EKSTERN RAPPORT

Nr 15/2018

Risiko- og sårbarhetsanalyse for økt integrasjon av AMS-DMS-SCADA

Christian Frøystad, Martin Gilje Jaatun
Karin Bernsmed, Marie Moe

Ekstern rapport nr 15-2018
Risiko- og sårbarhetsanalyse for økt integrasjon av AMS-DMS-SCADA

Utgitt av: Norges vassdrags- og energidirektorat
Redaktør: Janne Hagen
Forfatter: Christian Frøystad, Martin Gilje Jaatun
Karin Bernsmed, Marie Moe

Trykk: NVEs hustrykkeri
Forsidefoto: NVE
ISBN: 978-82-410-1789-6

Sammendrag: Rapporten beskriver risiko og sårbarhet i kraftnettet ved tettere kobling mellom AMS, DMS og SCADA. Sikkerhetsutfordringene ved økt integrasjon er håndterbare, gitt iverksetting av gode forebyggende tiltak.

Emneord: Informasjonssikkerhet, risiko, sårbarhet, ROS, ROS-analyse, AMS, DMS, SCADA

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

Telefon: 22 95 95 95
Epost: nve@nve.no
Internett: www.nve.no

2018-12-11

Forord

I Lysneutvalgets innstilling NOU 2015:13 *Digital sårbarhet – sikkert samfunn* ble avanserte måle- og styringssystem (AMS) omtalt. Utvalget bemerket at risiko og sårbarheter ikke hadde blitt tilstrekkelig kartlagt og vurdert forut for innføring for AMS, og etterlyste forsiktighet i det videre utviklingsforløpet. Rapporten påpekte at *[u]kritisk implementering av funksjonalitet som for eksempel knytter AMS tettere sammen mot driftskontrollsystemer, vil medføre en sårbarhetsoppbygging med et betydelig skadepotensial*. Utvalget anbefalte NVE å gjennomføre risiko- og sårbarhetsanalyser for utvidet bruk av AMS inn mot driftskontrollsystemene.

AMS er rullet ut i henhold til plan, og dataintegrasjon gjennom Elhub er i ferd med å blir realisert. Konkrete forespørsler om videre system- og dataintegrasjon er foreløpig ikke løftet frem, men en rekke aktuelle problemstillinger inngår allerede i den pågående diskusjonen. I etterkant av Lysneutvalgets arbeid har NVE etablert flere FoU-prosjekter knyttet til informasjonssikkerhet i kraftforsyningen. Vedlagte rapport fra SINTEF Digital er resultat av et spesifikt oppdrag om risiko ved integrasjon av AMS, DMS og SCADA.

Rapporten identifiserer en rekke potensielle uønskede hendelser, hvor de mest alvorlige gjelder tilsiktede og utilsiktede bryteroperasjoner i distribusjonsnettet. Rapporten drøfter egnede forebyggende tiltak, og konkluderer med at risikoen ved økt integrasjon er håndterbar. NVE mener innholdet i rapporten er egnet som utgangspunkt for nettselskaper som ønsker å vurdere konkrete integrasjonsløsninger. Også for andre interessenter vil beskrivelsen av risikobildet være nyttig.

Oslo, 11. desember 2018

Ingunn Åsgard Bendiksen
direktør

Eldri Naadland Holo
seksjonssjef

Dokumentet er elektronisk godkjent uten underskrift i henhold til interne rutiner.

