SINTEF

SINTEF A24258 - Åpen

Rapport

Informasjonssikkerhet og personvern: Støtte til risikoanalyse av AMS og tilgrensende systemer

Forfattere
Maria Bartnes Line
Inger Anne Tøndel
Gorm Johansen
Hanne Sæle

SINTEF
2014-08-26

SINTEF IKT
Postadresse:
Postboks 4760 Sluppen
7465 Trondheim
Sentralbord: 73593000
Telefaks: 73594302
postmottak.IKT@sintef.no
www.sintef.no
Foretaksregister:
NO 948 007 029 MVA

Rapport

Informasjonssikkerhet og personvern: Støtte til risikoanalyse av AMS og tilgrensende systemer

EMNEORD:
Informasjonssikkerhet
Personvern
Risikoanalyse
Metode
Sjekklister
AMS
IKT

VERSJON
1.1

DATO
2014-08-26

FORFATTERE
Maria Bartnes Line
Inger Anne Tøndel
Gorm Johansen
Hanne Sæle

OPPDRAGSGIVER
DeVID-prosjektet

OPPDRAGSGIVERS REF.
Jan A. Foosnæs (NTE)

PROSJEKTNR
102002502

ANTALL SIDER:
56

SAMMENDRAG
Rapporten støtter gjennomføringen av en risikoanalyse av AMS og tilgrensende IT-systemer hos et nettselskap hvor fokus for analysen er informasjonssikkerhet og personvern. Den gir sjekklister og anbefalinger som nettselskapene kan bruke i sine egne risikoanalyser. SINTEF har valgt å bygge på en metode som mange nettselskap er kjent med fra før, og som anbefales benyttet av NVE og Energi Norge.

Målgruppen for denne rapporten er primært den som har ansvar for, eller skal delta i, en slik risikoanalyse hos et nettselskap. Det inkluderer også toppledelsen, da denne typen arbeid inngår i den helhetlige prosessen med risikostyring og -håndtering. Prioritering av tiltak må gjøres ut i fra forretningsbehov, teknologivalg og løsninger.

UTARBEIDET AV
Maria B. Line
SIGNATUR
Maria B. Line

KONTROLLERT AV
Tor Onshus
SIGNATUR

GODKJENT AV
Sture Holmstrøm, Forskningssjef
SIGNATUR
Sture Holmstrøm

RAPPORTNR	ISBN	GRADERING	GRADERING DENNE SIDE
SINTEF A24258	978-82-14-05363-0	Åpen	Åpen

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
0.1	2013-01-07	Utkast til arbeidsgruppe AG4
0.2	2013-03-08	Bearbeidet i etterkant av AG4-møte 29. jan 2013
1.0	2013-03-22	Første versjon
1.1	2014-08-26	Bearbeidet etter erfaring med bruk av versjon 1.0.

Sammendrag

Denne rapporten støtter gjennomføringen av en risikoanalyse av AMS og tilgrensende IT-systemer, der fokus for analysen er informasjonssikkerhet og personvern. Et nettselskap kan benytte ulike metoder for å gjøre risikoanalyser. Vi har i denne rapporten valgt å bygge på en metode som mange nettselskap er kjent med fra før, og som anbefales av NVE og Energi Norge [5].

I tillegg til sjekklister som nettselskapene kan benytte i sine egne risikoanalyser, gir denne rapporten anbefalinger som utdyper anbefalingene gitt i NVEs veiledning i risikoanalyse [5]. Anbefalingene kan oppsummeres som følger:

- Risikoanalysen bør gjennomføres som et prosjekt, med en prosjekteier og gitte rammer. Metoden som er beskrevet i NVEs veiledning, kan benyttes også når man har fokus på informasjonssikkerhet og personvern.
- I valg av prosessleder og i sammensetning av analysegruppa bør man ta hensyn til behovet for å fremme kreativitet og hindre begrensninger. Noen i gruppa må inneha kompetanse om informasjonssikkerhet og personvern.
- Før analysemøtet bør det foreligge oppdaterte systemskisser og en oversikt over eksisterende og planlagte tiltak. Deltagerne i analysen bør gis en felles forståelse av arbeidets omfang og avgrensning.
- Det bør settes av to arbeidsmøter til å gjennomføre selve analysen. Første møte brukes til å forstå både metoden og systemet, samt å identifisere informasjonsverdier og uønskede hendelser. I andre møte vurderes sannsynlighet og konsekvens, dessuten identifiseres mulige tiltak.
- Konsekvens- og sannsynlighetsdimensjoner må tilpasses den enkelte virksomhet. Det anbefales å vurdere gjenbruk av tidligere benyttede dimensjoner.
- Sjekklister bør benyttes av prosessleder for å sikre at vesentlige punkter ikke blir utelatt. Sjekklister må ikke brukes på en slik måte at de hemmer deltagernes kreativitet.
- Før man identifiserer trusler og uønskede hendelser, bør man identifisere hvilke informasjonsverdier som finnes i systemet. Det er informasjon som har verdi, ikke systemet i seg selv, og man må vite hva som skal beskyttes for å kunne bestemme passende sikkerhetsnivå og akseptabel restrisiko.
- Identifikasjon av informasjonsverdier gir økt systemforståelse og er et viktig underlag for videre analyse. For hver informasjonsverdi bør man identifisere hvilke komponenter som er involvert i håndteringen av informasjonsverdien, og også informasjonsverdiens kritikalitet.
- Velg ut et begrenset antall informasjonsverdier for videre analyse. Identifiser målrettede og generelle angrep, ubevisste feilhandlinger og tilfeldige feil som kan ramme de informasjonsverdiene som er valgt ut.
- Eksisterende sikkerhetsmekanismer og barrierer legges til grunn for en vurdering av sannsynlighet og konsekvens. Gode diskusjoner kan være vel så viktige som nøyaktige estimater for sannsynlighet og konsekvens.
- Når man skal identifisere relevante tiltak, anbefales det å benytte *Eksempler for å oppnå kontrollmål* i *Veileder til sikkerhet i avanserte måle- og styringssystem* [4] som sjekkliste. I tillegg anbefales at man minimum vurderer tiltak markert med grå bakgrunn i vedlegg D.
- Presentasjon av resultatene må være oversiktlig og forståelig. Koblingen fra informasjonsverdier til hendelser, risiko og tiltak må bevares i rapporten.
- En risikoanalyse vil ikke avdekke alle nødvendige tiltak. Man bør i tillegg se til generelle anbefalinger og styringssystemer for informasjonssikkerhet.

SINTEF

Innholdsfortegnelse

Figurer

Tabeller

1 Introduksjon

1.1 Bakgrunn

AMS (Avanserte Måle- og Styringssystem) skal innføres hos landets strømkunder innen 1.1.2019[1]. Dette er en stor investering for nettselskapene, som må bytte ut alle strømmålere og implementere støttesystemer for å samle måledata og benytte disse videre til fakturering, planlegging og drift.

Hvert nettselskap må gjøre egne risikoanalyser basert på egne forretningsbehov, teknologivalg og løsninger. Det å gjøre risikoanalyser, er ikke nytt for selskapene, men AMS medfører en del nye utfordringer i forhold til tidligere. Hver kunde vil nå være en potensiell angriper, da det vil finnes en logisk vei fra hver enkelt husstand inn til innsamlingssystemet hos nettselskapet. Bryter-/strupefunksjonalitet skal implementeres, noe som gjør AMS mer attraktiv for potensielle angripere, da konsekvensene av et angrep kan bli svært omfattende. Informasjonsflyt mellom baksystemer forventes å bli endret etter innføring av AMS.

Det er ikke nødvendigvis bruk for nye metoder for å gjennomføre selve risikoanalysene, men det er behov for å kunne håndtere nye typer risiko. Denne rapporten skal være til støtte ved gjennomføring av risikoanalyser av de tekniske systemene som inngår i en AMS-infrastruktur ved å bidra til at de rette spørsmålene stilles[2]. Rapporten gir en støtte til å analysere risiko knyttet til informasjonssikkerhet og personvern for disse tekniske systemene. En slik analyse kan gjøres som del av en bredere vurdering av risiko knyttet til AMS, men i denne rapporten gir vi kun anbefalinger og støtte til den delen av en risikoanalyse som omhandler informasjonssikkerhet og personvern.

Rapporten er et resultat fra arbeidspakke 4 (WP4) i DeVID[3].

1.2 Informasjonssikkerhet og personvern

Med informasjonssikkerhet menes egenskapene konfidensialitet, integritet og tilgjengelighet. For en mer utfyllende beskrivelse av disse begrepene, henviser vi til kapittel 3 i *Risikovurdering av AMS. Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS* [1].

Med personvern menes at et hvert individ har rett til et privatliv og rett til å bestemme over egne personopplysninger. Datatilsynet gir følgende definisjoner: ”Personopplysninger er opplysninger og vurderinger som kan knyttes til en enkeltperson. Sensitive personopplysninger er opplysninger om rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling; helseforhold, seksuelle forhold, og medlemskap i fagforeninger.” Personopplysningsloven setter strengere krav til behandling av sensitive personopplysninger. Det kan imidlertid være personopplysninger som er følsomme utover de som formelt sett er definert til å være sensitive. Det må derfor utøves en viss grad av skjønn i behandling av ulike typer personopplysninger. For en mer utfyllende beskrivelse av personvern, henviser vi til Datatilsynet[4].

Begrepet *personsikkerhet* er utbredt i bruk i kraftbransjen. Dette må ikke forveksles med *personvern*. Personsikkerhet er knyttet til beskyttelse av et fysisk individ, mens personvern omfatter beskyttelse av *opplysninger* knyttet til individet. Vi vil i denne rapporten ikke berøre personsikkerhet.

[1] Brev fra OED til NVE 18.2.2013
[2] Begrepet "risikoanalyse av AMS" tolkes av svært mange som en risikoanalyse av *prosjektet for innføring av AMS*. Det er viktig å presisere at denne rapporten omhandler en risikoanalyse av de tekniske systemene som inngår i en AMS-infrastruktur.
[3] Demonstrasjon og verifikasjon av intelligente distribusjonsnett: http://www.sintef.no/Projectweb/DeVID
[4] Datatilsynet: www.datatilsynet.no

Figur 1-1viser hvordan informasjonssikkerhet og personvern består av både menneskelige, tekniske og organisatoriske aspekter. Dette kalles ofte MTO-perspektivet.

Figur 1-1 Informasjonssikkerhet og personvern

1.3 Relevante støttedokumenter

Det er gjort mye arbeid rundt risikoanalyser av AMS tidligere. Følgende dokumenter anbefales som støtte til gjennomføring av egne risikoanalyser:

- *Risikovurdering av AMS. Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS, SINTEF [1]:* Denne rapporten beskriver de ulike komponentene som inngår i en generisk AMS infrastruktur og gir en grunnleggende innføring i informasjonssikkerhet. Et omfattende sett av trusler mot AMS presenteres, sammen med fem ulike trusselscenarioer.

- *Security Threats in Demo Steinkjer. Report from the Telenor-SINTEF collaboration project on Smart Grids. SINTEF, Telenor, NTE, Aidon [2]:* Dette arbeidet tar utgangspunkt i AMS infrastruktur som er implementert i Demo Steinkjer, hvor et sett av slavenode-strømmålere sender data via et radio-mesh-nettverk til en masternode-strømmåler, som videresender over GPRS inn til NTEs sentralsystem. Det er gjort en trusselvurdering av dette oppsettet, og 30 relevante trusler, samt fem konkrete angrep, er identifisert og presentert.

- *Overordnet risiko- og sårbarhetsanalyse for innføring av AMS, Proactima, Energi Norge [3]:* Denne analysen presenterer risikoforhold relatert til innføringen av AMS for et tenkt nettselskap. Tre ulike faser er vurdert: strategisk fase, utrullingsfase og driftsfase. Personvern er med som en egen konsekvensdimensjon, i tillegg til forsyningssikkerhet og selskapets økonomi og omdømme.

- *Veileder til sikkerhet i avanserte måle- og styringssystem, NVE [4]:* Dette er en veiledning i hvordan nettselskapene skal kunne oppfylle forskriftskravene om sikkerhet i AMS. Alle kontrollmålene er samlet, og det presenteres en større samling eksempler på sikkerhetstiltak som kan bidra til at kontrollmålene oppfylles.

- *Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen, Proactima, NVE [5]:* Veiledningen beskriver hvordan et nettselskap kan gjøre en risiko- og sårbarhetsanalyse som et verktøy for etterlevelse av beredskapsforskriftens krav. Den er ikke spesifikt rettet inn mot informasjonssikkerhet, men dekker et bredere sikkerhetsaspekt som inkluderer forsyningssikkerhet, damsikkerhet og annet som inngår i beredskapsforskriften.

Det finnes mange ulike metoder som kan benyttes for å gjøre risikoanalyser. Vi har i denne rapporten valgt å bygge på en metode som mange nettselskap er kjent med fra før, nemlig den som beskrives i veiledningen fra NVE [5] og som er benyttet i rapporten fra Energi Norge [3]. Vi supplerer Energi Norges rapport ved at vi rendyrker fokusområdet informasjonssikkerhet og personvern og gir sjekklister og eksempler som nettselskapene kan ta inn i sine egne risikoanalyser. Mens Energi Norges rapport stopper ved mottak av AMS-data hos nettselskapet, vil denne rapporten også støtte risikoanalyse av IKT-baksystemer.

1.4 Arbeidsmåte

Denne rapporten er et delresultat fra WP4 i DeVID-prosjektet. I en tidlig fase ble ulike risikoanalysemetoder vurdert, og det ble konkludert med at den metoden som beskrives i *Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen* [5], med små tilpasninger også er velegnet for å vurdere risiko knyttet til informasjonssikkerhet og personvern.

Et første utkast av rapporten ble forelagt en arbeidsgruppe knyttet til DeVID WP4. Følgende nettselskaper deltok på møter hvor utkastet ble diskutert, og de har gitt viktige bidrag til rapporten:

- Agder Energi Nett
- BKK Nett
- Fredrikstad Energi
- NTE
- Skagerak Energi
- TrønderEnergi

Vi evaluerte første utkast av rapporten ved å benytte den i to risikoanalyser hvor vi stilte som prosessledere. Dessuten har vi studert tre andre risikoanalyser, hvor vår veiledning ikke var brukt i prosessen. Vi så på hvilke typer informasjonsverdier, trusler og hendelser som ble identifisert, og vi intervjuet prosessleder og/eller prosessansvarlig hos de respektive nettselskapene for å høre deres erfaringer fra prosessen. Funnene har vi brukt til å forbedre denne veiledningen. Evalueringsarbeidet og resultatene fra dette er beskrevet i NEF Teknisk rapport [16] og kort gjengitt i kapittel 3.

1.5 Organisering av rapporten

Denne rapporten er i det videre organisert som følger:

Kapittel 2: Metode
Her beskrives hvordan metoden fra *Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen* [5] kan benyttes når informasjonssikkerhet og personvern er hovedformålet med risikoanalysen. Det gis anbefalinger knyttet til aktivitetene:

- Planlegging
- Risiko- og sårbarhetsvurdering
- Risikohåndtering

Kapittel 3: Diskusjon
Synspunkter og resultater etter evaluering av metodestøtte og sjekklister hos nettselskapene presenteres her.

Kapittel 4: Referanser

Vedlegg A: Sjekklister
Vedlegget presenterer relevante standarder og sjekklister som kan være nyttige hjelpemidler under analysen.

Vedlegg B: Detaljanalyser
Vedlegget beskriver kort ulike metoder for gjennomføring av detaljanalyser. Detaljanalyser kan være nødvendig som underlag for hovedanalysen.

Vedlegg C: Systembeskrivelse
Vedlegget inneholder systemskisser for generell AMS-infrastruktur og beskrivelser av grensesnitt og tilgrensende systemer. Figurene og beskrivelsene kan brukes som utgangspunkt for et nettselskap som skal utarbeide skisser over egne systemer.

Vedlegg D: Sikkerhetstiltak
Vedlegget inneholder en liste over sikkerhetstiltak som bør vurderes etter anbefaling fra ISO/IEC 27001 [18]. Tiltakene er vurdert opp mot tiltakene i NVEs *Veileder til sikkerhet i avanserte måle- og styringssystem* [4].

1.6 Forkortelser og akronymer

AMS	Avansert(e) måle- og styringssystem(er)
CA	Certificate Authority
DeVID	Demonstrasjon og verifikasjon av intelligente distribusjonsnett (www.sintef.no/Projectweb/DeVID/)
DMS	Distribution Management System
ETA	Event Tree Analysis
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IEC	International Electrotechnical Organization
IEEE	Institute of Electrical and Electronics Engineers
IKT	Informasjons- og kommunikasjonsteknologi
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
KIS	Kundeinformasjonssystem
MTO	Menneske, Teknisk, Organisatorisk
MVDB	Måleverdi-database
NEF	Norsk Elektroteknisk Forening
NIS	Nettinformasjonssystem
NIST	National Institute for Standards and Technology
NorSIS	Norsk senter for informasjonssikring
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OED	Olje- og energidepartementet
SERTIT	Offentlig sertifiseringsmyndighet for IT-sikkerhet
SSL	Secure Socket Layer
TLS	Transport Layer Security
WP4	Arbeidspakke for informasjonssikkerhet og personvern i DeVID

2 Metode for risikoanalyse

Som allerede nevnt, bygger denne rapporten på NVEs veiledning [5]. For analyser som fokuserer på informasjonssikkerhet og personvern anbefaler vi noen justeringer av metoden anbefalt av NVE. Tabell 2-1 gir en oversikt over hvordan delaktivitetene i denne rapporten er relatert til anbefalingene fra NVE. De endrede delaktivitetene er markert med farge i høyre kolonne av tabellen.

Vi anbefaler at det legges inn et nytt steg før delaktivitet 2a, nemlig *Identifisering av informasjonsverdier*. Den grunnleggende tanken med informasjonssikkerhet er nettopp å beskytte informasjon. En systemkomponent kan lett erstattes, men brudd på konfidensialitet, integritet eller tilgjengelighet av informasjon kan ha omfattende konsekvenser. Vi mener dermed at et naturlig første trinn ved gjennomføring av en risikoanalyse er å identifisere de verdiene som lagres, behandles og/eller transporteres i systemet som er objektet i analysen. I tillegg presenterer vi noen endringer til de eksisterende punktene 2a-c. NVE beskriver risikoanalyse og sårbarhetsvurdering som to etterfølgende aktiviteter, mens vi heller anbefaler å utføre sårbarhetsvurderingen som en del av risikoanalyse-aktiviteten. Da vil verdiene for sannsynlighet og konsekvens ta inn i seg sårbarhetsvurderingen. Vi mener dessuten at det kan være noe forvirrende å ha en egen aktivitet som heter risikoanalyse og ønsker heller å kalle denne *vurdering av sannsynlighet og konsekvens* da det er det som blir gjort på dette stadiet.

