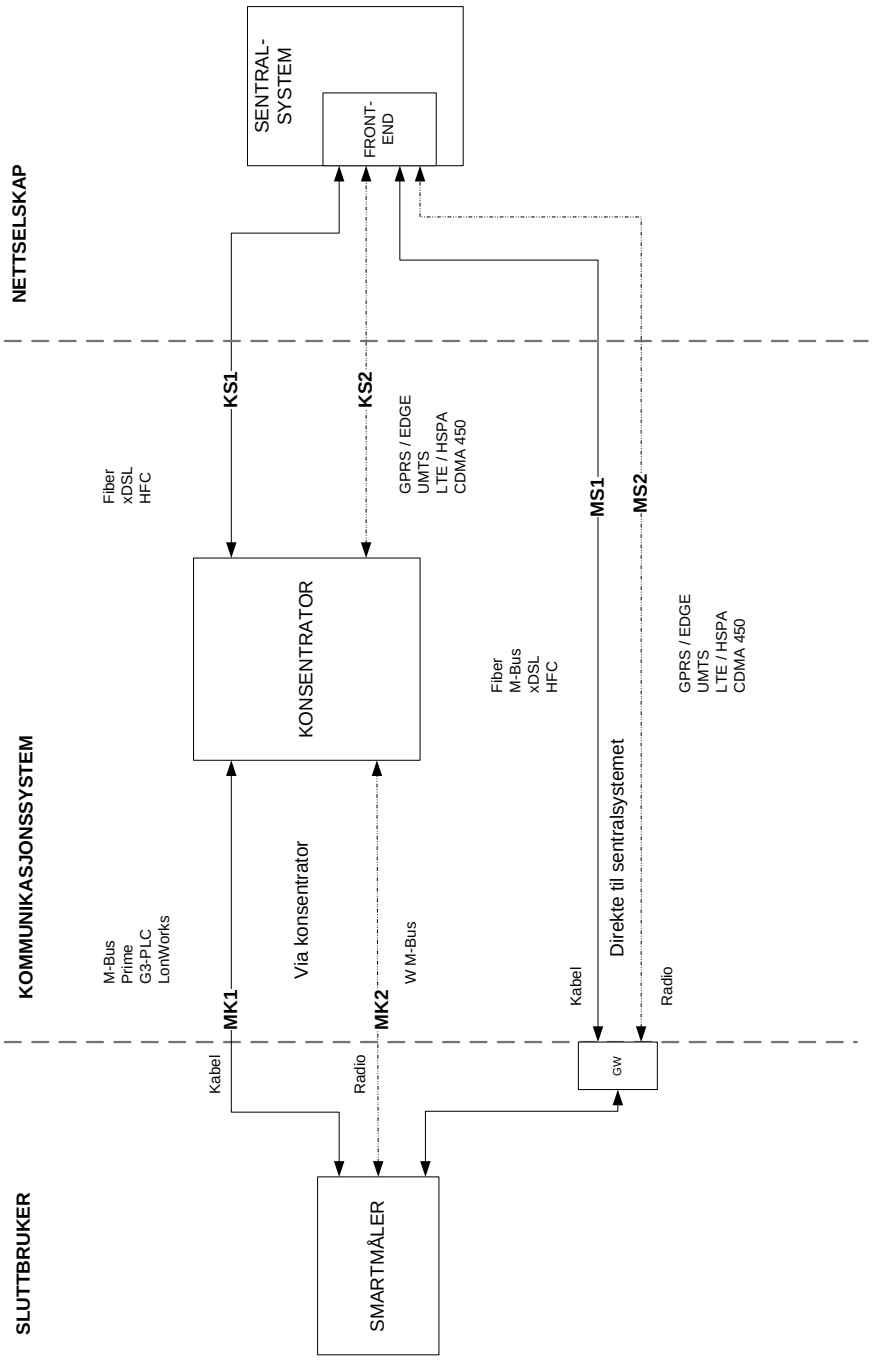
I denne seksjonen presenteres forskjellige kommunikasjonsteknologier som blir benyttet innen AMS. Enkelte teknologier som blir benyttet er meget omfattende og det vil derfor kun bli presentert de delene som har relevans til bruk innen AMS. Innføringen i disse teknologiene vil være konsise men ikke komplette da vi henviser til referanser og spesifikasjoner for utfyllende og supplerende informasjon. Denne seksjonen beskriver kommunikasjonprotokollene og seksjon 6.2 tar for seg sikkerhetsarkitekturer for de respektive kommunikasjonsprotokollene beskrevet i denne seksjonen.

5.3.1 PLC

PLC er en kommunikasjonsteknologi som benytter kraftkabler som overføringsmedium. Kraftoverføring skjer typisk på frekvenser på 50-60 Hz, noe som tillater andre signaler å bli overført i de resterende delene av frekvensspekteret. Frekvensene benyttet til slike kommunikasjonssignaler varierer mellom de forskjellige teknologiene men skjer oftest mellom 1,7 til 34 MHz. Ved å benytte Orthogonal Frequency Division Multiplexing (OFDM)



Figur 5.4: Kommunikasjonsprotokoller for AMS-kanalen vurdert i denne oppgaven



Figur 5.5: Protokoller og standarder for linkene i AMS-kanalen

kan data overføres på et stort antall bærefrekvenser fordelt utover frekvensrommet tilgjengelig. Et kommunikasjonsnett hvor alle enhetene, fra sluttbrukeren til kraftleverandøren, kan kommunisere vil kunne spenne utover store geografiske områder godt egnet for bruk i AMS. Slike nett kalles Broadband over Power Lines (BPL). Det er naturlig å sette opp nettet i et hierarki og se på de forskjellige nivåene hver for seg. For PLC i norsk sammenheng blir oppdelingen transportnett(høy spenning: > 22kV), distribusjonsnett(medium: 11-22kV og lav spenning: 230V) og til slutt hjemmenettverk, HAN. PLC kan benyttes på alle disse nivåene, men spenningstransformatorene hindrer oftest signaloverføring på tvers av disse delene av nettet. Dette fører til skaleringsproblemer og at et helhetlig PLC nettverk krever at flere teknologier benyttes samtidig for for å forme et kommunikasjonsnettverk for på tvers av nettnivåene. Lavspenningsdelen av distribusjonsnettet, som leverer strøm inn til bygg, vil sammen med smartmålerne være koblingspunktet ut til det smarte nettet. Båndbredden PLC kan gi på lav-volts distribusjonsnett er avhengig av nettleverandøren og modulasjonsteknologi benyttet, men oppnår typiske hastigheter fra 2-20Mbit/s levert til sluttbrukeren. På medium-spennings distribusjonsnettet oppnår man hastigheter opp mot 200Mbit/s som blir fordelt mellom sluttbrukere av switcher i transformatorstasjonene. Å benytte høyspentnettet til PLC-kommunikasjon er et omdiskutert tema. Høyspentledninger ble ikke designet for å frakte radiosignaler og gir uønskede sideeffekter. Mye av signalet går vekk i tap og utstråles til omgivelsene som radiosignaler. Dette kan skape interferens for mottakere i nærheten som benytter High Frequency (HF) radiofrekvenser (3-30MHz) [34]. Med hensyn til disse utfordringene er det lite sannsynlig at BPL, vil være tilgjengelig i nær framtid [52].

Vi vil nå se nærmere på noen av PLC-teknologiene som er aktuelle for AMS, spesielt over MK linker; PRIME og G3. Det eksisterer flere PLC teknologier men disse to anses å være dominerende i tiden framover grunnet muligheter for høy båndbredde relativt til tidligere PLC teknologier [65, 64].

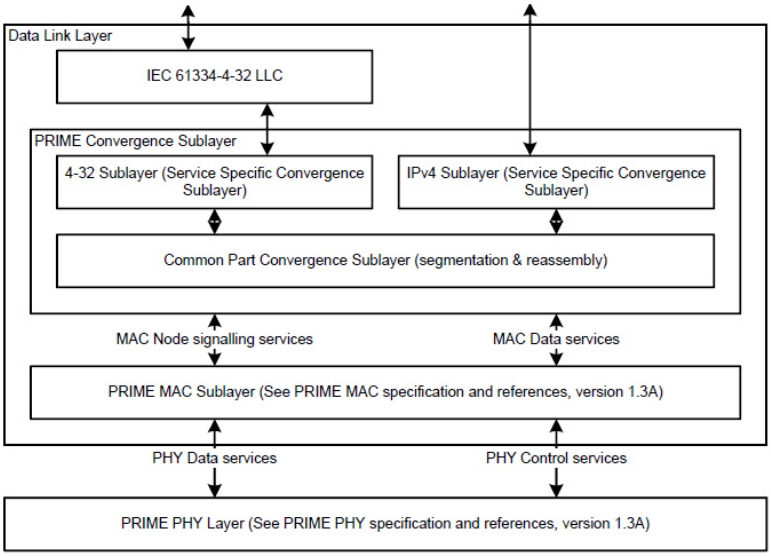
5.3.1.1 PLC - PRIME

Generelt

PRIME står for Powerline Intelligent Metering Evolution og er spesifikasjoner for det fysiske- og Media Access Control (MAC)-laget utarbeidet av store Europeiske aktører som Iberdrola, Itron, Landis+Gyr, og Texas Instruments. Teknologien er verken ferdig utviklet eller standardisert, men sikter på å bli en åpen, fri og ikke proprietær standard. PRIME benytter seg av OFDM og kan oppnå hastigheter opp til 130kbps. Kommunikasjonsprofilen for PRIME er vist i 5.6.

Det fysiske laget

Det fysiske laget i PLC PRIME overfører MAC Protocol Data Unit (MPDU)-er mellom nabonodene basert på OFDM. Signalene bruker en frekvensbåndbredde på 47.363kHz, som ligger i CENELEC-A spekteret som er begrenset til bruk innen kraftnettet. I tillegg til å sende/motta data og bringe dette videre til datalinklaget, utfører også det fysiske laget kontrolloperasjoner mot overføringsmediet; overvåke støy på kanalen(signal-to-noise ratio) etc.



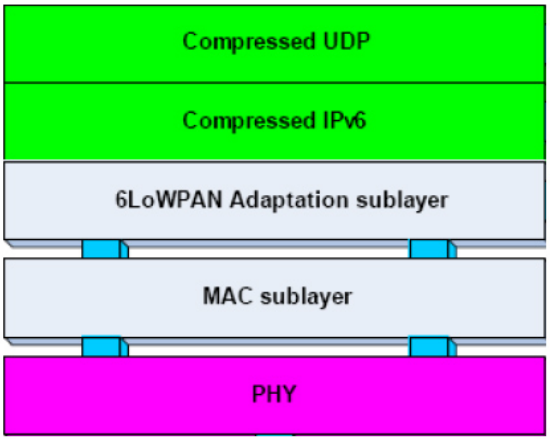
Figur 5.6: Kommunikasjonsprofil for PRIME PLC [65]

Datalinklaget

MAC-laget kaller nodene i et nettverk *base-* eller *service*-noder og kategoriserer nodene etter tre tilstander; *Disconnected*, *Terminal* og *Switch*. En base-node kan ses på som en rot-node som har et subnet med base-noder under seg. Alle noder starter i tilstanden Disconnected hvor de ikke kan kommunisere med noen andre noder. En node går fra å være Disconnected til å være Terminal når den får koblet seg mot en annen node og kan da sende og motta data. Når en Terminal-node får andre noder koblet opp mot seg, skifter de status til Switch og kan på denne måten motta og videresende data fra sine undernoder. Når en node har en kobling inn i nettet vil den ikke lenger prøve å koble seg inn nettet mot andre noder, noe som danner et tre med en rotnode(Base-noden), grener (Switch-noder) og løvnoder (Terminal-noder). I tillegg til administrasjon av noder og deres tilstand, har MAC laget har samtidig andre funksjonaliteter som håndtering av adresser, og enkelte linknivå sikkerhetsmekanismer etc. [9] PRIME innfører et konvergenslag som har både en generisk komponent og nettverkslagspesifikke komponenter. Her skiller vi mellom implementasjoner som benytter IEC 61334-4-32 og IPv4. Her utfører den generiske komponenten tjenester felles for begge standardene, mens de spesifikke komponentene utfører tjenestene som er forventet av de respektive lagene over.

Nettverk- og transportlaget

For systemer som benytter IEC 61334-4-32 over PRIME er ingen nettverk- eller transportlag benyttet. For IP-baserte systemer er standard IPv4 nettverkslag og TCP/UDP transportlag benyttet. [65].



Figur 5.7: Kommunikasjonsprofil for PLC-G3 [64]

5.3.1.2 PLC - G3

Generelt

G3 er en PLC teknologi som spesifiserer protokollene for det fysiske- og MAC-laget og ble designet for å tilby pålitelig IPv6 datakommunikasjon over kraftkabler benyttet i AMI. Standarden er utarbeidet av Maxim og er allerede implementert av store aktører innen AMS som ERDF, et av de største nettselskapene i Frankriket. G3 ble utviklet for tilby robust kommunikasjon med god ytelse tross strenge rammer satt ved bruk av kraftkabler som kommunikasjonsmedium. Samtidig skal G3 tilby kompatibilitet med eldre nettverks- og smartmåler teknologier, samt god skalerbarhet og fleksibilitet for framtidige funksjoner i AMS. Standarden er basert på åpne standarder for å støtte utstyr fra andre systemer og flere leverandører [64]. Kommunikasjonsprofilen for G3 er vist i 5.7.

Det fysiske laget

I likhet med PRIME utnytter også G3 OFDM og sender disse signaler i CENELEC A båndet. Selv om det også er støtte for FCC og CENELEC BCD bånd, var det CENELEC A bånd som først ble introdusert med spesifikasjonene for G3 [71]. G3 muliggjør kommunikasjon til tross for mye kanalstøy og interferens fra andre bånd, og har muligheten til å ta høyde for at andre smalbånds teknologier samtidig kan benyttes gjennom samme medium, i.e. PLC S-FSK. Totalt 36 databærere kan bli overført i frekvensbåndet mellom 34 kHz og 90 kHz hvor standarden spesifiserer tre forskjellige digitale modulasjonsmodus; ROBUST modus, DBPSK og DQPSK. G3 er designet for bruk i distribusjonsnett (medium: 11-22kV og lav spenning: 230V) og støtter kommunikasjon på tvers av spenningsnivå. [36]

Datalinklaget

Datalinklaget for G3 er todelt som vist på figur 5.7. MAC-laget er en implementasjon av MAC standarden for lavhastighets trådløse nettverk, Low Rate WPAN (LR-WPAN), spesifisert i IEEE 802.15.4 [80]. Dette laget håndterer overføring av MAC-rammer og sender de

til det fysiske laget for transmisjon. Kommunikasjonsprotokollen IEEE 802.15.4 er spesifisert for mindre enheter med begrensninger for fysisk størrelse og strømbruk, dermed rettet mot lavere overføringshastigheter. Som vanlig håndterer MAC-laget administrasjon av den underliggende fysiske kanalen som tilgangskontroll for transmisjon, ramme-validering etc. For detaljer henvises det til [80]. For å tillate IPv6 over IEEE 802.15.4-baserte nettverk benytter G3 et konvergenslag kalt IPv6 over Low power WPAN (6LoWPAN). Dette laget tilbyr i.e. innkapsling og header-komprimering av IPv6 pakker før de blir sendt videre til MAC-laget. Spesifikasjonene for dette konvergenslaget er utarbeidet av Internet Engineering Task Force (IETF) sin 6LoWPAN gruppe og tilgjengelig i RFC 4944. Se seksjon 6.2.1.2 for flere detaljer for 6LoWPAN.

Nettverkslag og transportlag

PLC G3 er kun spesifisert for IPv6 på nettverkslaget og benytter UDP som transportlags protokoll.

5.3.2 GPRS og EDGE

General Packet Radio Service (GPRS)

GPRS er en tilleggstjeneste som ble lagt på toppen av det allerede eksisterende kretssvitsjede kommunikasjonsnettverket Global System for Mobile Communication (GSM) for å tillate pakkesvitsjet traffikk mellom brukere og Internett. GSM er en Time Division Multiple Access (TDMA) basert trådløs kommunikasjonsteknologi på som benytter Gaussian Minimum-Shift Keying (GMSK) for signaloverføring, i Norge på frekvensbånd 900MHz og 1800MHz [6]. GPRS ble først standardisert av European Telecommunications Standards Institute (ETSI), men vedlikeholdes nå av 3rd Generation Partnership Project (3GPP). Båndbredden tilgjengelig gjennom ordinær GPRS avhenger hvor mange TDMA kanaler som dedikeres og kombineres til henholdsvis trafikk opp og ned til mobilterminalen. Organiseringen av trafikkapasitet for opp- og nedlink skjer under oppkoblingen mot nettverket og kan settes opp symmetrisk og asymmetrisk. Av de maksimalt 8 kanalene som er tilgjengelig gir en singel kanal 14.4 Kbps og maksimalt 8 kanaler 115.2 Kbps per terminal. Den opplevde båndbredden blir noe lavere da endel går med til signalisering og overhead.

GPRS benytter store deler av den eksisterende GSM-infrastrukturen men for å muliggjøre pakkesvitjet trafikk i nettverket måtte tre nye noder legges til den originale GSM-arkitekturen, Packet Control Unit (PCU), Gateway GPRS Support Node (GGSN) og Serving GPRS Support Node (SGSN). PCU er en del av Base Station Controller (BSC) eller BTS som skiller den krets- og datasvitsjede trafikken, håndterer og videresender datapakkene i radiokanalene til SGSN og GGSN. GGSN og SGSN er routere koblet til Internett hvor sistnevnte er routeren mobilterminalen er koblet til når den ikke er i hjemmenettverket. GGSN er lokalisert i hjemmenettverket for mobilterminalen og er allokert den offentlige IP-adressen for terminalen, samt at GGSN besitter den private IP-adressen til den den aktuelle SGSN om terminalen ikke er i hjemmenettverket. Selv om terminalen er koblet mot en SGSN i et fremmed nettverk er det alltid GGSN som kommuniserer med Internett på vegne av terminalen. Trafikk mellom SGSN og GGSN skjer gjennom tunnelering av IP-pakker i GPRS stammenettet. Ennå benyttes kun IPv4 over GPRS. Men det

er initiativer som er i gang med å utvikle standarder for å kunne benytte IPv6 over GPRS og liknende IP-baserte mobilnettverk [65, 29]. Alle detaljer og spesifikasjoner for GSM og GPRS finnes gjennom 3GPP hvor spesifikasjonene ligger åpent, [1].

Enhanced Data-rates for Global Evolution (EDGE)

EDGE er en forbedring og videreføring av GPRS som tillater høyere båndbredde for datatrafikk per terminal. EDGE tar høyde for at det er minoriteten av mobilterminaler koblet til en basestasjon som opplever betydelig reduksjon i signalkvalitet. Slik reduksjon kan komme av stor avstand til basestasjonen, fading og interferens med andre med andre radiosignaler etc. Ved å benytte ny modulasjonsteknologi muliggjør EDGE høyere båndbredde for de som oppfyller noe strengere krav for signaloverføringen enn GPRS gjør. I motsetning til ordinær GPRS, tar EDGE i bruk 8 Phase Shift Keying (PSK) og har kapasitet fra 236.8 Kbps til 473.6 Kbps med henholdsvis 1 til 8 kanaler. Det trengs ingen nye komponenter i GSM kjernenettet for å støtte EDGE i et eksisterende GSM nettverk. Ettersom det dreier seg kun om ny signalmodulering må små oppgraderinger gjøres i BSC og PCU, resten av nettet holdes uendret. Til tross for at dette betyr høyere last på GPRS komponentene i nettet, er slike nettkomponenter stort sett dimensjonert for utvidelser. [3]

Evolved EDGE er en utvidelse av EDGE standarden og øker båndbredden til omtrent 1 Mbps ved å benytte 16 og 32 Quadrature Amplitude Modulation (QAM), turbo koder samt høyere symbolrate. Denne oppgraderingen krever heller ingen nye noder eller andre oppgraderinger enn kun i BSC/PCU. Det er ikke alle nett som gir mulighet for Evolved EDGE ennå, men ses på som et alternativ for nett med lav prioritet for full 3G utbygging. [2]

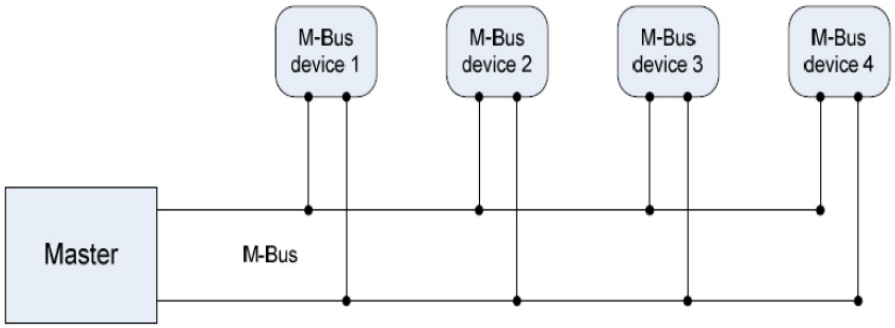
5.3.3 UMTS (W-CDMA)

Universal Mobile Telecommunications System (UMTS) regnes som den første tredjegenerasjons mobilteknologien og er arvtakeren til GSM. Forskjellen mellom GSM og tidlige versjoner av UMTS var hovedsaklig på radiogrensesnittet hvor andre metoder for multipleksing og kanalkoding ble utnyttet for å oppnå høyere båndbredde per kanal. Men UMTS nettene som bygges ut i dag har annen arkitektur enn GSM nettene og all trafikk er basert på IP. I likhet med GSM er også UMTS standardisert av ETSI og vedlikeholdes av 3GPP. Alle 3G nettverk i verden er ikke implementert helt likt og spesifikasjonene kan variere fra land til land. Vi tar i denne rapporten utgangspunkt i de standardiserte spesifikasjonene satt av ESTI.

Radiolinken i UMTS benytter frekvensbåndene 1885 - 2025 MHz og 2110 og 2200 MHz. Hovedsakelig er det en kombinasjon av Wideband Code Division Multiple Access (W-CDMA) og Frequency Division Multiple Access (FDMA) som blir benyttet i UMTS. Hver bærer i FDMA kan i tillegg bli delt inn i tidsluker som kombinerer de to allerede nevnte med TDMA. UMTS støtter dupleks overføring, hvorav det skilles på å gi opp- og nedkanalene forskjellige frekvenser eller delt i forskjellige tidsluker, respektivt FDD og TDD. Ytelsen for begge dupleksmodusene er tilnærmet like samt at FDD er mest egnet til symmetrisk trafikk og FDD er best egnet til asymmetrisk trafikk. Hastighetene som kan oppnås i UMTS varierer fra situasjon og implementasjon. Store avstander til basestasjonen, samt om terminalen er i bevegelse, begrenser drastisk tilgjengelig båndbredde.

EN 13757-1	Part 1: Data exchange
EN 13757-2	Part 2: Physical and link layer
EN 13757-3	Part 3: Dedicated application layer
EN 13757-4	Part 4: Wireless meter readout
EN 13757-5	Part 5: Wireless relaying
EN 13757-6	Part 6: Local bus

Tabell 5.2: Standarder for M-Bus - EN 13757



Figur 5.8: M-Bus nettverksstruktur [62]

Spesifikasjonene sier 2 Mbps for stillestående terminaler i nær tilknytning til basestasjonen, 384 Kbps for terminaler i bevegelse og 144 Kbps for terminaler i høy hastighet med store avstander til basestasjonen [4, 5]. I likhet med GPRS, er UMTS basert på SGSN og GGSN som fungerer på tilnærmet lik måte som i GPRS. Se seksjon 5.3.2. Home Subscription Server (HSS) i UMTS har samme funksjon som HLR i GSM og besitter data på abonnement identiteter, IP adresser/telefonnummere, sikkerhetsparametere etc. Som i GPRS er det GGSN som sitter med oppdatert informasjon om hvor UE er lokalisert og hvilken SGSN trafikk skal sendes til. UMTS er bakoverkompatibel med GSM, SS7 etc. [6]

5.3.4 EN 13757 - M-Bus

5.3.4.1 EN 13757-2 - M-Bus

Meter Bus (M-Bus), er en teknologi som ble utviklet av et samarbeid mellom professor Dr. Horst Ziegler ved University of Paderborn, Texas Instruments Deutschland GmbH og Techem GmbH. Systemet ble designet for å oppnå en- eller toveiskommunikasjon med målere for varme, gass og vann. Spesifikasjonene for M-Bus er standardisert av IEC i 6 deler, EN 13757 serien vist i tabell 5.2.

M-Bus er optimalisert for lavt energibruk og produksjonskostnader samt operere blant annet over Twisted Pair (TP)-bus og lokal bus (EN 13757-6). Da M-Bus er en bus, og ikke et nettverk, spesifiserer ikke standarden lag OSI-lag fire til seks. Derimot implementeres et administrasjonslag på tvers av alle de syv OSI-lagene. Dette administrasjonslaget håndterer e.g. adressering i det fysiske laget. Bussen har en hierarkisk modell hvor en *master*-node kontrollerer trafikken mot *slave*-nodene, figur 5.8. Masternoden er koblet mot et

innsamlingssystem og håndterer mottak og videresending av meldinger mellom slavenodene og dette innsamlingsystemet. Datalinklaget definerer fire forskjellige meldingsformater som benyttes i kommunikasjonsprotokollen. Formatet som benyttes for brukerdata kalles *Long Frame*, figur 5.9. Adresseringen skjer på basis av et felt i meldingene som kan ha verdiene 0-255 og begrenser antall noder på bussen til 250. Adresse 0 er satt som standard ved produksjon og forandres ved installasjon, og 254 og 255 er benyttet for broadcast til alle nodene på bussen, 251, 252, 253 er reservert til andre formål og framtidige utvidelser.

Applikasjonslag

Applikasjonslaget for M-Bus er basert på standard EN1434-3 som tar seg av koding av meldingene. Figur 5.9 viser de forskjellige meldingsformatene benyttet for M-Bus, kalt telegram i dokumentasjonen, [72]. Det er applikasjonslaget som står for kodingen av meldingene og direkte kommunikasjon med datalinklaget for transmisjon av disse mellom nodene på bussen. 13757-3 spesifiserer også at leverandør- og produktspesifikke applikasjoner skal kunne implementeres i applikasjonslaget, e.g. sikkerhetsmekanismer. Meldingsformatene definert for M-Bus er satt sammen av en en struktur bestående av:

- Meldingstypeindikator som spesifiserer hvilken retning meldinger sendes mellom master- og slavenoder.
- Dataheader som spesifiserer informasjon vedrørende nodestatus, krypteringsinformasjon etc. Mengden av dataheaderinformasjon er avhengig av meldingstypen.
- Variable datablokker for brukerdata
- Produsentspesifikke variabler

5.3.4.2 EN 13757-4 - Wireless M-Bus

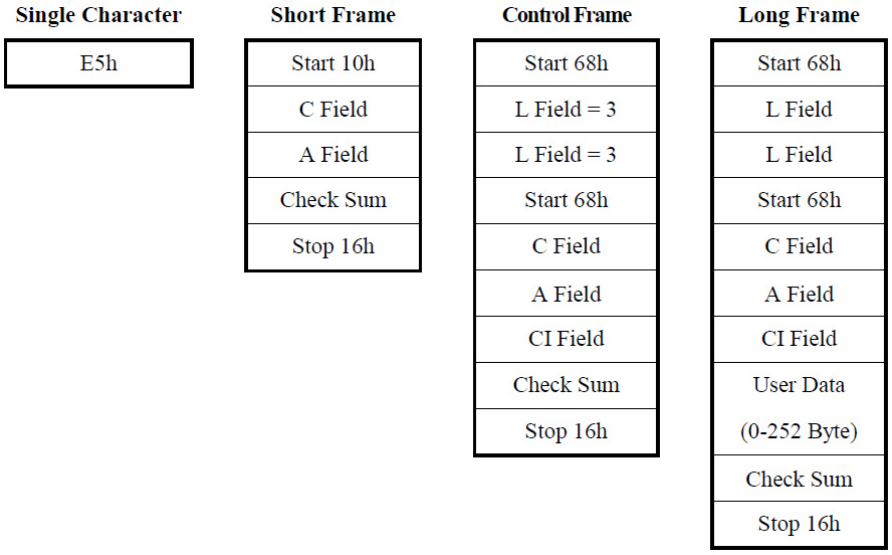
Trådløs M-Bus er spesifisert i EN 13757-4. Radioløsningen benytter frekvensbånd 868 - 980 MHz Short Range Device (SRD) og har en maksimal radius på 15m [4]. Nettverksstrukturen for trådløs M-Bus er vist i figur 5.10 og er noe ulik den kabelbaserte versjonen.