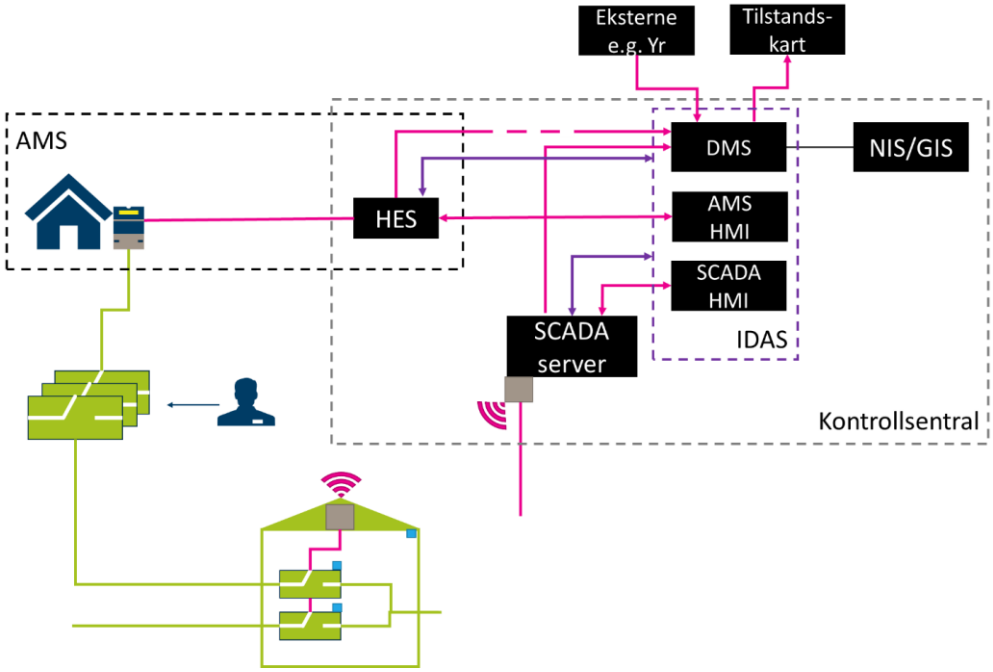
2018:01083 - Åpen

Rapport

ROS-analyse AMS-DMS-SCADA

Risikoanalyse av økt integrasjon mellom AMS, DMS og SCADA

Forfattere
Christian Frøystad
Martin Gilje Jaatun
Karin Bernsmed
Marie Moe



SINTEF Digital
Cyber Security and Safety
2018-12-13

SINTEF

SINTEF Digital
Postadresse:

Sentralbord: 73593000

info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

Rapport

ROS-analyse AMS-DMS-SCADA

Risikoanalyse av økt integrasjon mellom AMS, DMS og SCADA

EMNEORD:
AMS
DMS
SCADA
Risiko
ROS-analyse
Informasjonssikkerhet

VERSJON	DATO
1.3	2018-12-13

FORFATTER(E)
Christian Frøystad
Martin Gilje Jaatun
Karin Bernsmed
Marie Moe

OPPDRAGSGIVER(E)	OPPDRAGSGIVERS REF.
Norges vassdrags- og energidirektorat (NVE)	Janne Merete Hagen

PROSJEKTNR	ANTALL SIDER
102018488	35

SAMMENDRAG

Håndterbar risiko ved økt integrasjon

På oppdrag fra NVE tar denne rapporten for seg risiko ved økt integrasjon i kraftnettet. Økt integrasjon forstås i denne sammenheng som tettere kobling mellom DMS, AMS og SCADA (omtalt som IDAS). Rapporten har identifisert en rekke potensielle uønskede hendelser, hvor de mest alvorlige er "*Uvedkommende sender falske kommandoer med SCADA bryteroperasjoner til fjernstyrte brytere i distribusjonsnettet*" og "*Uvedkommende utfører endring i DMS-delen av IDAS som medfører at uhensiktsmessige SCADA bryteroperasjoner effektueres*". Det presenteres en rekke tiltak som vil redusere sannsynligheten og konsekvensen av disse og andre uønskede hendelser. Bransjen oppfordres til å bruke disse som et utgangspunkt, men nettselskapene eller andre aktører bør utvide både risikovurderingen og tiltakene i tråd med det konkrete systemet de utvikler. Det er også tjenlig om bedriftene gir en eller flere ansatte i oppgave å ha et spesielt fokus på mindre sannsynlige hendelser som potensielt kan få store konsekvenser om de inntreffer.