Tabell 2-1 Aktiviteter som inngår i en risikoanalyse

Hovedaktivitet		Delaktiviteter som anbefalt av NVE	Delaktiviteter anbefalt i denne rapporten
1. Planlegging	a	Formål og omfang	Formål og omfang
	b	Valg av konsekvens- og sannsynlighetsdimensjon	Valg av konsekvens- og sannsynlighetsdimensjon
	c	Informasjonsinnhenting	Informasjonsinnhenting
	d	Organisering	Organisering
	e	Klargjøring av sjekklister og analyseskjema	Klargjøring av sjekklister og analyseskjema
2. Risiko- og sårbarhetsvurdering	a	Identifisere farer, trusler og uønskede hendelser for delsystem/komponent	Identifisere informasjonsverdier
	b	Risikoanalyse	Identifisere farer, trusler og uønskede hendelser for hver informasjonsverdi
	c	Sårbarhetsvurdering	Vurdere sannsynlighet og konsekvens
	d	Identifisere mulige risikoreduserende tiltak	Identifisere mulige risikoreduserende tiltak
	e	Presentasjon av risikobilde	Presentasjon av risikobilde
3. Risikohåndtering	a	Tiltaksanalyse	Tiltaksanalyse
	b	Beslutning/tiltaksplan	Beslutning/tiltaksplan
	c	Beredskapsanalyse/beredskapsplan	Beredskapsanalyse/beredskapsplan
	d	Oppfølging	Oppfølging

I det følgende beskrives hvordan metoden kan benyttes når informasjonssikkerhet og personvern er hovedformålet med risikoanalysen. Strukturen er i tråd med aktivitetene som er skissert over i Tabell 2-1:

- Planlegging
- Risiko- og sårbarhetsvurderinger
- Risikohåndtering

! **Anbefaling:** Før man identifiserer trusler og uønskede hendelser, bør man identifisere hvilke informasjonsverdier som finnes i systemet. Det er informasjon som har verdi, ikke systemet i seg selv, og man må vite hva som skal beskyttes for å kunne bestemme passende sikkerhetsnivå og akseptabel restrisiko.

2.1 Planlegging

2.1.1 Formål og omfang

Hvorfor, hva og for hvem

Tilsvarende som i NVEs veiledning [5] vil vi også her understreke viktigheten av planleggingsfasen og et omforent syn på *hvorfor* man gjør analysen, *hva* som skal analyseres (systemavgrensing) og *for hvem* analysen gjennomføres. Risikoanalysen bør gjennomføres som et prosjekt, med gitte tids- og kostnadsrammer og med en prosjekteier og en prosjektleder. Prosjekteier kan være styret, en ledergruppe eller en leder. Avgrensing av arbeidet gjøres i samarbeid med prosjekteier.

I noen tilfeller vil risikoanalyse av informasjonssikkerhets- og personvernsaspekter av AMS være en egen analyse. I andre tilfeller vil informasjonssikkerhet og personvern inngå i en bredere analyse av risiko knyttet til AMS. Erfaringsmessig er det behov for to analysemøter på 4-5 timer hver for å dekke informasjonssikkerhet og personvern på en god måte. Vi anbefaler derfor at man utvider antallet møter om man også ønsker å dekke andre aspekter. Da kan det være behov for ulike deltakere på de ulike møtene.

Detaljnivå

Selv om metoden kalles strukturert grovanalyse, kan den også benyttes for mer detaljerte analyser. Detaljeringsgraden er gitt av systemet og de hendelsene man analyserer. *Veiledning til sikkerhet i avanserte måle- og styresystem* [4] benytter ikke begrepene grovanalyse og detaljert analyse. Det forutsettes at risiko- og sårbarhetsanalyse gjennomføres på det nødvendige detaljnivå for at man skal oppnå ønsket målsetting.

Detaljanalyser kan benyttes for det man innledningsvis antar har høy risiko, men kan også være nyttige for å øke organisasjonens kunnskap om systemet, dokumentere systemet, eller besvare spørsmål i hovedanalysen.

Dersom man ønsker å gå i detalj, finnes det flere metoder som kan være hensiktsmessige, se vedlegg B for noen eksempler. Resultater fra detaljanalysen kan med fordel tas inn i hovedanalysen slik at resultatene er samlet ett sted. Detaljanalysene kan refereres til eller vedlegges hovedanalysen som underlag for de vurderinger som er gjort.

> **!** **Anbefaling:** Risikoanalysen bør gjennomføres som et prosjekt, med en prosjekteier og gitte rammer. Metoden som er beskrevet i NVEs veiledning [5], kan benyttes også når man har fokus på informasjonssikkerhet og personvern.

2.1.2 Valg av konsekvens- og sannsynlighetsdimensjon

Tilsvarende som beskrevet i Energi Norges rapport [3] må hvert selskap ta stilling til sannsynlighetsskalaer og konsekvensdimensjoner og vurdere om disse tilfredsstiller eget behov. Det er viktig at hvert selskap har et forhold til hva de anser som sannsynlig og ikke, og hva de kan akseptere av konsekvenser. Det kan være en fordel å bruke samme eller tilsvarende dimensjoner i alt risikoarbeid, slik at det blir lettere å sammenligne risiko identifisert i ulike analyser. Det er ikke hensiktsmessig å ha informasjonssikkerhet som en egen konsekvensdimensjon. Et informasjonssikkerhetsbrudd er primært av interesse for virksomheten idet det har konsekvenser for forsyningssikkerhet, økonomi eller omdømme. Vi anbefaler derfor å bruke disse som konsekvensdimensjoner. Personvern kan imidlertid være en egen konsekvensdimensjon, eller personvern kan dekkes av dimensjonene økonomi og omdømme.

Som presisert også i innledningen, observerer vi at personsikkerhet og personvern er begreper som benyttes om hverandre i bransjen. Derfor ønsker vi her også å komme med noen presiseringer når det gjelder konsekvenser knyttet til personvern. Siden personvern er knyttet til behandling av opplysninger om individet, vil brudd på personvern svært sjelden ha konsekvenser for liv og helse. Det er også viktig å være klar over at brudd på krav til personvern ikke trenger å medføre at personlig informasjon blir kompromittert.

Personvernlovgivningen stiller krav til hvordan personlig informasjon skal håndteres, og at det skal være hjemmel for innsamling. Dersom kravene ikke er oppfylt kan dette føre til omdømmetap – og bøter eller overtredelsesgebyr – selv om data ikke er kompromittert.

Sannsynlighetsdimensjonene som man vanligvis benytter i virksomheten kan ha skalaer som oppleves store i arbeidet med IKT-hendelser. For IKT er man ikke vant til å tenke 100 år, 1000 år eller mer. Dersom man velger å benytte sannsynlighetsdimensjonen som er skissert her, må man derfor forvente at de fleste hendelsene vil bli karakterisert som 'Meget sannsynlig' eller 'Svært sannsynlig'. Dersom man ønsker å gjøre et mer grundig skille mellom hendelser i disse kategoriene må man velge en annen tidsinndeling. Det å bruke spesielle sannsynlighetsdimensjoner for IKT-hendelser vil imidlertid vanskeliggjøre sammenligning av risikoen for IKT-hendelser versus andre typer hendelser.

Siden vi anbefaler å benytte samme dimensjoner som man benytter ellers, gir vi ikke eksempler på konsekvens- og sannsynlighetsdimensjoner i denne rapporten. Slike eksempler er imidlertid tilgjengelige i blant annet Energi Norges rapport [3].

! **Anbefaling:** Konsekvens- og sannsynlighetsdimensjoner må tilpasses den enkelte virksomhet. Det anbefales å vurdere gjenbruk av tidligere benyttede dimensjoner.

2.1.3 Informasjonsinnhenting

Systembeskrivelse

Systemet som er objektet for risikoanalysen bør beskrives grundig i denne fasen slik at alt underlag er på plass når man starter analysen. I analysefasen bør man unngå lange diskusjoner om hvordan systemet egentlig virker. En god systembeskrivelse sikrer også at alle involverte har en felles forståelse av hva som er omfanget av arbeidet, og hvilke avgrensninger som gjelder. Vedlegg C gjengir ulike systemskisser og beskrivelser for et AMS-system.

Det kan imidlertid hende at man skal gjøre en første risikoanalyse på et system som ennå ikke finnes. Det vil da ikke eksistere komplett dokumentasjon for systemet. Likevel er det naturlig å anta at noe dokumentasjon, om enn på tanke- og skissestadiet vil finnes. Man vil ha en ide om hva slags funksjonalitet som skal være i systemet, hva det skal brukes til, hva slags type data som skal prosesseres og/eller lagres der, og hvilke tilkoplinger det skal ha til andre systemer. Man behøver ikke en komplett dokumentasjon av objektet, men nok til at alle involverte har en omforent forståelse av hva som er objektet for risikoanalysen.

Eksisterende og planlagte tiltak

Det er viktig at alle i analysegruppa er oppmerksom på at man skal vurdere risiko (konsekvens og sannsynlighet) *etter* eksisterende og allerede planlagte tiltak. En oversikt over eksisterende og planlagte tiltak bør derfor foreligge.

! **Anbefaling:** Før analysemøtet bør det foreligge oppdaterte systemskisser og en oversikt over eksisterende og planlagte tiltak. Deltagerne i analysen bør gis en felles forståelse av arbeidets omfang og avgrensning.

2.1.4 Klargjøring av sjekklister og analyseskjema

Ulike sjekklister og analyseskjema kan være til støtte ved gjennomføring av en risikoanalyse. Vedlegg A inneholder følgende hjelpemidler:

- Oversikt over relevante standarder
- Skjema for utfylling av informasjonsverdier
- Liste med uønskede hendelser

- Liste over interessenter
- Liste med sårbarheter
- Oversikt over relevante sikkerhetsmekanismer

Sjekklistene er ment brukt av prossessleder for å sikre at vesentlige punkter ikke blir uteglemt. De bør ikke deles ut til deltagerne. Sjekklistene må brukes slik at de fremmer, ikke hemmer, deltagernes kreativitet.

Det finnes mange ulike verktøy som støtter gjennomføring av risikoanalyser. Vi ønsker ikke å anbefale noen framfor andre i denne rapporten, men nevner her noen av de mer kjente verktøyene som allerede benyttes i bransjen:

- CIM risikomodul, utviklet av OneVoice
- DK Delta fra Datakvalitet AS
- EasyRisk
- Excel: er utbredt, typisk egenutviklede skjema inspirert av velkjente metoder og veiledninger
- Risk Analyzer, utviklet av Landax
- WhatIf: støtter utarbeidelse av trusselscenarioer og dokumentasjon av resultater

! **Anbefaling:** Sjekklister bør benyttes av prosessleder for å sikre at vesentlige punkter ikke blir utelatt. Sjekklister må ikke brukes på en slik måte at de hemmer deltagernes kreativitet.

2.1.5 Deltagere

For å sikre en mest mulig kreativ prosess bør arbeidsgruppen bestå av flere personer som ikke jobber sammen til daglig, og som har ulike oppgaver og perspektiver. Kompetanseområder som informasjonssikkerhet, personvern, samt inngående kjennskap til enkeltsystemer bør dekkes av arbeidsgruppen.

Det kan være til hjelp å ha en prosessleder utenfra, som ikke påvirker idemyldringen i en bestemt retning. En erfaren prosessleder vil lettere kunne balansere overordnede mål mot behov for å grave seg ned i detaljer. Ikke minst vil en ekstern prosessleder kunne håndtere inngrodde roller og konflikter i analysegruppen og sikre en god balanse mellom ulike fagområder.

! **Anbefaling:** I valg av prosessleder og i sammensetning av analysegruppa bør man ta hensyn til behovet for å fremme kreativitet og hindre begrensninger. Noen i gruppa må inneha kompetanse om informasjonssikkerhet og personvern.

2.1.6 Planlegging av analysemøtene

Vi anbefaler at risikoanalysen (aktivitet 2a-2d i Tabell 2-1) gjennomføres som to arbeidsmøter, hvorav hvert møte er på 4-5 timer. Alle nødvendige ressurspersoner bør være tilstede på begge møtene, og delta på hele møtet. Det kan være nyttig å ha ca. en uke mellom møtene, for å få noe tid til å innhente eventuell manglende informasjon identifisert i møte 1, og bearbeide resultatene fra dette møtet. En prosessleder, enten intern eller ekstern, har ansvar for gjennomføringen av arbeidsmøtene. Figur 2-1 illustrerer prosessen.

For gjennomføring av arbeidsmøtene er det nyttig med et møterom med whiteboard. Det er også behov for gule lapper og tusjer til alle deltakere. På møte 2 er det behov for risikomatrise for hver konsekvensdimensjon – for eksempel i form av en plakat.

Følgende agenda kan benyttes for møte 1:

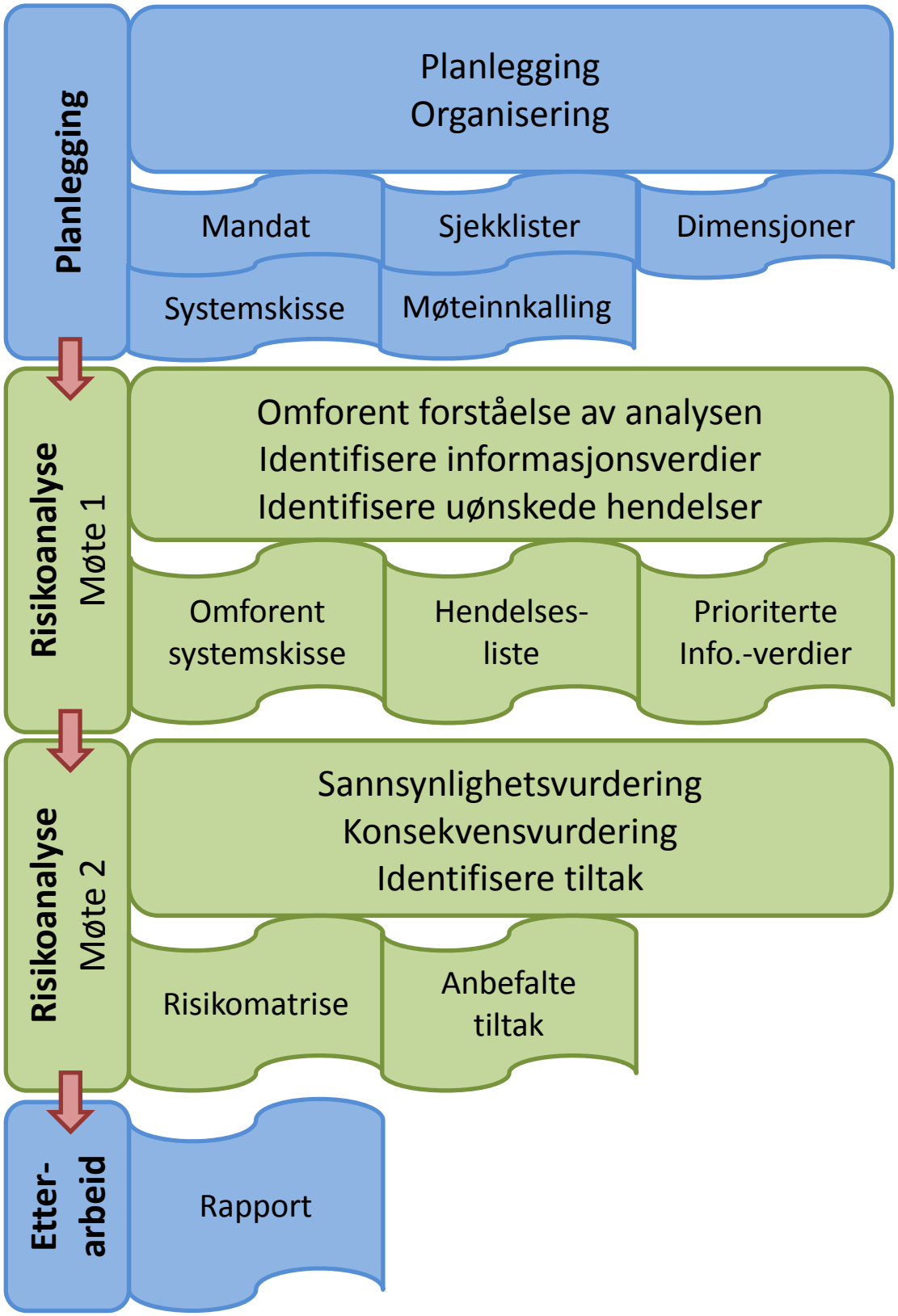
1) **Introduksjon:** Prosessleder ønsker velkommen, runde rundt bordet, hensikt med arbeidsmøtet, gjennomgang av agenda og metoden som benyttes.
2) **Gjennomgang av systemskisse:** Sikre omforent forståelse av objektet som skal analyseres. Vise skisser, være tydelig på avgrensninger.
3) **Identifisering av informasjonsverdier:** Idemyldring: Alle bidrar til å identifisere informasjonsverdier som hører til i systemet. "Hva er det vi ønsker å beskytte?"
4) **Prioritering av informasjonsverdier:** Runde i plenum med gjennomgang av informasjonsverdier. Gruppering. Velg ut et fåtall informasjonsverdier som brukes videre i analysen.
5) **Gjennomgang av prioriterte informasjonsverdier:** For de informasjonsverdiene som er valgt ut diskuteres det hvor i systemskissa disse informasjonsverdiene lagres eller deles.
6) **Identifisering av uønskede hendelser:** Idemyldring: Alle bidrar til å identifisere hvilke uønskede hendelser som kan skje for de utvalgte informasjonsverdiene – en informasjonsverdi om gangen. "Hva er vi redd for? Hva kan skje?"
7) **Avslutning:** Oppsummering av møtet, med innspill fra deltakerne på prosessen og informasjon om arbeidet videre.

Følgende agenda kan benyttes for møte 2:

1) **Introduksjon:** Prosessleder ønsker velkommen, runde rundt bordet med forventninger til møtet og refleksjoner fra forrige møte, hensikt med arbeidsmøtet, gjennomgang av agenda og metoden som benyttes.
2) **Gjennomgang av resultater fra møte 1:** Kort gjennomgang av systemet, informasjonsverdiene som er prioritert og de uønskede hendelsene som er identifisert.
3) **Sannsynlighets- og konsekvensvurdering:** Kreativ samarbeidsprosess i grupper: Plassering av de uønskede hendelsene i en eller flere risikomatriser, som kan være tegnet opp på ei tavle eller trykket opp på en plakat.
4) **Plenumsdiskusjon rundt sannsynlighet og konsekvens:** Diskuter sannsynlighets og konsekvensvurderingen. Fokuser på eventuelle uoverensstemmelser i vurderingene hos ulike grupper. Gjøre eventuelle endringer i gruppe-vurderingene.
5) **Identifisere tiltak:** Velg ut hendelser med høy risiko, og diskutert mulige tiltak.
6) **Avslutning:** Oppsummering av møtet, med innspill fra deltakerne på prosessen og informasjon om arbeidet videre.

Etter arbeidsmøtene dokumenteres resultatene i en rapport. Se kapittel 2.2.5.

> **!** **Anbefaling:** Det bør settes av to arbeidsmøter til å gjennomføre selve analysen. Første møte brukes til å forstå både metoden og systemet, samt å identifisere informasjonsverdier og uønskede hendelser. I andre møte vurderes sannsynlighet og konsekvens, dessuten identifiseres mulige tiltak.



Figur 2-1 Anbefalt organisering av analysen

2.2 Risiko- og sårbarhetsvurderinger

Som nevnt i innledningen, anbefaler vi noen endringer til metoden som er beskrevet i veiledningen fra NVE [5]. Med våre forslag til endringer blir stegene som følger:

a. Identifisere informasjonsverdier
b. Identifisere farer, trusler og uønskede hendelser for hver informasjonsverdi
c. Vurdere sannsynlighet og konsekvens
d. Identifisere mulige risikoreduserende tiltak
e. Presentasjon av risikobilde

Stegene a, b og c er illustrert i Figur 2-3.

2.2.1 Identifisere informasjonsverdier

Dette er en delaktivitet som ikke er inkludert i NVEs veiledning for risiko- og sårbarhetsanalyser i kraftforsyningen [5], men den er grundig beskrevet i OCTAVE-rammeverket for risikovurderinger [13]. Hensikten med informasjonssikkerhet er nettopp å beskytte informasjon som prosesseres, overføres og/eller lagres i et system. Dermed må man ha et bevisst forhold til hva slags type informasjon som faktisk finnes og må beskyttes. Denne fasen gjøres best som en idemyldring, gjerne ved bruk av gule lapper, slik at hver deltaker får kommet med alle sine innspill uten påvirkning eller begrensninger fra de andre.