5.3.5 LonWorks

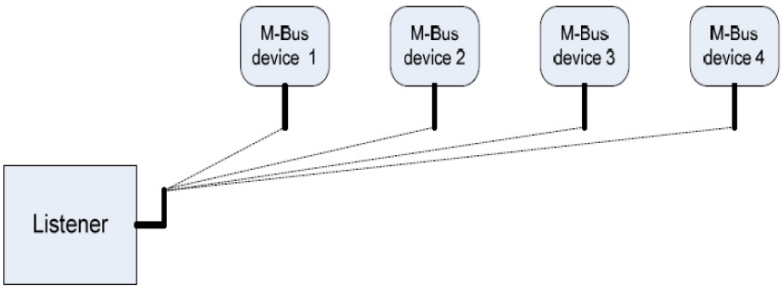
LonWorks er en nettverksplattform spesialdesignet for kontrollapplikasjoner. Ved bruk i AMS benyttes LonWorks som regel mellom målernoder og konsentratorer. Plattformen ble utviklet av Echelon Corp. i 1988 og er i ettertid standardisert av mange av de viktige standardiseringsorganisasjonene som GB, CECED, ISO, IEC, ANSI, CEA. Teknologien er helt åpen og spesifikasjonene er tilgjengelig gjennom LonMark Interoperability Association.

Kjernen i LonWorks er basert på deres egendesignede Neuron brikke og kommunikasjonsprotokollen LonTalk. Neuron brikken finnes i forskjellige varianter avhengig av implementasjon, men alle har lik arkitektur og er basert på 3 prosessorer som hver håndterer distinkte oppgaver; en for prosesser i MAC-laget, en for prosesser i nettverkslaget som

[4] Kan bli utvidet ved å benytte relémetoder spesifisert i EN 13757-5



Figur 5.9: M-Bus telegramformater [72]



Figur 5.10: Nettverksstruktur for trådløs M-Bus [61]

tar hånd om routing, adressering etc. Den siste prosessoren er en 8-bits prosessor for håndtering av egendefinerte applikasjoner. Om ønsket kan denne prosessoren implementeres som et rele mot en ekstern kraftigere prosessor slik at Neuron kun håndterer kommunikasjonen gjennom LonTalk. Dette designet ble valgt for å frakoble prosessorkraften som trengs til kommunikasjonshåndtering fra applikasjonsprosessene.

LonWorks er designet til å kunne operere over mange forskjellige medier men ble hovedsakelig designet for TP og kraftkabler basert på Differential Manchester koding. Neuron brikken har innebygget transciever for disse formålene. Gjennom ekstern transceiver kan også fiber, Infrared (IR), Radio Frequency (RF) og coaxialkabler benyttes. Overføringskapasiteten som kan oppnås er avhengig av implementasjon men normalt for kraftlinje er 5-10 kbit/s avhengig av frekvensen brukt, mens TP og fiber kan begge oppnå 1250 kbit/s. [44]

LonTalk protokollen omfavner alle 7 lag av OSI-modellen og er implementert i Neuron brikkens ROM. Protokollen baserer seg på et to typer meldinger; Standard Network Variable Types og Explicit Messages. Disse meldingene spres mellom nodene i nettverket basert på det som kalles *inn*- og *ut*-bindinger. En variabel som er definert som *ut* for en node er bundet opp mot en annen node hvor samme variabel er definert som *inn*. Adressering i nettverket skjer enten på basis av en unik 48-bits Neuronbrikke-ID som er kodet inn i brikken fra produksjon, en logisk brikke-ID som kan forandres eller på subnet-ID. [44]

5.3.6 SITRED

På begynnelsen av 90-tallet startet Italias største kraftselskap ENEL et prosjekt for å utvikle et system for sentralisert avlesning og styring av strømmålere og nettstasjoner i distribusjonsnettet. Systemet ble utviklet for toveis kommunikasjon på mellom- og lavspenningsdistribusjonsnett ved bruk av PLC. Dette kommunikasjonssytemet hadde to kommunikasjonsprofiler som skilles på bruk av forskjellig protokoller for linklaget og det fysiske laget. Den ene profilen er basert på LonTalk-protokollen, se seksjon 5.3.5, og den andre profilen er basert på ENELs proprietære protokollstakk, kalt SITRED (Integrated System for data Transmission on Electricity Distribution network). Begge profilene benytter samme proprietrære applikasjonslagsprotokoll. I følge OPENmeter støtter applikasjonslaget funksjonalitet for meldingsutveksling, nettverksadministrasjon samt sikkerhetsmekanismer(se seksjon 6.2.1.6) [62]. SITRED støtter foreløbig kun konsentratorløsninger hvor PLC er benyttet mot målernoden og GSM, PSTN eller satellitt benyttes mot sentralsystemet. For PLC spesifiserer SITRED Frequency Shift Keying (FSK) modulasjon i CENELEC A-båndet, definert av standard IEC 61334-5-2, som er robust men har relativt begrenset båndbredde på 2400 baud [25]. Ettersom SITRED er en proprietær løsning er ikke full spesifikasjon og dokumentasjon tilgjengelig.

5.4 Applikasjonslagprotokoller og dataformater

Denne seksjonen vil presentere enkelte applikasjonslags protokoller for bruk innen AMS. Enkelte av protokollene spesifiserer også transportlaget og/eller datamodell. Sikkerhetsar-

kitektur og sikkerhetsmekanismer for de aktuelle applikasjonslagprotokollene blir presentert i seksjon 6.2.2.

5.4.1 DLMS/COSEM - IEC 62056

Generelt

Device Language Message Specification (DLMS) er utviklet og driftes av DLMS User Association som i dag er den største målerorganisasjonen i Europa. DLMS er endel av IEC 62056 serien protokoller som er standardisert av Comité Européen de Normalisation / Committee for Standardization (CEN). Protokollen for applikasjonslag i DLMS er definert av Companion Specification for Energy Metering (COSEM). Spesifikasjonene for DLMS/COSEM er åpne og finnes på brukerorganisasjonens hjemmesider, [11], tilgjengelig for brukerorganisasjonens medlemmer. Spesifikasjonene[5] er definert i det brukerorganisasjonen kaller *coloured books*. Av de fire bøkene som beskriver standarden, beskriver den blå boken COSEM objektmodell og objektidentifikasjonssystem og den grønne boken DLMS/COSEM arkitekturen og protokoller. Standarden brukes allerede av selskaper i flere land [12] og kan benyttes over de aller fleste kommunikasjonsmedier innen AMS som GSM, GPRS, PSTN, xDSL, PLC, fiber, M-Bus etc. Bruk av DLMS/COSEM over IP-baserte løsninger og kommunikasjonsløsninger over PLC er spesifisert i IEC62056-serien av standarder.

Dataformat

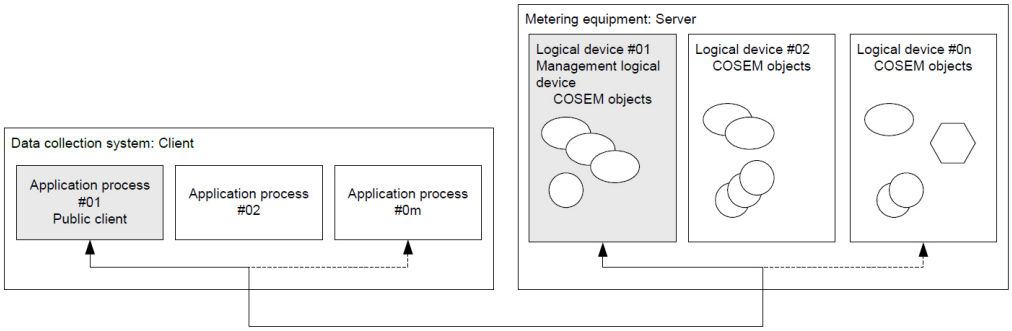
Når en måler skal leses av blir de aktuelle attributtene aksessert av DLMS laget, pakket inn i en DLMS Application Protocol Data Unit (APDU) før den blir sendt videre til transportlaget. Standarden spesifiserer datamodellen COSEM, identifikasjonssystemet Object Identification System (OBIS) og meldingssystemet DLMS. COSEM er en objektorientert modell som har spesifisert en rekke grensesnittklasser som kalles objekter(IEC 62056-62). Disse objektene adresseres av det logiske adresseformatet OBIS og inneholder attributter og metoder som kan identifisere objektet og utføre enkelte funksjoner(IEC 62056-61). Slik modelleres hver måler som en fysisk enhet med en eller flere logiske enheter avhengig av funksjonaliteten. Hver av disse logiske enhetene kan ses på som applikasjonsprosesser i COSEM.

Innen AMS er det sentralsystemet, konsentratorer eller andre enheter som samler inn data som har klient-rolle. Målerutstyret har rollen som server og blir aksessert av klienten for tjenester som er tilgjengelige. Hver klient har en spesifikk rolle for hver server, som gir tilgang til de forskjellige tjenestene i henhold til de forskjellige rollene. Denne koblingen mellom roller og deres tilgang til tjenester er definert gjennom *Association* objekter og vist i figur 5.11a og 5.11b.

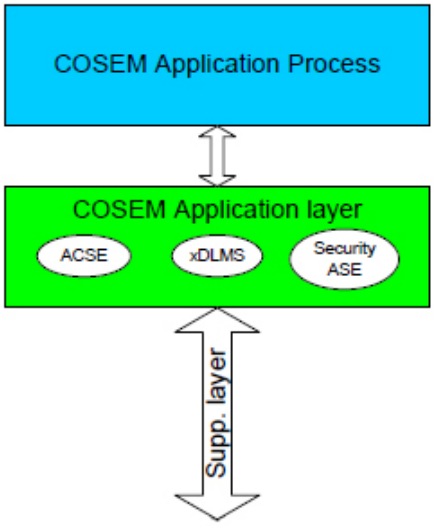
Applikasjonslag

Applikasjonslaget innholder to hovedelementer: The Association Control Service Element (ACSE) og xDLMS. ACSE tar hånd om administrasjon av applikasjonassosiasjoner mellom de logiske enhetene og grensesnittobjektene. DLMS/COSEM er en utvidelse av DLMS standarden og tilfører et bransjespesifikk domene for målerenheter

[5]Diskusjonen i denne rapporten er basert på de utdrag av standarden og informasjon tilgjengelig på brukerforeningens nettsider og er referert henholdsvis. Se seksjon 1.5 for begrunnelse.



(a) Applikasjonsprosesser og logiske enheter i COSEM [65]



(b) Lagdelt applikasjonslagsmodell i COSEM [13]

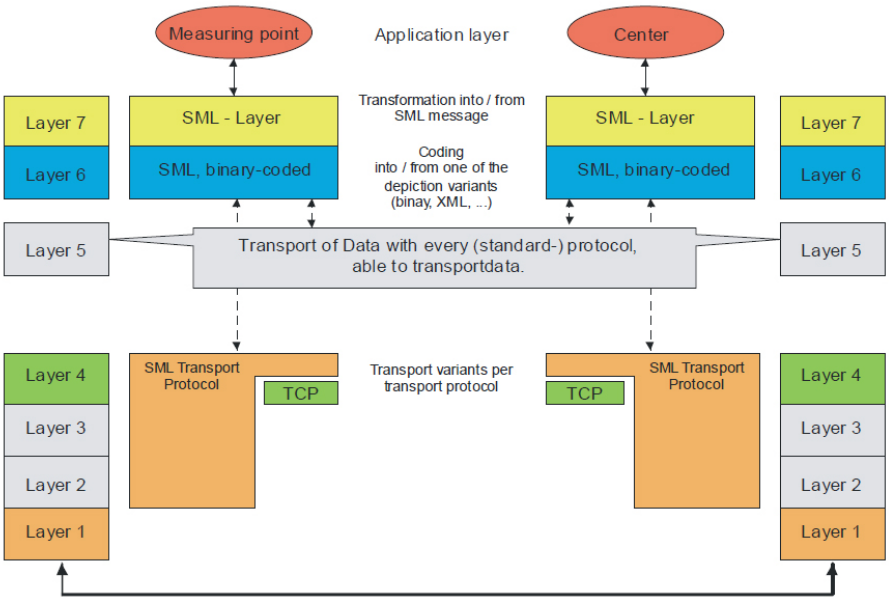
Figur 5.11: Overordnet applikasjonslagarkitektur for COSEM

og systemer for den eksisterende objektmodellen. xDLMS håndterer dermed kommunikasjonen mellom COSEM applikasjonsprosessene, og sørger for bakover kompatibilitet med den grunnleggende DLMS standarden.

5.4.2 SML

SML er en kommunikasjonsprotokoll utviklet av flere store selskaper innen kraftbransjen, E.ON, RWE, EnBW og Landis+Gyr gjennom et tysk prosjekt kalt SyM^2. Konseptet med SML var å utviklet en protokoll for applikasjonslaget for sentral datainnhenting og konfigurerering spesielt designet for bruk i kraftnett. Spesifikasjonene for protokollen er åpne men standardisering er fortsatt under arbeid av IEC.

Målet for protokollen var å designe en enkel struktur som var brukelig for innebygde systemer med strenge krav til resursbruk. Protokollen spesifiserer kun applikasjonslaget hvor den spesifiserer datamodell samt fil og dokumentstruktur for overføring av data mellom målernodene og sentralsystemet. Derimot spesifiserer den ikke objektmodell sammenliket med DLMS/COSEM standarden. På denne måten beskriver SML meldingsstruktur og lar funksjonssett og grensesnittklasser håndteres av andre standarder eller spesifikajoner. Protokollen har en sjulags OSI-modell hvor lag seks gir valg mellom XML-basert koding eller mer effektiv SML binærkoding [93], se figur 5.12.

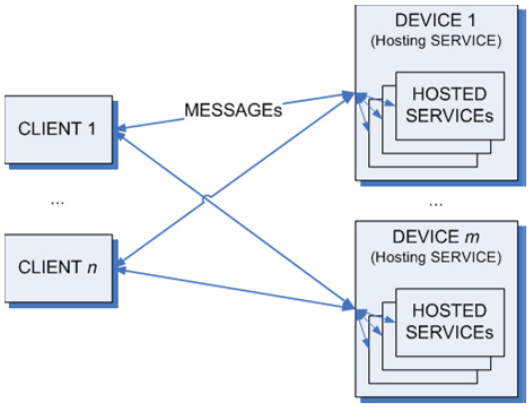


Figur 5.12: Kommunikasjonsmodell for SML [93]

SML ble designet for å være uavhengig utstyrsleverandør og av underliggende kommunikasjonsprotokoller noe som gjør applikasjonslagsprotokollen til et fleksibelt alternativ. Mest vanlig kommunikasjonsprofil er basert på TCP/UDP over IP som gjør at protokollen er tilgjengelig over en rekke underliggende kommunikasjonsmedier.

5.4.3 DPWS

Devices Profile for Web Services (DPWS) definerer en arkitektur for å muliggjøre implementasjon av sikre *web-services*[6] for enheter med strenge krav til resursbruk e.g. innbygde systemer. Arkitekturen håndterer alle ordinære web-service-tjenester som meldingsutveksling, tjenesteoppdagelse, tjenestebeskrivelse etc. DPWS 1.1 ble godkjent som standard av Organization for the Advancement of Structured Information Standards (OASIS) juni 2009 og bruk av standarden er lisensbasert.



Figur 5.13: Kommunikasjonsmodell for web services i DPWS

DPWS er basert på etablerte web-service standarder som Extensible Markup Language (XML) meldingsformat, Web Services Description Language (WSDL) standard for web-service-tjenestebeskrivelser samt Simple Object Access Protocol (SOAP) som standard protokoll for meldingsutveksling. DPWS spesifiserer kun protokoll for applikasjonslaget og benytter Hypertext Transfer Protocol (HTTP) og støtter både TCP og UDP som transportlagsprotokoll. Figur 5.13 viser den overordnede kommunikasjonsmodellen for DPWS. I et AMS vil både målernoder, `DEVICE` i figuren, settes opp med web-services som er tilgjengelig for sentralsystemet, `CLIENT` i figuren. Med hensyn til at DPWS spesifiserer en web-service-arkitektur basert på andre standarder beskrives ikke disse nærmere i denne oppgaven. For spesifikasjoner henvises det til DPWS dokumentasjonen [59] samt de respektive standardene for web-services brukt.

[6]Som definert av World Wide Web Consortium (W3C) `http://www.w3.org/2002/ws/`

Kapittel 6

Analyse og vurdering av informasjonssikkerhet for AMS-kanalen

Operasjon	Sikkerhetstjeneste
Innsyn / lese (Interception)	Konfidensialtet
Skape / skrive (Fabrication)	Integritet, autentisering
Modifisere (Modification)	Integritet
Slette / blokkere (Interruption)	Integritet, tilgjengelighet

Tabell 6.1: Tolking av krav til sikkerhetstjenester for data

6.1 Tolking av NVEs krav til informasjonssikkerhet

I denne seksjonen ser nærmere på NVEs krav til informasjonssikkerhet som ble presentert i seksjon 2.2.3.2. Hvert krav vil tolkes og for å se hvilke sikkerhetstjenester som må på plass for å oppfylle de forskjellige kravene som er satt. Kapittel 6 presenterer hvilke sikkerhetsmekanismer som kan benyttes i AMS for møte kraven som er satt og oppnå et akseptabelt nivå informasjonssikkerhet. Det generelle kravet om at " g) AMS skal gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner" må studeres. Da det ikke stilles direkte krav til sikkerhetstjenester vil det defineres gjennom tolkning av det generelle sikkerhetskravet til AMS. Ettersom kravene til sikkerhetstjenester som settes i denne oppgaven kun er basert på tolkninger er de ikke endelige. Krav til sikkerhetstjenester vil derfor kunne variere med tolkninger gjort av andre. Sikkerhetstjenester vil vurderes i forhold til mulige operasjon/angrep på informasjon i transitt ble lagt fram i seksjon 4.5.2.

NVE setter ingen definerte krav for informasjonssikkerhet for kommunikasjonssystemet i AMS, dermed gjelder det generelle kravet om informasjonssikkerhet også for kommunikasjonssystemet. For dette kravet tolkes ordet *sikkerhet* til å bety sikring mot uautoriserte eller ondartede tilsiktede operasjoner eller handlinger. Uautoriserte tilsiktede operasjoner kan utføres av og omfatter alle autoriserte og uautoriserte brukere og komponenter med tilgang til systemet. Dette kravet kan dermed tolkes som at AMS skal garantere for at alle operasjoner som utføres, både mot data og styrefunksjoner, er autoriserte. Dette vil videre si at AMS skal kunne forhindre alle operasjoner av uautoriserte brukere, samt uautoriserte operasjoner av autoriserte brukere. Ettersom det skilles på krav for data og styringssignaler, vil de respektive nå studeres separat.

6.1.1 Krav for data

Ordet "misbruk" vil kunne inkludere alle operasjoner med tanke på data. Alle uautoriserte utførelser av de respektive operasjonene kan ses på som misbruk av data. Tabell 6.1 viser hvilke sikkerhetstjenester som kan oppfylle de forskjellige kravene for data. Ved å benytte mekanismer som kan tilby konfidensialitet for datatrafikk vil man kunne hindre uautorisert innsyn. Om datatrafikk autentiseres og integriteten kan garanteres vil det ikke vær mulig å skape falsk datatrafikk. Om integriteten av data sjekkes vil ikke uautoriserte modifikasjoner være mulig. Om integriteten og tilgjengeligheten for datatrafikken kan sikres vil ikke uautorisert sletting eller blokkering skje uten at det blir oppdaget.

Operasjon	Sikkerhetstjeneste
Innsyn / Motta (Interception)	Konfidensialtet
Sende / Skrive (Fabrication)	Integritet, autentisering
Modifisere (Modification)	(Ingen krav)
Blokkere / Slette (Interruption)	(Ingen krav)

Tabell 6.2: Tolking av krav til sikkerhetstjenester for styringssignaler

6.1.2 Krav for styrefunksjoner

På lik måte som for data kan uautorisert tilgang til styrefunksjoner ses på som 'uønsket tilgang'. Kravet spesifiserer at det er mot 'styrefunksjoner' man skal gi sikkerhet mot uautorisert tilgang. Med benevnelsen styrefunksjon tolkes det i denne sammenheng at det er funksjonaliteten for sending og mottak av styringssignaler som skal sikres. I hovedsak vil dette innebære at det ikke skal være mulig å sende styringssignaler som ikke er autentiske, samt uautorisert mottak av autentiske styringssignaler. Tabell 6.2 viser hvilke sikkerhetstjenester som kan oppfylle de forskjellige kravene for styringssignaler. Uautorisert mottak av styringssignaler vil si det samme som å ha innsyn til innhold av slik trafikk, i.e. å ha innsyn til styringssignaler som sendes i AMS-kanalen. Slik uautorisert innsyn til styringssignaler vil unngås ved konfidensialitet. Å sende uautoriserte styringssignaler vil ikke være mulig om slik trafikk autentiseres og integriteten av slike meldinger sjekkes. Våre tolkninger av NVEs krav til informasjonssikkerhet setter ingen krav til modifikasjoner eller blokkering av styringssignaler.

6.2 Analyse av kommunikasjonsteknologi benyttet innen AMS

Det vil nå presenteres sikkerhetsarkitekturene for de forskjellige kommunikasjonsprotokollene lagt fram i kapittel 5. Det vil også her skilles på protokoller som definerer hele eller deler av protokollstakken og protokoller for applikasjonslaget. Disse studiene vil være grunnlag for vurderingen av sikkerheten i AMS-kanalen i dette kapittelet.

6.2.1 Kommunikasjonsprotokoller

6.2.1.1 PLC PRIME

PRIME tilbyr sikkerhetsfunksjonalitet i MAC-laget og definerer hovedsakelig to av totalt fire mulige sikkerhetsprofiler, hvor de forskjellige profilene kan benyttes etter behov. De forskjellige profilene er [9] :

Profil 0 er definert for transmisjon av data hvor konfidensialitet, autentisering og integritet ikke er nødvendig. Trafikk sendt med denne sikkerhetsprofilen flyter derfor åpent gjennom nettet og verifiseres verken av sender eller mottaker.

Profil 1 implementerer mekanismer for kryptering, autentisering og integritet av data basert på 128-bit AES-ECB og Cyclic Redundancy Check (CRC). Kryptering av data er på grunnlag av AES kryptering, autentisering basert på hemmelighold av nøkler for avsender og mottaker, integritet er basert på kryptert CRC-sjekksum.

Profil 2 og 3 De to siste sikkerhetsprofilene er ikke definert og tillater mulige framtidige utvidelser.

Konfidensialitet	128-bit AES-ECB
Integritet	Kryptert CRC sjekksum
Autentisering	Basert på hemmelighold av kryptonøkler

Tabell 6.3: Sikkerhetsmekanismer for PLC PRIME

6.2.1.2 PLC G3

Sikkerhetsmekanismer for PLC G3 er implementert i MAC-laget. G3 benytter MAC lag definert av IEEE 802.15.4.

IEEE 802.15.4 MAC-lag sikkerhetsmekanismer

MAC-laget definert for 802.15.4 implementerer mekanismer for kryptering, integritetssjekk samt mekanismer for å hindre duplikatmeldinger. Kryptering av data benyttet i denne spesifikasjonen er basert på CCM* som er en konfigurasjon av standard Counter with CBC-MAC (CCM) block cipher for bruk i IEEE 802.15.4. CCM* tilbyr to tilleggsmodus til de ordinære CCM funksjonalitetene; kun kryptering og kun meldingsintegritet. Advanced Encryption Standard (AES) er spesifisert som block cipher også for CCM*. [80]. Det er også mulighet for å tilby konfidensialitet og meldingsintegritet gjennom EAP som blir beskrevet i neste avsnitt.

IEEE 802.15.4 baserer seg på Extensible Authentication Protocol (EAP) for autentisering og tillater ingen noder å aksessere nettverket uten initiell identifisering og autentisering. Denne initielle autentiseringsmekanismen er en del av det som i dokumentasjonen blir kalt 6LoWPAN Bootstrapping Protocol (LBP). Identifiserings- og autentifiseringsprosessen benytter to parametere som er unik for hver node i nettverket; EUI-48 MAC adresse og en 128-bit PSK som er kjent kun for noden og autentiseringsserveren. Autentiseringsmatrialet, som aksesslister, akkreditiver etc., kan enten bli implementert manuelt i hver node i nettet eller blir administrert automatisk . For sistnevnte videresender nodene i nettet EAP-meldinger mot Authentication, Authorization, Accounting (AAA)-serveren gjennom en standard AAA protokoll i.e. RADIUS. EAP-protokollen er veldig fleksibel og gir muligheter for flere forskjellige autentiseringsmetoder, EAP-MD5, EAP-AKA, EAP-TLS etc. Anbefalt oppsett for G3 er EAP-PSK med AES-128. For flere detaljer se dokumentasjon for EAP-PSK og G3, [35].

IPv6/IPsec over IEEE 802.15.4

Selv om G3 er designet for IPv6 på nettverkslaget, er det ikke ennå muligheter for å benytte IPsec i G3. Som beskrevet i seksjon 5.3.1.2 benytter G3 et MAC-lag spesifisert for lav-hastighets trådløsnett og benytter konvergenslaget 6LoWPAN. 6LoWPAN er innebygget i MAC-laget mellom linklaget og nettverkslaget som vist på figur 5.7. Dette laget utfører innkapsling og headerkomprimering av IPv6 pakkene før de sendes, noe som ikke

er kompatibelt med IPsec per skrivende tidspunkt. Raza et al. legger i sin rapport fram et forslag for en utvidelse av dette konvergenslaget med støtte for IPsec. Deres forslag støtter både Authentication Header (AH) og Encapsulation Security Payload (ESP) sikkerhetsassosiasjoner[1]. Deres design muliggjør dermed autentisering, kryptering og integritetssjekk basert på veletablerte Internet Protocol version 6 (IPv6) mekansimer. [31]

Det er også andre aspekter å vurdere om man skal implementere IPsec over 802.15.4-baserte nettverk. IPsec ble designet for sikker kommunikasjon mellom noder med få begrensninger med tanke på prosessringskraft og trafikk mot nettet etc. Det er derfor ikke en protokoll som er optimalisert for å minimere meldingsutveksling og trafikk mot nettet. IPsec vil derfor produsere mer overhead og båndbredde enn hva som ofte er ønsket av noder som kjører en stakk med 802.15.4 og 6LoWPAN. [30]

Konfidensialitet	MAC-CCM*-AES-128, EAP-PSK, EAP-TLS
Integritet	CCM*
Autentisering	EAP-PSK

Tabell 6.4: Sikkerhetsmekanismer for PLC G3

6.2.1.3 GSM, GPRS / EDGE

GPRS var tilleggsfunksjonalitet som ble innført i GSM fra og med Release 97. GPRS benytter mange av de samme sikkerhetsmekanismene som eksisterte for den kretssvitsjede trafikken i tillegg til noen særegne for pakketrafikk. Forskjellen er at det er SGSN som håndterer sikkerhetsmekanismene for GPRS i motsetning til BSC for resterende trafikk i GSM. Da EDGE kun er en videreføring av GPRS, og baserer seg på samme arkitektur med annen signalmodulering, vil de samme mekanismene gjelde for både EDGE og GPRS. Man kan gruppere sikkerhetsmekanismer for GPRS inn i disse hoved komponentene:

- Subscriber Identity Module (SIM)
- Konfidensialitet av abonnement identiteter
- Autentisering av abonnement identiteter
- Konfidensialitet for brukerdata- og signaliseringstrafikk mellom MS og SGSN
- Informasjonssikkerhet i GPRS stammenett

De tre første punktene i listen over er felles for både kretssvitsjet trafikk og GPRS, de to siste er spesifikke for GPRS. SIM er et kort unikt per abonnement og benyttes til flere sikkerhetsmekanismer innen GSM/GPRS. SIM utfører identifisering av abonnementet mot nettetverket på grunnlag av International Mobile Subscriber Identity (IMSI) lagret i SIM og Authentication Center (AuC). Autentisering av abonnementet mot nettet skjer på grunnlag av algoritmen *A3* og hemmelig nøkkel *Ki* kun kjent for SIM og GSM-nettverksoperatøren. Konfidensialitet av datatrafikk basert på algoritmene *A5* og *A8*.

[1] IPsec blir presentert i seksjon 7.3.3

GPRS benytter deler av autentiseringsprosedyrene allerede definert for ordinær GSM. Forskjellen er at det er SGSN som håndterer sikkerhetsmekanismene for GPRS i motsetning til BSC for resterende trafikk i GSM [7]. Konfidensialiteten av data- og signaliseringstrafikk skjer på grunnlag av kryptering av linkene mellom ME og SGSN. Krypteringsalgoritmen som benyttes i GPRS, GPRS Encryption Algorithm (GEA) finnes i tre versjoner, GEA1, GEA2 og GEA3-A5/3, og er implementert i ME og SGSN. Hvilken av disse algoritmene som blir benyttet, eventuelt om kryptering ikke skal benyttes, avtales mellom ME og SGSN under den initielle autentiseringen mot nettverket. GEA1-GEA3 er implementert i logiske link kontroll laget og spesifikasjonene av de respektive algoritmene er aldri publisert og holdes hemmelig av 3GPP.