UTARBEIDET AV	SIGNATUR
Christian Frøystad	

KONTROLLERT AV	SIGNATUR
Per Håkon Meland	

GODKJENT AV	SIGNATUR
Maria Bartnes	

RAPPORTNR	ISBN	GRADERING	GRADERING DENNE SIDE
2018:01083	-	Åpen	Åpen

MANAGEMENT SYSTEM CERTIFICATION
DNV·GL
ISO 9001 = ISO 14001
OHSAS 18001

Dokumentet har gjennomgått SINTEFs godkjenningsprosedyre og er sikret digitalt

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
0.1	2018-10-22	Utkast til intern QA
0.2	2018-10-25	Utkast til ekstern QA (KraftCERT og SINTEF Energi)
0.3	2018-11-13	Nytt utkast til intern QA
1.0	2018-11-14	Første versjon levert til kunde (NVE)
1.1	2018-12-12	Gradering endret til Åpen
1.2	2018-12-13	QA før åpen publisering
1.3	2018-12-13	Ny versjon levert til kunde (NVE)

Innholdsfortegnelse

1 Bakgrunn 5

2 Metodikk 5

3 Systembeskrivelse 6

3.1 DMS 6

3.2 SCADA 6

3.3 AMS 7

3.4 Integrasjon: IDAS 8

4 Trusselbilde 11

5 Identifisering av verdier 12

6 Uønskede hendelser 21

6.1 Forbehold 22

6.2 Identifisering og vurdering av uønskede hendelser 23

6.3 Hendelser med høy risiko 29

6.4 Hendelser med middels høy risiko 29

6.5 Hendelser med middels lav eller lav risiko 29

6.6 Andre uønskede hendelser som bør hensyntas ved implementasjon av et konkret system 30

7 Anbefalinger om tiltak 31

8 Konklusjon 32

9 Referanser 33

A Skala for sannsynlighet 34

B Skala for konsekvens 35

Forkortelser

AMS	Avanserte måle- og styringssystem
CERT	Computer Emergency Response Team
DDoS	Distributed Denial of Service
DoS	Denial of Service
DKS	Driftskontrollsystem
DMS	Distribution Management System
DSO	Distribution System Operator
GIS	Geographic Information Systems
HES	Head End System
HMI	Human Machine Interface
IDAS	Integrated DMS, AMS and SCADA
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LFK	Leder for kobling
n/a	Not applicable
NIS	Network Information Systems
NSM	Nasjonal Sikkerhetsmyndighet
NVE	Norges vassdrags- og energidirektorat
PST	Politiets sikkerhetstjeneste
QA	Quality Assurance
RTU	Remote Terminal Unit
SCADA	Supervisory control and data acquisition
VPN	Virtuelt privat nettverk

1 Bakgrunn

På bakgrunn av bemerkninger fra Lysne-utvalget [11], bestilte NVE en risiko- og sårbarhetsanalyse av integrasjon mellom AMS, SCADA og DMS. Oppdraget lyder som følger:

Målet med prosjektet er å gjennomføre en forskningsbasert analyse av risikoen ved økt integrasjon mellom AMS, DMS og SCADA. Vi vil også gi anbefaling til sikring av grensesnitt og systemer dersom slik integrasjon skulle finne sted.

Analysen ble gjennomført av SINTEF høsten 2018. Siden bransjen er i utvikling og AMS under utrulling, tar rapporten utgangspunkt i et generalisert, fremtidig integrasjonsscenario. Rapporten skal understøtte bransjens arbeid med sikkerhet i strømnettet, samt NVEs arbeid med fremtidig regulering.

Siden analysen er gjennomført uten en konkret implementasjon på gjennomføringstidspunktet, må analysen regnes som innspill til risikoanalyse gjennomført av det enkelte nettselskap heller enn en autoritativ referanseanalyse.