En kreativ idemyldring rundt informasjonsverdier kan gjennomføres ved at alle deltakere i analysen får utdelt noen gule lapper og en tusj. Så setter man av noen minutter der deltakerne jobber hver for seg med å svare på spørsmålet: "Hvilke informasjonsverdier finnes i dette systemet?". Deltakerne bør oppfordres til å skrive kun en informasjonsverdi per lapp, og skrive stort og tydelig slik at lappen er lett å lese også på noe avstand. I denne fasen er det ingen rette eller gale svar – målet er å identifisere så mye som mulig for bearbeidelse i felleskap. Etter at alle har fått tid til å skrive ned de informasjonsverdiene de kommer på, deles dette i gruppa. Dette kan gjøres ved at alle deltakere hver for seg leser opp sine lapper og henger de på en vegg (se f.eks. Figur 2-2). Ofte vil det være lurt å sette en begrensning på hvor mange lapper hver deltaker kan henge opp i første runde – f.eks. til tre. Slik unngår man at sistemann til å presentere, ikke har noe nytt å komme med. Ofte vil noen deltakere komme på flere informasjonsverdier når de ser lappene til de andre. Dette bør det oppfordres til.

Figur 2-2 Idemyldring rundt informasjonsverdier

Når alle lapper er presentert og hengt opp, bør gruppen i fellesskap, evt. ledet av prosessleder, gruppere lappene slik at lignende informasjonsverdier samles. Da blir det lettere å få oversikt, og man får et godt

utgangspunkt for å prioritere informasjonsverdiene videre. Etter at lappene er gruppert, vil det også være hensiktsmessig å gjøre en vurdering av om det er noe som mangler, for eksempel ved å benytte sjekkliste over informasjonsverdier lenger bak i denne rapporten (se Tabell A-1 i vedlegg A.2).

De ulike informasjonsverdiene har ulik kritikalitet. Vi anbefaler derfor at man i plenum gjør en vurdering av hvilke informasjonsverdier som er viktigst for virksomheten, som grunnlag for det videre analysearbeidet. Dette kan gjøres gjennom en diskusjon der man tar sikte på å bli enige. Det er også mulig å gjennomføre stemmegivning, der hver deltaker f.eks. får fem stemmer de kan fordele på de informasjonsverdiene de synes er mest viktige. For de informasjonsverdiene som anses som spesielt viktige, anbefaler vi at man identifiserer hvor informasjonen "lever", dvs. hvilke komponenter og delsystemer som er involvert i behandling av informasjonen på en eller annen måte.

! **Anbefaling:** Identifikasjon av informasjonsverdier gir økt systemforståelse og er et viktig underlag for videre analyse. For viktige informasjonsverdier bør man identifisere hvilke komponenter som er involvert i håndteringen av informasjonsverdien, og også informasjonsverdiens kritikalitet

2.2.2 Identifisere uønskede hendelser

De allerede identifiserte informasjonsverdiene utgjør grunnlaget for denne fasen. Vi anbefaler imidlertid at det velges ut et begrenset antall (størrelsesorden tre) informasjonsverdier for videre analyse. Det vil som regel bli altfor omfattende å gå i dybden på alle, og mange vil nok kunne føre til ganske like resultater i den videre analysen. I utvelgelsen av informasjonsverdier bør man ta hensyn til:

- **Informasjonsverdiens kritikalitet:** Det er hensiktsmessig å prioritere de informasjonsverdiene man anser som viktigst og vurdere uønskede hendelser relatert til disse.
- **Relevante delsystemer:** Det er en fordel om de informasjonsverdiene som velges ut til sammen dekker de viktigste delsystemene som er objekt for risikoanalysen.
- **Konsekvensdimensjoner:** Det kan være nyttig å komme fram til et sett av hendelser som tilsammen dekker flere konsekvensdimensjoner (forsyningssikkerhet, økonomi, omdømme, personvern). Vurder derfor om de utvalgte informasjonsverdiene er tilstrekkelig for å vurdere de ulike konsekvensdimensjonene som er en del av analysen.

Vi anbefaler at man håndterer hver informasjonsverdi for seg. For hver informasjonsverdi gjør man da en idemyldring med gule lapper, tilsvarende den man gjorde for å identifisere verdiene. Som utgangspunkt for idemyldringen kan man ta utgangspunkt i spørsmålet: "Hvilke uønskede hendelser kan oppstå?" Det bør presiseres at man i prosessen skal vurdere alle mulige typer uønskede hendelser, inkludert målrettede angrep, generelle angrep, ubevisste feilhandlinger og tilfeldige feil. Hvilken komponent/delsystem som rammes og hvilke utfall det har, er stikkord som kan brukes ved beskrivelse av hendelser.

Etter at hendelsene er identifisert og gruppert, anbefaler vi at det blir tatt en gjennomgang av relevante sjekklister for hendelser, for å sikre at man har dekket så mye som mulig av det som kan gå galt. Denne rapporten inneholder tre relevante sjekklister:

- En liste over ulike hendelsestyper (se Tabell A-2).
- En liste over typiske svakheter og sårbarheter i IKT-systemer (se vedlegg A.5)
- Eksempler på hendelser som kan være relevante å vurdere for AMS (se Tabell A-3).

Listen over interessenter i vedlegg A.4 kan også brukes som inspirasjon.

En mulig svakhet ved en risikoanalyse er at man bare finner det man forventer å finne. Spesielt kan det være vanskelig å avdekke såkalte svarte svaner; usannsynlige hendelser med katastrofale konsekvenser. Det er ikke nødvendigvis hensiktsmessig å sikre seg mot denne typen hendelser, men det er nyttig å identifisere dem for å være bedre forberedt.

> **!** **Anbefaling:** Velg ut et begrenset antall informasjonsverdier for videre analyse. Identifiser målrettede og generelle angrep, ubevisste feilhandlinger og tilfeldige feil som kan ramme de informasjonsverdiene som er valgt ut.

2.2.3 Vurdere sannsynlighet og konsekvens

Når et sett av uønskede hendelser er identifisert, bør disse tilordnes en sannsynlighet og en konsekvens. Dette oppleves ofte som utfordrende. Spesielt er det vanskelig å vurdere sannsynlighet for ulike hendelser. Trusselbildet endrer seg hele tiden, og det er tilnærmet umulig å forutsi om noen kan ønske å utføre et dataangrep i nær framtid. Det er lite hjelp å hente i historiske data og statistikk, så man må gjøre en subjektiv vurdering.

En vurdering av sannsynlighet og konsekvens for en hendelse vil alltid være usikker og preget av de subjektive meningene til deltakerne i analysen, samt hvilken kunnskap deltakerne innehar og mangler. Men selv om verdiene man ender opp med er usikre, vil ofte diskusjonene rundt sannsynlighet og konsekvens være fruktbare. Man får diskutert trusselbilde, teknologien man benytter, hvilke rutiner man har, og hva som faktisk er viktigst å sikre. Det er derfor viktig at man får dokumentert viktige momenter fra diskusjonen, og ikke bare den verdien for sannsynlighet og konsekvens man ender opp med. Mest fokus bør rettes mot de hendelsene som anses å ha uakseptabel risiko, eller som ligger på grensen mellom å være akseptabel og uakseptabel. Det viktigste er ikke nødvendigvis nøyaktigheten av sannsynlighets- og konsekvens-vurderingene for enkelthendelser, men å vurdere de ulike uønskede hendelsene opp imot hverandre og gjøre en vurdering av hvilke hendelser som krever ytterligere tiltak.

Om man er mer enn fire deltakere i analysen kan det være hensiktsmessig å dele seg opp i mindre grupper under sannsynlighets- og konsekvensvurderingen. Ofte ønsker man å vurdere flere konsekvensdimensjoner for hver hendelse i samme analyse (f.eks. forsyningssikkerhet, økonomi, omdømme, personvern), og da kan gruppene dele disse konsekvensdimensjonene mellom seg. Slik oppfattes arbeidet som mindre repeterende for deltakerne (de trenger ikke vurdere alle konsekvensdimensjonene), og man kan lokke fram ulikheter i vurderinger. Rent praktisk kan vurderingen av sannsynlighet og konsekvens dokumenteres ved at deltakerne har en risikomatrise per konsekvensdimensjon de skal vurdere, samt en lapp per hendelse, og at de klistrer hendelseslappene på risikomatrisen[1]. En slik sesjon må dermed forberedes ved at prosessleder gjør klar lapper og risikomatriser på forhånd.

Etter at hver gruppe har gjort sine vurderinger, kan prosessleder ta en gjennomgang i plenum av hva gruppene har kommet fram til. Selv om gruppene har vurdert ut fra ulike risikodimensjoner, har de vurdert de samme hendelsene. Se derfor spesielt etter steder der det er store endringer i f.eks. sannsynlighets-vurderingene knyttet til samme hendelse. Å gå dypere inn i hva som ligger bak disse forskjellene i vurderinger kan gi gode diskusjoner som er nyttige – både for å få en mer nøyaktig vurdering av sannsynlighet og konsekvens, og for å øke forståelsen for systemet og trusselbildet man opplever. Mest tid bør benyttes på å diskutere de hendelsene som vurderes å ha høyest risiko, eller som ligger i grenseland mellom akseptabel og høy risiko. I mange tilfeller vil plenumsdiskusjonen føre til at gruppevurderingen endres.

NVEs veiledning tar opp utfordringen med at en hendelse ofte kan ha flere mulige utfall, der noen konsekvenser er mer vanlige enn andre. Noen utfall vil også være mer alvorlige. Hvilket utfall man velger å vurdere, vil påvirke sannsynligheten for hendelsen. Analysegruppa må i slike tilfeller gjøre et valg om hvordan man skal håndtere dette. En mulig løsning er å splitte det som i utgangspunktet er en hendelse til flere separate hendelser, slik at ulikhetene i konsekvens tas vare på. Som et eksempel kan hendelsen "Infeksjon av skadevare (malware) i sentralsystemet" deles opp i ulike hendelser, f.eks. "Infeksjon av

[1] Om en hendelse ikke er relevant for en konsekvensdimensjon trenger man ikke å klistre lappen for den hendelsen på risikomatrisa.

skadevare i sentralsystemene gjør systemene upålitelige i flere dager" og "Infeksjon i skadevare i sentralsystemene, med rask deteksjon og feilretting". Eventuelle presiseringer av en hendelse bør dokumenteres.

I sannsynlighetsvurderingen kan det være nyttig å gjøre en årsaksidentifisering: Hvem vil bevisst ønske å oppnå dette, hva er motivet og hvordan vil de gå frem; hva kan gå feil som fører til denne hendelsen? Ferske trusselvurderinger fra sikkerhetsfirma og myndigheter kan være til god hjelp, i kombinasjon med en egen vurdering av hvor attraktive systemer man opererer. En må dessuten ta hensyn til eksisterende sikkerhets-tiltak og barrierer og vurdere hvorvidt de vil kunne beskytte mot denne trusselen. I konsekvensvurderingen må man ta hensyn til evnen til gjenoppretting. Dermed vil konsekvensvurderingen ta opp i seg det som er definert som sårbarhetsvurdering i NVEs veiledning.

Som støtte i arbeidet med å vurdere sannsynlighet og konsekvens for hendelser, inneholder denne rapporten en liste over interessenter (vedlegg A.4). Denne kan være til hjelp for prosessleder, for å bringe nye momenter inn i diskusjonen.

! **Anbefaling:** Eksisterende sikkerhetsmekanismer og barrierer legges til grunn for en vurdering av sannsynlighet og konsekvens. Gode diskusjoner kan være vel så viktige som nøyaktige estimater for sannsynlighet og konsekvens.

2.2.4 Identifisere mulige risikoreduserende tiltak

For hendelsene som er tilordnet en uakseptabel høy risiko etter sannsynlighets- og konsekvensvurderingene, må det identifiseres tiltak. Tiltakene som identifiseres i analysemøtet, gir et grunnlag for å ta beslutninger senere. Selve utvelgelsen og implementeringen av tiltakene er egne aktiviteter og gjøres ikke som en del av risikoanalysen. Det er nettselskapets behov som skal styre prioriteringene, og det gjelder å finne balansen mellom investeringer i forebyggende mekanismer og konsekvensene av hendelser man ikke beskytter seg mot. Informasjonssikkerhetsansvarlig kan ikke gjøre denne jobben ut i fra eget perspektiv. Prioriteringer må forankres i ledelsen, det er der avgjørelsene må tas. Uansett må organisasjonen ha evnen til å håndtere uønskede hendelser.

Noen tiltak vil kunne redusere sannsynligheten for at noe skjer. Andre tiltak vil kunne begrense konsekvensen *når* en hendelse inntreffer. Som støtte til identifisering av relevante tiltak gir vedlegg A.6 en beskrivelse av sentrale sikkerhetstiltak. Dessuten inneholder vedlegg D en generell sjekkliste fra ISO/IEC 27001 [18] over tiltak som kan benyttes for å bedre informasjonssikkerhet og personvern. *Veileder til sikkerhet i avanserte måle- og styringssystem* [4] inneholder en rekke tiltak under delkapitlene *Eksempler for å oppnå kontrollmål*.

! **Anbefaling:** Når man skal identifisere relevante tiltak, anbefales det å benytte *Eksempler for å oppnå kontrollmål* i *Veileder til sikkerhet i avanserte måle- og styringssystem* [4] som sjekkliste. I tillegg bør man minimum vurdere tiltak markert med grå bakgrunn i vedlegg D.

2.2.5 Dokumentasjon og presentasjon

Man bør tidlig i prosjektet ha en klar formening om for hvem og hvordan resultatene fra analysen skal dokumenteres og presenteres. Etter arbeidsmøtene bør resultatene dokumenteres i en rapport. Prosessleder kan være rapportforfatter. Selskapets tidligere utførte risikoanalyser kan være mal for rapporten, eller man kan benytte rapportmalen i vedlegg I.A.1.a)(1)A.7. I rapporten bør man etterstrebe å bevare koblingen fra informasjonsverdier til hendelser og deres risiko, og videre til tiltak. Slik blir grunnlaget for anbefalingene fra risikoanalysen lettere tilgjengelig.

En presentasjon av analysen bør minimum inneholde:

- Forutsetninger:
  - Prosjektdefinisjon og systemavgrensning
  - Deltakere
  - Eksisterende og planlagte tiltak
- Resultat av analysen
  - Liste over uønskede hendelser
  - Risikomatrisene
  - Liste over foreslåtte tiltak

Dokumentasjon og presentasjon av risikobildet er det femte og siste steget i risikoanalyse-fasen (steg 2e i Tabell 2-1). Risikohåndtering (steg 3a-d i Tabell 2-1) vil også inngå i etterarbeidet, men vil typisk ikke være en del av rapporten.

! **Anbefaling:** Presentasjon av resultatene må være oversiktlig og forståelig. Koblingen fra informasjonsverdier til hendelser, risiko og tiltak må bevares i rapporten.

2.3 Risikohåndtering

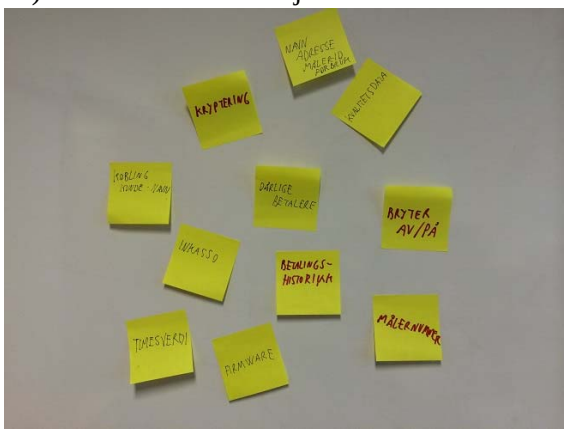
Som nevnt over bør nye tiltak foreslås i forbindelse med gjennomføringen av risikoanalysen. En full vurdering om nye tiltak, hvorvidt de foreslåtte tiltak er tilstrekkelige, eller om de skal gjennomføres, gjøres ikke under risikoanalysen, men som en egen aktivitet: *risikohåndtering*.

Risikohåndtering er kort omtalt i Energi Norges rapport [3] og mer utførlig beskrevet i *Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen* [5]. Aktivitetene som inngår her, er tiltaksanalyse, beslutning/tiltaksplan, beredskapsanalyse/beredskapsplan og oppfølging.

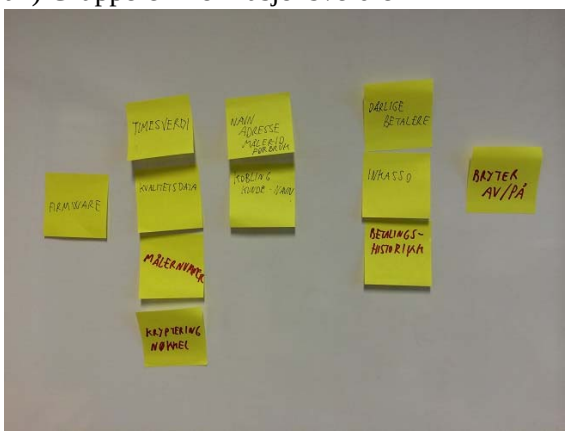
Selv om risikoanalyser er viktige for å identifisere og prioritere hvilke tiltak som er viktige å implementere, må man være klar over at enkelte nødvendige tiltak kan overses i slike analyser. Derfor bør man i arbeidet med informasjonssikkerhet også se til generelle og gode anbefalinger for dette arbeidet, og blant annet sørge for at noen har ansvar for sikkerheten, at det finnes policyer som dekker informasjonssikkerhet, at det gjøres jevnlige risikoanalyser, at slike analyser følges opp, at informasjonssikkerhet vurderes ved anskaffelser, at systemer er dokumenterte, at virksomheten har planlagt hva man skal gjøre dersom det skjer en hendelse, osv. Dette gjelder selv om ikke alle slike generelle tiltak er identifisert i en allerede gjennomført risikoanalyse.

! **Anbefaling:** En risikoanalyse vil ikke avdekke alle nødvendige tiltak. Man bør i tillegg se til generelle anbefalinger og styringssystemer for informasjonssikkerhet.