Sikkerheten på GPRS stammenettet varierer og er opp til nettverksoperatørene. GPRS kommunikasjonen i stammenettet er todelt; signalisering og brukerdatatrafikk. Signaleringstrafikk for GPRS skjer gjennom Signaling System no 7 (SS7) via Mobile Application Part (MAP) protokollen spesifisert av 3GPP og har ingen innebygde sikkerhetsfunksjoner for GPRS funksjonaliteten. Brukerdatatrafikken gjennom GTP-protokollen mellom SGSNer og GGSNer har heller ingen standardiserte sikkerhetsmekanismer spesifisert. Dette gjelder både på stammenettet innad og imellom nettverksoperatørene og når trafikken går via Internett. Xenakis, [96], lister opp noen vanlige sikkerhetsmekanismer nettverksoperatørene bruker å benytte for stammenettet:

- Network Address Translation (NAT) for å forhindre ikke-autorisert trafikk inn i stammenettet
- Brannmurer ved alle GGSN for å forhindre (a)forhindre eksterne angrep fra Internett mot ME og elementer i stammenettet, (b) forhindre at ME mottar ikke-autorisert trafikk.
- Statisk Virtual Private Network (VPN) koblinger mellom nettverkselementer for å oppnå konfidensialitet for traffikk. I.e. mellom SGSN og GGSN, mellom forskjellige GPRS stammenett.
- Brannmurer ved alle BG, samt statiske VPN koblinger mot andre BGer.

Konfidensialitet	Kryptering av signalerings- og brukerdata, mellom ME og SGSN, algortimesett GEA1-3
Integritet	Signaliseringsdata, 32-bit MAC, A_3
Autentisering	Signaliseringsdata, 32-bit MAC, A_3

Tabell 6.5: Sikkerhetsmekanismer for GSM/GPRS

6.2.1.4 UMTS

Informasjonssikkerheten i UMTS bygger på prinsippene fra sin forgjenger GSM. Selv om store deler av suksessen bak GSM var nettets stabile og solide arkitektur, viste det seg i ettertid at den hadde sine svakheter [48, 92]. Et av hovedmålene for UMTS var derfor å

Nettverksaksess	Tar i hovedsak for deg sikker tilknytning til 3G nettverket samt beskytter mot angrep på radiolinken
Nettverkssikkerhet	Beskriver sikkerhetsmekanismer for kommunikasjon mellom elementer i operatørens nettverk
Brukersikkerhet	Sikrer mobilterminalen mot angrep
Applikasjonssikkerhet	Tar for seg sikkerhet for tjenster og applikasjoner, både for bruker og nettverk, UMTS nettet
Synlighet og konfigurasjon av sikkerhet	Opplysning om hvilke sikkerhetsmekanismer som blir benyttet når man er koblet til et UMTS, samt opplysning til brukeren om hvilke sikkerhetsmekanismer som er tilgjengelige

Tabell 6.6: Sikkerhetsområder i UMTS

skape et nettverk hvor sikkerhetsproblemene for GSM ble utbedret i tillegg til nye sikkerhetsmekanismer ikke støttet av GSM. Målet for UMTS sikkerhetarkitekturen i UMTS var derfor å skape et nettverk som var fleksibelt og kunne tilpasses nye sikkerhetsutfordringer samt bakoverkompatibelt med GSM. Bakoverkompetabiliteten mellom UMTS og GSM fører også til sikkerhetsutfordringer i grensesnittene mellom nettverkene [92]. Spesifikasjon for sikkerhetsarkitekturen i UMTS deler opp i fem forskjellige seksjoner [6]:

Når en abbonent, kalt UE , kobler seg til det lokale UMTS nettverket iverksettes Authentication and Key Agreement (AKA)-protokollen. Denne protokollen utfører initiell autentisering og lar UE og det lokale UMTS nettverket avtale sikkerhetsparametere som valg krypteringsalgoritme, generering av krypteringsnøkkel etc. I motsetning til GSM tilbyr UMTS tosidig autentisering, hvor nettverket også må identifisere og autentisere seg for mobilterminalen. Dette skjer på basis av at det lokale nettverket må bevise for brukeren at det er godkjent av hjemmenettverket ved bruk av en autentiseringsvektor sendt fra hjemmenettverket til det tjenende lokale nettverket. SIM autentiserer nettverket på grunnlag av å verifiserer en meldingsautentiseringskode generert av lokalnettverket. Nettverket autentiserer UE på lik måte som i GSM på grunnlag av sammenlikning av RES generert av både SIM og SGSN. UMTS tilbyr integritetssjekk av signaliseringtrafikk. Denne integritetskontrollen blir utført av UE og RNC og er implementert i UMTS Integrity Algorithm (UIA). Algoritmen som benyttes i UIA er i spesifikasjonenene kalt *f9*. Denne algoritmen produserer en 32-bits meldingsautentiseringskode, MAC-I, som sendes med meldingen over radiolinken. Mottakeren genererer også en meldingsautentiseringskode basert på den mottatte meldingen, XMAC-I, som sammenliknes med den mottatte MAC-I. Både signalisering og brukerdata er kryptert mellom UE og RNC. I likhet med GSM, benyttes det også her symmetrisk kryptering basert på nøkkel, CK, kjent for både RNC og UE. Algoritmen som benyttes for konfidensialitet kalles UMTS Encryption Algorithm (UEA) hvor kjernefunksjonen er *f8* som er en del av algoritmesettet KASUMI definert for UMTS. Både *f8* og *f9* inngår i KASUMI som er en 64-bits block-cipher med Feistel struktur. Samme algoritme blir benyttet til både kryptering og dekryptering og tar inn en 128-bits nøkkel som blir brukt til å generere en ny nøkkel for hver runde internt i algoritmen. [6]

Konfidensialitet	128-bit kryptering av signalisering- og brukerdata mellom UE og RNC
Integritet	Signaliseringstrafikk, 32-bit MAC, f_9
Autentisering	Signaliseringstrafikk, 32-bit MAC, f_9

Tabell 6.7: Sikkerhetsmekanismer for UMTS

6.2.1.5 LonWorks

LonWorks implementerer ingen sikkerhetsmekanismer utenom en meldingsautentisering og all kommunikasjon sendes åpent over transmisjonsmediet. Dette valget ble tatt på grunnlag av at hemmelighold av trafikk ikke var et krav, men integriteten av meldinger skulle kunne bevises. Denne meldingsautentiseringen er basert på en proprietær en-veis hashfunksjon hvor speifikasjonene holdes hemmelig. Autentiseringsmekanismen blir i tidlige dokumentasjoner omtalt som kryptering, noe som kan skape forvirring. [45]

Hver node i nettverket har en 48-bit autentiseringsnøkkel som kan defineres av brukeren. Denne nøkkelen distribueres mellom nodene før de blir installert. Denne må ikke forveksles med Neuron brikke ID. Når en node `B` mottar en melding, `APDU`, kalkuleres et tilfeldig tall `r`, av algoritme `R()` , som sendes tilbake til avsender `A`. `A` benytter autentiseringsalgoritmen til å produsere hash, $\texttt{H}_A$, på basis av `APDU`, `r` og autentiseringsnøkkelen til mottakeren av meldingen. Dette resultatet, $\texttt{H}_A$, sendes tilbake til `B` som benytter samme autentiseringsalgoritme og parametere for å produsere $\texttt{H}_B$. Om $\texttt{H}_A$ er lik $\texttt{H}_B$ er meldingen autentisert og meldingsinnholdet blir prosessert. [45]

Konfidensialitet	Nei
Integritet	48-bits proprietær hashalgoritme
Autentisering	Basert på hemmelighold av nøkler

Tabell 6.8: Sikkerhetsmekanismer for LonWorks

6.2.1.6 SITRED

SITRED er en proprietær protokoll og dokumentasjon derfor utilgjengelig. Det er dermed uvisst hvordan SITRED implementerer sin sikkerhetsakitektur. I følge OPENmeter tilbyr SITREDs applikasjonslag sikkerhetsmekanismer som kryptering, autentisering og beskyttelse mot duplikatmeldinger [62]. Det er derfor uvisst hvordan disse mekanismene fungerer samt hva de beskytter e.g. om autentisering tilbyr integritetssjekk av både sender/mottaker samt data-integritet.

Konfidensialitet	Ja, i følge OPENmeter [62]
Integritet	Ja, i følge OPENmeter [62]
Autentisering	Ja, i følge OPENmeter [62]

Tabell 6.9: Sikkerhetsmekanismer for SITRED

6.2.1.7 EN 13757 - M-Bus

EN 13757-3, spesifiserer at leverandør- og produktspesifikke applikasjoner skal kunne implementeres i applikasjonslaget. I samme standard er det også spesifisert kryptering basert på en kombinasjon av Digital Encryption Standard (DES) og Cipher Block Chaining (CBC), som var anbefalt krypteringsalgoritmer da disse standardene først ble skrevet. I dag er denne DES erklært usikker [82].

Man står dermed fritt for å implementere andre sikkerhetsmekanismer i applikasjonslaget. Avhengig av hvilke overføringsteknologi og modus man benytter må disse sikkerhetsmekanismene kunne oppfylle tidskravene spesifisert i dokumentasjonen for M-Bus med hensyn til prosseserings- og responstid. Radiocrafts har produsert en brikke for trådløs M-Bus, RC1180-MBUS, implementert med 128-bit AES kryptering[10]. Meldingsautentisering støttes derimot ikke av M-Bus.

Konfidensialitet	56-bit DES, 128-bit AES
Integritet	Nei
Autentisering	Nei

Tabell 6.10: Sikkerhetsmekanismer for 13757 M-Bus

6.2.2 Applikasjonslagprotokoller og dataformater

6.2.2.1 DLMS/COSEM - IEC 62056

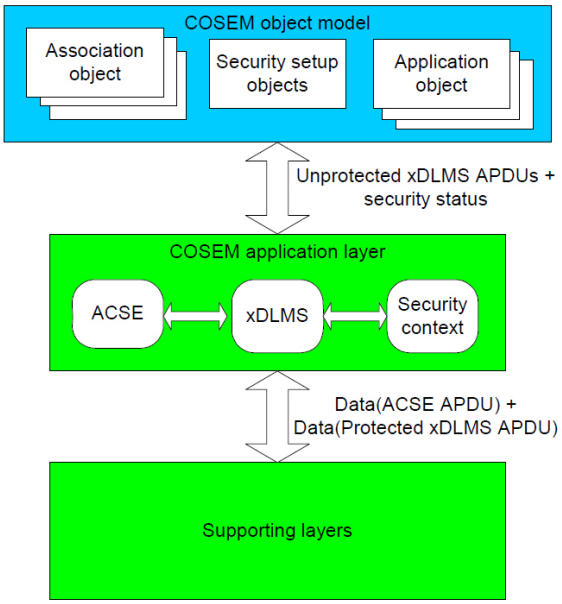
Sikkerhetsarkitekturen for DLMS/COSEM er spesifisert både i den blå og den grønne boken [11] og består i hovedsak av to elementer; sikkerhet for dataaksess og sikkerhet for datatransport. Sikkerhetsmekanismene for disse elementene er tilbudt delvis av COSEM applikasjonslag og delvis av COSEM objektene, se figur 6.1. Ved etablering av applikasjonsassosiasjoner[2] gjennom ACSE, blir to sikkerhetskontekster forhandlet, *applikasjonskontekst* og *autentiseringskontekst*. Applikasjonskonteksten definerer transportsikkerheten og hvilke mekanismer som skal benyttes, mens autentiseringskonteksten definerer nivå av aksessikkerhet for datakommunikasjonen.

Når en applikasjonsassosiasjon er etablert kan COSEM-tjenester blir benyttet til å få tilgang til attributter og metoder i COSEM objekter i henhold til aksessrettighetene gitt den aktuelle assosiasjonen. Sikkerhetstjenester blir utført på xDLMS datapakker (APDU) i henhold til applikasjonskonteksten som definerer transportsikkerheten. Applikasjonslagassosiasjonen gir COSEM-applikasjonslaget informasjon om hvilke tjenester som skal benyttes, `security status` i figur 6.1.

Aksessikkerhet

Aksesskontroll og er definert av autentiseringskonteksten som beskriver hvilke logiske enheter som har tilgang til hvilke grensesnittobjekter. Autentiseringskonteksten beskriver også hvordan grensesnittobjekter skal autentisere klienten. Det er definert tre tilgangsnivåer som definerer hvilke muligheter hver logisk enhet har i forhold til grensesnittprosedyrer

[2] se seksjon 5.4.1



Figur 6.1: Kobling mellom COSEM objektmodell og applikasjonslag [51]

som GET, SET, ACTION etc. *Lowest level security* tilbyr ingen autentisering av klienten. *Low Level Security (LLS)* benyttes kun når kommunikasjonskanalen allerede er tilstrekkelig beskyttet mot avlytting av trafikk samt duplikatmeldinger på andre nivå. LLS tilbyr kun passordbasert autentisering av klienten ovenfor serveren når dette nivået benyttes. Når *High Level Security (HLS)* benyttes autentiseres både klient og server ovenfor hverandre. Denne profilen benyttes når det er manglende og ikke tilstrekkelige sikkerhetsmekanismer i lavere protokollag.

Transportsikkerhet

For sikring av data defineres transportsikkerheten av xDLMS APDU meldinger i applikasjonskonteksten. DLMS/COSEM standarden definerer integritet og konfidensialitet som sikkerhetstjenester tilbudt for transportsikkerhet [13]. Ved sending av en xDLMS APDU gir COSEM objektet beskjed til COSEM applikasjonslaget om hvilke sikkerhetsmekanismer, samt nødvendige tilhørende parametre, som skal benyttes før meldingen sendes. Sammen med den sikre xDLMS APDU-meldingen mottar mottakeren informasjon om hvilke sikkerhetsmekanismer som har blitt benyttet slik at nødvendige operasjoner[3] kan gjennomføres før meldingen kan sendes til COSEM-objektet.

Anbefalte kryptografiske algoritmer benyttet for sikkerhetsmekanismer i *aksessikkerhet* og *transportsikkerhet* er definert i den grønne boken av DLMS/COSEM dokumentasjonen. Transportsikkerheten i COSEM kan tilby enten autentisering, konfidensialitet eller både autentisering og konfidensialitet av datatrafikk[13]. For autentisering benyttes hashbaserte meldingsautentiseringskoder og for konfidensialitet benyttes kryptering ved symmetrisk kryptografi[4] [13]. Det støttes også for autentisert kryptering e.g. ved bruk av AES-GCM-

[3] e.g. dekryptering, integritetssjekk etc.
[4] Det arbeides også med støtte for asymmetrisk kryptografi på [13]

Konfidensialitet	Ja. Valgfri algoritme, men AES-128 anbefales
Integritet	Ja. Valgfri algoritme
Autentisering	Ja. E.g. AES-GCM-128

Tabell 6.11: Sikkerhetsmekanismer for DLMS/COSEM

Konfidensialitet	ikke definert
Integritet	ikke definert
Autentisering	ikke definert

Tabell 6.12: Sikkerhetsmekanismer for SML

128 [51].

6.2.2.2 SML

SML spesifiserer kun meldingsstruktur og en står dermed fritt for valg av funksjoner, objekter og grensesnittobjekter ved hver implementasjon. Av den grunn spesifiserer ikke SML noen sikkerhetsarkitektur da eventuelle sikkerhetsmekansimer må hånteres av andre spesifikasjoner eller standarder. Et alternativ er å benytte SML som applikasjonslagprotokoll og implementere sikkerhetsmekanismer i et annet protokollag e.g. transportlaget eller nettverkslaget. OPENmeter beskriver en konfigurasjon av SML over TCP og Transport Layer Security (TLS) for sikker bruk over IP-baserte nettverk [63].

6.2.2.3 DPWS

Ettersom DPWS spesifieserer en arkitektur basert på eksisterende standarder for webservices er også sikkerhetsarkitekturen et sett med anbefalte sikkerhetsmekanismer for sikker kommunikasjon mellom *client* og *device*. Hvilke sikkerhetsmekanismer som tilbys av en client eller device kan spesifiseres gjennom e.g. WSDL. DPWS anbefaler bruk av TLS / Secure Sockets Layer (SSL). TLS/SSL tilbyr sikker ende-til-ende kommunikasjon mellom client og device ved tjenester som autentisering av sender/mottaker, samt integritetssjekk og konfidensialitet av all trafikk. DPWS kan benytte x.509.v3 sertifikater og spesifiserer ingen fast protokoll for sertifikatadministrering [59]. Det henvises til dokumentasjonen for de respektive sikkerhetsmekanismene for nærmere detaljer og spesifikasjoner.

6.2.3 Oppsummering

Sikkerhetsarkitekturene for de forskjellige protokollene varierer i kompleksitet og grad av sikkerhet. For kommunikasjonsprotokollene varierer protokollene fra proprietære integri-

Konfidensialitet	Definert av TLS/SSL (e.g. AES-128, AES-256)
Integritet	Definert av TLS/SSL (e.g. HMAC-SHA1)
Autentisering	Definert av TLS/SSL (i.e. TLS/SSL Handshake)

Tabell 6.13: Sikkerhetsmekanismer for DPWS

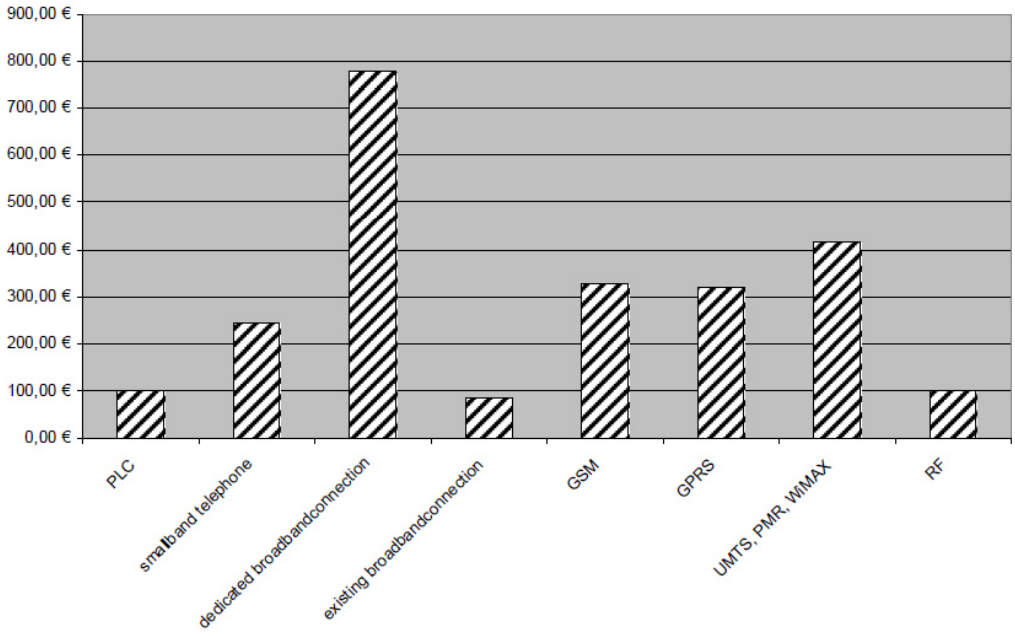
tetsalgoriter i LonWorks til mer fleksible og robuste løsninger med støtte for utvidelser i PRIME og G3. For aksessnettene GPRS og UMTS ser vi at arkitekturen for sikkerhet er lik, men nivå av sikkerhet varierer med bruk av forskjellige kryptografiske algoritmer samt aktuelle angrep for begge nettverkene. Sikkerhetsarkitekturen i begge disse nettene er baserer seg på Trusted Third Party (TTP) og er et prinsipp brukt i mange kommunikasjonsnett. En TTP er en node i nettet som tilbyr sikkerhetstjenester til alle de andre nettverksnodene. Ved bruk av TTP forutsetter det at alle nodene stoler på noden som tilbyr sikkerhetstjenestene. E.g. i GSM er nettverksoperatøren TTP og besitter alle krypteringsnøkler. Om nettverksoperatøren vil utnytte sin posisjon kan de kryptografiske nøklene benyttes til å overvåke trafikk, utføre maskerade angrep etc. Sikkerhetsarkitekturene for applikasjonslagsprotokollene varierer også hvor DLMS/COSEM må anses til å være den mest robuste standarden for bruk i AMS-kanalen. Standarden gir fleksibilitet i forhold til valg av algoritmer og kan implementere sikkerhetsmekanismer i applikasjonslaget uten videre krav til underliggende protokoller.

6.3 Vurdering av sårbarheter i AMS-kanalen

AMS-nettverket komme til å bli distribuert over store geografiske områder for å nå alle sluttbrukere knyttet til et nettselskap. For et slik nettverk er det hovedsakelig to kommunikasjonsalternativer. Første alternativ er at nettselskapene bygger dedikerte kommunikasjonsnett kun med tanke på AMS mot sine sluttbrukere. Alternativ to å benytte eksisterende kommunikasjonsnettverk. Deconinck publiserte i 2008 en rapport som vurderte forskjellige kommunikasjonsløsninger for AMS i Belgia [24]. Rapporten beskrev også en analyse på kostnadene ved bruk av de forskjellige alternativene, både innledende kostnader og kostnader og på lang sikt. Figur 6.2 viser at kostnadene ved å bygge et dedikert nett for AMS, også over en tidsperiode på 15 år, vil klart være det dyreste alternativet i forhold til de andre løsningene vurdert. Da første alternativ er utelukket med hensyn til de økonomiske utbyggingskostnadene ved et slikt nett, kan man med stor sannsynlighet anta at en kommer til å benytte eksisterende infrastruktur som kommunikasjonskanal for AMS.

Uavhengig av hvilket kommunikasjonsnett som blir benyttet vil den store angrepsoverflaten for AMS-nettverket føre til sårbarheter og utfordringer med tanke på informasjonssikkerhet. Om et kommunikasjonsnett kunne blitt holdt lukket for AMS ville angrepsoverflate vært redusert. Men å holde et slikt distribuert nett helt lukket vil være en komplisert oppgave da kabler og nettkomponenter ville måtte vært bevoktet og kontrollert til enhver tid mot angrep. Dette gjelder både fysiske angrep som avlytting av linker og grensesnitt, fysisk tukling og destruksjon, samt kontroll på at kun autoriserte personer har tilgang til andre nettverkkomponentene[5]. I et nett på størrelse med AMS må det ses på som en uoverkommelig oppgave å holde kontroll over alle linker og noder til enhver tid for å kunne garantere for sikker kommunikasjon. De fleste kabler og komponenter kan ses på som praktisk utilgjengelige for uvedkommende, da komponenter er låst inne i bygg eller installasjoner og kabler er nedgravet etc. For å kunne utføre angrep må da inntrengere enten bryte seg inn i bygg eller grave opp kabler for å at angrep skal være mulige. Men

[5] routere, switcher etc.



Figur 6.2: Estimert kostnad for bruk av forskjellig kommunikasjonsteknologi over en tidsperiode på 15 år [24]

for angripere med sterk motivasjon og store ressurser tilgjengelige, e.g. aktive angripere terrorister, er ikke disse scenarioene usannsynlige, se seksjon 4.4. Ettersom enkelte linker i AMS-kanalen vil være radioløsninger, øker tilgjengeligheten for angrep betraktelig. Konsekvensene ved radioløsninger blir nærmere diskutert senere i denne seksjonen.

Når eksisterende nett skal benyttes for kommunikasjon i AMS må man ta hensyn til de konsekvenser dette gir. De alternative nettene som er aktuelle er infrastruktur for telekommunikasjon[6] og distribusjonsnett for kraft[7]. Ved at nettselskapene benytte kraftkabler for kommunikasjon til sine målepunkter har enkelte fordeler. Selv om det i enkelte tilfeller vil være begrensninger for kablene med tanke på kvalitet og type av kabel, vil nettselskapene ha stor tilgjengelighet mot sine målepunkter gjennom kraftnettet. For det andre vil nettselskapet selv ha ansvaret for og driftingen av kommunikasjonskanalen mot målepunktene uten å trenge å forholde seg til tredjeparter. Nettselskapet vil i dette tilfellet står for og har enerett på kommunikasjon i de aktuelle linkene og komponentene i sitt nett. Men med samme prinsipp som diskutert i forrige avsnitt kan heller ikke slike nett ses på som lukkede da fysisk sikring er en uoverkommelig oppgave for nettverk i denne skala. Skaleringsproblemene med PLC på tvers av kraftnettnivåene[8] gjør at et helhetlig kommunikasjonsnettverk for et nettselskap er vanskelig. Derfor er ofte PLC løsninger oftest kun benyttet for siste ledd av distribusjonsnettet mot sluttbrukeren, e.g. mellom trafostasjoner og målepunkt. Videre mellom trafostasjonen og nettselskapets sentralsystemer benyttes andre kommunikasjonsnett.

[6] mobilnett og Internett
[7] PLC
[8] se seksjon 5.3.1

Siste alternativ er å benytte eksisterende radio- eller kabelbaserte telekommunikasjonsnett, e.g. GSM/GPRS, UMTS, Internett etc. Her kan vi skille på aksessnett og stammenett. I AMS er det stort sett Internett som kommer til å bli benyttet for kommunikasjonskanal mot nettselskapets sentralsystem. Men om måleren vil være direkte koblet mot Internett eller om et annet aksessnett benyttes på siste link mot målerpunktet vil variere. Selv om målet for nivå av informasjonssikkerhet i disse radiobaserte telekommunikasjonsnettene varierer, ble de opprinnelig designet for å være sikre mot angrep. Seksjon 6.2 viste at det mange likhetstrekk mellom sikkerhetsarkitekturene i disse nettene, samt at hvilke sikkerhetstjenester og nivå av sikkerhet i nettet varierer. Disse nettene ble designet for å kunne motstå angrep og i prinsippet skal kommunikasjon i slike nettet være sikker og utilgjengelig for uvedkommende. Men det er flere årsaker til at man ikke kan basere sikkerheten i AMS på sikkerhetsmekanismene eksisterende i disse nettene. For det første er ikke målene for nivå av sikkerhet like for som AMS. Dette gjør at sikkerhetsarkitekturen for disse nettene ikke nødvendigvis dekker alle kravene som settes for sikker kommunikasjon i AMS. For det andre er det, til tross sikkerhetsmekanismene i nettene, flere ulike angrep mot slike nett som utgjør en risiko for uautorisert tilgang til trafikken, se seksjon 6.2.1.4. For det tredje, om en baserer seg på at sikkerhetsmekanismene disse nettene tilbyr, vil en måtte kunne stole på at operatøren av nettet ikke utnytter sin makt og tilgang til kommunikasjon som TTP. Ettersom nettverksoperatøren er TTP kan dermed ikke slike nett ses på som lukket for AMS.

Økende antall nettselskaper i kraftbransjen har de siste tiår satset på utbygging av bredbånd til sine sluttbrukere. Dette har også ført til at mange energiselskaper har valgt å samarbeide gjennom den felleseide Bredbåndsalliansen [89]. Dette fører til at mange nettselskaper også tilbyr Internettilgang til sine sluttbrukere. Fiber[9] har vært et dominerende satsningsområdene. Internett ble designet for å være et robust transportnettverk for informasjon og trusselbildet da det ble designet var et helt annet enn hvilke trusler Internett står ovenfor i dag med tanke på informasjonssikkerhet, se seksjon 3.1. Da Internett stadig blir tatt i bruk i nye sammenhenger, har et helt annet fokus på sikker kommunikasjon i nettet vokst. Som en konsekvens av dette har tiltak for å sikre trafikken i nettet blitt nødvendig og og sikkerhetsutvidelser av eksisterende teknologier har blitt tatt i bruk e.g. IPsec. På en slik måte kan Internett brukes som det var designet til å være, en transportkanal for data, hvor sikkerhetstjenester må støttes av andre mekanismer. En kan med dette konkludere med at AMS-kanalen kommer til å bli implementert over nett som ikke kan ses på som sikre eller lukkede for AMS. Som en konsekvens må kommunikasjonsnettet mellom smartmåleren og sentralsystemet kun ses på som en transportkanal og sikkerheten for kommunikasjon må håndteres internt av AMS.

Konsekvensene for informasjonssikkerheten med tanke på valg av radioløsninger på linker må utdypes. Muligheten for angrep på trafikk i transitt begrenses som oftest av tilgjengeligheten til mediet signalet overføres i. I sin natur er radioløsninger dermed mer sårbare enn kabelbaserte løsninger da tilgjengeligheten til radiosignalene er større enn tilgjengeligheten til signalene overført gjennom kabler. I motsetning til signaler over kabler, er trådløse signaler mer eksponert ettersom utstråling av radiobølger er vanskelig å begrense og kan fanges opp på avstand, alt avhengig av antennetype og sendeeffekt. Radioløsninger er derfor mer sårbare for passive angrep som avlytting og trafikkanalyse enn

[9] e.g. Lyse, NTE, BKK

kabelbaserte løsninger. Tilgjengeligheten for signalene mellom sender og mottaker gir også en angriper økt mulighet for å utføre aktive angrep som ble beskrevet i seksjon 4.5.2. Det må presiseres at det konsekvensene ved bruk av radiolink kun øker sårbarheten for angrep på trafikk i transitt med tanke på økt tilgjengelighet til overføringssignalene. Angrepene beskrevet i seksjon 4.5.2 er også mulige for kabelløsninger men lavere tilgjengelighet til kommunikasjonsmediet gjør sannsynligheten lavere.