Analysen fokuserer kun på risiko relatert til informasjonssikkerhet. Risiko koplet til andre typer av uønskede hendelser enn målrettet angrep er ikke inkludert. Videre så dekker risikoanalysen kun scenarioet tettere integrasjon av AMS, DMS og SCADA. Det er allerede gjennomført flere grundige risikoanalyser koblet til de enkelte systemene, for eksempel "Risikovurdering av AMS" [3] og "Security Threats in Demo Steinkjer" [5] [6]. Trusler mot de enkelte systemene som er uavhengige av integrering er dermed ikke tatt med i denne analysen.

2 Metodikk

Risikoanalysen er gjennomført iht. standarden ISO/IEC 27005 Information Security Risk Management [1] og rapporten "Informasjonssikkerhet og personvern: Støtte til risikoanalyse av AMS og tilgrensende systemer" [2]. For å fremskaffe den nødvendige informasjonen, ble det gjennomført en workshop hos NVE den 27.08.2018. Her møtte representanter fra både nettselskap, forvaltning og leverandører for å gi sine perspektiver på hvordan integrasjonen vil se ut i fremtiden, hvilke verdier som må beskyttes og hvilke risikoer som er aktuelle.

For å oppnå bedre forståelse av DMS-ens rolle i økosystemet, ble det også gjennomført et besøk hos Powel den 04.09.2018. Her ble Powels løsning diskutert, samt hvordan distribusjonsnettet ser ut fra deres perspektiv.

Før ferdigstilling ble rapporten sendt til KraftCERT og SINTEF Energi for kommentarer og nyttige tilbakemeldinger.

Analysen er gjennomført med SINTEF sin bakgrunn fra forskning på kritiske infrastrukturer og kjennskap til forskningsfronten i kraftbransjen.

3 Systembeskrivelse

Denne rapporten tar for seg samspillet og integrasjonen mellom AMS, SCADA og DMS i kontekst av drift av strømnettet. Figur 4 viser hvordan interaksjonen forventes å fungere, med mulighet for enda tettere integrasjon i og med at det råder uenighet rundt definisjonen av henholdsvis SCADA og DMS. I tillegg ble det på workshopen hos NVE (se kapittel 2) hevdet at AMS skulle ha vært definert som et kontrollsystem i likhet med SCADA.