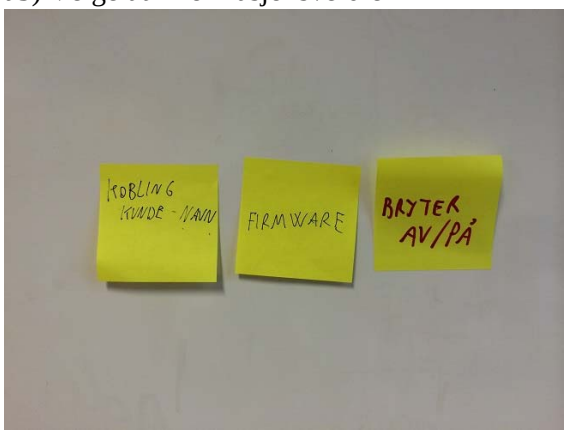
a1) Identifisere informasjonsverdier



a2) Gruppere informasjonsverdier



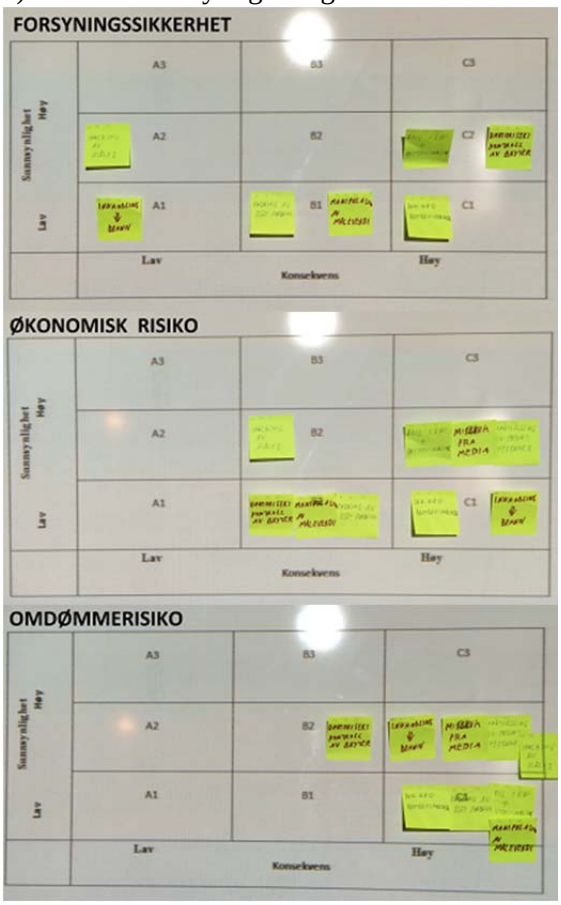
a3) Velge ut informasjonsverdier



b1) Identifisere uønskede hendelser

b2) Redusere antall ved å fjerne identiske hendelser og omformulere hendelsene

c) Vurdere sannsynlighet og konsekvens



Figur 2-3 Identifikasjon av informasjonsverdier og hendelser, samt vurdering av sannsynlighet og konsekvens

3 Diskusjon

Risikoanalyser slik det anbefales utført i DeVID-prosjektet skiller seg fra det som har vært anbefalingene ellers i bransjen primært på ett punkt: fokus på informasjonsverdier. I tillegg bidrar DeVID-prosjektet med sjekklister som kan benyttes underveis i arbeidet. Basert på erfaringer fra analyser utført i bransjen er det vanskelig å si om et fokus på informasjonsverdier gir bedre analyser. Det er en forskjell i hvilke hendelser som blir identifisert, om man sammenligner med tidligere analyser. Det er imidlertid ikke mulig å si om resultatet nå er bedre. Vi har brukt denne veiledningen til å gjennomføre risikoanalyser hos to ulike nettselskap, og tilbakemeldingene fra deltakere viser at de opplevde det som nyttig å bli bevisst informasjonsverdiene i systemet.

Kompetanse er helt klart det som peker seg ut som den største utfordringen for å få til gode risikoanalyser. Flere nettselskap opplever kompetanseutfordringer knyttet til informasjonssikkerhet og personvern. Sjekklistene kan benyttes for å bøte på dette, spesielt når det gjelder å identifisere hendelser og tiltak. Estimering av sannsynlighet og konsekvens for hendelser er likevel vanskelig. Dette kan ikke løses av sjekklister alene. Det mangler dessuten erfaringsdata for AMS, noe som øker kravene til kompetanse; man må forstå de tekniske mulighetene og begrensningene, samt trusselbildet. Prioritering av informasjonsverdier kan bidra inn i vurderingen av konsekvens.

Basert på våre erfaringer er det behov for støtte til å gjennomføre slike risikoanalyser. Mye av det som trengs av støtte er ikke nødvendigvis spesifikt for enkeltorganisasjoner eller enkeltsystemer, og kan derfor gis i form av en veiledning. Samtidig vil det alltid være behov for å vurdere alle aspektene i lys av hvert enkelt selskaps infrastruktur, systemer, løsninger, og ikke minst akseptabelt risikonivå. En veiledning vil derfor aldri kunne framstå som noe mer enn en veiledning. Hvert selskap er nødt til å gjøre sine egne vurderinger.

4 Referanser

1. *Risikovurdering av AMS. Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS.* SINTEF, 2012. ISBN 978-82-14-05280-0.

2. *Security Threats in Demo Steinkjer. Report from the Telenor-SINTEF collaboration project on Smart Grids.* SINTEF, Telenor, NTE, Aidon, 2012. ISBN 978-82-14-05301-2.

3. *Overordnet risiko- og sårbarhetsanalyse for innføring av AMS.* Proactima, Energi Norge, 2012. PT-1070549.

4. *Veileder til sikkerhet i AMS.* NVE, 2012.

5. *Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen.* Proactima, NVE, 2010. ISSN 1501-0678.

6. *Eksempelsamling. Risiko- og sårbarhetsanalyser for kraftforsyningen.* Proactima, NVE, 2012. ISBN: 978-82-410-0802-3, ISSN: 1501-2832.

7. *Veiledning til forskrift om beredskap i kraftforsyningen.* NVE, 2011. ISSN 1501-0678.

8. *Risikovurdering av informasjonssystem med utgangspunkt i forskrift til personopplysningsloven.* Datatilsynet. 2002.

9. *Sjekkliste for informasjonssikkerhet i kraftforsyningen.* NVE

10. *Håndbok for informasjonssikkerhet,* NorSIS, Nettutgave, www.norsis.no

11. *Sertifisering av IT-sikkerhet,* Nettutgave, www.sertit.no

12. ISO/IEC 15408 – Evaluation Criteria for IT Security – The Common Criteria, www.commoncriteriaportal.org

13. R. A. Caralli, J. F. Stevens, L. R. Young, W. R. Wilson, *The OCTAVE Allegro guidebook, v1.0*. Software Engineering Institute (SEI), Mai 2007, www.cert.org/octave/allegro.html

14. *Metode og verktøy for en samlet risikovurdering av kritiske infrastrukturer. Sluttrapport for DECRIS.* SINTEF A11636. www.sintef.no/decris

15. *NISTIR 7628: Guidelines for Smart Grid Cyber Security, Vol. 3, Supportive Analyses and References*, The Smart Grid Interoperability Panel – Cyber Security Working Group, August 2010. www.nist.gov

16. I. A. Tøndel, M. B. Line, G. Johansen, M. G. Jaatun, *Risikoanalyse av AMS knyttet til informasjonssikkerhet og personvern*, NEF Teknisk Møte 2014, s. 315-323

17. *Veileder i sikkerhetsarkitektur for virksomheter som behandler personopplysninger og sensitive personopplysninger*, Datatilsynet, August 2011.

18. *ISO/IEC 27001:2013 – Information Security Management Systems – Requirements*

A Sjekklister

Ulike sjekklister kan være til støtte ved gjennomføring av en risikoanalyse. I dette kapitlet presenterer vi flere som kan brukes. Anerkjente standarder inneholder noen som vi henviser direkte til, mens noen har vi utviklet og/eller tilpasset selv, fortrinnsvis basert på anerkjente standarder. Alt vi presenterer her, er ment å være direkte støtte til å gjennomføre en risikoanalyse knyttet til informasjonssikkerhetsmessige utfordringer, mens Energi Norges rapport [3] dekker AMS i et bredere perspektiv.

A.1 Relevante standarder

ISO/IEC 27005:2011 – Information Security Risk Management[1]– beskriver en komplett metode for risikoanalyse; hvilke prosesser og aktiviteter som inngår i dette arbeidet. Den sier derimot lite om hvordan man skal gå fram. Veiledningen fra NVE [5] gir imidlertid en metodebeskrivelse som er spesifikt tilpasset oppfyllelse av Beredskapsforskriften [7].

The OCTAVE Allegro Guidebook[2]- denne er utviklet ved Software Engineering Institute, Carnegie Mellon University, USA, og er et eksempel på *hvordan* man kan gå fram for å gjøre en risikoanalyse. Den gir helt konkret støtte til å vurdere alle mulige trusler knyttet til *en* informasjonsverdi. Det kan være nyttig å bruke denne på to-tre informasjonsverdier til å begynne med, for å få gode idéer til hva som bør inkluderes. Appendiks 3 i The OCTAVE Allegro Guidebook presenterer flere spørreskjema som kan bidra til å kartlegge på hvilke måter en informasjonsverdi kan skades. Spørreskjemaene dekker både elektronisk lagring, fysiske omstendigheter og menneskene som behandler informasjonen.

ISO/IEC 27001:2013 –Information Security Management Systems – Requirements[1] [18]– beskriver et komplett styringssystem for informasjonssikkerhet i en organisasjon. Standarden inneholder en omfattende liste av tiltak som anbefales vurdert, og et utdrag av denne listen er inkludert i vedlegg D. Alle tiltakene vil kanskje ikke være relevant å vurdere når det gjelder AMS og tilgrensende IKT-systemer, men listen kan likevel med fordel brukes som en sjekkliste, hvor man for hvert tiltak vurderer relevans og behov. Mens 27001 omhandler selve styringssystemet for informasjonssikkerheten, fokuserer ISO/IEC 27002 på tiltakene.

ISO/IEC 15408 – Evaluation Criteria for IT Security[3] – vanligvis kalt Common Criteria [12] – støtter evaluering og sertifisering av programvare utifra et informasjonssikkerhetsperspektiv. Det finnes ulike evalueringsnivå, og jo høyere nivå man følger, jo strengere er kravene gjennom hele utviklingsprosessen. En sertifiseringsprosess tar ofte lang tid, og man risikerer at når evalueringen endelig er klar, er produktet (eller i det minste den versjonen som er evaluert) utdatert. Men Common Criteria inneholder mye bra som kan brukes underveis i utviklingsprosessen i forhold til å spesifisere sikkerhetskrav. Det er SERTIT[4] som er offentlig sertifiseringsmyndighet i Norge.

Security Profile for Advanced Metering Infrastructure[5] – er utarbeidet av The Advanced Metering Infrastructure (AMI-SEC) Task Force som ble etablert i 2007 for å utvikle konsistente sikkerhetsretnings-linjer for AMI. Sikkerhetsprofilen er generell og i liten grad benyttet i dette prosjektet. NVEs *Veileder til sikkerhet i avanserte måle- og styringssystem* [4] er mer målrettet og relevant for utrulling av AMS i Norge.

[1] Denne kan kjøpes fra Norsk Standard, www.standard.no
[2] Denne kan lastes ned gratis fra http://www.cert.org/octave/allegro.html
[3] Denne kan lastes ned gratis fra www.commoncriteriaportal.org
[4] SERTIT: www.sertit.no
[5] Denne kan lastes ned gratis fra www.osgug.ucaiug.org

A.2 Informasjonsverdier

En visualisering eller beskrivelse av ulike typer informasjonsverdier kan være nyttig. Nedenfor er et forslag til hvordan dette kan gjøres. Tabell A-1 viser noen informasjonsverdier man typisk vil finne for AMS. Vi har markert hvilke av egenskapene konfidensialitet, integritet, tilgjengelighet og personvern som kan være relevante for hver av dem. I kolonnene *Lagres, Prosesseres og Kommunikasjon* kan det beskrives hvilke systemkomponenter som er involvert i behandlingen av hver informasjonsverdi.

I tabellen har vi foreslått at man gjør en vurdering på kritikalitet. Vi ønsker imidlertid ikke å gi en eksempelvurdering, men lar dette være opp til selskapene selv å vurdere. For ulike typer personopplysninger, er det den som er behandlingsansvarlig i henhold til personopplysningsloven som må vurdere kritikalitet og bestemme nødvendig beskyttelsesnivå. Forøvrig er det viktig at hvert selskap selv går gjennom hele listen, vurderer om de nevnte informasjonsverdiene er relevante, om flere bør legges til, og om klassifiseringen stemmer i hvert tilfelle.

Som bakgrunn for analysen bør man også ha en oversikt over hvor lenge ulike typer data og nøkler lagres.

Tabell A-1 Ulike informasjonsverdier med tilhørende attributter – eksempel på vurdering

	Informasjonsverdi	Konfidensialitet	Integritet	Tilgjengelighet	Personvern	Kritikalitet	Lagres[1] (varighet)	Prosesseres[1]	Kommunikasjon[2]
D1	Måleverdi (enkeltkunde) med målerID	X	X		X				
D2	Målerverdier (mange kunder) med målerID	X	X	X	X				
D3	Tidsserier som viser forbruksmønster (anonymiserte)								
D4	Tidsserier som viser forbruksmønster (ikke anonymiserte)	X			X				
D5	Navn og adresser				X				
D6	Navn, adresser og målerID				X				
D7	Navn, adresser, målerID og periodisk forbruk (Faktura)	X			X				
D8	Krypteringsnøkkel[3]	X	X	X					
D9	Kontrollmeldinger, inkludert bryter/strupe kontrollmeldinger		X	X					
D10	Software/firmware	(X)	X	X					
D11	Software/firmware oppdateringer	(X)	X	X					
D12	Alarmer		X	X					
D13	Prisinformasjon		X						
D14	Autentiseringsinformasjon	X	X	X	(X)				

[1] I kolonnene "Lagres" og "Prosesseres" kan systemnavn føres inn. Det bør også angis hvor lenge data lagres.
[2] Kommunikasjonskanal kan synliggjøres med henvisning til figur.
[3] Ulike typer krypteringsnøkler kan ha ulik kritikalitet og dermed behov for egne rader i tabellen.

A.3 Uønskede hendelser

Med uønskede hendelser mener vi informasjonssikkerhetsbrudd, det vil si brudd på konfidensialitet, integritet eller tilgjengelighet.

Uønskede hendelser kan grovt deles inn i tre typer basert på årsak:

- *Tilfeldige hendelser:* Dette er hendelser som skjer tilfeldigvis eller ved uhell. Eksempler kan være lynnedslag, svikt i strømforsyning, brann, diskcrash, kommunikasjonsfeil og menneskelige feil.

- *Generelle angrep:* Disse skjer ved at man blir et tilfeldig offer for et eller flere av de angrepene som til stadighet spres på Internett. Generelle angrep er ikke rettet mot et spesielt IKT-system, men heller mot IKT-system generelt. De kan ha som mål å få tilgang til konfidensiell informasjon, samle personopplysninger for salg og bruk til svindel, tilgang til prosessorkraft, tastelogging for å samle brukernavn og passord, logge en brukers nettaktivitet for å lage en markedsføringsprofil, kryptere filer for så å kreve penger for dekryptering. Ondsinnet kode (malware) brukes typisk til slike angrep. Spredning av malware kan foregå via e-post, nettsider, fildelingstjenester, minnepinner og andre kanaler.

- *Målrettede angrep:* Disse er rettet mot et spesielt system, med mål om å ramme en spesiell organisasjon eller en spesiell samfunnsfunksjon. Dette kan være alt fra fysiske angrep til angrep via Internett. Angripere som forsøker seg på målrettede angrep gjennom IKT-infrastrukturen, er ofte dedikerte og har god kunnskap om systemene det gjelder. De kan bruke kombinasjoner av teknikker, f.eks. avlytte kommunikasjonslinjer, datainnbrudd, manipulere kontrollsystemer, samle informasjon fra ansatte gjennom sosial manipulering som så brukes videre for å få tilgang til systemer. Egne ansatte kan også være delaktige i slike angrep. Ondsinnet kode (malware) er et av flere verktøy som typisk brukes til slike angrep.

Som støtte til å komme på hva som kan gå galt i IT-systemet kan man ta utgangspunkt i lister over hendelsestyper, og se om de er relevante for informasjonsverdiene og de teknologiene som benyttes for lagring, prosessering og overføring av disse verdiene.

Tabell A-2 Liste over hendelsestyper sortert på årsak (basert på tabell i ISO/IEC 27035:2011)

Hendelseskategori	Beskrivelse	Eksempel
Naturkatastrofe	Naturkatastrofe man ikke rår over.	Jordskjelv, flom, kraftig vind, lynnedslag, kollaps/sammenbrudd.
Sosial uro	Ustabilitet i samfunnet.	Terrorisme, krig.
Fysisk skade	Skade pga. fysiske handlinger, enten forsettlig eller ved uhell.	Brann, vannskader, dårlig miljø (forurensing, støv, frost), ødeleggelse av utstyr, tyveri av utstyr, fikling med utstyr.
Svikt i infrastruktur	Svikt i systemer og tjenester som støtter informasjonssystemene.	Strømbrudd, nettverksfeil, feil på air-condition.
Strålingsforstyrrelse	Forstyrrelse på utstyr pga. stråling.	Elektromagnetisk stråling, jamming, varmestråling.
Teknisk feil	Feil i informasjonssystemet eller relaterte ikke-tekniske innretninger, inkludert menneskelige feil som resulterer i utilgjengelighet eller ødeleggelse av informasjonssystemet.	Maskinvarefeil, programvarefeil, overbelastning, tap av vedlikeholdsevne.
Skadevare (malware)	Infeksjon av skadevare på systemet fører til tap av konfidensialitet, integritet eller tilgjengelighet av data, og/eller påvirker normal operasjon av systemet.	Virus, ormer, trojanske hester, spionvare, ondsinnet kode på nettsider.
Teknisk angrep	Angrep på systemet via nettverk eller på andre tekniske måter, enten ved å utnytte sårbarheter i systemet (konfigurasjoner, protokoller eller programmer) eller med makt.	Scanning av nettet, utnyttelse av sårbarheter, utnyttelse av bakdører, forsøk på å logge inn, tjenestenektangrep, angrep på kommunikasjonskanalen.
Brudd på regler	Brudd på regler, enten forsettlig eller ved uhell.	Bruk av ressurser til andre formål enn tiltenkt, brudd på opphavsrett.
Kompromittering av funksjoner	Kompromittering av funksjoner i informasjonssystemet, når det gjelder sikkerhet – enten forsettlig eller ved uhell.	Misbruk av rettigheter, skaffe seg rettigheter man ikke har, nekte for handlinger man har utført, brudd på tilgjengelighet av personell.
Kompromittering av informasjon	Kompromittering av informasjon, enten konfidensialitet, integritet eller tilgjengelighet – forsettlig eller ved uhell.	Avlytting av kommunikasjon, sosial manipulering, phishing, gjøre data kjent offentlig, tap av data, tyveri av data, uautorisert modifisering av data, feil ved registrering eller prosessering av data, deteksjon av hvor sensitive data eller systemer er lokalisert.
Skadelig innhold	Spredning av uønsket innhold, slik at det skader nasjonal sikkerhet, sosial stabilitet og/eller allmennsikkerhet.	Ulovlig innhold, innhold egnet til å skape panikk, innhold som angriper samfunnet eller personer, spam.

I Tabell A-3 gir vi noen eksempler på uønskede hendelser som er relevante for AMS og kategoriserer disse ut ifra hva slags type brudd de representerer.

Tabell A-3 Eksempler på uønskede hendelser relevante for AMS

Uønsket hendelse	Konfidensialitet	Integritet	Tilgjengelighet	Personvern
Svikt i infrastruktur				
Gravemaskin kutter kommunikasjonskabler			X	
Brann, vannskader, ødeleggelse av utstyr hos nettselskap rammer baksystemene			X	
Teknisk feil				
Komponentsvikt; massiv utskiftning av komponenter			X	
Falske alarmer sendt fra målere		X		
Feil i innsamlede måledata		X		X
Viktige alarmer og statusmeldinger kommer ikke frem			X	
Måleverdi registreres ikke			X	
Feil i prisinformasjon eller måleverdi kommunisert mot kunder		X		
Måler responderer ikke på kontrollmeldinger			X	
Programvareoppdatering feiler; forårsaker feil på måler	X	X	X	X
Skadevare (malware)				
Malware eller systematisk feil medfører at målere jammer hverandre slik at ingen fornuftig kommunikasjon virker			X	
Sikkerhetshull i programvare utnyttes av generelle angrep (malware); enten i baksystemer, nettstasjon eller enkeltmålere	X	X	X	X
Ransomware – malware som krypterer filer, angriper krever betaling for dekryptering			X	
Teknisk angrep				
Montørenhet på avveie brukes for å få tilgang til måler	X	X	X	X
Falsk programvareoppdatering installert på målere	X	X	X	X
Krypteringsnøkler slettes			X	
Angriper etablerer uønskede kanaler for informasjonsflyt	X	X	X	X
Tjenestenektangrep mot baksystemene rammer evnen til å kommunisere			X	
Kompromittering av funksjoner				
Uautorisert bruk av bryte-funksjon		X		
Uvedkommende får tilgang til og endrer data i baksystemer	X	X	X	X
Kompromittering av informasjon				
Kunde manipulerer måledata (egne eller andres)		X		
Forbruksdata for identifiserte forbrukere på avveie resulterer i presseoppslag	X			X
Utro tjener selger informasjon til kriminelle	X			X
Utro tjener bruker sin tilgang til systemet til angrep eller spredning av sensitiv informasjon	X	X	X	X

A.4 Interessenter

Denne listen med ulike interessenter kan hjelpe med å utvide perspektivet. Det er nyttig å tenke gjennom alle mulige aktører når man skal kartlegge årsaker til en hendelse, samt ved vurdering av sannsynlighet og konsekvens. Kanskje er det flere enn man først kommer på som kan ha interesse av et informasjons-sikkerhetsbrudd; enten av å utføre noe selv eller som kan bli påvirket av det på et vis. Jo flere som kan ha interesse av en hendelse, jo større vil sannsynligheten være for at den inntreffer.