6.4 Vurdering av konsekvenser ved angrep mot AMS-kanalen

I denne seksjonen presenteres en vurdering av konsekvensene ved eventuelle angrep mot AMS-kanalen. Istedet for å studere hver oppgave AMS skal utføre hver for seg, blir de forskjellige trafikklassene definert og beskrevet i seksjon 4.3 studert. På dette viset kan også andre og framtidige oppgaver for AMS vurderes ved å klassifisere trafikken den aktuelle oppgaven genererer i henhold til disse klassene. Konsekvenser for hvert angrep vil ikke bli beskrevet. Diskusjonen vil konsentreres rundt eventuelle brudd på sikkerhetstjenestene beskrevet i seksjon 3.1.1.1. Denne vurderingen gir ikke oversikt over angrep og eller trusler. Det henvises til seksjonene 4.4 og 4.5 respektivt for å korrelere interessenter for AMS-data, motivasjon for angrep, angrep mot AMS-kanalen, og konsekvensene presentert i denne seksjonen. Denne diskusjonen ser i hovedsak på angrep mot trafikk i transitt[10], men i enkelte sammenhenger blir også angrep fra andre klassifiseringer diskutert. Hver trafikklasse vil bli gradert i forhold til **små**, **mellomstore** eller **store konsekvenser**. Under beskrives karakteristikken for hver av konsekvensgraderingene:

Små konsekvenser
: Lineære, åpenbare og isolerte konsekvenser. Dette vil si konsekvenser som har begrensede direkte konsekvenser som kan forutses etter et hendelsesforløp.

Moderate konsekvenser
: Konsekvenser som nødvendigvis ikke både er åpenbare eller isolerte. Moderate konsekvenser kan enten være åpenbare og mer distribuerte eller mindre åpenbare og isolerte. For førstnevnte vil konsekvensene ha større omfang men samtidig åpenbare og kunne forutses. For sistnevnte vil konsekvensene være mindre forutsigbare men fortsatt ha mindre omfang.

Store konsekvenser
: Komplekse konsekvenser som ikke er åpenbare og samtidig distribuerte. Store konsekvenser vil kunne forekomme når et hendelsesforløp kan gi distribuerte uventede konsekvenser. Denne graderingen er satt til den høyeste grunnet uvissheten rundt omfanget av konsekvensene.

6.4.1 Målerverdier

Generelt vil måledata og måleverdier sendt over AMS-kanalen inneholde verdier kun for ett aktuelt målepunkt. Dette gjelder spesielt for løsninger hvor målernoden kommuniserer direkte med sentralsystemet, se *MS*-linker i seksjon 5.1.2. På denne måten kan en si

[10] se seksjon 4.5.2

konsekvensene ved angrep mot slik trafikk er isolert rundt sluttbrukeren for det aktuelle målepunktet. For løsninger hvor konsentratorer blir benyttet vil det samme gjelde mellom sluttbruker og konsentrator, altså *MK*-linker. For *KS*-linker vil den aggregerte informasjonen for flere målernoder være tilgjengelige og gi økning i omfang og konsekvens ved eventuelt angrep.

Om integriteten av denne type trafikk ikke kan garanteres i AMS-kanalen vil dette i hovedsak ha konsekvenser for faktureringsgrunnlaget for de aktuelle målepunktene. Dette kan skje ved å forfalske eller modifisere slik trafikk under veis i AMS-kanalen. Konsekvensene for brudd på integriteten ved denne klassen trafikk er nok så åpenbare da de ikke iverksetter noen former for prosess hos mottaker. Motivasjonen for slike angrep kommer an på hvem angriperen er. E.g. kan slike angrep utnyttes til å redusere forbrukstall for en målernode med motivasjon om tyveri av strøm. Om konfidensialitet for måledata og måleverdier ikke opprettholdes i AMS-kanalen vil dette kunne utnyttes til overvåkning og ha konsekvenser for personopplysningsloven, se seksjon 2.2.3.5. Om tilgjengeligheten for denne type trafikk hindres vil også dette få konsekvenser for faktureringsgrunnlaget.

Med hensyn til at konsekvensene av slike angrep er meget isolerte og åpenbare graderes måledata og måleverdier til **små konsekvenser**.

6.4.2 Hendelser og alarmer

Hendelser og alarmer rapporteres hurtig til sentralsystemet og videresendes fortløpende fra konsentrator til sentralsystemet uten noen form for aggregering. På denne måten kan også konsekvensene for hendelser og alarmer ses på som nok så isolerte da en hendelse/alarm kommer kun fra et målepunkt uansett hvor i AMS-kanalen de observeres.

Prosessene som iverksettes i sentralsystemet ved mottak av hendelser og alarmer kommer an på hvilken hendelse eller alarm som ble sendt. Enkelte hendelser og alarmer vil kun bli registrert og lagret uten noen videre prosess, mens andre vil iverksette videre tiltak for utbedring av de eventuelle problemet e.g. alarm om jordfeil, anlegg uten spenning etc. Men om en ser på alle hendelser eller alarmer i ett må integriteten for denne typen trafikk ses på som essensiell da reaktive prosesser iverksettes unødig om falske hendelser eller alarmer mottas. På lik måte som for annen trafikk kan også slik trafikk benyttes til overvåkning om konfidensialitet av trafikken ikke overholdes i AMS-kanalen. Men med hensyn til at dette oftest er automatisk generert trafikk på grunnlag av lokale forhold ved målepunktet, må nyttverdien av slik trafikk ses på som liten da det er få interessenter for slik data. Om tilgjengeligheten for slik trafikk hindres vil det kunne forårsake at reaktive tiltak ikke iverksettes. Dette gjør at reaktive tiltak bør i størst mulig grad kunne håndteres lokalt om nødvendig.

Til tross for at konsekvensene ved angrep mot hendelser og alarmer er mindre åpenbare må konsekvensene ses på som meget isolerte. Derfor graderes denne trafikklassen til **moderate konsekvenser**.

6.4.3 Konfigureringkommandoer

Konfigureringskommandoer sendes fra sentralsystem mot én, en gruppe eller alle målernoder, enten direkte eller indirekte via konsentratorer. En kan dermed ikke si at angrep mot slik

trafikk kun kan gi isolerte konsekvenser, men derimot kan få stort omfang ved å rette angrep mot kommandoer for en gruppe eller alle målernoder.

Integriteten ved slik trafikk må ses på som kritisk og er avhengig av hvilke konfigureringer som iverksettes hos mottakeren. Konfigureringer varierer fra enkeltparametre til programvareoppdateringer og patcher. For alle er integriteten essensiell, men kompleksiteten for konsekvensene ved eventuelle angrep må antas å økte med grad av kompleksitet på konfigurasjonene som gjøres. Herav vil e.g. angrep mot konfigurasjonskommandoer for enkeltparametre gi mer åpenbare konsekvenser enn for programvareoppdateringer. Konsekvensene ved tap av konfidensialitet for denne type trafikk må ses på som åpenbare og nytteverdien for slike angrep er lav.

Med hensyn til kompleksiteten og det store omfanget av konsekvenser for slik type trafikk graderer vi konfigureringskommandoer til **store konsekvenser**.

6.4.4 Styringssignaler

Styringssignaler sendes fra sentralsystemet mot én eller en gruppe målernoder, enten direkte eller via konsentratorer. Omfanget av konsekvensene for slik trafikk må dermed ses i hensyn til hvor stor gruppe målepunkter denne type signaler distribueres til. Det presiseres også at slike signaler ikke kan sendes til alle målepunkter samtidig.

Åpning og stenging av krafttilførsel gjennom bryterfunksjonaliteten kan føre til drastiske konsekvenser og i enkelte tilfeller også føre til risiko for liv og helse. Dette er med tanke på at elektrisitet i dag benyttes til nødvendigheter som oppvarming, kommunikasjonsutstyr etc. som vil settes ut av drift om elektrisk krafttilførsel blir stengt. De direkte konsekvensene for angrep på slik type trafikk kan ses på som åpenbare, men de indirekte ringvirkningene er komplekse. Integriteten for styringssignaler må derfor ses på som kritisk og styringssignaler ikke skal kunne forfalskes. Nytteverdien av innsyn og overvåkning av slik trafikk må ses på som lav, men med hensyn til personopplysningsloven bør konfidensialiteten opprettholdes også for slik trafikk.

Ettersom de indirekte konsekvenser ved angrep på slik trafikk er komplekse, samtidig med at omfanget kan være stort om signalene sendes til store grupper målepunkter, graderes styringssignaler trafikk til **store konsekvenser**.

6.4.5 Trafikk til/fra lokalt tilleggsutstyr

Trafikk generert i sammenheng med lokalt tilkoblet display vil føre til kommunikasjon begge veier mellom målerpunktet og sentralsystemet. Da sentralsystemet ikke er spesifisert til å kommuniserer med tilleggsutstyr for flere målerpunkter samtidig må konsekvensene anses til å være isolerte. Da konsekvensene også kan ses på som åpenbare graderes slik trafikk til **små konsekvenser**.

Konsekvensene ved angrep mot denne type trafikk er avhengig av hvilken type trafikk tilkoblet tilleggsutstyr genererer. Det anbefales å vurdere hvilke direkte og indirekte konsekvenser angrep mot slik trafikk kan forårsake i de enkelte tilfeller. I den sammenheng bør konsekvenser ved angrep som fører til brudd på alle sikkerhetstjenestene beskrevet i seksjon 3.1.1.1 vurderes.

6.4.6 Annen trafikk

Det er ennå uvisst hvilke tredjeparts tjenester som kommer til å bli benyttet over AMS kanalen. Av den grunn er det vanskelig å analyse hvilke konsekvenser eventuelle angrep vil medføre. Derimot må tredjepart akseptere nivå av sikkerhet AMS-kanalen kan tilby og vurdere hvorvidt det er akseptabelt nivå for sikkerhet for tjenesten som ønsker å utnytte AMS-kanalen. Disse tjenestene bør vurderes på samme vis som gjort i denne oppgaven med hensyn til kompleksitet, koblinger til andre systemer, samt størrelse på omfang. Det har i enkelte forskriftshøringer vært snakk om alarmer som en tredjeparts tjeneste gjennom AMS-kanalen [87]. Dette er et tilfelle hvor sikkerheten i AMS-kanalen må vurderes for de enkelte nettselskapene.

6.4.7 Drøfting av konsekvenser og risiko ved angrep

En si at retningen av trafikken i AMS-kanalen har relevans for dens konsekvenser. Ettersom en smartmåler kun skal kunne kommunisere med en konsentrator eller sentralsystemet vil angrep mot data sendt fra målernode mot sentralsystemet få isolerte konsekvenser for den enkelte målernoden. Derimot kan data sendt fra sentralsystemet være sendt til én, en gruppe eller alle målernodene i et AMS. Det er dermed tilknyttet større konsekvenser relatert til data distribuert fra sentralsystemet til mange målernoder samtidig. Om en studerer linkene i den generiske arkitekturen nærmere kan vi også se at konsekvensene varierer for hvilken link som blir angrepet. Ettersom kommunikasjonen over linkene direkte koblet til målernoder, *MK* og *KS*, kun transporterer data relatert til en aktuell målernode vil konsekvensene være lavere for disse linkene enn for angrep mot kommunikasjonlinker som transportere data på vegne av mange målernoder, *KS* linker. I vurderingen av konsekvenser for de forskjellige trafikklassene i seksjonene over har det stort sett kun blitt diskutert de direkte konsekvensene av angrep. Vi vil nå diskutere kompleksitet AMS innfører og indirekte konsekvenser ved angrep mot AMS-kanalen. Som definert i seksjon 2.2.3.1 vil en oppgave AMS skal kunne utføre bestå av et sett funksjoner. AMS skal kunne utføre mange forskjellige oppgaver og hver av de funksjonene som trengs for å utføre disse oppgavene må vurderes med hensyn til informasjonssikkerhet. Når en oppgave skal vurderes er det viktig å se på sammensetningen av funksjoner og hvilke konsekvenser denne sammensetningen har for sikkerheten. Dette kan forklares gjennom et eksempel e.g. sammenhengen mellom styringssignaler og konfigurasjonskommandoer. Ut ifra deres definisjoner er konfigurasjonskommandoer og styringssignaler distinkt forskjellige. Men som presentert i seksjon 4.3.4 kunne en konfigurasjonskommand benyttes som styringssignal om funksjonalitet for struping/bryting av effektuttak ved maksgrense var iverkseatt. Om en videre studerer egenskapene for de forskjellige oppgavene ser en at styringssignaler ikke skal kunne distribueres til alle målernodene samtidig. Men både funksjon for iverksetting av utkobling ved maksgrense og konfigurasjonskommando for definering av maksgrense kan distribueres til alle målernodene samtidig. Av dette ser man at en ved å utnytte konfigurasjonskommandoer vil kunne styre tilførselen av kraft til alle målernodene samtidig. Dette betyr at disse oppgavene må håndteres med likt nivå av sikkerhet og at angrep kan gi de samme konsekvensene.

En videreføring er nærmere studier av automatiserte prosesser og på hvilket grunnlag de iverksettes. Da AMS muliggjør toveis kommunikasjon mellom kraftnett og sluttbruker

åpner det for mange dynamiske og adaptive konsepter for optimalisering av kraftdistribusjon og produksjon. Slike dynamiske krever automasjon som baserer seg på parametre hentet eller generert på grunnlag av verdier fra kraftnettet. Integriteten av innsamlet data samt kontroll av datagrunnlag er essensiell for korrekt oppførsel for og samspill mellom disse automatiserte prosessene. E.g. et konsept for adaptiv produksjon har automatiserte prosesser for produksjon på grunnlag av momentant forbruk. Om integriteten ved de innsamlede forbruksdata ikke er korrekt vil de automatiserte prosessene for dynamisk produksjon iverksettes på feil grunnlag. At slike prosesser iverksettes på feil grunnlag kan videre få konsekvenser. Slike konsekvenser kalles *indirekte konsekvenser* eller *ringvirkninger*.

Granskning av mulige direkte og indirekte konsekvenser i AMS er et tverrfaglig studie hvor vi her velger å trekke fram et eksempel hvor konsekvens har relevans til elkraft. I et kraftsystem må det være balanse mellom produksjon og forbruk av effekt for at frekvensen skal være stabil. Frekvensen i det norske nettet er nominelt 50Hz, og skal under normale omstendigheter kontrolleres innenfor intervallet 49,90-50.10 Hz [28]. Ved feil og spesielle hendelser kan avviket bli større. Hvis frekvensavviket kommer over en gitt størrelse kan nettet kollapse og man får en *blackout*. En kan nå se for seg en et scenario hvor en angriper har funnet en mulighet for å sende falske styringssignaler eller konfigureringskommandoer. Angriperen kan nå, ved å benytte slike falske styringssignaler og konfigureringskommandoer, respektivt kan kutte forbruket for alle målenoder i et AMS. Om antallet målernoder er vesentlig høyt vil reduksjonen i totalforbruk antakelig kunne skape ubalanse i forhold til produksjon. En slik ubalanse kan gjøre at frekvensen i nettet synker under akseptabel nivå og i verste fall forårsake en blackout. Omfanget av en slik blackout vil være avhengig av robust kraftnettet er og hvilke reaktive tiltak som kan iverksettes for å begrense ubalansen og forhindre en blackout. Sikkerhetsutvalget beskriver også et scenario hvor manipulasjonsangrep mot styrings- og konfigurasjonskommandoer kan forårsake sammenbrudd i kraftnettet [75]:

> Fra produksjonsverkene går den elektriske energien via overføringsnett og distribusjonsnett ut til den enkelte abonnent. I takt med økende effektivisering er IKT-avhengigheten i driften av overføringsnettene økende, og dermed også potensielt IKT-sårbarheten.
>
> Alle komponenter i overføringssystemet er utstyrt med automatisk vern som kobler ut strømmen på linjer og andre komponenter etter gitte kriterier (kortslutning, spenningsfall, lynnedslag osv). Komponentene inneholder i økende grad mikroprosessorer, som gjør tilknytting til datanett mulig. Dette muliggjør sentralisert konfigurasjon av disse, slik at kriteriene for utkobling av strømmen kan endres. Hvis utenforstående skulle greie å skaffe seg tilgang til innstillingene av slike vern kan disse programmeres til å bryte strømmen selv under normale driftsforhold. En vellykket manipulasjon med slike komponenter kan i sin ytterste konsekvens føre til nettsammenbrudd.

Da kraftnettet må ses på i sin helhet, transport- og distribusjonsnett, kan et sammenbrudd i nettet gi store kaskadeeffekter. Wang og Rong presenterer i sin rapport studier av kaskadeeffekter ved angrep eller feil i det amerikanske kraftnettet [73]. Gjennom simuleringer hvor nodene i kraftnettet blir rangert etter elektrisklast viser de at angrep mot to noder i kraftnettet kan forårsake en total kollaps av hele det amerikanske kraftnettet.

Rapporten viser også at under visse forhold kan angrep mot noder med lav last gi større kaskadeeffekter enn angrep mot noder med størst last. Dette påpeker igjen viktigheten av autentisering av avsender og integritet av trafikken sendt i AMS-kanalen.

Et annet perspektiv for innført kompleksitet gjennom AMS vil være koblinger mot andre systemer. E.g. må det knyttes høy risiko til koblingene mellom AMS og kraftproduksjon. Kontroll- og overvåkningssystemer, SCADA systemer, er benevningen for sentraliserte IT-baserte kontrollsystemer ofte benyttet i kraftbransjen og i mange andre industrielle anlegg. SCADA systemer har i de siste år blitt i økende grad for utsatt dataangrep, [18] [57], og en kan se på koblingen mellom slike systemer og AMS til å gi økt risiko gjennom en vesentlig økning i angrepsoverflate for SCADA-systemer [37]. Dette presiserer også viktigheten av perimetersikring mellom slike sammenkoblede systemer.

Det en kan se utifra denne diskusjon er at risikoen ved AMS mest sannsynlig er nok så individuell og isolert i årene etter utrulling da systemene hovedsakelig vil bli brukt til innsamling av målerverdier. Men ettersom AMS blir knyttet til og koblet opp imot andre systemer for å realisere konsepter for et framtidig og dynamisk *smart strømnett*, vil risikoen bli mer distribuert, omfattende og kompleks. En må se risikoen AMS innfører fra forskjellige perspektiver. Det eksisterer individuelle konsekvensene knyttet til overvåkning av sluttbrukere, mer komplekse konsekvenser knyttet til tilgrensende systemer og konsekvenser knyttet til teknisk elkraft e.g. konsekvenser for stabilitet i kraftnettet.

6.5 Vurdering av sikkerhetstjenester for AMS-kanalen

Det vil nå diskuteres de forskjellige sikkerhetstjenestene som ble introduserte i seksjon 3.1.1.1 og viktigheten av hver tjeneste. Det henvises til seksjon 4.4 for definisjoner av trusler mot AMS-kanalen.

Konfidensialitet av trafikk sendt i AMS-kanalen er hovedsakelig for å hindre passive angrep som innsyn og overvåkning. Innsyn og overvåkning av andre trafikklasser enn målerdata og måleverdier må anses til å ha liten nytteverdi men kan utnyttes til en viss grad av overvåkning. Brudd på konfidensialiteten vil kunne gi innsyn i innmeldt måledata og gi konsekvenser med tanke på lov om personvern. Brudd på konfidensialiteten vil også kunne brukes til overvåkning av og aktivitet ved målepunkter, definert som motiverte lyttere. Til tross for at data som sendes over AMS-kanalen er kryptert, vil en tredjepart kunne tilegne seg en viss kunnskap om informasjonen som sendes ved å studere trafikkmønstre. For at slike angrep skal være mulig må en tredjepart ha tilgang til kommunikasjonskanalen for å føre statistikk over størrelse, hyppighet og retning av den krypterte trafikken i kanalen. Som vi lærte i 6.3, kommer AMS-kanalen til å implementeres over usikre kommunikasjonsnett og derfor kan slike angrep være sannsynlige.

Hvilken informasjon man kan få ut av slik trafikkanalyse er avhengig av hvor i AMS-kanalen trafikken studeres. Se seksjon 5.1.2 for analyse av de forskjellige linkene i det generiske arkitekturen for AMS-kanalen. Av å studere kommunikasjonen til og fra en enkelt måler, *MK* og *MS*-linker, vil man kunne tilegne unik informasjon om en unik måler. Ettersom data mellom konsentratorer og innsamlingssystemer, *KS* linker, som oftest er aggregert data fra flere målere vil et slikt angrep kunne tilegne kunnskap om området for den aktuelle konsentratoren. Om kryptering er benyttet vil det være vanskelig å skille mellom informasjon fra de forskjellige målerne om dataene er aggregert. En viss grad

av statistisk informasjon kan mulig oppnås om trafikken over *MK* linker korreleres med informasjon observert over *KS* linkene mot de underliggende målerne. For AMS kunne et slikt angrep gitt informasjon om e.g. :

- hvor hyppig et målepunkt; melder inn forbruksdata, mottar styringssignaler etc.
- et målepunkt er aktivert eller deaktivert

Et alternativ for å redusere nytten ved slike angrep er å minimere de statistiske data slik trafikkanalyse kan gi. Dette gjelder all trafikkarakteristikk. E.g. å benytte padding til å skape en uniform størrelse på forskjellige typer meldinger etc.

For at oppgaver i AMS skal kunne utføres korrekt er en avhengig av at integriteten av all kommunikasjon i AMS-kanalen kan garanteres. Viktigheten av integritet for styringssignaler og konfigurasjonsskommandoer ble presisert av diskusjonen om konsekvenser av angrep i seksjon 6.4. Men integriteten for måledata og måleverdier er også viktig med hensyn til faktureringsgrunnlag, både for sluttbruker og nettselskap. Om en angriper på en eller annen måte greier å modifisere måleverdiener uten at dette bli oppdaget av sentralsystemet, vil sluttbrukeren for det aktuelle målepunktet bli fakturerert på feilaktig grunnlag. E.g. kan en sluttbruker selv prøve å redusere sine innmeldte måleverdier for å stjele strøm. I dette tilfellet kan si at det er i nettselskapets interesse å kunne garantere for integriteten av måledataene. Om en angriper greier å øke måleverdier for en målernode vil automatiserte forbruks og faktureringprosesser mulig ikke oppdage at måleverdiene er modifiserte i AMS-kanalen og sluttbrukeren bli fakturert på feil grunnlag. Det er i dette tilfellet i sluttbrukerens interesse at integriteten kunne garanteres. Dette eksemplet viser viktigheten av integriteten av data i sammenheng med automatiserte prosesser. Integriteten av data sent over AMS-kanalen sjekkes også av kontrollprosedyrer i sentralsystemet e.g. hvor målerverdier sjekkes at ikke er urimelig høye eller lave etc. Da slike kontrollprosedyrer ikke er endel av AMS-kanalen studeres ikke dette nærmere i denne oppgaven.

Tilgjengelighet er også essensielt for et velfungerende AMS. Angrep som påvirker tilgjengeligheten for et system er ofte kalt tjenestenektangrep[11] og benytter forskjellige metoder som reduserer ytelsen eller gjør tjenester totalt utilgjengelige for autentiske brukere. Da AMS kontrollerer og styrer krafttilførsel bør det settes høye krav til tilgjengelighet og robusthet for kommunikasjon og systemkomponenter. E.g. kan hindring av fremkommelighet for styringssignaler, benyttet for lastreduksjon, få konsekvenser og skape ustabilitet i kraftnettet [37]. Tilgjengeligheten for måleverdier må også presiseres da det stilles strenge tidskrav for innsamling og rapportering av verdier, se seksjon 2.2.3.1 og endelig forskriftstekst [87]. Hindring av tilgjengeligheten for tjenester og utførelser av oppgaver i AMS må ses på som kritisk, og de teknologier som blir benyttet bør vurderes og konfigureres for å minimere risikoen for slike tjenestenektangrep.

I tillegg til at alle disse sikkerhetstjenestene bør benyttes, må også presiseres valg av riktige og sikre sikkerhetsmekanismer, samt korrekt implementeringen av disse. Om kvaliteten og sikkerhetsnivået for sikkerhetsmekanismene implementert er for lavt vil kan kunne komme i en situasjon hvor egne verktøy eller script blir utviklet og distribuert for å knekke disse sikkerhetsmekanismene. LeMay, Gross et al. beskriver dette fenomenet slik:

[11] DoS-angrep

" (...) if meter communications are not properly secured, it may be possible for skilled developers to distribute scripted utilities for capturing and analyzing those communications. This could lead to something like the 'script kiddy' phenomenon that has occurred in the realm of computer cracking" [37].

Da frafall av sikkerhetstjenestene i enkelte tilfeller kan få store konsekvensene bør det være systemer som overvåker sikkerhetsmekanismenes tilstand. Slike systemer kalles Intrusion Detection Systems (IDS) og har i oppgave å detektere og loggføre ondsinnet aktivitet som truer sikkerheten ved systemet. Om systemet også kan iverksette reaktive tiltak mot ondsinnet aktivitet kalles systemet Intrusion Detection and Prevention Systems (IDPS) [58]. For AMS bør ikke bare trusler mot AMS-kanalen identifiseres tidlig, men reaktive tiltak bør iverksettes. Et selvfølgeig reaktivt tiltak vil være å forsøke å stoppe eventuelle angrep samt rapportere ved alarm om hendelse eller feil. Et alternativ for reaktive tiltak er hindre utførelsen av enkelte AMS-oppgaver i forhold til hvilke sikkerhetstjenester som er under angrep. E.g. ikke tillate styringssignaler om integriteten ikke kan garanteres, tillate styringssignaler men ikke innsamling av måledata om konfidensialiteten ikke kan garanteres etc.

6.6 Utfordringer for informasjonssikkerhet i AMS-kanalen

Av diskusjon om sikkerhetstjenester for AMS-kanalen i forrige seksjon, ser vi nødvendighet ved å implementere en robust sikkerhetsarkitektur som kan skape sikre ende-til-ende forbindelser mellom nodene i AMS-nettverket. En slik felles sikkerhetsarkitektur for AMS-kanalen er ikke trivielt å designe ettersom valg av kommunikasjonsløsning mest sannsynlig vil variere for hver målernode. Grunnet lokale begrensninger som tilgjengelighet for kommunikasjonsmedier og kommunikasjonsnett vil kommunikasjonsprofilen til en hvis grad tilpasses hvert enkelt forhold. Sikkerhetsarkitekturen for AMS-nettverket må dermed kunne håndtere og operere i et nettverk som må ses på som heterogent. I.e. betyr dette utfordringer med tanke på at sikkerhetsmekanismene må være kompatible med og kunne tilby likt nivå av sikkerhet for alle disse kommunikasjonsprofilene. Ettersom det i enkelte tilfeller kun er et alternativ for kommunikasjon mellom målernoden og sentralsystemet, e.g. kun PLC, bør ikke dette gi konsekvenser i form av redusert nivå av sikkerhet. Med andre ord bør avhengigheten mellom sikkerhetsarkitekturen og kommunikasjonsnett minimeres. Europakommisjonen avsluttet i 2010 et prosjekt for å studere sammenhengen mellom sikkerhet i heterogene kommunikasjonsnett og kritiske infrastrukturer, INTERSECTION[12]. Prosjektet var et underprosjekt av *Secure, Dependable and Trusted Infrastructures* og hadde som mål og skape et rammeverk for å gjøre kritiske infrastrukturer mer resiliente[13]. Rammeverket skal ta høyde for et stadig økende trusselbilde gjennom økende bruk av IKT samt mulige kaskadeeffekter grunnet økte avhengigheter mellom infrastrurer[46]. Resultatet av prosjektet er ikke offentlig, men prosjektet presiserer sikkerhetsutfordringene i dagens samfunn.