3.1 DMS

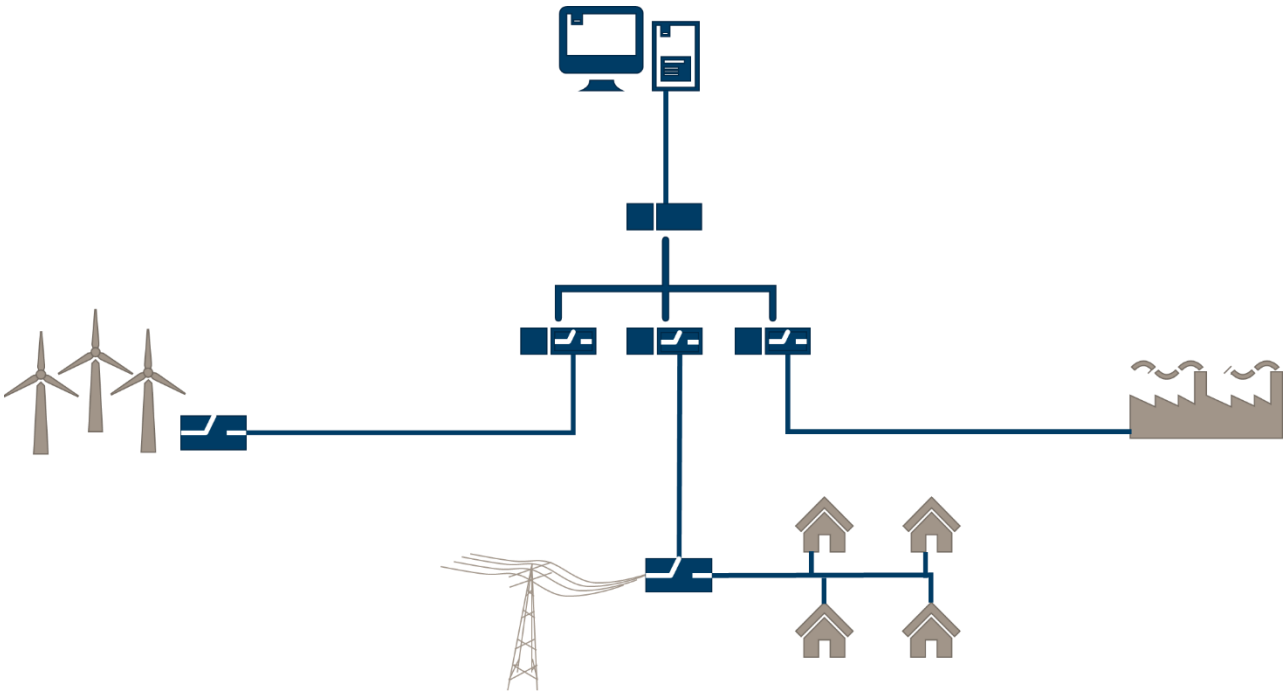
Distribution Management System (DMS) har som hovedoppgave å representere topologien i nettet slik at man bedre kan forstå konsekvensen av endringer i nettet. På driftssentralen er det *leder for kobling* (LFK) som har regien på DMS. LFK er den eneste som kan godkjenne endringer i nettet, og har ansvaret for at disse endringene reflekteres i DMS. DMS er en kartapplikasjon med nettverkstopologien lagt ut, hvilket gir et godt grunnlag for å forutse hva som skjer dersom en bryter kobles ut. Følgelig vil LFK ha god oversikt over hvilke områder som blir uten strøm dersom en bryter legges ut eller en feil oppstår på en ledning. DMS mottar tilstandsinformasjon på automatiserte/fjernstyrte brytere fra SCADA, men i Norge gjennomføres det for tiden ikke kommandoer fra DMS til SCADA. Dette kommer av at DMS i så tilfelle måtte regnes som driftskontrollsystem iht. beredskapsforskriften fra NVE, §7 [4]. Det bemerkes likefullt at det ellers i Europa finnes oppsett hvor DMS samhandler direkte med SCADA. DMS-data repliseres ut i åpen sone for tilgjengeliggjøring av statusinformasjon til f.eks. kunder og andre systemer. Det innhentes også informasjon fra f.eks. AMS-head-end og kundebehandlingssystemet, dog kan ingen av disse systemene endre tilstand i DMS-en eller oppdatere topologien, men vil bare komme som meldinger til LFK som i tur må vurdere om DMS skal oppdateres med relevant informasjon.

I tillegg kan DMS ta inn informasjon om lokasjon på samtlige biler og montører/installatører, samt andre sensorer og typer data driftssentralen kan trenge.

3.2 SCADA

Supervisory Control And Data Acquisition (SCADA) befinner seg i grenseland mellom den fysiske og den digitale verden. SCADA består av en samling maskinvare (PLCer[1], servere, switcher) og en programvarepakke som står for kontroll og datainnsamling. Det er regulert som et driftskontrollsystem iht. beredskapsforskriften fra NVE, §7 [4]. SCADA-systemet i nettet omfatter sensorer og aktuatorer som muliggjør fjernovervåkning og -styring. Enkelte omtaler den dedikerte arbeidsstasjonen for SCADA-operasjoner på kontrollrommet som SCADA-systemet eller SCADA, men begrepet innbefatter også det underliggende systemet som vist i Figur 1. Per dags dato er det forholdsvis enkelt å etterinstallere sensorer der det behøves, men aktuatorer er i liten grad utbredt. Alle transformatorstasjoner er automatisert, men det har hittil ikke lønnet seg å automatisere de fleste mindre enheter. Følgelig er majoriteten av nettet operert manuelt og dermed ikke kontrollert gjennom SCADA, men heller ved at LFK sender personell ut til et koblingspunkt.