Eksempler på interessenter:

- Nettselskapet
- Eiere av nettselskapet
- Lokale styresmakter, politikere
- Nasjonale styresmakter, politikere
- Utenlandske styresmakter
- Media, journalister
- Privatkunder
- Bedriftskunder
- Borettslag, boområder
- Målerleverandører
- Driftssystem-leverandører
- IKT-system-leverandører
- Selgere av informasjon i markedsøyemed
- Ulike grupper internt i nettselskapet: toppledelsen, mellomledere, alle ansatte, SCADA-operatører, montører ute
- Kraftprodusenter
- NVE
- Statnett
- Konsulenter, forskere
- Teleoperatør
- Fagforeninger
- Organiserte hackermiljøer
- Privatetterforskere

A.5 Typiske svakheter og sårbarheter i IKT-systemer

IKT-systemer, rutinene som omslutter dem og menneskene som bruker dem, er forskjellige. Denne listen gir en oversikt over typiske sårbarheter eller svakheter man kan finne for IKT-systemer. Listen er basert på en guide til IKT-sikkerhet i smart grid utgitt av National Institute for Standards and Technology (NIST) – NISTIR 7628, vol. 3 [15].

En vurdering av svakhetene til systemet er viktig for å kunne gi et godt estimat av sannsynlighet og konsekvenser av hendelser.

Sårbarhetsklasse 1: Mennesker, policy, prosedyrer

- Mangelfull trening
- Mangelfulle bakgrunnssjekker av personale
- Sikkerhetspolicy og/eller personvernspolicy er ikke god nok
- Prosedyrer for å sikre at man har oppdatert programvare er ikke tilstrekkelige
- Endringshåndtering og håndtering av konfigurering er ikke god nok
- Unødvendige tilgangsrettigheter i systemet
- Mangelfull risikohåndtering, f. eks. ved at ledelsen er for lite involvert, mangelfulle beredskapsplaner eller prosesser for hendelseshåndtering, utilstrekkelig med sikkerhetsgjennomganger.

Sårbarhetsklasse 2: Sårbarheter i programvare/firmware

- For dårlig kvalitet på koden slik at den blir uforutsigbar (kan gi problemer med brukergrensesnitt og muligheter for angripere)
- Muligheter for å omgå autentisering eller autoriseringsløsninger
- Sårbarhet i krypteringen
- Feilhåndtering i programvare gjort på en slik måte at angripere kan få tilgang til informasjon eller funksjonalitet de kan bruke videre
- Logiske feil eller bugs i programvaren
- Prosesser og rutiner i virksomheten passer ikke med prosessene som programvaren legger opp til, noe som gjør at systemet ikke blir bruk som tiltenkt
- Input- og outputdata blir ikke tilstrekkelig sjekket – noe som åpner for en rekke angrep
- Logging er mangelfull, eller kan omgås
- Passord blir ikke håndtert på en god nok måte
- Angripere kan få tilgang til filer de ikke var ment å få tilgang til gjennom å skrive inn eller endre sti/ link til data
- Svakheter i protokoller eller implementasjon av disse
- Mangelfull håndtering av sesjoner

Sårbarhetsklasse 3: Plattformsårbarheter

- Sikkerhetsarkitektur og -design er ikke god nok, og er f.eks. basert på "security by obscurity" eller bruker hjemmesnekrede eller dårlig standardiserte løsninger.
- Manglende beskyttelse mot ondsinnet kode
- Implementert sikkerhetsfunksjonalitet er ikke aktivert
- Nødvendige sikkerhetsoppdateringer er ikke tilgjengelige fra leverandør
- Tjenester er installert, aktivert og kjører selv om det ikke er behov for dem
- Sikkerhetsmekanismer er dårlig konfigurert

Sårbarhetsklasse 4: Nettverk

- Manglende sjekking av integritet av protokoll- og meldingsdata
- Mangelfull inndeling i nettverkssoner, eller manglende kontroll av trafikk som sendes mellom soner
- Dårlig valg av protokoll
- Svakheter i autentiseringsprosesser eller i hvordan autentiseringsnøkler håndteres
- Ikke nok redundans
- For lett å få fysisk tilgang til komponenter

A.6 Typiske sikkerhetsmekanismer

I det følgende gir vi en beskrivelse av generelle og viktige sikkerhetstiltak. Store deler av teksten er hentet fra Norsk senter for informasjonssikrings (NorSIS) sikkerhetsleksikon[1]. For en oversikt over ytterligere sikkerhetstiltak henvises det til vedlegg D og NVEs veileder [4].

Antiviruskontroll
Programvare som søker gjennom filer og datamaskinens minne for å finne og fjerne datavirus. Det er også vanlig å installere antivirusprogramvare på eposttjeneren eller brannmuren for å oppdage virus som kommer inn via internett. Antivirus fjerner ikke bare datavirus, men som oftest også mange andre former for malware som f.eks ormer, trojanere, spyware osv. dette avhenger litt av hvor avansert antivirus programmet er.
Alle datamaskiner som er koblet til et nettverk bør ha antivirus installert. Det samme gjelder en enkeltstående datamaskin hvor minnepinner eller andre flyttbare medier benyttes for filoverføring. Dette er en svært rimelig sikkerhetsmekanisme som kan hindre et stort antall generelle angrep, samt en del målrettede angrep.

På datamaskiner som kjører spesialisert programvare utover vanlige kontorsystemer, kan det være nødvendig å teste oppdateringer framfor å installere dem direkte fra leverandør. Dette vil imidlertid kreve ressurser og tid, så rutinene for oppdateringer må bestemmes ut ifra beskyttelsesbehovet.

Brannmur
En brannmur er enten et program som ligger på datamaskinen eller en fysisk boks som står mellom to nettverk. Den kan beskytte mot angripere utenfra ved å filtrere bort ondsinnet nettrafikk.

Hendelseshåndtering
Uansett hvilke sikkerhetsmekanismer man velger å implementere, må man alltid være forberedt på at uønskede hendelser kan inntreffe. Trusselbildet er i stadig endring, og det er helt umulig å beskytte seg mot alt. Derfor må organisasjonen være i stand til å oppdage og håndtere uønskede hendelser. Standarden ISO/IEC 27035 Information Security Incident Management gir en grundig beskrivelse av hendelses-håndteringsprosessen inndelt i fem ulike faser: planlegging, deteksjon, vurdering, respons og evaluering. Denne er imidlertid hovedsakelig rettet mot dedikerte respons-team/IT-sikkerhetsavdelinger. Vi anbefaler derfor at man tenker bredere enn standarden og jobber kontinuerlig for å sikre at hele organisasjonen er godt trent for å oppdage uønskede hendelser på et tidlig stadium og respondere ut ifra hendelsens art og omfang.

HTTPS
HTTPS er en sikker utgave av HTTP. Den sikrer kommunikasjonen mellom klient og tjener med kryptering, ved bruk av Secure Socket Layer (SSL) eller Transport Layer Security (TLS). Når du er inne på en nettside sikret med HTTPS, blir begynnelsen av adressen i nettleseren endret fra «http://» til «https://»

Intrusion Detection Systems (IDS)
IDS er programvare som følger med trafikken på nettverket og logger unormale hendelser. Et IDS vil kun logge hendelser, men ikke gjøre noe for å stoppe dem. Det finnes tre typer IDS: nettverksbasert, vertsbasert og applikasjonsbasert. Nettverksbasert IDS overvåker trafikken på nettverket, vertsbasert IDS overvåker trafikken på en enkelt klient eller server, mens applikasjonsbasert IDS overvåker en applikasjon.

Nettverksbasert
Fordeler: Kan overvåke hele nettverket med få noder/sensorer. Enkle å sikre mot angrep, kan også være usynlige for angripere.
Ulemper: Klarer ikke alltid å analysere alle pakker dersom det er mye trafikk på nettet. Kan ikke analysere krypterte data.

[1] www.norsis.no/leksikon

Vertsbasert
Fordeler: Kan analysere og gi detaljert informasjon om hva som skjer på en enkelt maskin. Kan identifisere hvilke prosesser og brukere som utfører angrep. Kryptert nettverkstrafikk er blitt dekryptert når den kommer til denne IDSen og kan dermed analyseres.
Ulemper: Krever mye tilsyn, genererer mye data for hver datamaskin. Er sårbare for angrep.

Applikasjonsbasert
Fordeler: Kan se på interaksjonen mellom brukerne og applikasjonen. Kan lese data som applikasjonen holder kryptert.
Ulemper: Veldig sårbar for angrep. Ikke god til å oppdage endringer i programmet som kan forårsakes av skadelig kode.

Intrusion Prevention Systems (IPS)
IPS er programvare som følger med trafikken på nettverket og stopper unormale hendelser. Et IPS gjør det samme som et intrusion *detection* system, men i stedet for kun å logge hendelsene, vil den kunne sette i gang tiltak som en respons på hendelsen. Et godt IPS vil kunne stoppe flere angrep enn en vanlig brannmur.

Kryptering
Å kryptere vil si å gjøre en leselig tekst uleselig for andre ved hjelp av en matematisk funksjon (krypterings-teknikk/algoritme) og en forhåndsbestemt nøkkel. Å dekryptere vil si å oversette en kryptert tekst tilbake til lesbar tekst ved hjelp av en matematisk funksjon (krypterings- teknikk/algoritme) og en forhåndsbestemt nøkkel.

Symmetrisk kryptering er basert på én enkelt krypteringsnøkkel. Den samme nøkkelen brukes både til kryptering og dekryptering. Asymmetrisk kryptering er basert på et matematisk relatert nøkkelpar istedenfor én enkelt krypteringsnøkkel. Den ene nøkkelen er privat og skal holdes hemmelig av eieren, mens den andre nøkkelen er offentlig og kan sendes til alle som ønsker en kopi. Asymmetrisk kryptografi gjør det mulig å kryptere med den ene nøkkelen, og dekryptere med den andre.

Sertifikater
Certificate Authority (CA): Et firma eller en organisasjon som utsteder og vedlikeholder digitale sertifikater for bruk av andre. En CA garanterer at identiteten på sertifikatet stemmer overens med identiteten til den som har bestilt sertifikatet. En CA blir ofte omtalt som en tiltrodd tredjepart (trusted third party).

Sikkerhetsoppdatering
Oppdatering av programvare for å rette en feil eller mangel som kan utnyttes av en angriper. Programvare-leverandører gir jevnlig ut sikkerhetsoppdateringer til sine produkter, og disse bør installeres så snart som mulig. Det er imidlertid behov for å teste slike oppdateringer for å se hvordan de eventuelt påvirker annen programvare på maskinen, spesielt i miljøer hvor det er ekstremt høye krav til oppetid/tilgjengelighet.

Dersom maskinvaren eller annen programvare er av en slik art at nye sikkerhetsoppdateringer ikke er mulig å installere, må andre sikkerhetsmekanismer implementeres. Dette kan være brannmurer, plassering i sikrere soner, deteksjonssystemer eller annet.

Sikkerhetsrevisjon
En sikkerhetsrevisjon er en gjennomgang av et system for å stadfeste at det tilfredsstiller de sikkerhetskrav som stilles til det[1]. Formålet med å gjennomføre sikkerhetsrevisjon er å:

- Kontrollere at det er gjennomført nødvendige sikkerhetstiltak
- Verifisere at sikkerhetstiltakene fungerer
- Kontrollere at lover og regler om informasjonssikkerhet følges

[1] Kilde: Norm for informasjonssikkerhet i helsesektoren

- Sikre at etablerte prosedyrer for sikkerhet benyttes og fungerer etter hensikten

Soneinndeling
Ulike digitale tjenester har ulike krav til sikkerhetsnivå. En organisasjon kan derfor etablere flere nettverkssoner, hvor hver sone tilfredsstiller et gitt sikkerhetsnivå. Kontrollsystemer vil typisk plasseres i en mye sikrere sone enn tjenester som støtter samarbeid med eksterne organisasjoner. Datatilsynet har utgitt en veileder i sikkerhetsarkitektur for virksomheter som behandler personopplysninger og sensitive personopplysninger [17].

SSL – Secure Sockets Layer
Protokoll for autentisering og kryptering av nettverkskommunikasjon. SSL er den mest brukte protokollen for å opprette sikre nettverksforbindelser over Internett.

Tilgangskontroll
Tilgangskontroll er en kombinasjon av identifisering, autentisering og autorisering.

Identifisering er å gi seg til kjenne. Når man logger seg på datamaskinen, identifiserer man seg først ved å angi brukernavn, så autentiserer man seg med å angi passord.

Autentisering vil si å bevise at man er den man utgir seg for å være. Autentisering skal bekrefte en påstått identitet. Dette kan skje gjennom noe du vet (passord), noe du er (fingeravtrykk/ biometri) eller noe du har (nøkkelkort). To faktor-autentisering, også kalt sterk autentisering benyttes når to av disse metodene benyttes i kombinasjon. Den som autentiseres kan være en person som bruker en datamaskin, kun en datamaskin eller et program.

Autorisering er prosessen med å beslutte å gi en person, en datamaskin eller et program tillatelse til å bruke bestemte IT-ressurser. Eksempler på en IT-ressurs kan være filer, nettverksstasjoner og prosesser.

A.7 Rapportmal

Denne malen kan benyttes som struktur på en rapport om risikoanalysen.

Sammendrag
Beskrivelse av de viktigste resultatene og videreføring av arbeidet.

1. **Introduksjon**
   Beskrivelse av hva som gjøres, hvorfor det gjøres og for hvem det gjøres. Evt. mandat for analysegruppa gjengis eller refereres til.

2. **Metode**
   Kort beskrivelse av metoden som benyttes. Hvilke møter er avholdt. Deltagerliste.

3. **Risikoanalyse**
   3.1 Systembeskrivelse.
   Skisser og tekst som beskriver systemet og avgrensinger av oppgaven. Detaljerte beskrivelser av deler av systemet eller funksjonalitet inkluderes eller refereres til dersom dette er nødvendig for å forstå de vurderinger som er gjort. Forutsetninger må dokumenteres.
   3.2 Konsekvens- og sannsynlighetsdimensjoner
   Tabeller som viser hvilke konsekvens- og sannsynlighetsdimensjoner som benyttes i analysen.
   3.3 Informasjonsverdier
   Liste over informasjonsverdier. De som blir valgt ut for videre analyse, beskrives detaljert.
   3.4 Uønskede hendelser/trusler
   De uønskede hendelsene som ble identifisert i møtet listes opp. Dersom alle fremgår av risikomatrisen, kan man evt. henvise til denne.
   3.5 Identifiserte tiltak
   En liste over eksisterende og planlagte tiltak som man tok høyde for ved fastsettelse av sannsynlighet og konsekvens.
   3.6 Risikovurdering
   Presentasjon av risikomatrisene. Dette kan for eksempel gjøre som vist i Tabell A-4 og Tabell A-5.

4. **Forslag til tiltak**
   Analysegruppas forslag til tiltak, utover eksisterende og allerede planlagte, listes opp.

5. **Diskusjon/Konklusjon**
   Erfaringer fra analysemøtene bør dokumenteres. Videre arbeid beskrives.

Tabell A-4 Risikomatrise

Sannsynlighet			
Høy	A3	B3	C3
	A2	B2	C2
Lav	A1	B1	C1
	Lav		Høy
	Konsekvens		

Tabell A-5 Risikovurdering

ID	Trussel/Hendelse	Forsynings-sikkerhet	Økonomisk risiko	Omdømme-risiko
1	Innkobling fører til uheldige hendelser	A1	C1	C2
2	Feil prissignaler	A2	A1	B2
3	Hacking av ...	A2	B2	C2
4	...	B1	A2	C1
5	...	B1	B1	C1
6	...	B2	A2	A3
7	...	C1	C2	C1
8	...	C1	B1	C1
9	...	C1	C1	C1
10	...	C1	C1	C1
11	...	C1	B1	B2
12	...	C2	B1	B2
13	...	C2	C1	C1
14	...	Ikke relevant	C2	C2

Tabell A-4 viser en generell 3x3 risikomatrise. Fargebruken må tilpasses det enkelte selskap. Generelt gjelder at rød sone representerer en uakseptabel risiko hvor tiltak må iverksettes for å bringe risiko ned i gul eller grønn sone.

I Tabell A-5 er all risiko presentert i en tabell som dekker alle konsekvensdimensjoner. Dette gir en svært god totaloversikt.

B Detaljanalyser

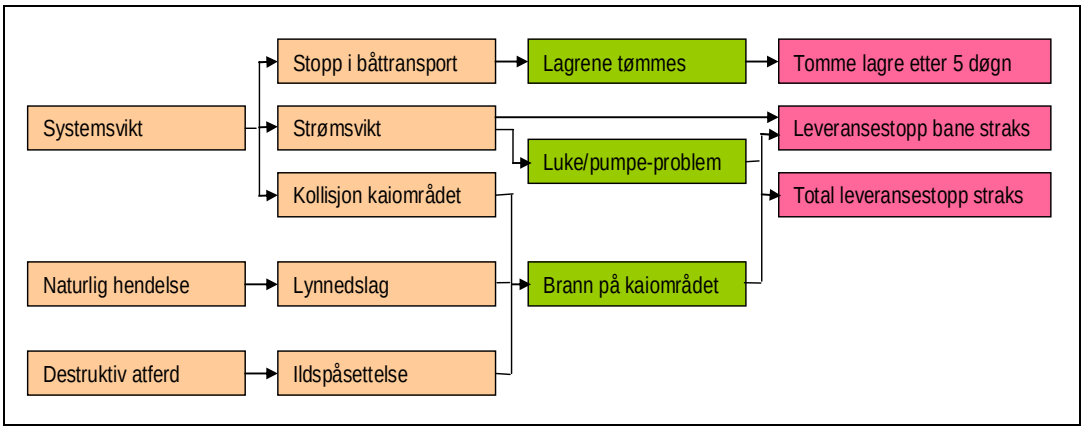
Detaljanalyser kan benyttes for det man innledningsvis antar har høy risiko, men kan også være nyttige for å øke organisasjonens kunnskap om systemet, dokumentere systemet, eller besvare spørsmål i hovedanalysen. Noen av de nedenstående eksemplene er fra andre domener enn AMS.

B.1 Barriereanalyse

Hensikten med en barriereanalyse er å identifisere eksisterende barrierer og status for disse. Eksempler på slike barrierer er fysisk beskyttelse, adgangskontroll og redundans. Barrierer bør kategoriseres etter hvilke årsaker de skal forhindre. Svikt i barrierer kan analyseres ved hjelp av feiltreanalyse (Fault Tree Analysis, FTA) hvor barrieresvikt er topphendelsen.

B.2 Årsaksanalyse

Hensikten med en årsaksanalyse er å identifisere alle mulige årsaker til den uønskede hendelsen. Også til dette kan feiltreanalyse benyttes som metode. Figur B-1 er et eksempel på en type årsaks-/konsekvensanalyse. Dette diagrammet gir på et overordnet nivå en oversikt over årsaker til tre "hovedhendelser" (grønt i figuren): *Lagrene tømmes*, *luke/pumpe-problem*, *brann på kaiområdet*, og gir samtidig tre mulige konsekvenser (rødt) med hensyn til leveringssikkerhet, som følge av disse tre hendelsene.