Kompatibilitet og sikkerhet er også en utfordring med tanke på proprietære protokoller. Proprietære protokoller er ofte laget og vedlikeholdt av spesifikke utstyrsleverandører

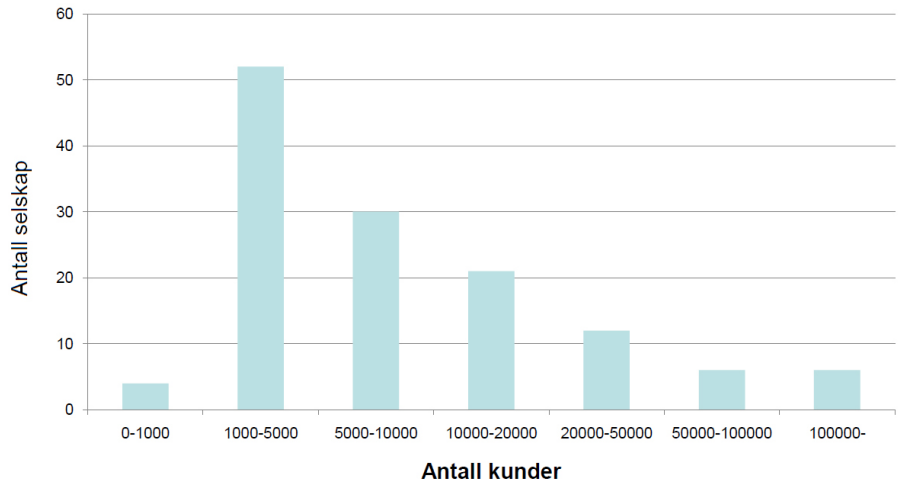
[12](INfrastructure for heTErogeneous, Resilient, SEcure, Complex, Tightly Inter-Operating Networks)

[13]Et system kan sies å være *resilient* om det har muligheten til å lære av, reagere på, overvåke og forutse hendelser. [54]

eller selskaper for bruk i egne systemer. Spesifikasjoner og dokumentasjon for slike proprietære systemer er med hensyn til opphavsrett og innsyn kun tilgjengelige for internt bruk, eventuelt for utvalgte partere ved spesiell tillatelse. Proprietære protokoller har som regel definerte grensesnitt som kan benyttes for å oppnå kompatibilitet mot andre protokoller og utstyr. Men da slike protokoller ofte er designet for ett bestemt formål eller system er fleksibiliteten begrenset. Ettersom dokumentasjon for slike protokoller er utilgjengelige vil mangel på kunnskap om interne operasjoner og mekanismer sette begrensninger for optimalisering og tilpasning mot andre systemer. Begrenset tilgang til protokollenes interne oppbygning og operasjon av funksjoner har også et sikkerhetsmessig aspekt. Ved begrenset innsikt til hvordan protokoller er bygget opp og opererer har en lite grunnlag for å vite om protokollen utfører de tjenester den hevder å utføre, samt om de er implementert korrekt. Dette betyr at en proprietær protokoll kan hevde at den utfører e.g. integritetssjekk av meldinger uten at tjenesten faktisk er implementert. Om den aktuelle tjenesten er til stede, er det vanskelig å vite om den er implementert korrekt og at det ikke eksisterer latente feil. En viss oversikt kan oppnås gjennom testing[14]. Et eksempel på en proprietær protokoll er SML som er beskrevet i seksjon 5.4.2 og 6.2.2.2. Standarder og protokoller hvor dokumentasjon er åpen og tilgjengelig for analyse, har relativt til proprietære protokoller større forutsetning for å tilby sikre tjenester. Ved å gjøre dokumentasjon åpen og tilgjengelig for vurdering av alle, vil mangfoldet av vurderinger øke sannsynligheten for at sikkerheten er håndtert på korrekt. Sikkerhet basert på hemmelighold bør unngås. Svakheter i sikkerhetsalgoritmene benyttet i GSM og GPRS er et eksempel på hvor hemmelighold av protokollers operasjon førte til at slike nett i dag ses på som usikre, [48].

En annen utfordring for informasjonssikkerhet i vil være kostnadene knyttet til design, implementasjon og realisering av sikkerhetsarkitekturer, ikke kun for AMS-kanalen men for et AMS generelt. Vurderingene av konsekvenser i seksjon 6.4 viste at størrelsesorden for omfang og konsekvenser er avhengig av type angrep og hvor angrepet blir rettet. Men fra en sluttbrukers perspektiv kan en si at sikkerhetsnivået bør være likt uavhengig av hvor i kraftnettet sluttbrukeren befinner seg. Grunnet nettselskapenes monopol på distribusjonsnett i sine geografiske områder har en sluttbruker, i de fleste tilfeller, ingen alternativer med hensyn til valg av nettselskap. En sluttbruker er dermed bundet til nettselskapet som har monopol i sitt lokale området. Ettersom det er nettselskapenes ansvar å sikre AMS er en sluttbruker implisitt nødt til å akseptere nivå av sikkerhet det lokale nettselskapet tilbyr i AMS. For de 130 nettselskapene i Norge er variasjonen i antall sluttbrukere stor. Ytterpunktene i figur 6.3 viser at enkelte nettselskaper har under 1000 sluttbrukere mens andre har over 100.000 sluttbrukere. Ut ifra de store variasjonene i størrelse må en også anta at resursene tilgjengelig, i.e. kapital og kompetanse for informasjonssikkerhet, for bruk på arbeid for sikring av AMS, til en viss grad er proporsjonal til størrelsen av nettselskapene. En kan basert på dette se for seg at nivå av sikkerhet for de forskjellige nettselskapene vil variere og være avhengig av størrelsen på nettselskapet. Avhengigheten mellom tilgjengelige resurser for nettselskapene og nivå av sikkerhet i AMS, kan føre til en situasjon hvor sikkerheten i AMS for mindre nettselskaper er på et lavere nivå i forhold til i større nettselskaper og dermed medføre større risiko. Selv om konsekvensene for eventuelle angrep vil være uendret vil et lavere nivå av sikkerhet medføre større sannsynlighet for suksessfulle angrep og derav større risiko.

[14] *Conformance testing, type testing*



Figur 6.3: Størrelsesorden på nettselskap i Norge [47]

6.7 Oppsummering og overordnete krav for sikker AMS-kanal

Basert på diskusjonen om konsekvenser av angrep samt diskusjonen om sikkerhetstjenester i dette kapittelet viser tabell 6.14 hvilke sikkerhetstjenester som er essensielle for de forskjellige trafikklassene. Tabellen rangerer hvor nødvendige og viktige de forskjellige sikkerhetstjenestene er ved tre nivåer *lav*, *middels* og *høy*, hvor *høy* er høyeste nivå av nødvendighet. Vi ser at nødvendigheten til sikkerhetstjenester generelt meget høyt, men spesielt for integritet og tilgjengelighet, samt noe lavere for konfidensialitet. Strenge krav til integritet gjenspeiler store konsekvenser ved angrep som bryter integriteten til mange av trafikklassene, samt kompleksiteten med tanke på koblingen mot automatiserte prosesser. De generelt lavere kravene til konfidensialitet er grunnet lav nytteverdi av innsyn til flere av trafikklassene, med unntak av måleverdier. Nivå for tilgjengelighet varierer mellom de forskjellige trafikklassene, men er rangert til høy for måleverdier og styringssignaler med tanke på store konsekvenser ved utilgjengelighet. For trafikk til/fra lokalt utstyr er nødvendigheten for alle sikkerhetstjenestene satt til middels ettersom denne trafikklassen ikke er studert nærmere i denne oppgave. Det samme gjelder for annen trafikk.

	Konfidensialtet	**Integritet**	**Tilgjengelighet**
Måledata	Høy	Høy	Høy
Hendelse/alarm	Lav	Høy	Middels
Konfigureringskommandoer	Lav	Høy	Høy
Styringssignaler	Lav	Høy	Høy
Trafikk til/fra lokalt tilleggsutstyr	Middels	Middels	Middels
Annen trafikk	Middels	Middels	Middels

Tabell 6.14: Krav til sikkerhetsmekanismer i AMS-kanalen

Kapittel 7

Forslag til sikkerhetsarkitektur for AMS-kanalen

I dette kapittelet presenteres løsning for sikring av AMS-kanalen. Løsningen som presenteres kan redusere risikoen ved innføring av AMS ved å senke sannsynligheten for suksessfulle angrep mot AMS-kanalen, til tross for at konsekvensene ved forskjellige angrep forblir den samme. Forslaget lagt fram vil oppfylle de krav til informasjonssikkerhet som er satt av NVE[1] og samtidig på best mulig måte sikre kommunikasjonen i forhold til utfordringene beskrevet i kapittel 6. Det vil først bli presentert de forskjellige overordnede egenskapene med sikkerhetsarkitekturen og deretter valg av sikkerhetsmekanismer samt konfigurasjoner av de respektive. Til slutt i dette kapittelet vurderer vi løsningen og diskuterer karakteristikk og egenskaper i forhold til kravene til sikkerhet.

7.1 Forutsetninger

En forutsetning for at et distribuert kommunikasjonssystem kan anses som sikkert er at alle systemkomponentene er på likt nivå sikkerhetsmessig. I.e om en komponent anses å være sikker mot angrep, må de resterende komponentene være på likt nivå eller ha et høyere nivå av sikkerhet for at hele systemet kan ses på som sikkert. En som vil angripe slikt system vil finne hvor sikkerhetsnivået er lavest, uavhengig om dette er underveis i nettet eller direkte i de kommuniserende nodene. E.g. er det ingen nytte i å oppnå sikker kommunikasjon mellom sender og mottaker om sikkerheten lokalt for sender og mottaker er lavere enn sikkerheten underveis i nettverket. Med dette forutsettes det at nivået av sikkerhet i de kommuniserende nodene i AMS er på nivå eller høyere enn hva vi oppnår i AMS-kanalen. Det vil med andre ord si at det skal ikke være noen punkter med lavere sikkerhet enn AMS-kanalen. De kommuniserende nodene i AMS-nettverket vil si målernoder, konsentratorer, og sentralsystem.

Arkitekturen som presenteres baserer seg hovedsakelig på veletablerte standarder og teknologier som har gjennomgått grundig granskning av fagmiljøer. I sine krav skriver OPENmeter “It is recommended that proven standards and industry best practices used for IT systems are implemented. (. . .) Existing systems should be considered and adapted, and security measures not reinvented.” [60]. Ved å benytte veltestede og godt etablerte systemer og standarder minimerer man sjansen for sårbarheter, design feil samt latente feil som nye systemer kan inneholde. Grunnet høye krav til sikkerhet, store konsekvenser samt en omfattende utbedringsprosess ved eventuelle feil har vi valgt å følge dette OPEN meter sine anbefalinger ved designet av denne sikkerhetsarkitekturen.

Seksjon 2.1 beskrev at AMS vil være fundamentet for framtidens kraftnett og at to-veis kommunikasjon mellom kraftnettet og sluttbruker er essensielt for realisering av kommende konsepter for det *smarte strømnett*. Selv om AMS de første årene etter utrulling hovedsakelig kommer til å bli benyttet for automatisk innmelding av målerverdier, bør systemet designes for et framtidig scenario slik at framtidige investeringer minimeres når behovet for mer funksjonalitet øker. Med dette sagt bør AMS, med tilhørende sikkerhetsarkitektur, designes så fleksibel som mulig at det til størst mulig grad kan tilpasses framtidige krav. Dette gjelder også at systemet skalerer og har muligheter for utvidelser.

Krav fra NVE sier at et AMS skal inkludere alle sluttbrukere som underligger et nettselskap, se seksjon 2.2.3.1. Med hensyn til at det vil være mange forskjellige behov

[1] seksjon 2.2.3

og begrensninger i realiseringen av kommunikasjon mot alle sluttbrukere vil løsningen presentert i denne oppgaven være aktuell for flertallet av sluttbrukerne. I tilfeller hvor implementasjon ikke lar seg gjennomføre, e.g. grunnet utilgjengelig kommunikasjonskanal, vil andre løsninger måtte vurderes. Alternative løsninger diskuteres i seksjon 7.6

7.2 Karakteristikk ved sikkerhetsarkitekturen

7.2.1 AMS og kompatibilitet til kommunikasjonsnett

Seksjon 6.2 og 6.3 viste at en ikke kan legge sikkerhet i kommunikasjonsnettet til grunne for sikring av AMS-kanalen. På denne måten vil kommunikasjonsnettet kun stå for transport av data mellom nodene i AMS-nettet og sikkerhetsarkitekturen vil bli håndtert internt. Dette betyr at løsningen må kunne benytte et vilkårlig underliggende kommunikasjonsløsning da kommunikasjonsstien mellom målernode og sentralsystemet oftest må ses på som *heterogent*. Med et heterogent nett mener vi et komplett kommunikasjonsnett som er basert på forskjellige kommunikasjonsprotokoller og teknologier. Internett er et eksempel på et heterogent nett e.g. hvor to kommuniserende noder kan benytte forskjellige aksessnett. Heterogenitet i nettet gjelder spesielt for linker mellom målernoder og sentralsystemet samt mellom konsentratorer og sentralsystemet, respektivt *MS* og *KS* linker. MS og KS linker strekkes ofte over store geografiske områder hvor eksisterende kommunikasjonsnett vil bli benyttet. For *MK*-linker, vil avstanden være begrenset og direkte kommunikasjonsløsninger mellom målernoder og konsentratorer er sannsynlige, e.g. PLC, trådløs M-bus.

7.2.2 Ende-til-ende sikkerhet i AMS-kanalen

Alle linkene i kommunikasjonsstien må anses som usikre og sikre ende-til-ende forbindelser mellom målernodene og sentralsystemet må implementeres. Sikkerhetsarkitekturen må også kunne håndtere sikre ende-til-ende forbindelser mellom målerpunkter og sentralsystemet som kommuniserer indirekte via konsentratorer. Med *alle linkene* presiseres det at kommunikasjonsnettet AMS-kanalen utnytter som regel er heterogen hvor mange forskjellige overføringsteknologier benyttes med forskjellige sikkerhets nivå. For sikre ende-til-ende forbindelser i heterogene nett må sikkerhet implementeres i de øvre lagene i protokollstakken. Forskjellige sikkerhetsarkitekturer i de underliggende kommunikasjonsnettene kan føre til kompatibilitets- og sikkerhetsutfordringer i grensesnittene mellom de forskjellige nettene. Sårbarhetene som oppstår mellom GSM og UMTS nettverk viser utfordringene for grensesnitt mellom sikkerhetsarkitekturer [92]. Om sikre ende-til-ende forbindelser implementeres i de øvre lag vil kommunikasjon i AMS-nettverket være sikker uavhengig av underliggende kommunikasjonsnett.

7.2.3 Sikkerhetsmekansimer i protokollstakken

I en sikkerhetsarkitektur for et kommunikasjonssystem kan sikkerhetsmekanismer implementeres i forskjellige lag av OSI-stakken[2]. Som en konsekvens av hvordan OSI er bygget

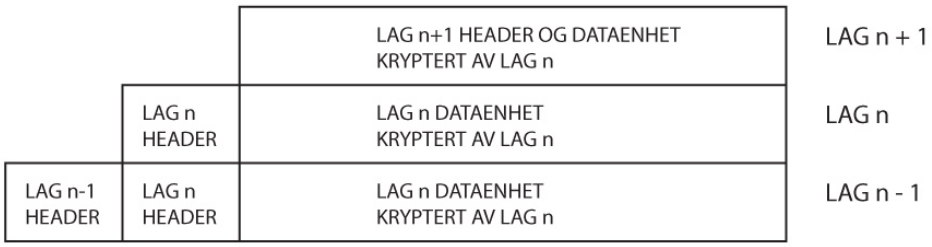
[2]se figur 5.1 på side 48

opp vil de sikre forbindelsene bli mer fragmentert jo laver i stakken sikkerhetsmekanismene implementeres. Til en viss grad kan en også si at jo høyere i stakken sikkerhetsmekanismene implementeres, jo større mulighet er det for å oppnå sikre ende-til-ende forbindelser. Da de to laveste lagene av protokollstakken opererer link for link, vil ikke ende-til-ende sikkerhet være mulig å oppnå på disse lagnivåene. Derimot i de øvre lag, e.g. applikasjonslaget, vil tjenester og kommunikasjon som oftestr være ende-til-ende på tvers av nettverk uavhengig av de underliggende lag. Data vil i de fleste tilfeller være de samme fra de er levert til underliggende lag hos avsender til de er mottatt og levert til applikasjonslaget hos mottaker. OSI-modellen gir også begrensninger for hvilke lag som kan implementere ende-til-ende kryptering. Dette er illustrert i figur 7.1a. *Header* er tjenesteparametere for det aktuelle laget og *dataenhet* er nyttedataene som skal bli sendt. Om kryptering er implementert i lag n vil hele dataenheten for lag n være kryptert. Dataenheten for lag n vil inneholde både header og dataenhet for lag $n+1$. Siden kryptering er implementert i lag n vil ikke header og dataenhet være tilgjengelig for lag $n+1$ om ikke disse dekrypteres før de leveres til lag $n+1$. Dette gir problemer da headeren for lag $n+1$ er uleselig og ikke kan prosesseres grunnet at den er kryptert av lag n. Lik resonering kan dermed gis for lag $n+m$ om m er et vilkårlig positivt heltall og kryptering er implementert i lag n. Om en studerer figur 7.1a nærmere kan en se at forskjellig informasjon er tilgjengelig og sendes ukryptert avhengig av hvilket lag kryptering er implementert, samt hvor i nettet en observerer dataene. I.e. om kryptering hadde vært implementert i lag $n+1$ ville header for lag n og $n+1$ være tilgjengelig og leselig for lag $n-m$, mens dataenhet for lag $n+1$ fortsatt ville vært kryptert og kun leselig for lag $n+1$. Av dette ser en at de underliggende protokollagene setter begrensninger for hvor i stakken sikkerhetsmekanismer kan implementeres. Forskjellig informasjon sendes også åpent avhengig av hvilket protokollag som implementerer kryptering. Et sentralt punkt å poengtere er at ikke alle nettverksnoder på vei fra sender til mottaker involverer prosessering av alle lag av protokollstakken. Dette er illustrert i figur 7.1b. Figuren viser en forenklet modell av kommunikasjon mellom en målernode og et sentralsystem som kommuniserer over Internett. Figuren viser at målernoden og sentralsystemet prosesserer alle lagnivå, mens e.g. en ruter i kommunikasjonsstien prosesserer kun de tre nedre lagnivå.

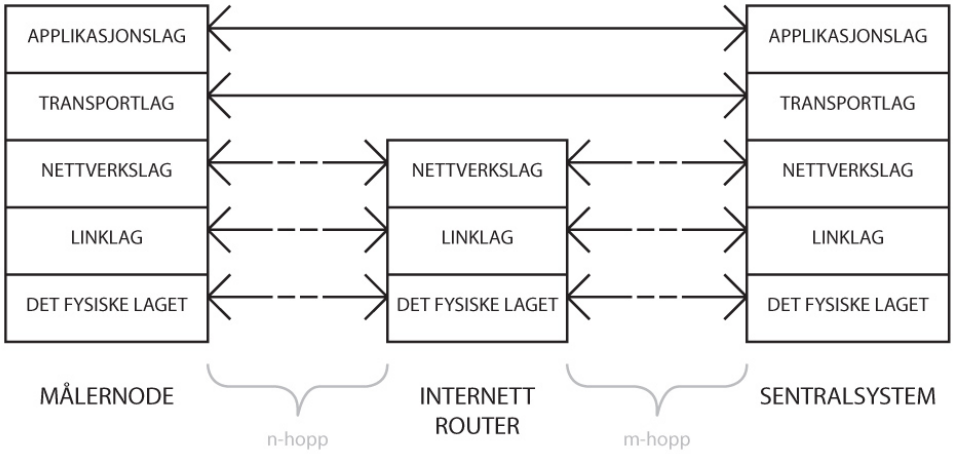
En kan dermed si at jo høyere i OSI-modellen kryptering implementeres, jo mer informasjon sendes åpent og er tilgjengelig for underliggende lag. Implementering av kryptering i lavere lag begrenses av at overliggende lag ikke får tilgang til nødvendig.

7.2.4 Forsvar i dybden

Systemer med høyrisiko bør ikke baseres på kun ett lag av sikkerhet. Høyrisikosystemer bør ikke utsettes for at én feil gir konsekvenser for sikkerheten i hele systemet. Derimot bør en benytte flere lag av sikkerhet for å få den totale risikoen til et akseptabelt nivå. Dette kalles *forsvar i dybden*. Med forsvar menes det i denne sammenheng tiltak, eller barrierer, som er planlagt og iverksatt for å bryte et spesifisert uønsket hendelsesforløp. Tiltak og barrierer er sikkerhetssammenheng mekanismer som tilbyr forskjellige sikkerhetstjenester. Ideelt skal barrierene på alle nivå være intakt og på den måten greie å forhindre ulykker allerede på første nivå. Men ettersom feil, modifiseringer og eventuell utkobling av barrierer på alle nivå kan føre til redusert funksjon, vil brudd på sikkerheten fortsatt kunne oppstå. En



(a) Kryptering av OSI-lagheadere



(b) Prosessering av OSI-lag i nettverk

Figur 7.1: OSI-lag og kryptering

vil altså minimere sannsynligheten for at alle barrierene svikter samtidig. Slike situasjoner vil kun oppstå om det eksisterer avhengighet mellom barrierene, noe som vil si at flere barrierer blir svekket eller satt ut av funksjon av en enkelt hendelse. NIST har publisert et dokument med prinsipper å følge for informasjonssikkerhet i IT systemer og skriver følgende om sikkerhet i flere lag, [33]:

> Securing information and systems against the full spectrum of threats requires the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. This is due to the highly interactive nature of the various systems and networks, and the fact that any single system cannot be adequately secured unless all interconnecting systems are also secured.
>
> By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected.

OPEN meter oppfordrer også til å følge prinsippet om forsvar i dybden og skriver i kravspesifikasjonen for AMI følgende, [60] "The concept of defense in depth should be applied to the global system: security at each layer of infrastructure, from the AMI centralized system to the end-point meter, including networks."

Ettersom AMS må ses på som å et system med høy risiko velger vi derfor å designe sikkerhetsarkitekturen for AMS-kanalen etter prinsippet om *forsvar i dybden*. Forsvar i dybden kan også realiseres gjennom innføring av ikke-tekniske barrierer e.g. organisatorisk informasjonssikkerhet, se seksjon 3.3.5. Da dette kapittelet kun beskriver arkitektur for sikker overføring i AMS-kanalen, presenteres slike barrierer her.

7.3 Kommunikasjonsprofil og konfigurasjoner

I denne seksjonen presenteres et forslag til sikkerhetsarkitektur i AMS-kanalen. Det vil først bli presentert en begrunnelse for valg av teknologi og et overblikk av løsningen. Deretter diskuteres hvordan de enkelte teknologiene kan konfigureres til å oppnå akseptabelt nivå av informasjonssikkerhet. Til slutt vil det presenteres en vurdering av løsningen samt andre vurderinger og forslag for en sikker arkitektur for AMS-kanalen.

7.3.1 Valg av teknologi og overblikk

I og med de store investeringene knyttet til AMS er det viktig at de systemene som rulles ut er framtidsrettet slik at de kan håndtere oppgaver og krav som settes til AMS, også i framtiden. Om løsninger designes etter minimumskrav for å oppfylle dagens behov, vil eventuelle framtidige utvidelser føre til store kostnader knyttet til redesign eller installering av nye systemer som oppfyller de framtidige behovene. Slik kan en si at en framtidsrettet løsning vil være en løsning som er fleksibel og modulær samt hvor avhengigheten mellom de forskjellige modulene er lav. I en modulær løsning vil en kunne erstatte og bytte ut de eksisterende modulene med nye moduler som tilbyr funksjonalitet som oppfyller framtidige behov. Om avhengigheten mellom disse modulene er lav, vil bytte av en slik modul kun kreve moderate endringer eller tilpasninger for å innarbeide den nye modulen til å fungere i den eksisterende løsningen.

Med hensyn på kommunikasjonsteknologier og standarder for bruk i AMS, bør valg av disse skje gjennom en slik modulær tankegang. Om mulig vil dette hjelpe til å minimere kostnader ved eventuelle framtidige utvidelser eller endringer. For AMS-kanalen vil dette hovedsakelig dreie seg om hvilken *kommunikasjonsprofil* som velges for de forskjellige linkene og hvordan disse profilene er satt sammen. Med ordet kommunikasjonsprofil menes det sammensetningen av protokoller i de forskjellige protokollagene. For løsninger hvor avhengigheten mellom protokollagene er stor vil muligheten for forandringer i kommunikasjonsprofilen være begrenset. En kan anta at et bytte av en full kommunikasjonsprofil for AMS vil medføre store kostnader, med hensyn til eventuelt bytte av kommunikasjonsutstyr og tilrettelegging for kompatibilitet mot applikasjoner etc. En modulær og fleksibel kommunikasjonsprofil vil derimot ikke ha disse sterke avhengighetene mellom protokollagene og føre til mindre forandring i kommunikasjonsprofilen. Ettersom et protokollag baserer seg på tjenester tilbydt av det underliggende laget, samt tilbyr tjenester til det overliggende protokollaget, er ikke total uavhengighet mellom protokollagene mulig. Derimot kan nivå av avhengighet til en viss grad kontrolleres ved å velge protokoller som er fleksible med tanke på alternativer for underliggende protokoller. Et alternativ er å starte med valg av protokoll for applikasjonslaget, for deretter å studere de forskjellige tilgjengelige og mulige kommunikasjonsprofilene for dette valget. Ut ifra en slik prosess kan en se hvilke applikasjonslagprotokoller som er mest fleksible med tanke på underliggende protokoller. *Topp-til-bunn* vurdering av kommunikasjonprofilen for AMS-kanalen har flere fordeler. De kommuniserende applikasjonene, endenodene for AMS-kanalen, må være kompatible med valgt applikasjonslagsprotokoll og de tjenester protokollen tilbyr. Om valgt applikasjonslagsprotokoll ikke tilbyr muligheter for funksjonalitet nødvendig for framtidige behov, må applikasjonslagprotokoll byttes. Ved et slikt bytte vil underliggende protokoller vurderes og applikasjoner i endenodene måtte tilpasses til den nye applikasjonslagprotokollen. Det kan også antas at store kostnader knyttest til et slikt bytte og tilpasninger av ny applikasjonslagprotokoll da det er mye spesialdesignet utstyr brukt innen AMS.

Vurderingen av kommunikasjonsprofil for AMS-kanalen tar dermed utgangspunkt i hvilken applikasjonsprotokoll som er mest egnet med tanke på funksjonalitet og fleksibilitet til underliggende kommunikasjonsprofil. Med hensyn til diskusjon om ende-til-ende sikkerhet og protokollag, i seksjon 7.2, vil et lag av sikkerhet implementeres i applikasjonslaget. Dette gir muligheter for sikre ende-til-ende forbindelser i applikasjonslaget og utgjøre ett av lagene med tanke på forsvar i dybden. Av denne grunn vil også applikasjonslagprotokoll vurderes på tilgjengelige sikkerhetsmekanismer. Underliggende kommunikasjonsprofil skal deretter velges utifra kravene om fleksibilitet og modularitet, kompatibilitet med kommunikasjonsnett som beskrevet i seksjon 7.2.1, samt gi muligheter for minst ett lag av ende-til-ende-sikkerhet.

Det vil nå bli presentert hvilken applikasjonsprotokoll og underliggendekommunikasjonsprofil som ble valgt for sikkerhetsarkitekturen i AMS-kanalen samt begrunnelse for valgene. Se seksjon 7.3.5 for en vurdering av de andre protokollene studert i denne oppgaven.

7.3.1.1 Applikasjonsprotokoll

Den anbefalte applikasjonslagprotokollen for AMS-kanalen er DLMS/COSEM - IEC 62056. Standarden definerer både applikasjonslagprotokoll og dataformat som tillater en rekke alternativer for underliggende kommunikasjonsprofiler. Fleksibiliteten med tanke på kommunikasjonsprofiler gjør at OPENmeter også anbefaler DLMS/COSEM som applikasjonslagsprotokoll for mange av sine løsninger for AMS [65]. Ved at standarden bare definerer applikasjonslagprotokoll gjør at den kan benyttes i sammenheng med mange kommunikasjonsmedier og kommunikasjonsnett, e.g. lokale busser, PLC, Internett, GPRS/UMTS. Standarden er også åpen og tilgjengelig gjennom DLMSs brukerorganisasjon. Disse egenskapene har gjort at DLMS/COSEM - IEC 62056 er det beste alternativet til en åpen, interoperabel standard for smarte målere, nasjonalt og internatsjonalt[3]. Datamodellen spesifisert av DLMS/COSEM tilbyr god funksjonalitet og muligheter som kan oppfylle framtidige behov. Ettersom standarden kan tilby denne funksjonaliteten og samtidig tillate en fleksibel underliggende kommunikasjonsprofil, er den egnet til bruk i mange ledd i AMI ikke kun AMS-kanalen. I AMS-kanalen kan protokollen benyttes for alle linker og løsninger i den generiske arkitekturen presentert i denne oppgaven. Haugen vurderte i sin rapport DLMS/COSEM til en av de mest framtidsrettede og aktuelle applikasjonslagsprotokollene for AMS. I sine vurderinger ga Haugen standarden maksimal karakter på fem av seks vurderingskriterier og en total vurdering til 23 av totalt 24 poeng[4], se figur 5.3 [41]. At DLMS/COSEM er den mest aktuelle applikasjonslagprotokollen tilgjengelig støttes også av Craemer og Deconinck i deres rapport [25] samt Štruklec og Maršić i deres rapport ved navn "Implementing DLMS/COSEM in Smart Meters" [91].

Blant applikasjonsprotokollene studert i denne oppgaven tilbyr DLMS/COSEM standarden den mest robuste og fleksible sikkerhetsarkitekturen. I seksjon 6.2.2.1 ble det vist at standarden alene kan tilby autentisering av sender/mottaker ved det som kalles *aksessikkerhet*, samt integritetssjekk av og konfidensialitet for datatrafikk gjennom *transportsikkerhet*. Ved riktig konfigurasjon kan DLMS/COSEM skape sikre ende-til-ende forbindelser mellom applikasjonslagsprosesser og oppnå et akseptert nivå[5] av sikkerhet i applikasjonslaget.