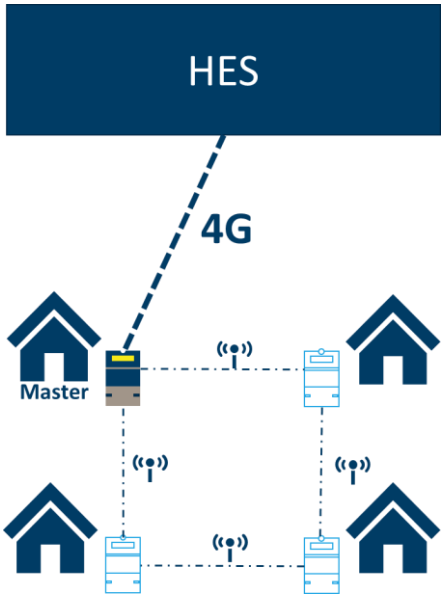
[1] Programmable Logical Controller (*norsk: Programmerbar Logisk Styring*)



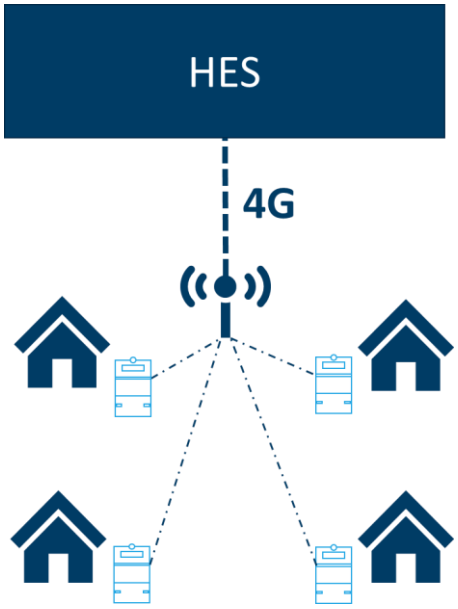
Figur 1 Et høynivåbilde av SCADA hvor man fjernstyrer brytere i strømnettet

3.3 AMS

Avanserte måle- og styringssystem (AMS) foretar målinger i den enkelte husstand. Det rapporteres om forbruk, evt. feil, som jordfeil, og det er innebygde funksjoner for å koble ut kunden ved hjelp av bryter- eller strupefunksjon. Strupefunksjon er i praksis en bryter som kobles ut når et gitt tak for effektforbruk er nådd. AMS-målere er knyttet til det sentrale Head End System (HES) gjennom lokale masternoder. Masternodene har mobiltilkobling (GPRS, 4G, 3G, 2G) til HES, mens vanlige AMS-målere tilknyttes masternoden gjennom et radiobasert maskenettverk slik som vist i Figur 2.



Figur 2 Eksempel på maskenettverk for sammenkobling av slave-noder med master-node i AMS for kommunikasjon med HES



Figur 3 Eksempel på et alternativt oppsett for AMS, hvor smartmålerne kommuniserer over radio med en sender montert i nærområdet (ikke i en annen smartmåler), som i sin tur sender videre til HES over 4G

Figur 3 viser et alternativt oppsett for AMS, hvor man ikke er avhengig av masternode i en spesifikk smartmåler. Det monteres en sender i nabolaget som tilstøtende smartmålere kan koble seg opp mot. Denne senderen tar seg av fjernkommunikasjon mot HES. Det finnes også mulighet for å ha direkte kobling til HES fra samtlige smartmålere, samt andre mulige konstellasjoner av nettverket.