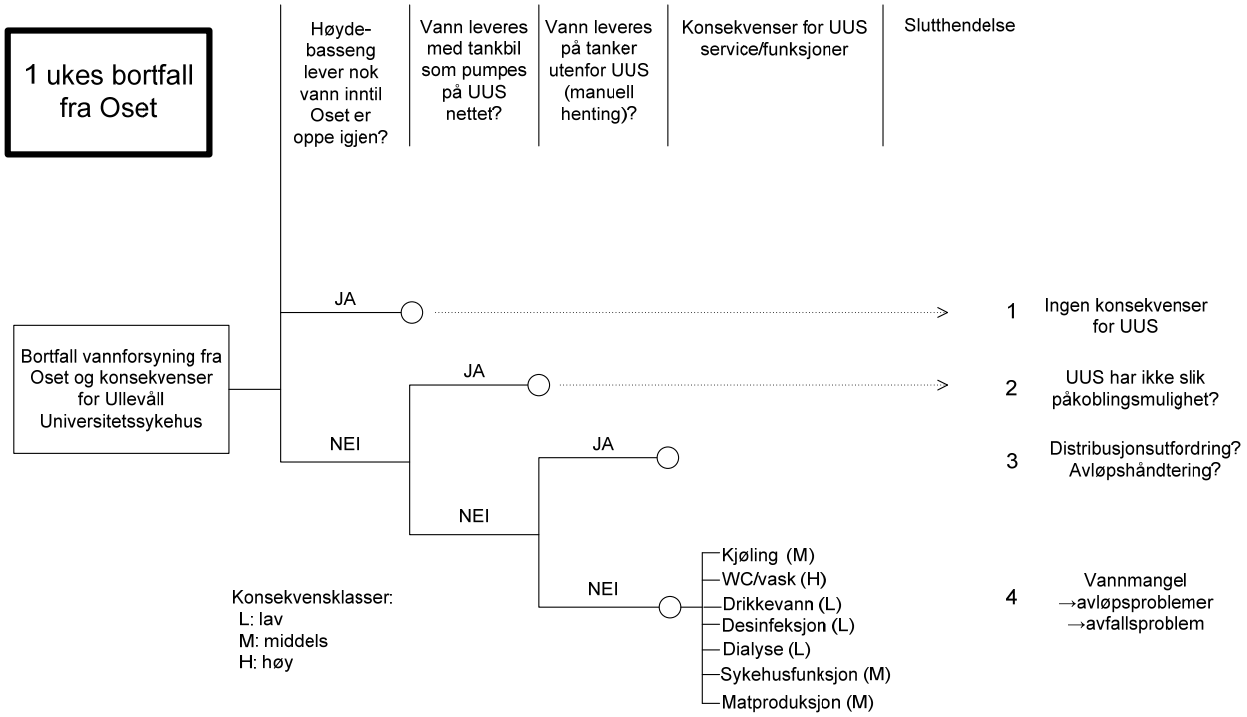
Figur B-1 Overordnet årsaks-/konsekvensdiagram for leveringssikkerhet fra en oljeterminal [1]

B.3 Konsekvensanalyse

Det er viktig å identifisere alle mulige konsekvenser av en uønsket hendelse. Konsekvensdimensjoner som drepte og skadde, miljøkonsekvenser, materielle skader og omdømmetap kan typisk inkluderes. Til dette brukes ofte hendelsestreanalyse (Event Tree Analysis, ETA). Ved en slik analyse kan man beregne sannsynligheter for de ulike konsekvensene.

Figur B-2 viser et eksempel på et ETA-diagram. Her vil første oppgave være å definere selve hendelsen. I eksempelet er brukt "*En ukes bortfall av vannforsyning*" og man har sett på konsekvensene for Ullevål Universitetssykehus.

[1] Figuren er hentet fra DECRIS [14]



Figur B-2 Hendelsestre for scenariet "En ukes bortfall av vannforsyning fra Oset" [1]

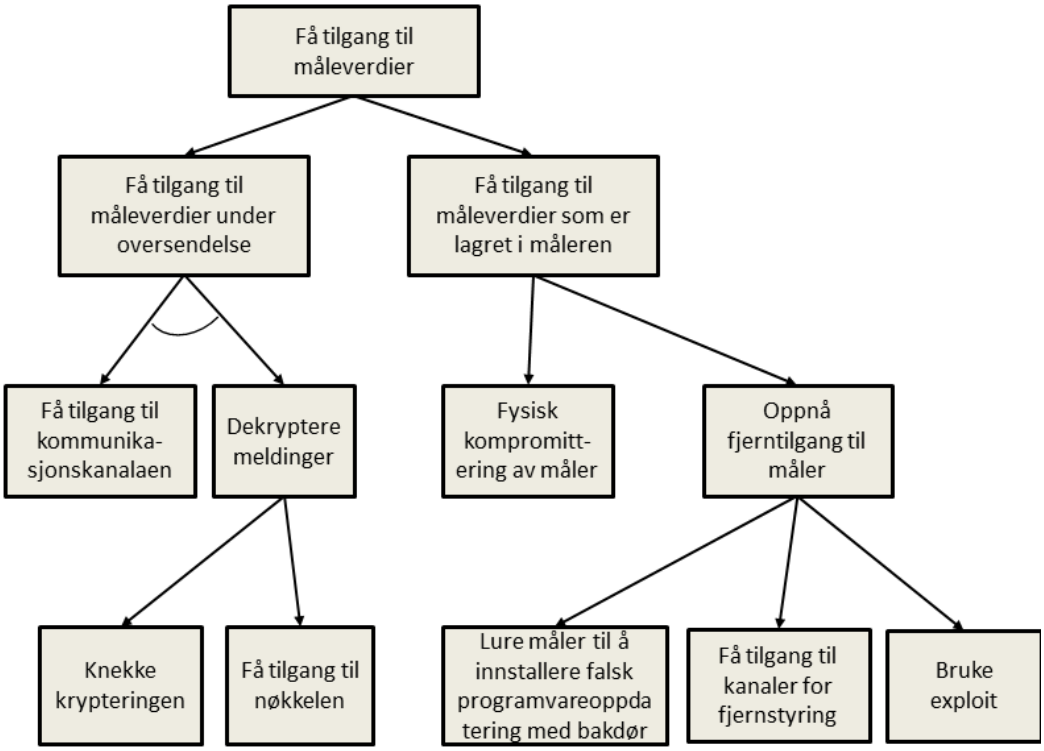
B.4 Angrepstrær

I tilfeller der man ønsker å studere nærmere hvor sårbar man er for en viss type angrep, kan det være hensiktsmessig å tegne opp et angrepstre som viser hvordan en angriper kan gå frem for å oppnå et gitt angrepsmål i systemet. Dette kan gi viktig input i arbeidet med å vurdere sannsynlighet og konsekvens (kapittel 2.2.3).

Figur B-3 viser et eksempel på et angrepstre som beskriver mulige strategier en angriper kan ta for å få tilgang til måledata. Angrepsmålet beskrives på toppen. Så detaljeres ulike strategier videre nedover som følger:

- *Alternative strategier*: Vises som vanlige piler. Da er det nok for en angriper å oppnå ett av alternativene for å lykkes med angrepet. Et eksempel finnes mot toppen av treet i figuren, der en angriper kan velge å få tilgang til måleverdier under oversendelse eller få tilgang til måleverdier lagret i målere.
- *Behov for å oppnå flere undermål samtidig:* Vises som en sammenkobling av pilene som leder mot løvnodene. Da må angriper oppnå begge/alle målene for å lykkes med angrepet. Et eksempel er detaljeringen av hvordan en angriper kan få tilgang til måleverdier under oversendelse. For å få til dette må angriper både få tilgang til kommunikasjonskanalen og dekryptere de meldingene som sendes.

[1] Figuren er hentet fra DECRIS [14]



Figur B-3 Eksempel på angrepstre

B.5 Dataflyt-diagrammer, og bruk av trussellister som STRIDE

Dataflyt-diagrammer (Data Flow Diagrams – DFDs) gir en oversikt over grensesnittene til et system, og hvordan informasjon flyter på disse grensesnittene og mellom interne deler av systemet. Dataflyt-diagrammene viser ikke sekvens i dataflyten, men viser hvor forskjellig data prosesseres, lagres og kommuniseres. Dette gjør det mulig å analysere hvor data er mest sårbare.

Dataflyt-diagrammer benytter følgende symboler:

- Rektangler: representerer aktører/systemer som gir input-data eller tar imot output-data
- Sirkler: representerer prosesser/funksjoner som prosesserer data
- Horisontale linjer: representerer datalagere (filer/databaser)
- Piler: representerer dataflyt

Når man bruker dataflytdiagrammer for å vurdere sikkerheten til et system er det i tillegg lurt å tegne opp tillitsgrensene i systemet, det vil si der data flyter fra en sone til en annen. Et eksempel er dersom data flyter fra et eksternt system til et internt system, eller mellom interne systemer med ulik grad av beskyttelse og tillit. Dette gjøres gjerne ved å tegne inn en stiplet linje som markerer grensen.

Figur B-4 viser et eksempel på et enkelt dataflytdiagram som viser flyt av måledata, alarmer og statusmeldinger mellom en målernode og tilgrensende systemer, i de tilfeller måledata sendes til nettselskapet via nettstasjonen. I dette diagrammet er det tegnet inn to tillitssoner: En der data deles med HAN og eventuelt display hos kunde, og en der data oversendes til nettstasjon. Det er her data er mest sårbar for angrep. Derfor er det viktig å studere truslene på tillitsgrensene spesielt.

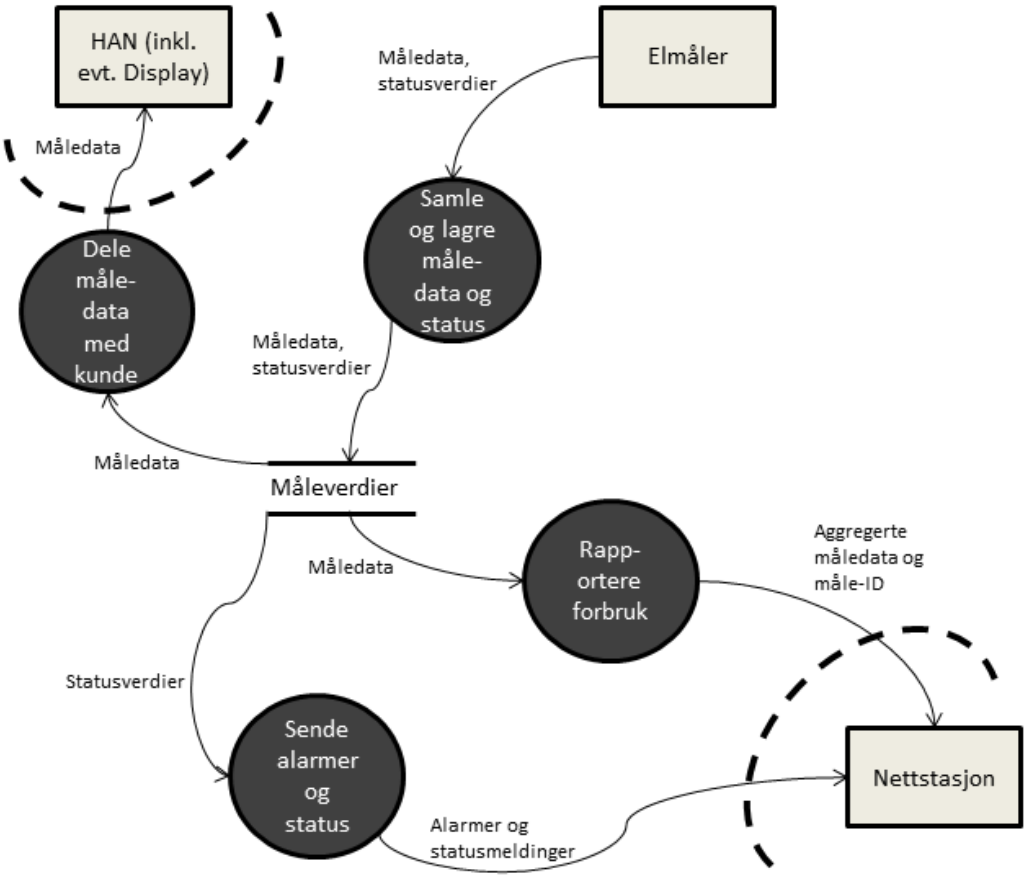
Som en hjelp til å studere trusler kan man bruke trussellister, f.eks. STRIDE (foreslått av Microsoft) som har fått navn fra første bokstav i de seks trusselkategoriene den inkluderer:

- **Spoofing identity:** Gi seg ut for å være noen andre – bruke andres autentiseringsinfo
- **Tampering with data:** Uautorisert endring av data
- **Repudiation:** Brukere nekter for å ha utført en handling, og systemet har ikke mulighet til å bevise
- **Information disclosure:** Uautoriserte får tilgang til informasjon
- **Denial of service:** Tjeneste utilgjengelig
- **Elevation of privileges:** Angriper får privilegier den ikke skulle hatt

Fremgangsmåten for å analysere mulige angrep mot systemet vil da være som følger:

1. For hver tillitsgrense: Gå gjennom trusselkategoriene i STRIDE, og spørre seg om trusselen er relevant (f.eks. om det kan skje 'spoofing' på dette grensesnittet og hvem som vil gjøre det).
2. Notere seg alle truslene man finner relevante.
3. Gå gjennom eksisterende tiltak og barrierer og se om de vil motvirke trusselen

De identifiserte truslene og oversikten over sikkerhetstiltak som er på plass, kan så brukes i vurderingen av sannsynlighet og konsekvens.



Figur B-4 Et eksempel på dataflytdiagram

C Systembeskrivelse

AMS og dets komponenter er beskrevet i eksisterende risikoanalyser av AMS [1,3]. I denne rapporten har vi utvidet systemet til også å inneholde baksystemer.

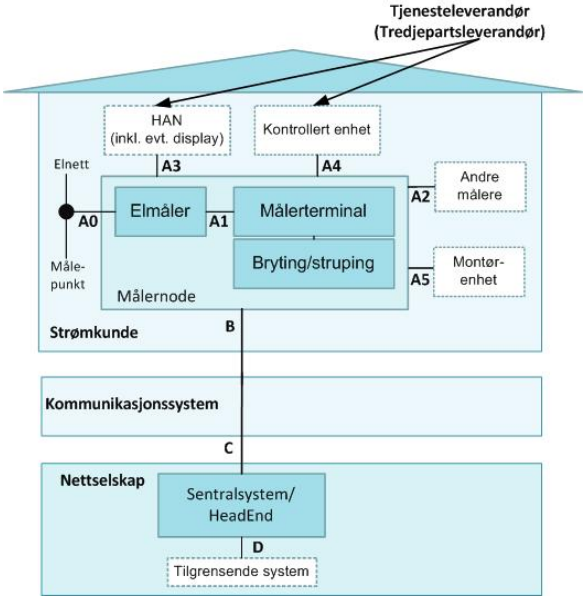
Når personvern og informasjonssikkerhet er fokus for analysen, må analysegruppen ha god oversikt over hvordan data flyter mellom ulike enheter. Dataflyt kan visualiseres i figurer som for eksempel vist i Figur B-4 og/eller beskrives i tabellform som vist i Tabell A-1.

Systemskisser er vist på de neste sidene. Tabell C-1 beskriver tilgrensende system som KIS, NIS etc. Viktige grensesnitt i figurene er beskrevet i Tabell C-2. De samme figurene er vist i større format bakerst i dette vedlegget. Det er også vist en systemskisse hvor AMS datainnsamling er tjenesteutsatt. Figuren synliggjør at tjenesteutsetting kan medføre flere angrepspunkter. Det er viktig at figurer og beskrivelser er korrekte i forhold til det eksisterende eller planlagte system. Dette krever kjennskap til de ulike kommunikasjonsprotokollene som benyttes. Figurene og beskrivelsen bør være kvalitetssikret og omforente før analysemøtet.

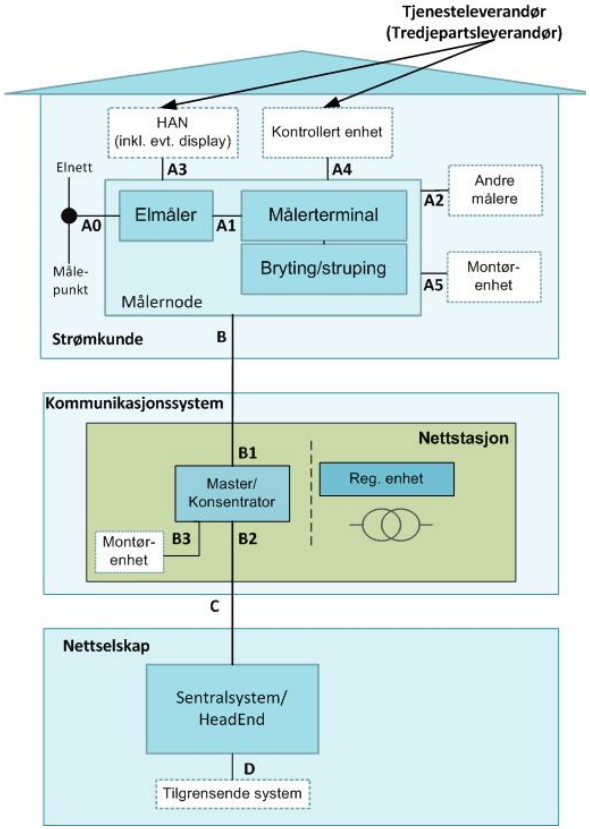
Tabell C-1 Eksempler på tilgrensende system

KIS (KundeInformasjonsSystem)	System for avregning og fakturering av kundene. Inneholder persondata (navn, adresse, …) [1]
NIS (NettInformasjonsSystem)	Datasystem for å holde rede på kunder, produksjon og hvordan disse er knyttet sammen gjennom nettet.
MVDB (MåleVerdiDataBase)	Database for lagring av registrerte måleverdier fra AMS.
Datautveksling	System for utveksling av data fra nettselskap til ekstern aktør, f.eks. den planlagte datahuben til Statnett.
DMS (Distribution Management System)	Driftskontrollsystem for distribusjonsnettet. Mulighet for visualisering av belastning, avbrudd, effektflyt, spenning m.m. i distribusjonsnettet. Viser data om strømforbruk, spenning, m.m. for enkeltkunder.
Portal	System for utveksling av informasjon med tredjepart og/eller strømkunde. F.eks. at måleverdi skal presenteres for strømkunde innen kl. 0900 neste dag, eller gjøres tilgjengelig for kraftleverandør med fullmakt fra strømkunde innen kl. 0900 neste dag. Ref. MAF §4-3 og §4-4
Arbeidsordresystem	System for automatisk generering og/eller registrering av arbeidsordre. (Både når arbeidsordre blir igangsatt og når den blir ferdigstilt.)

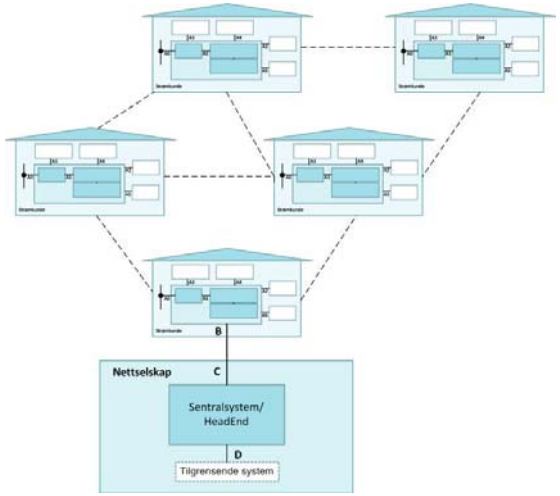
[1] Alle målepunkt har en gitt *MålepunktID* for unik identifisering. *MålepunktID* er "koblingsnøkkelen" mellom bl.a. registrerte verdier fra AMS-systemet (målerstand, …), geografisk lokalisering av kunde og personopplysninger.