7.3.1.2 Underliggende kommunikasjonsprofil

Fleksibiliteten til underliggende kommunikasjonsprofil for DLMS/COSEM gjør at det er mange alternative protokoller å benytte seg av. Kmethy forteller i en presentasjon om "Security of meter data exchange over open networks" fra 2007 følgende om DLMS/COSEM standarden "Due to the orthogonality of DLMS/COSEM, the object model and the communication profiles can be developed independently" [51]. Med dette utgangspunkt står en fritt til å velge kommunikasjonsprofil med hensyn til lokale forhold krav og begrensninger for hver implementasjon. Men for foreslått sikkerhetsarkitektur for AMS-kanalen i denne oppgaven, settes det krav om forsvar i dybden samt krav om en framtids-

[3]Statisikk over internasjonale implementasjoner av DLMS/COSEM kan finnes ved brukerorganisasjones nettsider [12]

[4]Haugen benyttet opprinnelig sju vurderingskriterier men kun seks er omtalt i denne rapporten. Se seksjon 5.2

[5]I henhold til diskusjon i seksjon 6.7

rettet løsning, respektivt i seksjon 7.2 og 7.2.4.

Av diskusjon vedrørende bruk av kommunikasjonsnett i seksjon 6.3, kan en anta at AMS-kanalen kommer til å ta i bruk eksisterende infrastruktur for kommunikasjon. Videre kan en utifra diskusjon vedrørende PLC og BPL, i seksjon 5.3.1 og 6.3, anta at det er liten sannsynlighet for at kraftnettet alene kan brukes som kommunikasjonsnett for AMS-kanalen i årene framover med de teknologier som tilgjengelige per skrivende stund. Ut ifra dette konkluderes det at AMS-kanalen kommer, med høy sannsynlighet, til å benytte eksisterende infrastruktur for telekommunikasjon.

AMS står for kommunikasjon mellom komponentene i strømnettet, og vil være fundamentet for konsepter i det kommende *smarte strømnettet*. Inter-AMS kommunikasjon, i.e. kommunikasjon på mellom flere AMS, vil da mest sannsynlig gå over heterogene nett ettersom tilgjengelig kommunikasjonsløsninger og nett vil variere for de forskjellige nett og deres lokasjon. Ettersom kommunikasjon i heterogenenett fører til kompatibilitets- og skaleringsproblemer trengs en universell måte å kommunisere på på tvers av alle kommunikasjonsteknologiene. Nettverksløsninger basert på IP muliggjør kommunikasjon på tvers av heterogenenett og er et av de største susksesskriteriene til den utbredte bruken av protokollen samt penetrasjon av Internettilgang globalt[6]. IP spesifiseres i nettverkslaget og det finnes løsninger for implementasjon over de fleste protokoller for link- og det fysiske laget. Antall alternative protokoller for transportlag over IP er også stort. Løsninger ved bruk av TCP/IP er et utbredt alternativ i mange sammenhenger, ettersom Transmission Control Protocol (TCP) kan tilby pålitelig overføring. Det mest benyttede alternative til TCP er User Datagram Protocol (UDP), gjerne benytted i applikasjoner uten krav om pålitelighet for overføring. Figur 7.2 viser veksten i tilgang til Internett i Norge til og med 2009. Figuren er hentet fra en rapport Eikland, Budde og Kleppe skrev på "Nettselskapets rolle i det fremtidige norske kraftmarkedet med AMS-infrastruktur" i 2010 hvor tallene er hentet fra MedieNorge[7] [50]. Med hensyn til den kontinuerlige veksten av penetrasjon for både kabelbasert[8] og trådløs[9] Internettilgang samt IP-baserte tjenester i Norge og Europa, må teknologien anses til å være tilgjengelig for overskuelig framtid [53]. Med dette kan en med stor sannsynlighet anta at IP kommer til å ha en nøkkelrolle for kommunikasjon i smarte strømnett[55, 41, 67, 17], og er grunnen til at en kommunikasjonsprofil for AMS-kanalen basert på IP anbefales i denne oppgaven.

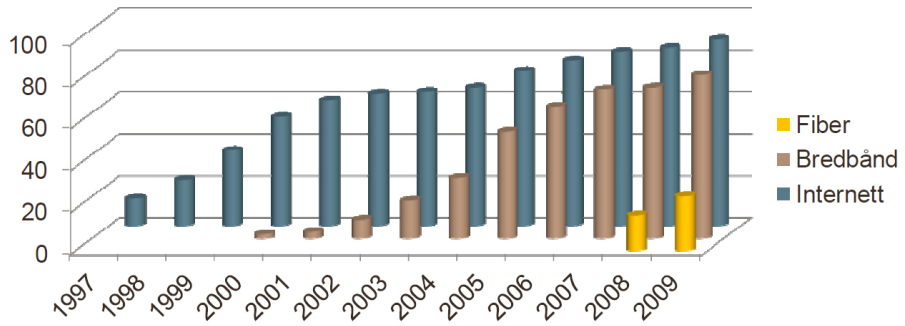
Det eksisterer det to versjoner av IP, IPv4 og IPv6. IPv4 er den dominerende, men grunnet adressemangel og begrensede funksjoner vil bruk av IP migrere fra IPv4 til IPv6. IPv6 benytter seg av 128-bits adresserom relativt til 32-bits adresserom benyttet i IPv4. I tillegg har IPv6 mulighet for større datapakker samt flere konfigurasjonsmuligheter og støtte for e.g. multicast og integrering av IPsec. I et framtidig smart strømnett hvor alle kommuniserende enheter må ha en unik adresse vil adressemangelen for IPv4 adresser skape begrensninger og problemer. Det anses derfor at IPv6 vil være den mest aktuelle IP versjonen i framtiden [55, 17, 41, 67]. Ettersom IPv6 ikke ennå er fullt implementert og støttet i Internett setter ikke denne oppgaven noen krav om bruk av IPv6. Men om IPv4

[6] I følge Wansink og Buddle bruker 25% av verdens befolkning Internett per i dag og bruken anses til å øke kontinuelig i tiårene framover, spesielt i store land som Russland, India og Kina [15]

[7] `http://medienorge.uib.no/`

[8] Kabelbasert bredbånd migrerer fra xDSL til FTTx

[9] 3G og 4G/LTE



Figur 7.2: Utvikling av Internettilgang i husholdninger [50]

benyttes bør implementasjonen til størst mulig grad legges opp for bruk av IPv6 på sikt og minimere nødvendige endringer og tilpasning av kommunikasjonsprofilen ved en slik overgang.

For implementasjon av ett lag av sikkerhet i kommunikasjonsprofilen under applikasjonslaget anbefaler denne oppgaven bruk av IPsec. IPsec er en veletablert og robust standard som er kompatibel med IPv4 og integrert og et krav for IPv6. Med de avgrensningene satt av målene for sikkerhetsarkitekturen i AMS-kanalen var IPsec et klart valg. Implementasjon av sikkerhetsmekanismer i protokollag under nettverkslaget ville satt krav til sikkerhetsmekanismer i underliggende kommunikasjonsløsning. Av diskusjon om at alle nivå av sikkerhet skal håndteres av sikkerhetsarkitekturen internt, seksjon 7.2.2 og 7.2.1, er ikke sikkerhetsmekanismer i link- eller det fysiske laget et alternativ. Å implementere sikkerhetsmekanismer i transportlaget er heller ikke en god løsning da det begrenser fleksibiliteten med tanke på valg av protokoll. Valg av transportprotokoll bør kunne velges avhengig av behovene og kravene for hvert bruksområdet, e.g. bruk av pålitelig eller upålitelig overføring respektivt ved bruk av TCP og UDP. DLMS/COSEM kan benyttes over flere transportlagsprotokoller og støtter både UDP/IP og TCP/IP. Bruk av IPsec i nettverkslaget tillater fritt valg av underliggende protokoller og samtidig fleksibilitet med tanke på transportprotokoll. Selv om IPsec allerede støttes brukt over de fleste[10] underliggende kommunikasjonsløsninger hvor IP støttes, må kommunikasjonsprofilen i enkelte tilfeller tilpasses. Seksjon 6.2.1.2 viser at arbeid pågår for å muliggjøre IPsec over IPV6, ved bruk av et konvergenslag kalt 6LoWPAN, for PLC G3 løsninger basert på 802.15.4.

Sikkerhetsarkitekturen for IPsec blir presentert i seksjon 7.3.3 og viser at IPsec kan tilby mekanismer som gjør at nettverkslaget alene kan gi et lag av sikre ende-til-ende forbindelser i AMS-kanalen. Ettersom IPsec kreves ved bruk av og er integrert i IPv6 gjør valget til en framtidsrettet løsning.

7.3.2 DLMS/COSEM

Se seksjon 6.2.2.1 for sikkerhetsarkitekturen for DLMS/COSEM standarden.

[10] GPRS, UMTS, Internett etc.

7.3.2.1 Konfigurasjon

DLSM/COSEM tilbyr en sikkerhetsarkitektur som alene kan sikre forbindelser mellom applikasjonslagsprosesser hos avsender og mottaker, uavhenging av sikkerhet i underliggende lag. Sikkerhetsarkitekturen i DLMS/COSEM muliggjør en fleksibel konfigurasjon som kan tilby forskjellige sikkerhetsmekanismer for å oppnå et akseptabelt nivå av sikkerhet. Etter kravet om forsvar i dybden må også sikkerheten implementert i applikasjonslaget alene kunne gi et tilstrekkelig nivå av sikkerhet. Vi diskuterer nå alternative for DLMS/COSEM og forslag til konfigurasjoner. *Aksessikkerheten* i DLMS/COSEM standarden definerer autentiseringskontekster som beskriver hvilke logiske enheter som har tilgang til hvilke objekter med tilhørende attributter og metoder. Nivå for aksessikkerhet kan enten settes til ingen autentisering, passordbeskyttet autentisering(LLS) og gjensidig kryptografisk autentisering (HLS). Autentisering av kommunikasjon er essensielt for integriteten av kommunikasjon og må prioriteres. Aksessikkerheten står for autentisering av både xDLMS APDU meldinger og ASE APDU meldinger hvor sistnevnte ikke er beskyttet av transportsikkerheten. Ved å benytte autentisering gjennom aksessikkerhet vil også integriteten av disse kunne bekreftes. Bruk av HLS anbefales for å sikre integriteten av avsender/mottaker.

Transportsikkerhet gir muligheter for kun autentisering, kun kryptering eller både autentisering og kryptering. Transportsikkerhet opererer kun på xDLMS APDU meldinger og kan tilby integritet og konfidensialitet for slike meldinger. Da kryptering ikke håndteres av aksessikkerheten må dette gjøres gjennom transportsikkerhet. På lik måte som for integriteten av avsender og mottaker, tatt hånd om av autentisering i aksessikkerhet, bør integritet av data sikres gjennom autentisering i transportsikkerhet. DLMS/COSEM gir også mulighet for bruk av autentisert kryptering, som kan være et alternativ og må vurderes i de enkelte tilfeller. Valg av symmetrisk eller asymmetrisk kryptografi til bruk i sikkerhetsmekanismene må også vurderes i forhold til hver implementasjon. Disse vurderingene bør gjøres med hensyn til nøkkelhåndtering og administrasjon, skalerbarhet og ytelsesperspektiver. Med ytelse tenkes det her på anbefalte nøkkelstørrelser for symmetrisk og asymetrisk kryptografi i henhold til prosesseringskraft og båndbredde for overføring av nøkler, sertifikater etc. DLSM/COSEM spesifiserer bruk av symmetrisk kryptografi og støtte for asymmetrisk kryptografi er under arbeid, se seksjon 6.2.2.1.

Ved å benytte sikkerhetskonfigurasjon beskrevet i denne seksjonen vil en implementasjon av DLMS/COSEM kunne tilby både ende-til-ende integritet og konfidensialitet av kommunikasjonen i applikasjonslaget.

7.3.3 IPsec

IP security (IPsec) er et sett av protokoller som kan tilby autentisering, konfidensialitet og nøkkelhåndtering på IP nivå i nettverkslaget. IPsec er en utvidelse av IP protokollen og er kompatibel med Internet Protocol version 4 (IPv4) og integrert i IPv6. Ved å implementere sikkerhetstjenester under transportlaget er protokollen transparent for overliggende lag og applikasjoner. IPsec er svært fleksibel og gir systemer muligheten til å velge nødvendig sikkerhetsprotokoller, forhandle hvilke algoritmer som skal benyttes for de forskjellige tjenestene samt å generere og utveksle nødvendige nøkler for de aktuelle tjenestene. IPsec tilbyr to forskjellige protokoller for sikker kommunikasjon, AH og ESP. Figur 7.3 viser

	AH	ESP (encryption)	ESP (encryption and authentication)
Access control	X	X	X
Connectionless integrity	X		X
Data origin authentication	X		X
Rejection of replayed packets	X	X	X
Confidentiality		X	X
Limited traffic flow confidentiality		X	X

Figur 7.3: Sikkerhetstjenester i IPsec [82]

hvilke tjenester de respektive protokollene tilbyr.

IPsec innfører begrepet Security Associations (SA). En *sikkerhetsassosiasjon* er en énveis assosiasjon mellom sender og mottaker og definerer hvilke sikkerhetstjenester som skal benyttes for kommunikasjon knyttet til den aktuelle assosiasjon. Det kreves derfor en sikkerhetsassosiasjon for hver retning ved sikker toveis kommunikasjon. Sikkerhetstjenestene knyttet til en SA er definert som et sett av tjenestene enten AH eller ESP kan tilby, ikke begge. Måten IPsec knytter forskjellig innkommende og utgående trafikk mot forskjellig SA er meget fleksibel. Forskjellige trafikkprofiler er spesifisert ut ifra parametre i IP og øvre protokollag og deres kobling mellom trafikkprofil og tilhørende SA er lagret i Security Policy Database (SPD). E.g. kan utgående trafikk mappes mot riktig SA på grunnlag av sender og mottakers IP adresse, brukernavn fra operativsystem, type transportprotokoll etc.

Vi ser av figur 7.3 at man ved å benytte AH kan oppnå dataintegritet og autentisering av trafikk. På denne måten kan en garantere at data ikke er modifisert i transitt samt at trafikken er generert av rett avsender. I tillegg beskytter AH mot duplikatmeldinger og adresse-spoofing [82]. Siden autentiseringen i AH er basert på melding autentiseringskoder må sender og mottaker dele en hemmelig nøkkel. Ved å benytte ESP protokollen kan en oppnå konfidensialitet av trafikk inkludert konfidensialitet av meldingsinnhold og *begrenset trafikkflyt konfidensialitet*. Begrenset trafikkflytkonfidensialitet reduserer statistisk informasjon tilgjengelig gjennom trafikkanalyse ved bruk av padding av meldinger. Om begrenset trafikkflytkonfidensialitet oppnås er avhengig av konfigurasjon av ESP. I tillegg til konfidensialitet kan også ESP tilby autentisering av sender/mottaker og integritetssjekk av nyttelast.

IPsec kan operere både i *trafikk*-modus og i *tunnel*-modus. Sammenhengen mellom hvordan sikkerhetstjenester opererer under de respektive modusene er avhengig av om enten AH eller ESP benyttes, samt om IPsec benyttes på IPv4 eller IPv6 trafikk. En forenklet modell vil si at sikkerhetsmekanismer i trafikkmodus opererer på kun nyttelasten og tar ikke hånd om meldingsheader. I transportmodus opererer sikkerhetsmekanismene både på meldingsheader og nyttelast, ved å kapsle meldingen inn i en ny melding hvor den orginale meldingen blir nyttelast i den nye meldingen. Vi henviser til [82] og [77] for nærmere spesifikasjoner.

Sikkerhetsassosiasjon- og nøkkeladministrering i IPsec kan enten gjøres manuelt eller automatisert. Ettersom manuell administrering av sikkerhetsassosiasjoner ikke ska-

lerer, er en automatisert løsning for større systemer nødvendig. Internet Key Exchange (IKE) er en komponent av IPsec for gjensidig autentisering og administrering av sikkerhetsassosiasjoner. En utvidet og oppdatert utgave av IKE finnes, IKEv2 [27]. IKE er også kalt Oakley/ISAKMP. Oakley er en utvidet generisk utgave av Diffie-Hellman nøkkelutvekslingsalgoritme som beholder fordelene ved algoritmen men samtidig utretter dens svakheter. Internet Security Association and Key Management Protocol (ISAKMP) er et rammeverk for nøkkeladministrering og forhandling om sikkerhets parametre [82].

7.3.3.1 Konfigurasjon

Fleksibiliteten og konfigurasjonsmulighetene ved IPsec passer godt med kravene for sikkerhetsarkitekturen i AMS-kanalen. Det vil nå presenters enkelte konfigurasjoner og egenskaper ved IPsec som kan utnyttes til å skape akseptabelt nivå av sikkerhet i nettverkslaget. Av AH og ESP er det ESP som er den mest aktuelle protokollen med tanke på at den kan tilby for både dataintegritet, autentisering av sender/mottaker og konfidensialitet.

KS: Konsentrator - Sentralsystem For linkene mellom konsentratorer og sentralsystemet vil det være mest naturlig å sette opp ESP i *tunnel*-modus. Ettersom sikkerhetstjenestene opererer på både header og nyttelast vil et slikt oppsett minimere andel av data som sendes åpent og ubeskyttet. Ved å benytte tunnelmodus på KS-linker hindrer en også innsyn i trafikk til/fra en spesifikk måler bak konsentratoren. Ettersom meldingsheaderen vil være uleselig vil det være vanskelig ved angrep på KS-linker å avgjøre hvem en melding sendt over linken er adressert til, enten en spesifikk måler eventuelt terminert i konsentratoren.

MS: Målernode - Sentralsystem På linker mellom målernoder og sentralsystemet har det ikke samme hensikt å benytte tunnelmodus som for på KS-linker. En melding sendt over MS-linker må uansett være adressert den spesifikke målernoden eller sentralsystemet, og derfor er det mest hensiktmessig å benytte *transport*-modus for slike linker.

MK: Målernode - Konsentrator På samme måte som for MS-linker vil en ikke kunne skjule hvilken målernode trafikk over disse linkene er addresert til. Derfor anbefales transport-modus for slike linker.

Konfigurasjon av sikkerhetsassosiasjoner, SA, må utdypes. Det er en sikkerhetsassosiasjon som definerer hvordan en spesifikk trafikkflyt skal behandles i forhold til sikkerhetstjenester. IPsec tillater også nøstede sikkerhetsassosiasjoner som gir muligheten for en fleksibel konfigurering av sikkerhetstjenestene for hver trafikkflyt. Nøsting av SA gjør at en trafikkflyt også kan autentiseres gjennom ESP. Detaljert konfigurering av sikkerhetsassosiasjoner for trafikkflyt i AMS-kanalen gjør at en kan behandle trafikk begge retninger forskjellig utifra hvordan SA den spesifikke trafikkflyten mappes mot. Med hensyn til hvor essensielle forskjellige sikkerhetstjenester er for de forskjellige linkene, kan sikkerhetsassosiasjonene konfigureres og settes etter nivå av sikkerhet nødvendig for hver retningene på alle linkene i AMS-kanalen. Riktig oppsett av SA vil samtidig la komponentene i nettverket ignorere trafikk som ikke er beskyttet av IPsec, eventuelt ikke er kryptert eller avsender ikke kan autentiseres. [77].

For administrering av sikkerhetsassosiasjoner vil et automatisert alternativ være mest hensiktsmessig da dette skalerer bedre enn manuell konfigurasjon. IKEv2 utnytter Oakley-/ISAKMP til å opprette en midlertidig sikkerhetsassosiasjon mellom sender og mottaker for å utveksle og forhandle sikkerhetsparametre [76]. En automatisert SA administrering gjennom IKEv2 gjør at sikre forbidelser mellom nye noder i AMS-nettverket kan oppnås uten at de på forhånd har noen kjennskap til hverandre. IKEv2 gjør det samtidig mulig å definere gyldigheten for sikkerhetsassosiasjoner, slik at tidligere assosiasjoner kan gjøres ugyldige og den sikre forbindelsen ikke lenger er tilgjengelig.

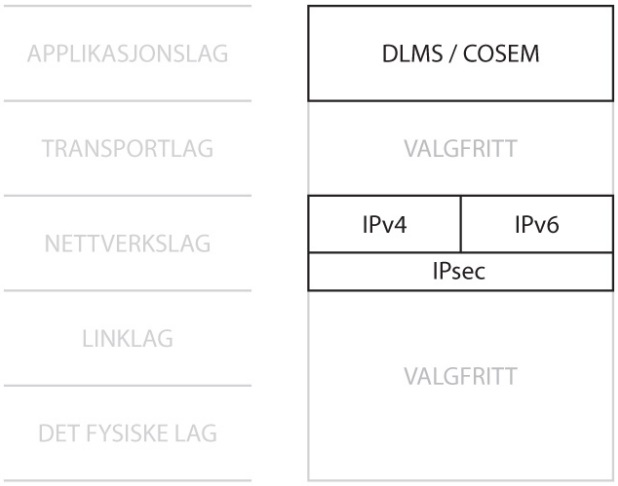
IPsec definerer ikke noen faste algoritmer, men lar valg av disse stå åpent og må vurderes for hver implementasjon. Derimot må to kommuniserende parter ha minimum en felles algoritme av hver type for å kunne skape en sikker forbindelse for kommunikasjonen. IKEv2 håndterer forhandlingene om hvilke algoritmer som er tilgjengelig hos hver part. Men også for IKEv2 er valg av algoritmer åpent, også her må minst en algoritme av hver type være felles for at IKEv2 skal kunne danne den midlertidige sikre forbindelsen benyttet til forhandling av parametre og oppsett av sikkerhetsassosiasjonene. De forskjellige typene algoritmer deles inn etter algoritmer for kryptering, integritet, generatorer for psaudo-tilfeldige tall, etc. De eksakte algoritmene kalles i IPsec dokumentasjonen *transformer*. For IKEv2 er en oversikt over typer og forslag til alternative for algoritmer gitt i RFC4307[11], hvor alternative Diffie-Hellman grupper også er gitt [76]. Algoritmetyper og forslag til alternative algoritmer for ESP og AH er definert i RFC 4835 [56].

Ved å benytte IPsec med automatisert SA administrering, IKEv2, vil en kunne skape sikre ende-til-ende forbindelser mellom nettverksnodene i AMS-nettverket. Å implementere sikkerhetsmekanismer i nettverkslaget gjør sikkerhetsmekanismene transparent for overliggende lag i stakken inklusive applikasjonslaget. Samtidig tillater den automatiserte SA administreringenen dynamikk i nettverket hvor sikre kanaler kan opprettes og oppheves etter behov.

7.3.4 Oppsummering

Figur 7.4 viser kommunikasjonsprofilen anbefalt for sikker kommunikasjon i AMS-kanalen. Kommunikasjonsprofilen implementerer DLMS/COSEM som applikasjonslagsprotokoll. Standarden definerer både datamodell og applikasjonslagsprotokoll tilbyr fleksibilitet for underliggende kommunikasjonsprofil med mange alternativer til protokoller på alle lag. Sikkerhetsarkitekturen for DLMS/COSEM tilbyr også de nødvendige sikkerhetsmekanismene som alene kan skape sikre ende-til-ende forbindelser mellom noder i AMS-nettverket. I nettverkslaget implementerer profilen IP som nettverksprotokoll. Med hensyn til protokollens uavhengighet til underliggende kommunikasjonsmedier er IP til et godt alternativ for universell kommunikasjonsprotokoll i heterogene nett. Både IPv4 og IPv6 kan benyttes, men ved valg av IPv4 anbefales implementasjonen å tilrettelegge for en framtidig overgang til IPv6. Ved at både IPv4 og IPv6 støtter bruk av IPsec vil nettverkslaget alene kunne tilby sikkerhetsmekanismer for å skape sikre forbindelser på linkene i AMS-kanalen. I figur 7.4 er IPsec illustrert som et lag under IP. Dette kan føre til forvirring og det må presisere

[11] En utvidet oversikt over alternative algortimer for IKEv2 med referanse til tilhørende RFC er gitt av Internet Assigned Numbers Authority (IANA). `http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xml`



Figur 7.4: Kommunikasjonsprofil for sikker AMS-kanal

at IPsec i hovedsak er integrert i nettverkslaget og er en utvidelse av IP. Hensiktsmessig plassering av IPsec over eller under IP i en slik figur er avhengig av konfigurasjon og hvilke felt av IP-pakker som blir beskyttet av sikkerhetsmekanismene i IPsec. Underliggende kommunikasjonsmedium velges fritt etter hva som er mest hensiktsmessig og tilgjengelig i de enkelte tilfeller. Transportlagsprotokoll velges også fritt etter behov. Eneste minstekrav er at kommunikasjonsmediet har muligheter for eller kan tilpasses IPv4, IPv6 samt IPsec.

7.3.5 Protokoller som ikke ble valgt

Det vil nå bli gitt en kort begrunnelse hvorfor de følgende standardene og protokollene ikke ble valgt som en del av sikkerhetsarkitekturen for AMS-kanalen.

LonWorks Med hensyn til at LonWorks spesifiserer alle lag av protokollstakken tilbyr standarden liten fleksibilitet med tanke på kommunikasjonsprofil. I tillegg er funksjonalitet tilgjengelig begrenset noe som gjør LonWorks lite fremtidsrettet og et uaktuelt valg for AMS-kanalen.

M-Bus - EN 13757 M-Bus har attraktive egenskaper men ble ikke valgt som løsning i denne oppgaven med hensyn til lite fleksibilitet i kommunikasjonsprofil, samt svak sikkerhetsarkitektur. Et alternativt bruksområdet vil være over MK-linker, se seksjon 7.6

SITRED Ettersom dette er en proprietær protokoll har full analyse av spesifikasjoner ikke vært mulig. Men med tanke på liten fleksibilitet for kommunikasjonsprofil vil dette anses til å være en lite framtidsrettet løsning.

SML SML ble ikke et aktuelt alternativ hovedsakelig med hensyn til at protokollen ikke spesifiserer noen sikkerhetsarkitektur. Dette er i konflikt med mål om forsvar i dybden samt en fleksibel kommunikasjonsprofil. Et alternativ for bruk av SML ville vært

å implementert sikkerhetsmekanismer i transportlaget, noe som setter begrensninger for kommunikasjonsprofil.

DPWL Standarden tilbyr en framtidsrettet løsning med fleksibilitet i kommunikasjonsprofil, gode muligheter for funksjonalitet samt sikker ende-til-ende kommunikasjon. Men med hensyn til at standarden er relativt ung, samt lite benyttet i kraftbransjen ble ikke DPWL valgt som alternativ for sikkerhetsarkitekturen for AMS-kanalen.

7.4 Andre vurderinger ved sikring av AMS-kanalen

Ved design av en sikker kommunikasjonsløsning er det mange kriterier som må håndteres for å oppnå et akseptabelt nivå av sikkerhet. Det vil nå kort bli presentert noen punkter med relevans til sikkerhetsarkitekturen for AMS-kanalen.

7.4.1 Implementasjon

Ved realisering av systemer er det essensielt at funksjonalitet og tilhørende sikkerhetsmekanismer implementeres og konfigureres korrekt. Se seksjon 3.3.3. Dette betyr at det ikke skal finnes noen måte å unngå sikkerhetsmekanismene grunnet feil eller svakheter i deres implementasjon. Med dette settes det høye krav til applikasjonssikkerhet og at implementering av tjenester skjer i samsvar med prinsipper for god applikasjonssikkerhet. Dette inkluderer også administrering av kryptografiske nøkler. I tilfeller hvor standarder benyttes er det også essensielt å verifisere at implementasjonen er i henhold til kravene standarden spesifiserer. Om det er avvik mellom krav og implementasjon er det også sannsynlig at det er avvik mellom egenskapene ved den faktiske implementasjonen og egenskapene standarden spesifiserer. Det må også presiseres hvor viktig verifisering av korrekt implementasjon av standarder er ved bruk av tjenester eller utstyr fra tredjepart. For AMS er det hvert enkelt nettselskaps ansvar å tilby sikker kommunikasjon i deres respektive AMS-nett. Det er dermed implisitt nettselskapenes ansvar og garantere at utstyr og tjenester benyttet i AMS er i henhold til standarder. Verifisering av standarder vil avdekke eventuelle avvik som kan medføre sårbarheter for informasjonssikkerheten i AMS. Slike vurderingen må gjøres av nøytrale tredjeparter. Commen Criteria er et internationalt initiativ som er startet for å verifisere korrekt implementasjon av informasjonssikkerhet og standarder [19]. Deres mål er å kunne vurdere systemer av kompetente og uavhengige lisensierte laboratorier for å verifisere at bestemte sikkerhetsegenskaper er oppfylt. OPENmeter skriver følgende om korrekt implementasjon [66]:

> Besides, one must be very careful not to consider only the technology: the way this technology is implemented can have a significant impact on its level of robustness.
>
> Very often one associates the use of a given technology to a particular level of security; this method is misleading and incomplete: it is always necessary to study also the implementation of this technology in the context of the project in which it is used (setting up, configuration, management, use, upgrade, administration, etc).