Direkte kommunikasjon

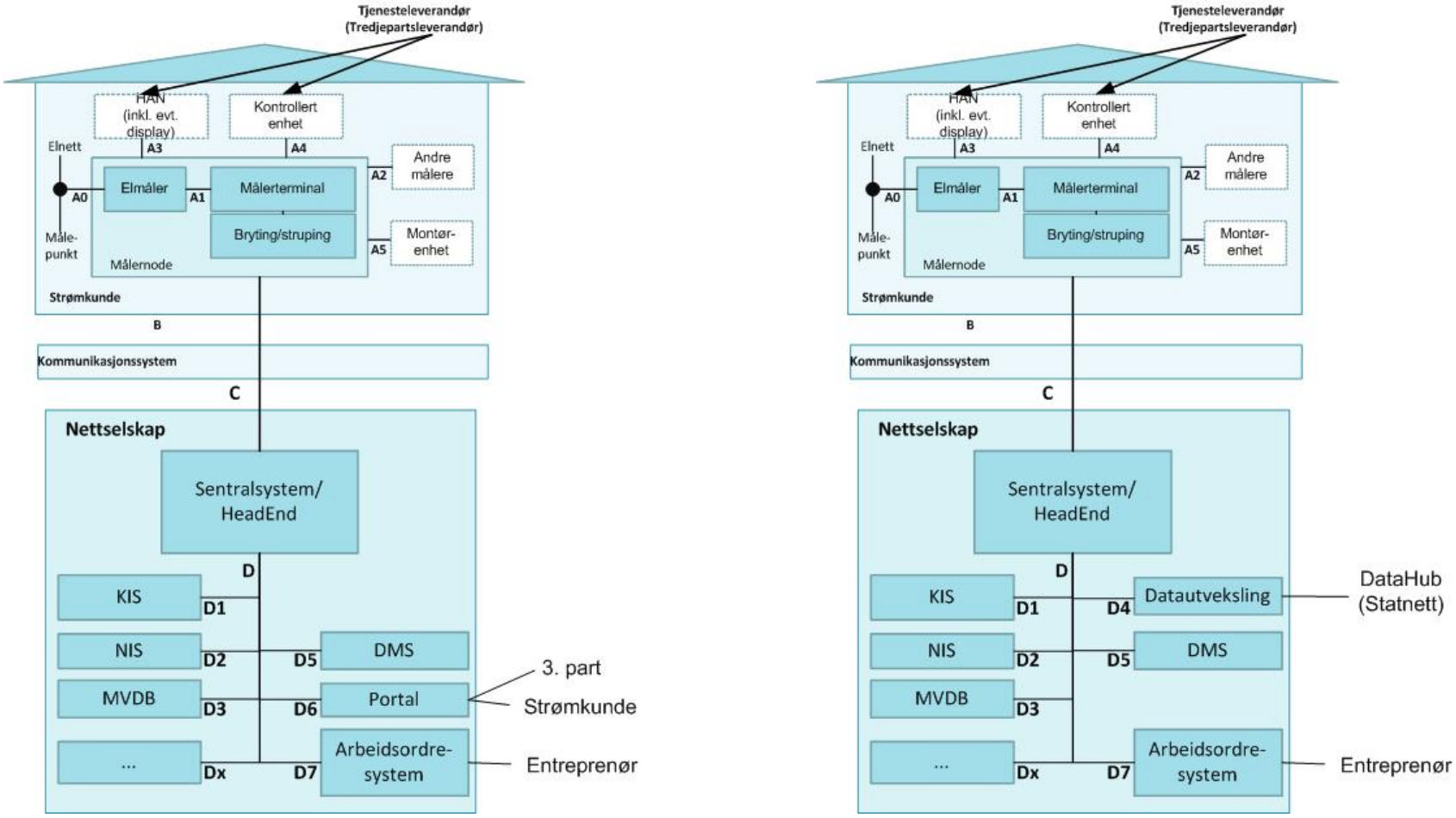


Kommunikasjon via konsentrator i nettstasjon



Kommunikasjon vha. mesh

Figur C-1 Eksempler på ulike systemskisser for AMS

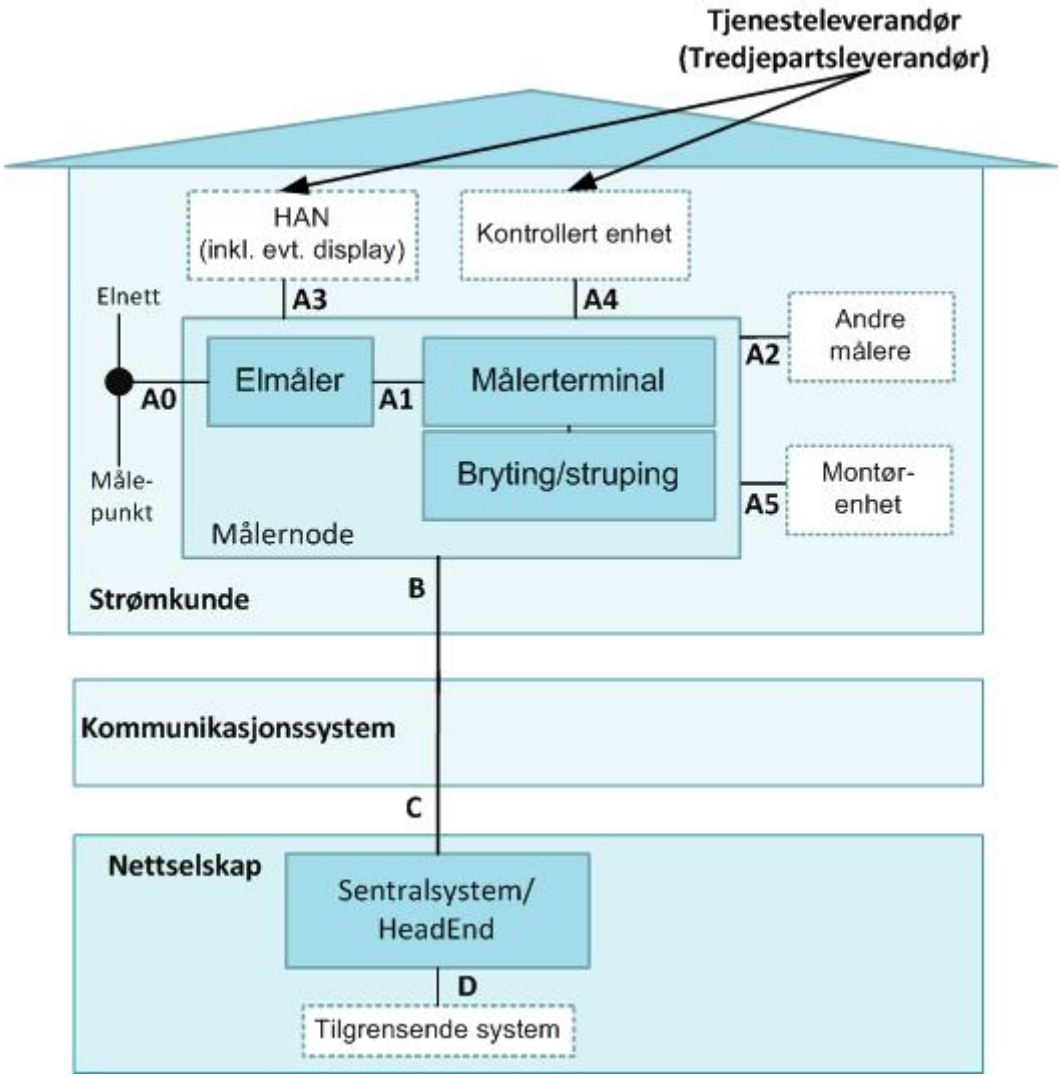


Med portal mot 3. part **Med sentral datahub**

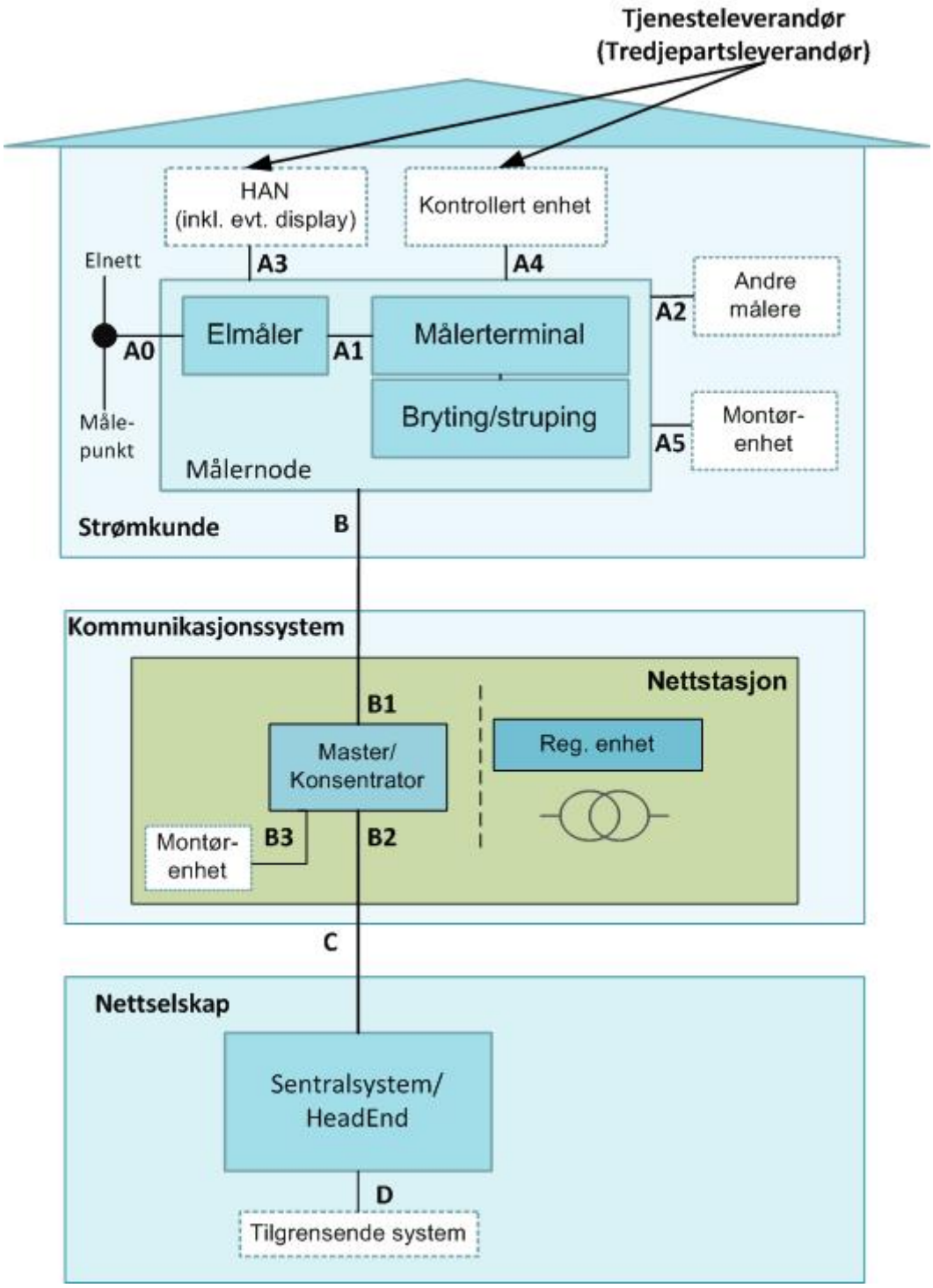
Figur C-2 Eksempler på tilgrensende systemer

Tabell C-2 Beskrivelse av grensesnitt

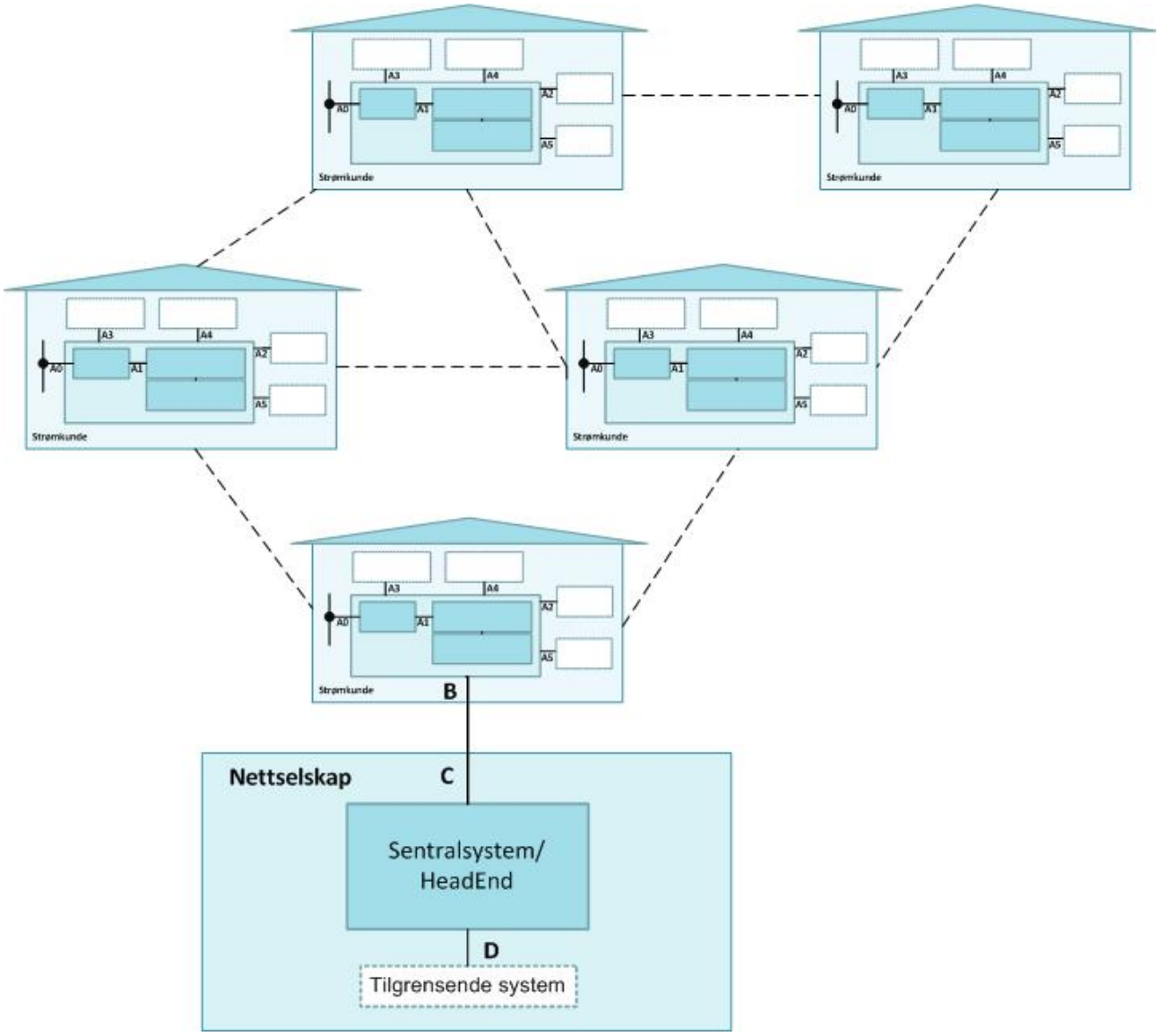
Nr	Involverte systemer	Beskrivelse
A0	Målepunkt -|- Elmåler	Elmåler registrerer forbruk av elektrisitet i målepunktet hos strømkunde.
A1	Elmåler -|- Målerterminal	Måleverdi overføres fra Elmåler til Måleterminal. Måleverdi lagres midlertidig i Målerterminal.
A2	Målerterminal -|- Andre måleinstrumenter (vann, gass, fjernvarme osv.)	Andre måleinstrumenter kan tilkobles Målerterminalen, og bruke samme kommunikasjonssystem for å samle inn verdiene til Sentralsystemet/HeadEnd.
A3	Målernode -|- HAN (inkl. evt. display) (fysisk atskilt fra Elmåler og Målerterminal)	Målernode har et grensesnitt mot HAN (Home Area Network) hvor kunden f.eks. kan ha et display for presentasjon av forbruksinformasjon.
A4	Målernode -|- Kontrollert enhet. Kan benyttes til lokal styring	Målernode har et grensesnitt mot en kontrollert enhet som f.eks. er teknologi for lokal styring av enkeltapparater.
B	Målernode -|- Kommunikasjonssystem	Målernoden består av Elmåler og Målerterminal. Via Målernodes kommunikasjonsmodul utveksles data til Kommunikasjonssystemet.
C	Kommunikasjonssystem -|- Sentralsystem/HeadEnd	Kommunikasjonssystemet overfører data videre til Sentralsystemet/HeadEnd.
D	Sentralsystem -|- Tilgrensende system	Sentralsystemet fungerer som et grensesnitt mellom Tilgrensende system og resten av AMS-systemet. Dette kan være f.eks. å innhente informasjon fra Målepunktene og overføre dette for videre behandling i andre systemer, eller å videreformidle signaler og informasjon mot Målerterminaler i AMS-systemet.



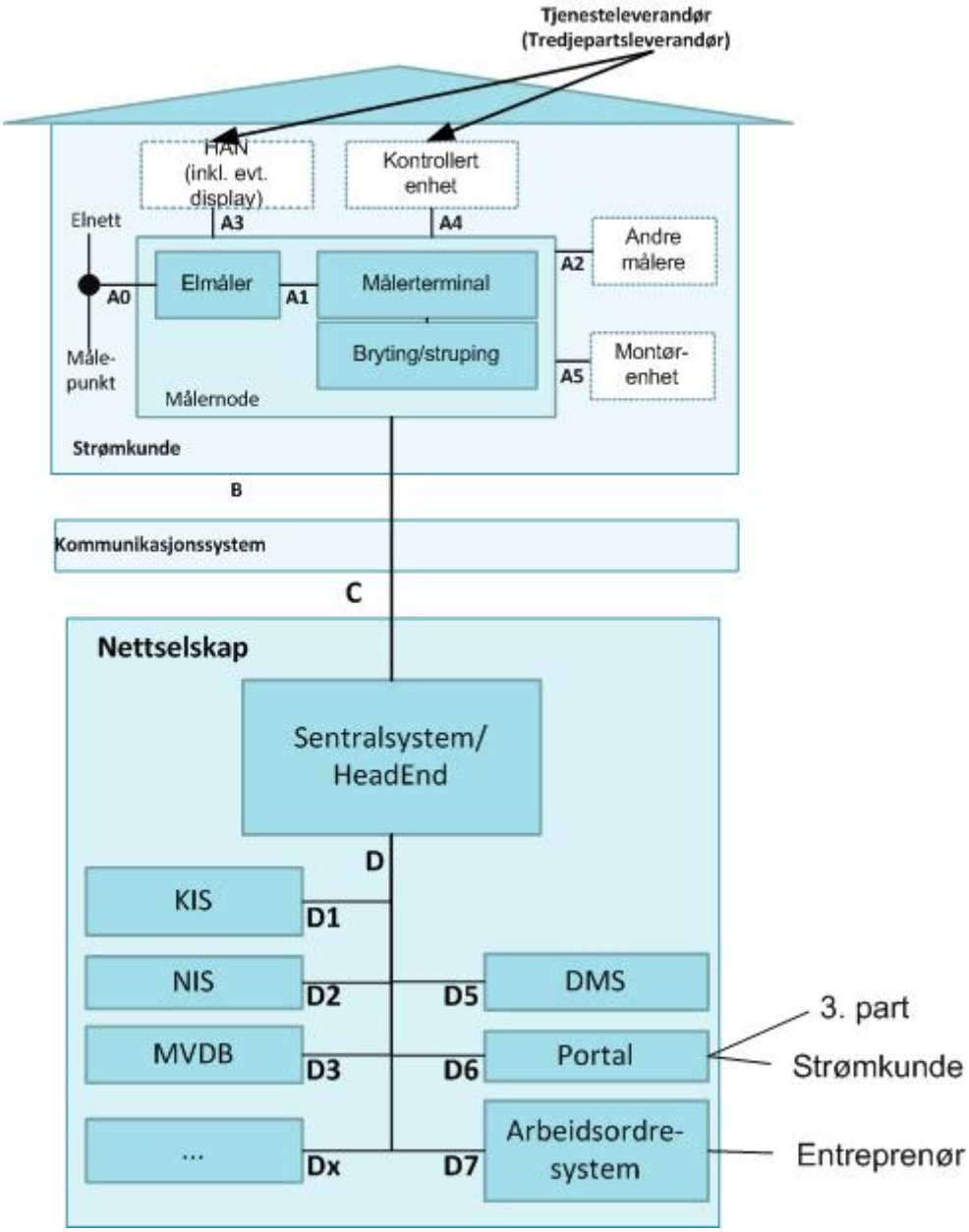
Figur C-3 Direkte kommunikasjon med sentralsystem



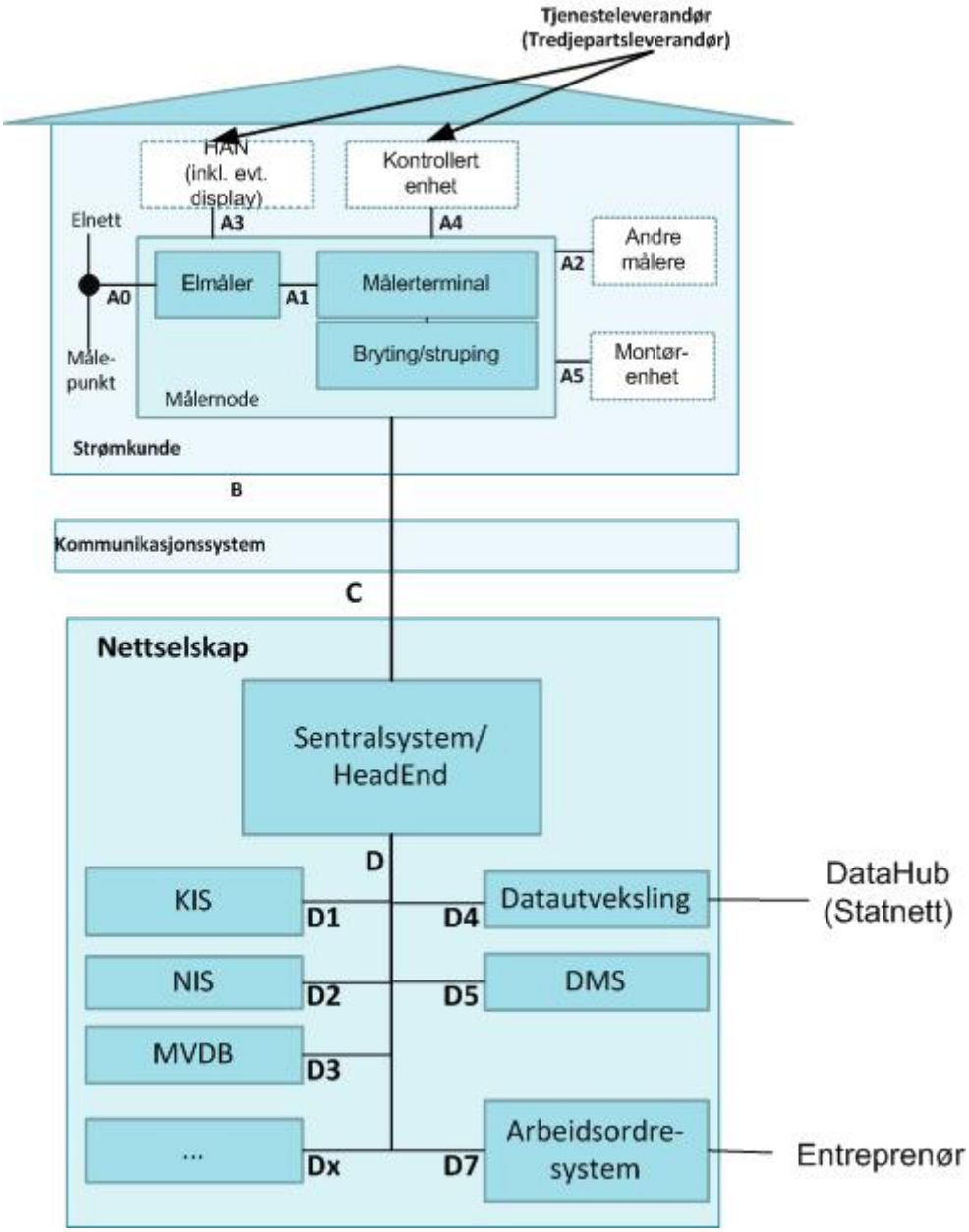
Figur C-4 Kommunikasjon via konsentrator i nettstasjon



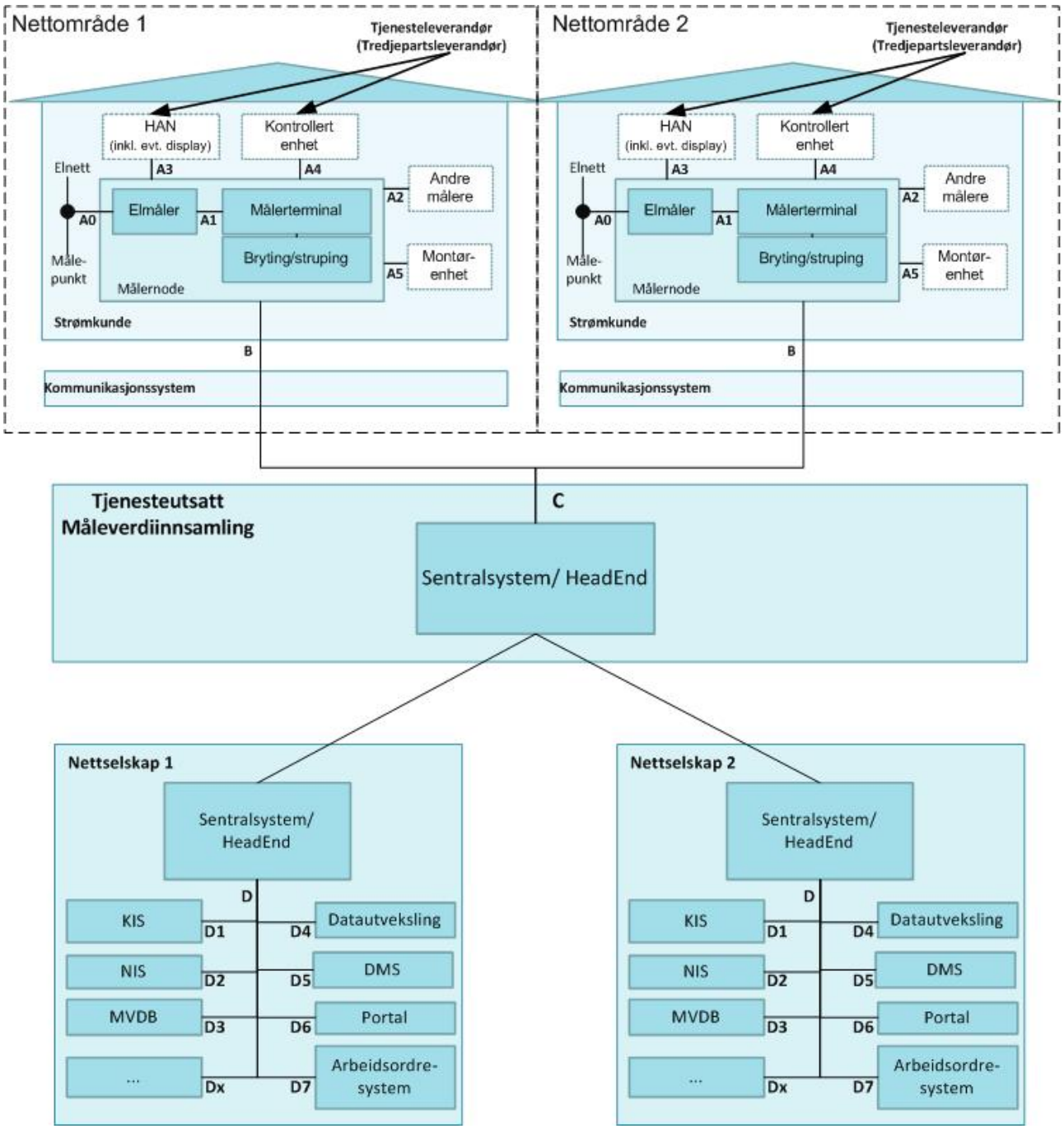
Figur C-5 Kommunikasjon vha. mesh



Figur C-6 Tilgrensende systemer med portal mot 3. part



Figur C-7 Tilgrensende systemer med forbindelse til datahub



Figur C-8 Tjenesteutsetting av datainnsamling hvor ulike nettselskap bruker samme leverandør

D Sikkerhetstiltak som bør vurderes etter anbefaling fra ISO/IEC 27001

I Tabell D-1 er det synliggjort hvordan de fleste relevante tiltak fra ISO/IEC 27001 [18] er dekket av veiledningen [4]. Relevante tiltak som ikke er dekket av veiledningen, er markert med grå bakgrunn. Kolonnene "Id" og "Veiledning" inneholder referanse til NVEs veiledning [4].

Tabell D-1 Sikkerhetstiltak fra ISO/IEC 27001 [18] med referanser til NVEs veiledning [4]

Tema	Undertema	Sikkerhetstiltak	Id	Veiledning
A) Sikkerhetspolicy	Policy for informasjonssikkerhet	Policy for informasjonssikkerhet	A.1.1	B1
		Gjennomgang av policy for informasjonssikkerhet	A.1.2	B1
B) Organisering av informasjons-sikkerhet	Intern organisering	Ledelsens forpliktelser og engasjement i informasjonssikkerhet	B.1.1	B1
		Koordinering av informasjonssikkerhet	B.1.2	B1
		Ansvarsfordeling	B.1.3	B1
		Autorisasjonsprosess for systemer for informasjonshåndtering	B.1.4	
		Konfidensialitetsavtaler	B.1.5	
		Myndighetskontakt	B.1.6	
		Kontakt med spesielle interessegrupper	B.1.7	
		Uavhengig gjennomgang av informasjonssikkerhet	B.1.8	
	Eksterne aktører	Identifisering av risiko knyttet til eksterne aktører	B.2.1	
		Informasjonssikkerhet knyttet til kundebehandling	B.2.2	
		Inkludere informasjonssikkerhet i tredjepartsavtaler	B.2.3	A3
C) Håndtering av informasjonsverdier	Ansvar for informasjonsverdier	Oversikt over informasjonsverdier[19]	C.1.1	
		Eierskap til informasjonsverdier	C.1.2	
		Akseptabel bruk av informasjonsverdier	C.1.3	C1
	Klassifisering av informasjon	Retningslinjer for klassifisering	C.2.1	
		Informasjonsmerking og håndtering	C.2.2	
D) Sikkerhet knyttet til medarbeidere (HR)	Før ansettelse	Roller og ansvar	D.1.1	
		Bakgrunnsundersøkelse	D.1.2	
		Ansettelsesbetingelser	D.1.3	
	Etter ansettelse	Lederansvar	D.2.1	

[19] Tiltak markert med grå bakgrunn er tiltak i ISO/IEC 27001 [18] som ikke er dekket av NVEs veiledning [4].

Tema	Undertema	Sikkerhetstiltak	Id	Veiledning
		Opplæring og holdningsskapende arbeid	D.2.2	
		Disiplinærtiltak	D.2.3	
	Terminering av ansettelsesforhold	Ansvarsfordeling	D.3.1	
		Tilbakelevering av utstyr	D.3.2	
		Fjerning av rettigheter	D.3.3	
E) Fysisk sikring	Sikre områder	Sikkerhetssoner	E.1.1	G1
		Fysisk adgangskontroll	E.1.2	G1
		Sikring av kontorer, møterom og øvrige fasiliteter	E.1.3	G1
		Beskyttelse mot eksterne trusler	E.1.4	G1
		Arbeid i sikre områder	E.1.5	
		Besøk og varelevering	E.1.6	
	Utstyrssikkerhet	Oppbevaring og sikring av utstyr	E.2.1	
		Støtteverktøy	E.2.2	
		Sikker kabling	E.2.3	
		Vedlikehold	E.2.4	
		Sikring av utstyr utenfor egne, kontrollerte områder	E.2.5	G1
		Sikker håndtering ved avhending og gjenbruk	E.2.6	C1
F) Kommunikasjon og driftsledelse	Operasjonelle prosedyrer	Dokumenterte prosedyrer	F.1.1	
		Endringshåndtering	F.1.2	
		Arbeidsdeling	F.1.3	
		Adskillelse av testmiljø og driftsmiljø	F.1.4	A1
	Håndtering av tredjepart	Tredjeparts leveranser	F.2.1	A3, B4
		Kontroll av tredjeparts tjenester	F.2.2	A3
		Endringshåndtering av tredjeparts tjenester	F.2.3	A3
	Systemplanlegging og akseptanse	Håndtering av kapasitet (kommunikasjon, lagring, regnekraft)	F.3.1	
		Akseptansekriterier	F.3.2	E1
	Beskyttelse mot skadelig kode	Tiltak mot skadelig kode	F.4.1	C5
	Sikkerhetskopi	Rutiner for sikkerhetskopiering	F.5.1	D5
	Nettverkssikkerhet	Perimetersikring	F.6.1	C3
		Sikring av nettverkstjenester	F.6.2	C2

Tema	Undertema	Sikkerhetstiltak	Id	Veiledning
	Håndtering av lagringsmedia	Retningslinjer for hvordan data skal slettes	F.7.1	
		Avhending av lagringsmedia	F.7.2	C1
		Prosedyrer for håndtering av informasjon	F.7.3	
		Sikker lagring av systemdokumentasjon	F.7.4	B3
	Informasjonsutveksling	Prosedyrer for informasjonsutveksling	F.8.1	
		Avtaler om informasjonsutveksling	F.8.2	
		Transport av fysiske lagringsmedia	F.8.3	
		Elektronisk informasjonsutveksling	F.8.4	
		Økonomisystemer	F.8.5	
	Elektronisk handel	Elektronisk handel	F.9.1	
		On-line transaksjoner	F.9.2	
		Offentlig tilgjengelig informasjon	F.9.3	
	Monitorering	Revisjonslogger	F.10.1	D2
		Monitorering av systembruk	F.10.2	D2
		Beskyttelse av logger	F.10.3	D2
		Administrator og operatørlogger	F.10.4	D2
		Logging av feil	F.10.5	D2
		Klokkesynkronisering	F.10.6	
G) Tilgangskontroll	Overordnede krav til tilgangskontroll	Policy for tilgangskontroll	G.1.1	C1
	Brukertilgang	Brukerregistrering	G.2.1	C1
		Brukerrettigheter	G.2.2	C1
		Håndtering av passord	G.2.3	C1
		Fornyet gjennomgang og kontroll av brukerrettigheter	G.2.4	C1
	Brukeransvar	Bruk av passord	G.3.1	
		Ubevoktet brukerutstyr	G.3.2	
		Policy for rydding av pulter og møterom og hvilken informasjon som blir stående på forlatte skjermer	G.3.3	
	Nettverkstilgang	Policy for nettverkstjenester	G.4.1	C3
		Brukeridentifisering av eksterne forbindelser	G.4.2	C3
		Identifisering av tilkoblet utstyr i nettverket	G.4.3	C3

Tema	Undertema	Sikkerhetstiltak	Id	Veiledning
		Beskyttelse av tilgangsporter for fjernstyring og konfigurasjon	G.4.4	C3
		Segregering av nettverk	G.4.5	C5
		Konfigurasjonskontroll ("connection control" og "routing control")	G.4.6	C3
	Tilgang til operativsystem	Sikre påloggingsprosedyrer	G.5.1	C1
		Brukeridentifikasjon og autentisering	G.5.2	C1
		Passordhåndtering	G.5.3	C1
		Bruk av systemhjelpemidler	G.5.4	
		Bruk av tidsavbrudd (skjermsparere med krav om ny innlogging, krav om ny tilkobling til nettverk etc.)	G.5.5	
	Tilgang til applikasjoner og informasjon	Begrensninger i informasjonstilgang	G.6.1	C1
		Isolering av sensitive systemer	G.6.2	C1
	Mobile tjenester og fjerntilgang	Retningslinjer for bruk av mobile tjenester og fjerntilgang	G.6.3	C1
H) Anskaffelse, utvikling og vedlikehold av informasjons-systemer	Sikkerhetskrav til informasjonssystemer	Kravanalyse og spesifikasjon	H.1.1	A1
	Korrekt dataprosessering	Validering av inn-data	H.2.1	
		Kontroll med intern dataprosessering	H.2.2	
		Meldingsintegritet	H.2.3	
		Validering av ut-data	H.2.4	
	Kryptering	Policy for kryptering	H.3.1	A1
		Håndtering av nøkler	H.3.2	A1, C6
	Sikkerhet for systemfiler	Beskyttelse av operasjonell programvare, testdata og kildekode	H.4.1	A1
	Sikkerhet i utviklings- og støtteprosesser	Endringskontroll (prosedyrer)	H.5.1	E1
		Rutiner for gjennomgang av applikasjoner etter endringer i operativsystem	H.5.2	E1
		Versjonskontroll og rutiner for tilhørende programvare	H.5.3	
		Informasjonslekkasje	H.5.4	
		Rutiner for tjenesteutsatt programvareutvikling	H.5.5	A3
	Teknisk sårbarhet	Risikohåndtering av tekniske sårbarheter	H.6.1	A1, D1
I) Hendelses-håndtering	Rapportering av hendelser og svakheter	Rutiner for rapportering av hendelser og avdekkede svakheter	I.1.1	A1, D1

Tema	Undertema	Sikkerhetstiltak	Id	Veiledning
	Forvaltning av sikkerhetshendelser og forbedringer	Ansvarsfordeling og prosedyrer i forbindelse med sikkerhetsbrudd og forbedringer	I.2.1	A1, D1, D3
		Læring	I.2.2	A1
		Innsamling av bevis	I.2.3	A1
J) Kontinuitets-planlegging (Business continuity management)	Informasjons-sikkerhetsaspekter innen kontinuitets-planlegging	Inkludere informasjonssikkerhet i kontinuitetsplanleggingen (business continuity management process)	J.1.1	
		Planer og risikoanalyser for drift under og etter sikkerhetsbrudd	J.1.2	B2
		Planer for tilbakeføring til normal drift	J.1.3	
K) Samsvar	Samsvar med lover og forskrifter	Identifikasjon av gjeldende lover og forskrifter for informasjonssikkerhet, personvern og lagring av data	K.1.1	
		Retningslinjer for IPR	K.1.2	
	Samsvar med standarder og retningslinjer	Identifikasjon av gjeldende standarder og retningslinjer	K.2.1	
		Teknisk kontroll av samsvar med standarder og krav	K.2.2	
	Revisjon av informasjonssystemer	Rutiner for revisjon og beskyttelse av revisjonsdata	K.3.1	B3

Teknologi for et bedre samfunn

www.sintef.no