7.4.2 Muligheter for oppdateringer og utvidelser

Det bør også stilles krav til utstyr om muligheter for framtidige oppdateringer og eventuelle utvidelser. Sikkerhet er ikke en endelig løsning på et problem, men må ses på som en kontinuerlig prosess med forandringer. Teknologisk framdrift og en verden i konstant forandring gjør at trusselbilde endrer seg med tid og må evalueres jevnlig for å iverksette tiltak for å håndtere nye trusler. Albrechtsen og Hovden skriver følgende om en kontinuerlig sikkerhetsevaluering[12] "Sikkerhet må skapes og gjenskapes hver dag. Det finnes ingen endelige løsninger" [70]. komponenter i AMS-nettet må derfor i størst mulig grad ha muligheten for å utvide sikkerhetsmekanismer til å håndtere en framtidig sitasjon. Med muligheter for utvidelser mener vi oppdatering av programvare, korrekt håndtering av nøkkeloppdatering, utvidelse av nøkkelstørrelser, bytte av usikre kryptografiske algoritmer etc. For sikker håndtering og administrering av kryptografiske nøkler, samt anbefalte algoritmer, nøkkelstørrelser og andre tilhørende parametre, anbefales det å benytte internasjonale anbefalinger av organisasjoner som NIST [39].

7.4.3 Tilgjengelighet

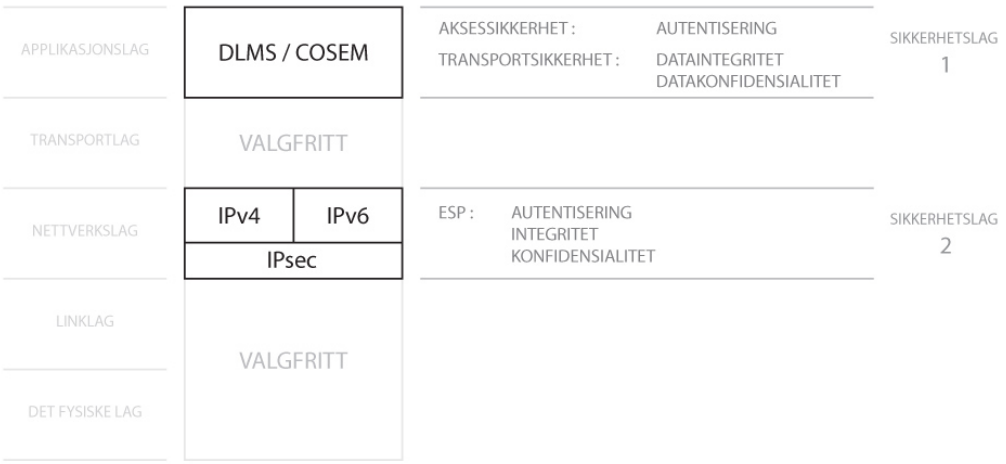
Tilgjengeligheten for tjenester ved bruk av AMS i kraftbransjen er kritisk. Ettersom AMS blant annet skal stå for styring av krafttilførsel og innsamling av forbruksdata for hver enkelt sluttbruker må konsekvensene ved at slike tjenester ikke er tilgjengelige til enhver tid, ses på som store[13]. Av dette kan en si at alle komponenter i AMS-nettverket, inkludert linker og noder, har strenge krav med hensyn til oppetid og tilgjengelighet. For sikkerheten i AMS-kanalen vil dette være relatert til at sikkerheten ikke skal være svekket ved midlertidig bortfall av enkelt tjenester. Sikkerhetssystemer kan konfigureres til å iverksette tiltak basert på slike systemtilstander. Kommuniserende nettverksnoder i AMS bør derfor utføre eller begrense funksjonalitet i forhold til tilgjengelighet for tjenester. E.g. kan mottatte styringssignaler ignoreres om integriteten ikke kan garanteres, måleverdier tilbakeholdes om nødvendige kryptografiske nøkler ikke er tilgjengelige og sendes når kryptering er mulig etc. Videre kan mottakere av meldinger benytte bekreftelsesmeldinger, også kjent som `ACK`, for å indikere avsenderen at meldingen ikke ble blokkert underveis. Integriteten av slike bekreftelsesmeldinger må også kunne sjekkes. Nettverksnoder bør også aktivt kunne benytte *alarm-* og *hendelsesmeldinger* for å varsle sentralsystemet om sikkerhetsrelatert informasjon. E.g. utilgjengelige sikkerhetsmekanismer i nettverkslaget. Et IDPS for AMS kan tilby slike tjenester og bør derfor vurderes [58]. I 2010 publiserte Berthier, Sanders og Khurana en rapport hvor de presiserte viktigheten av samt et forslag til et IDS for AMI [49].

7.5 Overblikk

Et overblikk over sikkerhetsarkitekturen for AMS-kanalen er vist i figur 7.5 og 7.7. Figur 7.5 viser kommunikasjonsprofilen samt hvilke sikkerhetstjenester som er implementert i

[12] Prolog i ROSS-magasinet som ble utgitt i sammenheng med Sikkerhetsdagene 2011 `www.sikkerhetsdagene.no`.

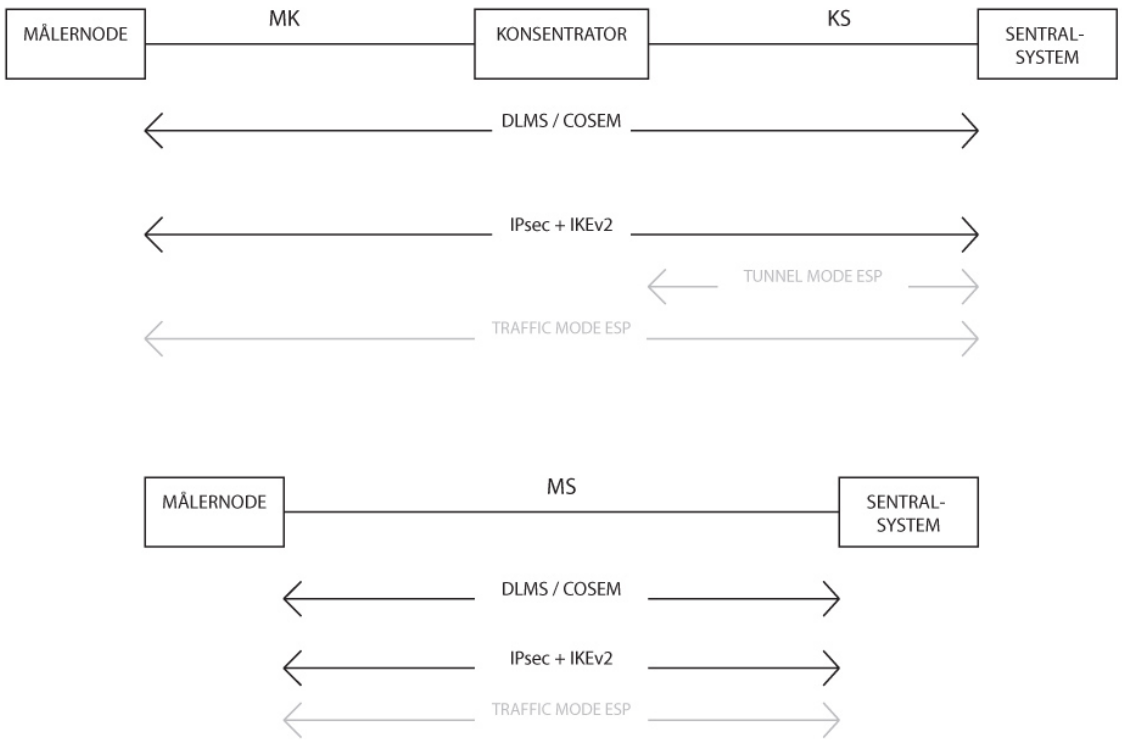
[13] Kapittel 6 diskuterte konsekvenser ved bortfall/hindring av enkelte tjenester i AMS



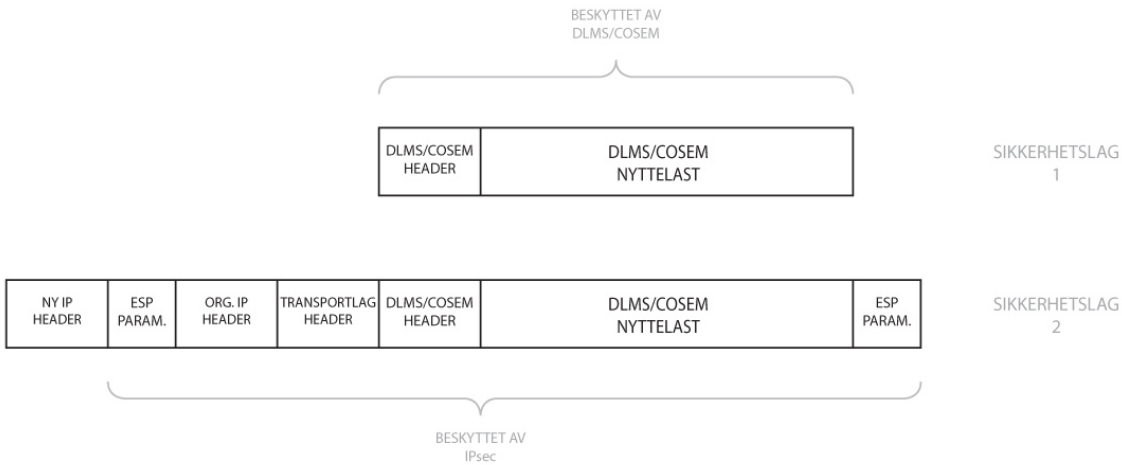
Figur 7.5: To lag av sikkerhet vist i kommunikasjonsprofil

hvert lag. Applikasjonslagsprotokollen DLMS/COSEM står for *sikkerhetslag 1* og utfører autentisering, dataintegritet og datakonfidensialitet av trafikk mellom applikasjonslagprosser. IPsec i nettverkslaget utgjør *sikkerhetslag 2* og utfører gjennom ESP sikkerhetsassosiasjoner autentisering, integritet og konfidensialitet av trafikk på nettverkslagsnivå. Det skal understrekes at det varierer ut ifra konfigurasjon av både *sikkerhetslag 1* og *2* hvilen type meldinger, samt hvilke deler av meldinger, som beskyttes av hvilke sikkerhetsmekanismer. Se seksjon 7.3 E.g. er DLMS/COSEM header integritetsbeskyttet men ikke kryptert og vil sendes åpent. Nummerering av sikkerhetslagene gjort ut ifra i hvilken rekke følge de er utført på data som sendes. I.e. betyr dette at om et angrep skal bryte konfidensialiteten for kommunikasjon mellom to kommuniserende noder må kryptering i sikkerhetslag *2* først brytes for deretter i lag *1*.

Figur 7.6 viser noen konfigurasjoner av sikkerhetslagene for de forskjellige linkene i den generiske AMS-arkitekturen. DLMS/COSEM kan skape sikre ende-til-ende forbindelser på applikasjonslaget mellom alle nettverksnodene i AMS-nettverket, både direkte og indirekte via konsentratorløsninger. IPsec kan også skape sikre ende-til-ende forbindelser i nettverkslaget, både for direkte og indirekte konsentratorløsninger. For løsninger med konsentrator kan KS-linkene konfigureres med ESP sikkerhetsassosiasjoner i tunnelmodus. På en slik måte kan ESP sikkerhetsassosiasjoner i trafikkmodus sendes gjennom denne tunnelen på KS-linken og skape sikre ende-til-ende forbindelser mellom målernodene og sentralsystemet. Figur 7.7 viser effekten denne konfigureringen har på datapakkene i nettverkslaget for KS-linkene. Figuren viser hvordan en IPv4 pakke ville bli beskyttet av begge sikkerhetslagene, samt hvordan en IPsec sikkerhetsassosiasjon i tunnel-modus vil beskytte hele IP-pakken over KS-linken ved å kapsle pakkene inn i en ny IP-pakke. For IPv6 er prinsippet likt, men andre felter av IP-pakken er beskyttet. For spesifikasjoner på bruk av IPsec i IPv6 henvises det til Stallings [82]. For IPsec benyttes IKEv2 for automatisert nøkkelutveksling og administrasjon av sikkerhetsassosiasjoner i nettverkslaget. Dette gjør at sikre forbindelser mellom nettverksnoder i AMS-nettverket blir etablert tidlig og gir DLMS/COSEM, i sikkerhetslag 1, sikre omgivelser for innledende oppsett og administrering for sikre forbindelser i applikasjonslaget.



Figur 7.6: Sikkerhetsarkitekturen og linker i den generiske arkitekturen



Figur 7.7: Sikker nettverkslagpakke over KS-linker med ESP i tunnelmodus

7.6 Vurdering av løsning

Av diskusjonen vedrørende valg av applikasjonslagsprotokoll i seksjon 5.2 må DLMS/COSEM anses på som et sikkert og framtidig alternativ for bruk innen AMS. OPENmeter støtter dette valget og anbefaler standarden for de fleste løsninger i sine dokumenter. Ettersom OPENmeter er det ledende initiativet for standardiseringsarbeid innen AMI og smarte nett i Europa, kan en for seg at DLMS/COSEM kommer til å bli et aktuelt valg for mange land i det europeiske kraftmarkedet. Standarden tilbyr en robust arkitektur som alene kan stille med sikkerhetsmekanismer for å muliggjøre sikker ende-til-ende kommunikasjon mellom nodene i AMS-nettverket. Krav om en fleksibel og framtidig kommunikasjonsløsning er oppfylt ved å benytte IP som nettverksprotokoll. Protokollen kan være et alternativ for en universell kommunikasjonsprotokoll for det framtidige smarte strømnettet, samt at den er kompatibel med en rekke underliggende kommunikasjonsløsninger og Internett. For IP kan overgangen fra IPv4 til IPv6 kan i følge Miao og Chen deles opp i 4 fem faser; migrasjonsfasen, transisjonsfasen, integratjonsfasen, sammenkjøring- og kompatibilitetsfasen og fasen hvor begge versjonene eksistere parallelt [67]. For AMS må alle disse fasene bli håndtert ved framtidig migrasjon fra IPv4 til IPv6 noe som kan skape utfordringer.

Til tross for all datatrafikk mellom applikasjonslagsprossesene i DLSM/COSEM ikke er kryptert, blir dette håndtert av IPsec i nettverkslaget. IPsec integreres i nettverkslaget og kan alene tilby nødvendige sikkerhetsmekanismer for å etabler sikre ende-til-ende forbindelser mellom noden i AMS-nettverket. Ved å benytte ESP i tunnel-modus over KS-linker vil ikke bare nyttelasten være kryptert, men også header informasjon. Ved slikt oppsett vil også løsningen gi konfidensialitet for ruting informasjon og hindrer former for angrep e.g. trafikkanalyse.

En sikkerhetsarkitektur med to sikkerhetslag gir mange fordeler. Bortfall eller angrep mot sikkerhetsmekanismer i ett lag vil dermed ikke gi direkte sikkerhetsbrudd da det andre sikkerhetslaget fortsatt vil beskytte trafikken. Men for at et slikt forsvar i dybden skal være effektivt må implementeringen være korrekt. At sikkerhetslag 1 og 2 implementeres respektivt i applikasjonslaget og nettverkslaget skaper en viss uavhengighet mellom lagene. Denne uavhengigheten må også gjennomføres på andre vis, e.g. ved at disse ikke benytter felles resurser som nøkkelservere etc. Om det eksisterer noen former for avhengighet vil en feil kunne få konsekvenser for begge disse lagene. Om slike situasjoner oppstår vil denne løsningen kunne reagere ved å innrette funksjonalitet etter situasjonen som har oppstått. Slik funksjonalitet er også med å begrense risiko ved å minimere sannsynligheten for angrep på trafikk med store konsekvenser.

Fleksibiliteten til underliggende kommunikasjonsteknologier ved bruk av IP gjør også at kommunikasjonsprofilen skal kunne være kompatibel og benyttes mot de aller fleste sluttbrukere i Norge. Valget av hvilken kommunikasjonsnett og teknologi som blir benyttet i de ulike tilfeller er avhengig av nettverkstopologien og geografien i området som AMS skal implementeres. Kommunikasjonsprofilen tillater både radio- og kabel løsninger hvor infrastruktur for telekommunikasjon vil være det dominerende valget. Tabell[14] 7.1 viser de mest akutelle alternativene for Norge.

For radioløsningene kan man anta at tilgangen til de forskjellige nettene vil variere og forandre seg med tid ettersom nye teknologier blir etablert og erstatter eldre standarder.

[14]CDMA 450, også kjent som ICE.net, er i Norge implementert over det gamle NMT nettet.

Kabel	Fiber (FTTx), xDSL
Radio	GSM/GPRS, UMTS/HSPA, LTE, CDMA 450

Tabell 7.1: Aktuelle kommunikasjonsnett for AMS i Norge

Derimot er det liten sannsynlighet for at framtidige telekommunikasjonsnett ikke vil støtte en kommunikasjonsprofil basert på IP og være koblet mot Internett.

For de tilfeller hvor kabelbaserte løsninger er tilgjengelig vil fiber være et framtidsrettet valg med hensyn til responstid og overføringskapasitet i smarte nett [90]. En stor fordel vil være for nettselskaper som har bygget ut fiber i sine regioner og kan benytte FTTH som kommunikasjonsnett i AMS. Ved hensyn til varierende kostnader og pålitlighetsproblemer ved bruk av tredjepartsleverandør for kommunikasjonsnett er det ennå usikkert hvilke løsninger som vil bli de dominerende innen AMS i Norge.

I tilfeller hvor alternativene nevnt over ikke er tilgjengelige er PLC eller andre radio-/kabel løsninger et alternativ siste link mot sluttbruker. Om IP kan støttes over slike teknologier varierer, men alternativer eksisterer e.g. PLC G3 beskrevet i seksjon 5.3.1.2. Om IP/IPsec over slike linker ikke er mulig bør andre kommunikasjonsteknologier med sikkerhetsmekanismer vurderes, e.g. radio/kabelbasert M-Bus. Uansett teknologi vil applikasjonsprotokollen DLMS/COSEM kunne skape sikre ende-til-ende forbindelser mellom målernoden og sentralsystemet. Dette vil kun føre til ett sikkerhetslag, og det anbefales i de enkelte tilfeller å vurdere konsekvensene slike valg medfører. Alternativt kan tiltak som redusert funksjonalitet gjennomføres e.g. ved å gi det aktuelle målepunktet dispensasjon for krav om mottak av styringssignaler etc.

Om sikkerhetsarkitekturen beskrevet i dette kapittelet implementeres etter de kriterier som er satt kan en anta at sannsynligheten for suksessfulle angrep mot trafikk i AMS-kanalen er redusert. Løsningen tilbyr muligheter for og oppfyller alle krav til sikkerhetstjenester diskutert i seksjon 6.7. Løsningen oppfyller også nasjonale krav til informasjonssikkerhet i AMS-kanalen. Dette er basert på tolkning av NVEs krav og tilhørende definisjon av nødvendige sikkerhetstjenester i seksjon 6.1. Selv om konsekvensene ved angrep vil forbli uendret vil man ved å benytte seg av disse sikkerhetsmekanismer senke sannsynligheten for suksessfulle angrep og dermed redusere den totale risikoen ved kommunikasjon i AMS-kanalen.

Kapittel 8

Konklusjon

Risikoen ved innføring av AMS i kraftsektoren er stor med hensyn til komplekse og omfattende konsekvenser ved eventuelle angrep. Økt integrering av IKT i kraftsektoren fører til gjensidig avhengighet mellom samfunnets mest vitale infrastrukturer; kraftforsyning og telekommunikasjon. I år 2000 omtalte Sårbarhetsutvalget i sin utredning at forhold som bidro til at dagens samfunn stadig sto ovenfor nye sikkerhetsutfordringer var blant annet teknologisk utvikling, økt kompleksitet, effektiviseringspress og elektroniske trusler. Sårbarhetsutvalget vurderte også kraftforskyningen og informasjons- og kommunikasjonsteknologi som de mest aktuelle tema for vurderingen av forhold som truet de grunnleggende samfunnsverdiene. I utredningen ble det presisert at økende bruk av IKT i kraftsektoren, i form av kontroll- og styringssytemer for effektivisering og sentralisert drift av kraftnettet, førte til nye typer sårbarheter for samfunnet da det måtte ses på som "en sammenkobling av driftssystemene for kraftforsyningen og verden for øvrig".

Selv om vurderingene Sårbarhetsutvalget gjorde på slutten av 90-tallet ikke ble basert på innføring av AMS er karakteristikken for sårbarhetene like. Effektivisering og optimalisering av kraftproduksjon og distribusjon gjøres mulig gjennom AMS ved bruk av ny teknologi. Dette fører til økt kompleksitet og økt gjensidig avhengighet mellom infrastruktur for kraftforsyning og telekommunikasjon. AMS vil samtidig også drastisk øke angrepsoverflaten for begge infrastrukturene i en tid hvor antallet og nye typer elektroniske trusler stadig øker. Basert på statistikk over SCADA- og Internettrelaterte angrep de siste tiår kan en anta at trusselbildet for IKT systemer vil fortsette å øke. Dette er grunnet økning i angrepsoverflate gjennom bruk av IKT i nye kontekster, utfordringer for sikkerhetsarbeid som resultat av økt kompleksitet, samt at utvikling av nye verktøy gjør terskelen for å utføre angrep lavere.

I følge sikkerhetsindustrien er det ikke et spørsmål *om* AMS vil bli utsatt for angrep, men et spørsmål om *når* samt at alle komponenter vil være sårbare i varierende grad. Ved at AMS tilgjengeliggjør detaljopplysninger om kraftforbruk og muligheten til monitorering av aktivitet ved målepunkt, kan informasjonen AMS innhenter ha nytteverdi for mange ulike aktører, ikke kun innen kraftsektoren. Ettersom data innhentet gjennom AMS kan knyttes til privatpersoner, og er beskyttet av personopplysningsloven, er bruken av slik informasjon innhentet gjennom ulovelig angrep begrenset. Derfor anses kriminelle og aktive angripere som de mest sannsynlige truslene som kan nyttegjøre angrep mot AMS. Dette grunnes også med at kompetanse innen IKT- og AMS-systemer vil varierer for de

forskjellige klassene av trusler, hvor de nevnte gruppe ses på som mest sannsynlige til å ha tilstrekkelige resurser for utførelse av angrep. AMS vil stå ovenfor mange av de samme angrepene og sikkerhetsutfordringene som andre distribuerte datasystemer. Store sikkerhetsutfordringer for AMS vil være nydesignet utstyr og komplekse systemer med kortlevetid i industrien hvor svakheter med tanke på informasjonssikkerhet kan eksistere. Spesielt vil utfordringene være store for utstyr som har høy grad av fysisk eksponering og lav grad av fysisk sikring mot mulige trusler, e.g. smartmålere og komponenter i kommunikasjonsnettet. Fysisk eksponering øker tilgjengeligheten for å utnytte svakheter i sikkerheten, både for uetiske aktører og aktive angripere.

Konsekvensene ved eventuelle angrep mot AMS kan være store og er avhengig av hvilke funksjoner som angripes. Ettersom all funksjonalitet i AMS baserer seg på kommunikasjon mellom sluttbrukere og nettselskapet, over et kommunikasjonsnett med stor angrepsoverflate, kan en anta at sannsynligheten for angrep mot nettet er stor. Konsekvensene mot data og signaler sendt i nettet gir både direkte og indirekte konsekvenser som avhenger av kompleksiteten av trafikken som sendes. Angrep mot målerverdier har kun direkte og isolerte konsekvenser da de involverer kun en sluttbruker og ikke iverksetter noen form for prosess ved mottak hos sentralsystemet. Kompleksitet og muligheter for distribusjon av konfigurasjonskommandoer og styringssignaler til flere sluttbrukere samtidig gjør at angrep mot slik trafikk kan gi indirekte konsekvenser og er mer omfattende. Økt kompleksitet kommer av automatiserte prosesser som iverksettes hos mottakeren som kan gi indirekte konsekvenser og ringvirkninger. Analysene i denne oppgaven viser at angrep mot stryingssignaler, i enkelte tilfeller kan gi samfunsmessige konsekvenser gjennom kaskadeeffekter som fører til ustabilitet og sammenbrudd av hele kraftnettet. Variasjon av konsekvenser for forskjellige angrep viser at integritet og tilgjengelighet av trafikk er essensielt for at automatiserte prosesser i AMS skal kunne operere på korrekt grunnlag. Dette gjelder alle trafikklasser i AMS. Konfidensialitet av trafikk er relevant med hensyn til personvern og overvåkning og bør derfor også prioriteres.

I Norge er nettselskaper pålagt å installere AMS for alle sine målepunkter innen 1.januar 2017 etter krav fra NVE. Med hensyn til risikoen ved innføring av AMS står nettselskapene ovenfor store sikkerhetsmessige utfordringer. Da AMS gir nettselskapene store fordeler for administrering av kraftdistribusjon må de ta høyde for risikoen ved å sikre systemene tilstrekkelig. Risikoen sluttbrukere blir utsatt for er avhengig av sikkerheten det lokale nettselskapet kan tilby. Ettersom nettselskapene har monopol på nett og distribusjon i sine områder har sluttbrukere ingen alternativer om nettselskapene ikke tilbyr tilstrekkelig sikring av AMS. Samtidig vil sikring av AMS føre til økte utgifter og må ses i sammenheng med tilgjengelige resurser for nettselskapene. I Norge er det 130 nettselskaper og antall sluttbrukere per nettselskap varierer fra under 1000 til flere 100.000. En må da anta at det vil eksistere en avhengighet mellom tilgjengelige resurser for sikring og nivå av sikkerhet i AMS for de forskjellige nettselskapene. Mindre nettselskaper med lite resurser tilgjengelig kan dermed forårsake samfunnsmessig risiko da angrep mot AMS i ett nettselskap kan få ringvirkninger for hele kraftnettet. Etter krav fra NVE skal kommunikasjon i AMS være sikret om nettene som skal benyttes ikke kan ses på som lukkede og kun benyttes for AMS. Det antas at AMS vil benytte eksisterende infrastruktur for kommunikasjon mellom sluttbruker og nettselskap ettersom utbyggingen av et dedikert kommunikasjonsnett for AMS vil involvere store kostnader. Vurdringene i denne oppgaven viser at ingen

av de aktuelle kommunikasjonsnettene for AMS er lukkede og det ble derfor presentert en løsning hvor sikkerheten i nettet blir håndtert internt av AMS. Gjennom bruk av sikkerhetsmekanismer kan man redusere risikoen ved innføring av AMS gjennom å redusere sannsynligheten for suksessfulle angrep. Sikkerhetsarkitekturen er basert på forsvar i dybden og implementerer to uavhengige lag ende-til-ende sikkerhet. Ved at hvert av disse sikkerhetslagene alene tilbyr nødvendige sikkerhetsmekanismer for å gi akseptabelt nivå av sikkerhet, vil kommunikasjonen fortsatt vil være beskyttet om ett av lagene brytes. Ved å benytte ende-til-ende sikkerhet vil også informasjonen tilgjengelig i transitt minimeres da ingen ledd mellom målernoden og sentralsystemet har innsyn i hva som sendes. Et sikkerhetslag håndteres av applikasjonslagprotokollen DLMS/COSEM og sikkerhetslag to håndteres av IPsec i nettverkslaget. Begge disse protokollene er etablerte standarder hvor deres robusthet er bevist gjennom utbredt bruk i industrien. Sikkerhetsarkitekturen implementerer mekanismer som kan tilby integritet og konfidensialitet av trafikk på begge lag samt oppfordring om implementering av reaktive tiltak som begrenser AMS-funksjonalitet ved redusert sikkerhet. Ettersom angrep mot integriteten av trafikken i AMS er vurdert til å ha store konsekvenser kan e.g. styringssignaler ignoreres av mottaker om integriteten av signalet ikke kan garanteres. Dette følger også prinsippet Sårbarhetsutvalget presiserer hvor en blir nødt til å inngå kompromisser mellom funksjonalitet og sikkerhet. Ved å forutsette korrekt og sikker implementering i forhold til standarder kan denne løsningen tilby et akseptabelt nivå av sikkerhet for AMS-kanalen. Ved at løsningen kan benyttes over et stort antall kommunikasjonsteknologier anser vi at den kan være aktuell mot størsteparten av sluttbrukere i Norge. Løsningen oppfyller også nasjonale krav til informasjonssikkerhet i AMS samt anbefalinger på grunnlav av vurderingene gjort i denne oppgaven. Av alle protokollene som ble vurdert ser en at mange standarder setter begrensning for underliggende kommunikasjonsnett samt gir få muligheter for framtidige utvidelser. Kommunikasjonsprofilen for sikkerhetsarkitekturen ble derfor valgt på grunnlag av fleksibilitet mellom protokollagene samt å minimere avhengighet til underliggende kommunikasjonsnett . Ved å benytte IP kan sikkerhetsarkitekturen i de fleste tilfeller kommunisere på tvers av nett som må ses på som heterogene og vil være en framtidig løsning. For å muliggjøre utvidelser og minimere begrensninger vil det være essensielt å også ta høyde for framtidige behov da AMS vil være fundamentet for smarte strømnett. I følge mange aktører i telekommunikasjonsindustrien er det stor sannsynlighet for at kommunikasjon i det smarte strømnettet vil være basert på IPv6. Ved integrering og krav om bruk av IPsec oppfyller protokollen behovet for universell og sikker kommunikasjon på tvers av forskjellige kommunikasjonsnett.

I smarte strømnett vil den gjensidige avhengigheten mellom kraftforsyning og IKT ytterligere økes hvor behovet for sikker kommunikasjon mellom alle de involverte komponentene vil være kritisk. Et smart strømnett vil skape et nytt økosystem som vil ha innvirkning på alle aktørene i samfunnet. Det er derfor mange forskjellige motivasjoner for realiseringen av et slikt smart strømnett, ikke kun effektivisering av kraftdistribusjon. Det må derfor i tiden framover vurderes om nettselskapene alene skal stå ansvarlig for sikkerheten i AMS da nettet også vil benyttes til andre formål. Ved innføringen av AMS er det essensielt at nettselskapene er klare over risikoen et slikt system medfører, spesielt om informasjonssikkerheten ikke er håndtert korrekt. Sikring av AMS involverer informasjonssikkerhet på forskjellige plan, både teknisk og organisatorisk, som setter implisitte krav

til innhenting av nødvendig kompetanse. Den økende bruken av IKT i kraftsektoren fører til nye tverrfaglige problemstillinger hvor begge industriene må involveres for å kartlegge tette koblinger, sårbarheter og risiko som oppstår på tvers av disse fagområdene. Ettersom innføringen av AMS i enkelte tilfeller kan medføre samfunnsmessig risiko bør det være i samfunnets interesse å tilse at sikkerheten i AMS til en hver tid er på et akseptabelt nivå.

8.1 Videre arbeid

I kapittel 3 ble områder for informasjonssikkerhet innen AMS presentert. Denne oppgaven har kun studert et av underområdene; informasjonssikkerhet for kommunikasjonsteknologi i AMS-kanalen. Derfor vil videre arbeid innen sikring av AMS involvere alle områdene nevnt i kapittel 3. For andre underområder for kommunikasjon i AMS vil mange diskusjoner og analyser presentert i denne oppgaven være aktuelle.

Risiko ved innføring av AMS kan anses å være et produkt av sannsynligheten for angrep og konsekvensen av eventuelle suksessfulle angrep. Løsningen presentert i kapittel 7 reduserer den totale risikoen ved å senke sannsynligheten for angrep mot kommunikasjonen i AMS-kanalen. Ettersom løsningen kun reduserer sannsynligheten vil konsekvensene forbli uendret. Derfor vil arbeid for å redusere den totale risikoen ved AMS også inkludere tiltak for å redusere de eventuelle konsekvensene angrep mot informasjonssikkerheten. Diskusjon vedrørende angrep og konsekvenser ble presentert i seksjon 6.4.

Implementasjon og testing av den foreslåtte løsningen for sikker kommunikasjon i AMS-kanalen gjenstår. Implementasjon og testing vil kunne vise hvor stor reduksjon i sannsynlighet for angrep løsningen gir, samt andre ytelses parametre i forhold til utstyr og nivå av sikkerhet. Spesielt gjelder dette utvikling og testing av system for reaktiv funksjonalitet begrensning i forhold til sikkerhetsnivå i AMS-kanalen. Se seksjon 7.4.

NVE har pålagt at alle nettselskaper å utføre Risiko og Sårbarhet (ROS)-analyser av AMS. En slik analyse involverer dermed analyse av alle aspektene presentert i kapittel 3. Datatilsynet og Nasjonal sikkerhetsmyndighet har utviklet veiledere for ROS-analyser av IKT-systemer. Disse dokumentene bør danne grunnlaget for analysene nettselskapene gjør av AMS [79, 20].

Bibliografi

[1] 3rd Generation Partnership Project. *Specification Numbering*. http://www.3gpp.org/specification-numbering, [13.11.2011].

[2] 3rd Generation Partnership Project. *Technical Specification Group GSM/EDGE Radio Access Network; Feasibility study for evolved GSM/EDGE Radio Access Network (GERAN)*, v. 10.0.0, Mars 2011.

[3] 3rd Generation Partnership Project. *Technical Specification Group GSM/EDGE Radio Access Network; Overall description*, v. 10.0.0, Mars 2011.

[4] 3rd Generation Partnership Project. *Technical Specification Group Radio Access Network; Physical layer - General description*, v. 10.0.0, Mars 2011.

[5] 3rd Generation Partnership Project. *Technical Specification Group Radio Access Network; UTRAN overall description*, v. 10.2.0, Juni 2011.

[6] 3rd Generation Partnership Project. *Technical Specification Group Services and System Aspects; Network architecture*, v. 11.0.0, September 2011.

[7] 3rd Generation Partnership Project. *Technical Specification Group Services and System Aspects; Network architecture*, v. 11.0.0, Juni 2011.

[8] A. Ipakchi, F. Albuyeh. *Grid of the future*, journal, power and energy magazine, vol 7, nr 2, side 52 - 62, ieee, 24.Februar 2009.

[9] PRIME Alliance. *Draft Standard for PoweRline Intelligent Metering Evolution*, v. 1.3e, [u.å.]. http://www.prime-alliance.org/Docs/Ref/PRIME-Spec_v1%203%20E_201005.pdf.

[10] Radiocrafts AS. *RC1180-MBUS: Wireless M-Bus Multi-Mode RF Transceiver Module*, datablad, revisjon 1.4, radiocrafts as, 2008. http://www.radiocrafts.com/uploads/rc1180-mbus_data_sheet_1_4.pdf, [13.09.2011].

[11] DLMS User Association. *DLMS/COSEM Specification*. www.dlms.com/documentation/dlmscosemspecification/index.html, [13.11.2011].

[12] DLMS User Association. *Who provides DLMS/COSEM metering systems?* http://www.dlms.com/faqanswers/generalquestions/whoprovidesdlmscosemmeteringsystems.php, [13.01.2012].

[13] DLMS User Association. *EXCERPT FROM - DLMS UA 1000-2 - Architecture and Protocols*, versjon 7.05, 22.Desember 2009.

[14] L. Ekeberg, I. Bruvik. *Svar på høring om forslag om lov om endringer i industrikonsesjonsloven og vassdragsreguleringsloven*, rapport, fornyings- og administrasjonsdepartementet, 21.April 2008. `http://bit.ly/aW3Vjn`, [27.11.2011].

[15] K. Wansink, P. Budde. *2010 Global - Key Telecoms, Mobile and Broadband Statistics*, utgave 7, rapport, August 2010. Referanse til eksklusivt sammendrag da full rapport ikke ble innhentet, `https://www.budde.com.au/Research/2010-Global-Key-Telecoms-Mobile-and-Broadband-Statistics.html?r=51`, [13.01.2012].

[16] Computer Emergency Response Team Coordination Center. *CERT Statistics (Historical)*, oppdatert 12.02.2009. `http://www.cert.org/stats/`, [13.11.2011].

[17] Inc. Cisco Systems. *Internet protocol Architecture for the Smart Grid*, rapport, 9. Juli 2009. `http://www.smartgridnews.com/artman/uploads/1/CISCO_IP_INTEROP_STDS_PPR_TO_NIST_WP.pdf`, [13.01.2012].

[18] Symantec Corporation. *Vulnerability Trends - SCADA vulnerabilities*, nettsted, [u.å.]. `http://www.symantec.com/business/threatreport/topic.jsp?id=vulnerability_trends&aid=scada_vulnerabilities`, [12.01.2012].

[19] Common Criteria. *The Common Criteria Recognition Arrangement*, nettsted. `http://www.commoncriteriaportal.org/ccra/`, [27.01.2012].

[20] Datatilsynet. *Risikovudering av informasjonssystem*, veileder, 15.Februar 2002.

[21] Datatilsynet. *Veileder i sikkerhetsarkitektur- For virksomheter som behandler personopplysninger og sensitive personopplysninger*, veileder, August 2006.

[22] Datatilsynet. *Guide for processing of personal data in connection with automatic metering systems within the energy sector*, veileder„ [u.m.] 2010. `http://bit.ly/xhfZzt`, [24.01.2012].

[23] M. Davis. *SmartGrid Device Security: Adventures in a new medium*, webcast, ioactive, 21.06.2011. `http://www.brighttalk.com/webcast/170/4127`, [13.11.2011].

[24] G. Deconinck. *An evaluation of two-way communication means for advanced metering in Flanders (Belgium)*, rapport,Instrumentation and Measurement Technology Conference Proceedings, 2008. IMTC 2008. IEEE, side 900-905, 20.Juni 2008.

[25] K. D. Craemer, G. Deconinck. *Analysis of State-of-the-art Smart Metering Communication Standards*, Mars 2010.

[26] ISO 27000 Directory. *The ISO 27000 Directory- An Introduction to ISO 27001, ISO 27002....ISO 27008*, nettsted. `http://www.27000.org/`, [27.01.2012].

[27] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen. *RFC 5996 - Internet Key Exchange Protocol Version 2 (IKEv2)*, rfc, September 2010. `http://tools.ietf.org/html/rfc5996`, [13.01.2012].

[28] E. Bruun, R. Mangelrød, R. K. Mork, et al. *Funksjonskrav i kraftsystemet (Veileder for funksjonskrav i kraftsystemet i Norge)*, statnett, nist, 28.April 2008.

[29] J. Arkko , G. Kuijpers et al. *RFC 3316 - IPv6 for Some 2G and 3G Cellular Hosts*, rfc, April 2003. `http://tools.ietf.org/html/rfc3316`, [13.11.2011].

[30] S. Daniel Park , K. Kim et al. *IPv6 over Low Power WPAN Security Analysis*, 22. Juni 2006. `http://tools.ietf.org/html/draft-daniel-6lowpan-security-analysis-01`, [13.11.2011].

[31] S. Raza , S. Duquennoy et al. *Securing Communication in 6LoWPAN with Compressed IPsec*, 12.August 2011.

[32] V.C Gungor, D. Sahin, T. Kocak, et al. *Smart Grid Technologies: Communication Technologies and Standards*, journal, industrial informatics, ieee transactions, vol 7, nr 4, 529 -539, 7.November 2011.

[33] G. Stoneburner, C. Hayden, A. Feringa. *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, revisjon a, nist, Juni 2004.

[34] The National Association for Amateur Radio. *FCC Notice of Proposed Rulemaking on Carrier-Current Devices, Including BPL*. `http://p1k.arrl.org/~ehare/bpl/NPRM_hyperlinks.html#Reports`, [13.11.2011].

[35] Électricité Réseau Distribution France. *PLC G3 MAC Layer specification*, [u.å.]. `http://www.maxim-ic.com/products/powerline/pdfs/G3-PLC-MAC-Layer-Specification.pdf`.

[36] Électricité Réseau Distribution France. *PLC G3 Physical Layer Specification*, [u.å.]. `http://www.maxim-ic.com/products/powerline/pdfs/G3-PLC-Physical-Layer-Specification.pdf`.

[37] M. LeMay , G. Gross , C. A. Gunter , S. Garg. *Unified Architecture for Large-Scale Attested Metering*, hawaiian international conference on system sciences„ Januar 2007.

[38] O. S. Grande, H. Sæle, I. Graabak. *Market based demand response research prjoject summary*, rapport, sintef energiforskning as, 31.Desember 2008.

[39] NIST Computer Security Division Security Technology Group. *Cryptographic Toolkit*, veileder, national institute of standards and technology. `http://csrc.nist.gov/groups/ST/toolkit/index.html`, [13.01.2012].

[40] The Smart Grid Interoperability Panel - Cyber Security Working Group. *NISTIR 7628:Guidelines for Smart Grid Cyber Security - Vol. 3, Supportive Analyses and References*, nist, v. 3, August 2010.

[41] H. Christian. *Vurdering av kommunikasjonsalternativer for informasjonsutveksling med AMS mellom smarte hus og et smart kraftnett*, NTNU, institutt for telematikk, Juni 2010.

[42] T.J. Hammons. *Integrating Renewable Energy Sources into European Grids*, artikkel, Universities Power Engineering Conference, 2006. UPEC '06. Proceedings of the 41st International, vol 1, 142 -151, 4.Juni 2007.

[43] M. R. Kleveland, B. I. Sigurdarson, Ø. H. Snefjellå, P. A. Strøm, K. Haugene. *Lastutkobling i Smarte Hjem- Hvordan integrere variabel kraftproduksjon ved hjelp av lastutkobling i hjemmet?*, prosjektrapport, eksperter i team, ntnu, Mai 2010. `http://folk.ntnu.no/pettestr/Prosjektrapport_m_vedlegg.pdf`, [27.11.2011].

[44] LonMark International. *Layer 1-6 : Interoperability Guidelines*, v. 3.4, September 2005.

[45] LonMark International. *Introduction to the LonWorks Platform*, rev.2.0, 2009.

[46] INTERSECTION. *Project Detail- Concept and project objective(s)*, nettsted, samarbeidsprosjekt iverksatt av europakommisjonen (underligger program for secure, dependable and trusted infrastructures), [u.å]. `http://www.intersection-project.eu/project-detail`, [08.01.2012].

[47] T. Jonassen. *Utkoblbar overføring og andre aktuelle tariffsaker*, presentasjon, nve, næringspolitisk verksted tariffer og anleggsbidrag i distribusjonsnettet, 31.Mai 2011. `http://www.energinorge.no/nett/naeringspolitisk-verksted-tariffer-og-anleggsbidrag-i-distribusjonsnettet-article8237-244.html`, [13.09.2011].

[48] E. Barkan, E. Biham, N. Keller. *Instant Ciphertext-Only Cryptanalysis of GSM encrypted communication)*, August 2003.

[49] R. Berthier, W. H. Sanders, H. Khurana. *Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions*, rapport, smart grid communications (smartgridcomm), 2010 first ieee international conference on, side 350 - 355, 4. November 2010.

[50] K. Eikland, H. E. Budde, K. Kleppe. *Nettselskapets rolle i det fremtidige norske kraftmarkedet med AMS-infrastruktur*, versjon 1.01, rapport, avenir as, 17.Februar 2010.

[51] Győző Kmethy. *DLMS/COSEM over PLC : Security of meter data exchange over open networks*, presentasjon, metering europe, vienna, 2.Oktober 2007. `http://www.dlms.com/downloads/dlmscosemoverplcviennagk070921.pdf`, [13.01.2012].

[52] B.W. Kwon. *Broadband over Power Lines (BPL): Developments and Policy Issues*, rapport, organisation for economic co-operation and development, 4.Juni 2009. `http://www.oecd.org/dataoecd/58/62/43230875.pdf`, [13.01.2012].

[53] H. Lancaster, P. Kwon. *European Fixed Broadband and Internet Market*, utgave 6, rapport, September 2010. Referanse til eksklusivt sammendrag da full rapport ikke ble innhentet, `https://www.budde.com.au/Research/European-Fixed-Broadband-and-Internet-Market.html`, [13.01.2012].

[54] E. Hollnagel, D. D. Woods, N. Leveson. *Resilience Engineering: Concepts and Precepts*, ashgate publishing group, September 2006.

[55] M. Lobashov. *End-to-End Communication Architecture for Smart Grids*, rapport, ieee transactions on industrial electronics, vol 58, no. 4, April 2011. Referanse til eksklusivt sammendrag da full rapport ikke ble innhentet, `https://www.budde.com.au/Research/European-Fixed-Broadband-and-Internet-Market.html`, [13.01.2012].

[56] V. Manral. *RFC 4835 - Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*, rfc, April 2007. `http://tools.ietf.org/html/rfc4835`, [13.01.2012].

[57] J. McNabb. *Vulnerabilities og Wireless Watermeter Networks* black hat usa las vegas, 3.August 2011.

[58] K. Scarfone, P. Mell. *NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)*, Februar 2007. `http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf`, [12.01.2012].

[59] D. Driscoll, A. Mensch. *Devices Profile for Web Services Version 1.1*, offentlig beskrivelses utkast versjon 1, 27.Januar 2009. `http://docs.oasis-open.org/ws-dd/dpws/1.1/pr-01/wsdd-dpws-1.1-spec-pr-01.html`, [13.09.2011].

[60] The OPEN meter Consortium. *D1.1: Report on the identification and specification of functional, technical, economical and general requirements of advanced multi-metering infrastructure, including security requirements*, v. 1.0, Juli 2009.

[61] The OPEN meter Consortium. *D2.1: General overview of state-of-the-art technological alternatives*, part 1, v. 3.0, Juni 2009.

[62] The OPEN meter Consortium. *D2.1: General overview of state-of-the-art technological alternatives*, part 4, v. 1.0, Juni 2009.

[63] The OPEN meter Consortium. *D2.3: Identification of research needs from bottom-up approach*, v. 1.0, 3.November 2009.

[64] The OPEN meter Consortium. *D3.1: Design of the overall system architecture - Amendment*, v. 1.3, Desember 2010.

[65] The OPEN meter Consortium. *D3.1: Design of the overall system architecture*, v. 1.1, Februar 2010.

[66] The OPEN meter Consortium. *D3.2: Specification of OPEN meter OSI layers and multimetering networking interfaces*, v. 2.0, Juni 2011.

[67] X. Miao, and X. Chen. *Research on IPv6 Transition Evolvement and Security Architecture of Smart Distribution Grid Data Communication System*, rapport, electricity distribution (ciced), 2010 china international conference on, side 1 - 5, 22. Mars 2010.

[68] JD (Justis og beredskapsdepartementet). *LOV-2000-04-14-31: Lov om behandling av personopplysninger (personopplysningsloven).* `http://www.lovdata.no/all/nl-20000414-031.html`, [27.11.2011].

[69] Olje og energidepartementet. *LOV-1990-06-29-50: Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven).* `http://www.lovdata.no/all/nl-19900629-050.html`, [27.11.2011].

[70] Redaktører: E. Albrechtsen og J. Hovden. *Sikkerhet må skapes og gjenskapes hver dag. Det finnes ingen endelige løsninger*, magasin, ross-magasinet: Sikkerhet må skapes og gjenskapes hver dag. det finnes ingen endelige løsninger, sikkerhetsdagene 2011, 2011. `http://www.sikkerhetsdagene.no/_media/rosspubl_web.pdf`, [13.01.2012].

[71] Maxim Integrated Products. *Supplement to PLC G3 physical layer specification for operation in CENELEC B/C/BC/D/BCD/BD frequency bands*, [u.å.]. `http://www.maxim-ic.com/products/powerline/pdfs/G3-PLC-CENELEC-Supplement-B.pdf`.

[72] Horst Prof. Dr. Ziegler. *The M-Bus: A Documentation*, rev. 4.8, November 1997.

[73] J. Wang, L. Rong. *Cascade-based attack vulnerability on the US power grid*, Desember 2009. artikkel i Safety Science, Vol 47, Nr 10, Side 1332 - 1336.

[74] I. Graabak , H. Sæle. *Kravspesifikasjon fullskala utbygging av Avanserte Måle og Styringssystemer (AMS)(toveiskommunikasjon)*, version 1.0, sintef energi as, September 2011.

[75] Sårbarhetsutvalget. *NOU 2000:24 - Et sårbart sammfunn*, (nou) norsk offentlig utredning, 4.Juli 2000.

[76] J. Schiller. *RFC 4307 - Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*, rfc, December 2005. `http://tools.ietf.org/html/rfc4307`, [13.01.2012].

[77] S. Kent, K. Seo. *RFC 4301 - Security Architecture for the Internet Protocol*, rfc, Desember 2005. `http://tools.ietf.org/html/rfc4301`, [13.01.2012].

[78] R. Shirey. *RFC 2828 - Internet Security Glossary*, rfc, Mai 2000. `http://www.ietf.org/rfc/rfc2828.txt`, [14.12.2011].

[79] Nasjonal sikkerhetsmyndighet. *Veiledning i risiko- og sårbarhetsanalyse*, veileder, 12.Mai 2011.

[80] IEEE Computer Society. *Part 15.4: Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Personal Area Networks*, September 2006.

[81] T. Kavitha , D. Sridharan. *Security Vulnerabilities In Wireless Sensor Networks: A Survey*, 2010.

[82] W. Stallings. *Cryptography and Network Security: Principles and Practices*, 4.utgave, 2006. Prentice Hall. ISBN: 0-13-202322-9.

[83] Norges vassdrags-og energidirektorat. *FOR 1999-03-11 nr 301: Forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester.* `http://www.lovdata.no/for/sf/oe/xe-19990311-0301.html`, [27.11.2011].

[84] Norges vassdrags-og energidirektorat. *FOR-2002-12-16-1606: Forskrift om beredskap i kraftforsyningen.* `http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20021216-1606.html`, [07.12.2011].

[85] Norges vassdrags-og energidirektorat. *Dokument 12: Avanserte måle- og styringssystem (AMS) -Forslag til endringer i forskrift 11. mars 1999 nr. 301*, Juni 2008.

[86] Norges vassdrags-og energidirektorat. *Dokument 12: Avanserte måle- og styringssystem (AMS) -Forslag til endringer i forskrift 11. mars 1999 nr. 301*, Juni 2009.

[87] Norges vassdrags-og energidirektorat. *Dokument 7: Avanserte måle- og styringssystemer -Oppsummering av høringsuttalelser og endelig Forskriftstekst*, Juni 2011.

[88] Norges vassdrags-og energidirektorat. *Veileder nr. 1-2011: Veiledning til forskrift om beredskap i kraftforsyningen*, Mars 2011.

[89] Ventelo. *Fakta om Ventelo.* `http://www.ventelo.no/konserninfo/`, [07.12.2011].

[90] A. Aggarwal, S. Kunta, P. K. Verma. *A Proposed Communications Infrastructure for the Smart Grid*, rapport, innovative smart grid technologies (isgt), side 1 -5, 22.Mars 2010.

[91] G. Štruklec, J. Maršić. *Implementing DLMS/COSEM in Smart Meters*, rapport, energy market (eem), 2011 8th international conference on the european, side 747 - 752, 22.Juli 2011.

[92] U. Meyer, S. Wetzel. *On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks*, 3.Januar 2005.

[93] M. Wisy. *SML - Smart Messaging Language*, versjon 1.02, spesifikasjon, emsycon gmbh, 19.Januar 2008.

[94] S. Woodhouse. *Information Security: End User Behavior and Corporate Culture*, 21.November 2007.

[95] M. Carpenter , J. Wright. *Advanced metering infrastructure attack methodology*, v. 1.0, 5.Januar 2009.

[96] C. Xenakis. *Security Measures and Weaknesses of the GPRS Security Architecture*, 8.November 2006.

Tillegg A

Grunn- og detaljkrav for AMS

Dette vedlegget er basert på dokumentet "Kravspesifikasjon fullskala utbygging av Avanserte Måle- og Styringssystemer (AMS) (toveiskommunikasjon) Versjon 1.0" [74]

Oversikt over grunnkrav og detaljkrav i kravspesifikasjon:
Kravspesifikasjon fullskala utbygging av Avanserte Måle- og Styringssystemer (AMS) (toveiskommunikasjon) Versjon 1.0

Ingeborg Graabak
Hanne Sæle

September 2011

Trafikklasser:

Målerverdier
Konfigurasjonskommando
Styringssignaler
Hendelser/alarm

Rettning (trafikk sendes fra) :

Fra sentralsystem
Fra målernode

Kan sendes til:

1	Én målernode
G	En gruppe målernoder
A	Alle målernoder

Grunn-krav	Detalj-krav	Relevant til IKT	Navn i kravspesifikasjon	Trafik-klasse	Spesifikasjon av trafikk	Rettning	Kan sendes til
0.1							
	1	Nei					
	3	Nei					
	4	Ja	Endre hyppighet på måleintervall	Konf. Kom.	Parameter på hyppighet for registrering av måleverdi	Fra sentralsys.	1,G,A
0.2							
	123	Ja	Tilgang på detaljert beskrivelse av grensesnitt i Innsamlingssys				
0.3							
	6	Nei	Vi tar hovedsakelig for oss AMS i kraft		Skaper ikke trafikk		
	7	Nei	--				
	123	Ja	Se 0.2				
0.4							
	8	Nei					
	125	Ja	Sikkerhet for å unngå at registrerte data mistes		Skaper ikke trafikk		

0.5										
	41	Ja	Sentralisert åpning og stenging av målepunkt	Styrings-signal	Signal om åpning/stegning	Fra sys	1,G			
	42	Nei								
	43	Nei								
	44	Ja	Sentralisert begrensning av uttak av effekt i det enkelte målepunktet	Styrings-signal	Parameter for å iverksette max effekt uttak per måler	Fra sys	1,G,A			
	45	Ja	Endring av grenser for maksimalt uttak av effekt i et anlegg	Konf.kom.	Parameter for max effekt uttak per måler	Fra sys	1,G,A			
	71	Ja	Krav til bryter							
0.6										
	48	Nei								
	49	Nei								
	50	Ja	Registrering av hendelse	Hendelse / alarm	Hendelsesalarm m forskjellige param: • Jordfeil, jfr. krav nr. 50. • Anlegg uten spenning • Lysbuedeteksjon • Dør åpen i nettstasjon • Vann i nettstasjon • Høy temperatur i komponent i kraftsystemet • Manglende olje i komponent i kraftsystemet	Fra måler	kan skje flere målere samtidig om miljøforandring			
	56	Ja	Routing av informasjon lokalt	Annen trafikk		Lokalt mellom måler og tilleggsustyr				
0.7										

	93	Ja	Håndtering av angrep og overvåkning av kritiske systemfunksjoner		Skaper ikke trafikk		
	126	Ja	Sikkerhet mot at utenforstående påvirker informasjonen i innsamlingsystemet		Skaper ikke trafikk		
	127	Nei					
	128	Ja	Alarm ved forsøk på datamanipulering		Alarm ved forsøk på datamanipulering	Fra måler	1
	129	Ja	Alarm ved innbruddsforsøk		Alarm ved forsøk på innbrudd i Målenode	Fra måler	1
0.8							
	67	Nei					
	68	Nei					
0.9							
	10	Ja	Automatisk overføring av måleverdier	Målerverdier		Fra målere, eller konsentrator	1, G, A
	11	Nei					
	12	Nei					
0.10							
	8	Nei					
	9	Ja	Krav til overføring	Målerverdier	Måledata	Fra måler	1
	10	Ja	Se 0.9				
0.11							
	8	Nei					
	9	Ja					
	10	ja					
0.12							
	54	Ja	Tilkobling av lokalt utstyr		Krav, ikke trafikk		

	55	Ja	Routing av informasjon til lokalt tilleggsutstyr fra sentralsystemet	Annen trafikk	Mellom sentral sys og lokalt utstyr, må klassifiseres mtp sikkerhetsnivå	Begge veier	1
	56	Ja	Se 0.6				
0.13							
	55	Ja	Ja				
	56	ja	Ja, se 0.12				
Tillegg							
	130	Ja	Fjernstyring av parametre	Konf.kom	Statiske parametre	Fra sys	NA
	131	Ja	Oppgradering av programvare i Målerterminal og kom.sys	Konf.kom	Firmware upd, patcher	Fra sys	1,G,A

Tillegg B

Oversikt over AMS protokoller

Dette vedlegget er hentet ut fra på dokumentet “State of the art technologies and protocols - Description of state of the art communication protocols and data structures” [62]

TILLEGG B. OVERSIKT OVER AMS PROTOKOLLER

Specification	Field of application					Data model	Communication media supported								Ref. para
	Local AMR	Remote AMR	AMI	Home automation			Local bus	PSTN	GSM	GPRS	Internet	PLC	Walk by radio	Mesh radio	
IEC 61334 PLC	-	Y	Y	-		Y	-		-	-	-	Y	-	-	6.1
IEC 62056-21"FLAG"	Y	Y	-	-		-	Y		Y	Y	-	-	-	-	6.2
IEC 62056-31 Euridis	Y	Y	-	-		-	Y		-	-	-	-	-	-	6.3
IEC 62056 DLMS/COSEM	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	-	6.4
EN 13757 M-Bus	Y	Y	Y	Y		-	Y		-	-	-	-	Y	-	6.5
SML	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	6.6
DIN 43863-4		Y	Y			Y		Y	Y	Y	Y				6.7
IEC 60870-5	Y	Y	-	-		-	-	-	-	-	-	-	-	-	6.8
IEC 61968-9	NA	NA	NA	NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	6.9
SITRED	Y	Y	Y	-								Y			6.10
PRIME	Y	Y	Y	-								Y			6.11
I IEC 61850							Y								6.12
KNX				Y			Y		Y	Y	Y	Y			6.13
Zigbee SmartEnergy			Y	Y										Y	6.14
6LoPAN														Y	6.15
Homeplug				Y								Y			6.16
Z-Wave														Y	6.17
Wavenis										Y				Y	6.18
EverBlu	Y	Y	Y	-						Y				Y	6.19
OPERA/UPA	-	Y	Y	-		-	-	-	-	-	Y	Y	-	-	6.20
ITU–G.hn	-	-	-	Y		-	-	-	-	-	Y	Y	-	-	6.21