3.4 Integrasjon: IDAS

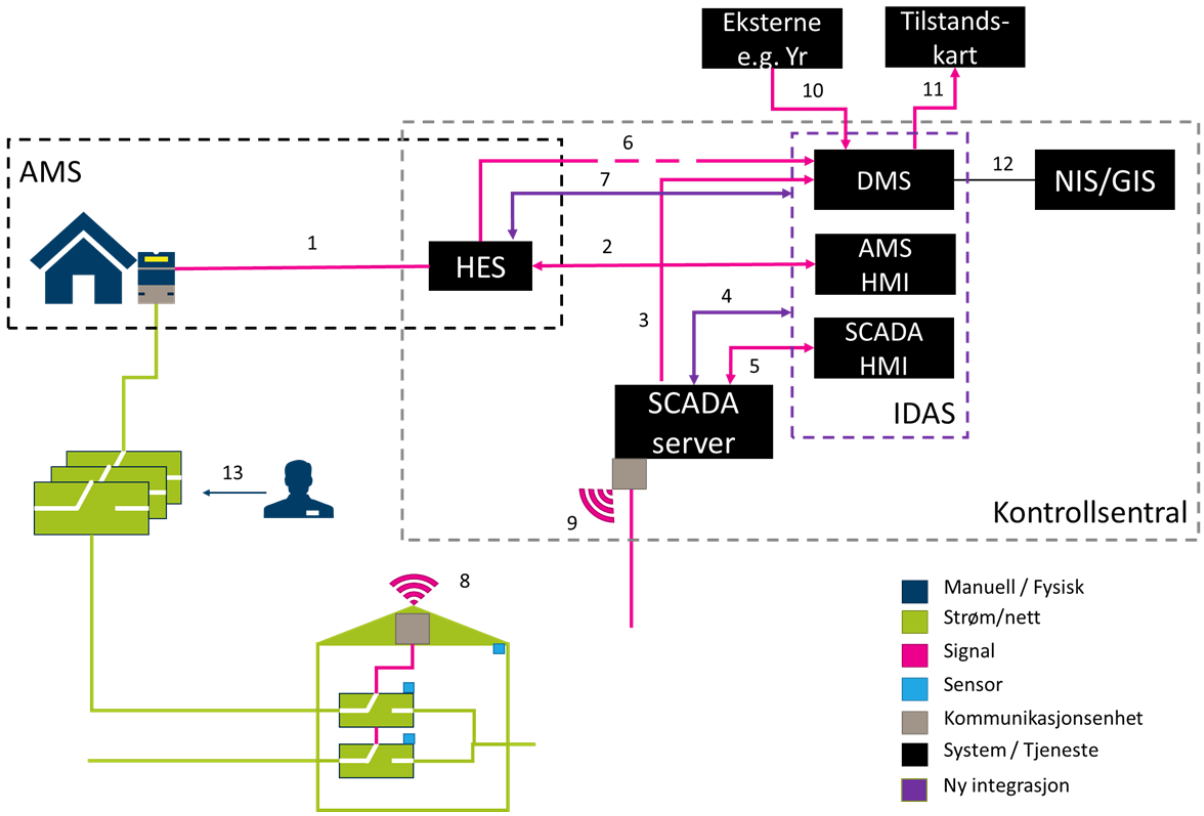
Økt integrasjon i styring av kraftsystemer gjelder alle tilfeller hvor eksisterende systemer knyttes tettere sammen. Spesielt interessant blir dette når systemer som tidligere har vært konstruert for å unngå å falle under kategorien driftskontrollsystemer, kobles sammen med eksisterende driftskontrollsystemer. I denne rapporten ser vi, i tråd med oppdraget, spesifikt på det siste tilfellet uten at vi med det begrenser "økt integrasjon" til å bare gjelde de elementene vi presenterer her.

Tettere integrasjon mellom AMS, DMS og SCADA medfører at DMS kommer tettere på det operative, utover å være et segregert system for økt situasjonsforståelse. Dersom man øker integrasjonen dithen at et system både kan dekke oppgavene til DMS og sende kontrollsignaler til SCADA og AMS vil dette være et driftskontrollsystem[2]. I denne rapporten har vi valgt å kalle dette for *Integrated DMS, AMS and SCADA* (IDAS).

Dagens integrasjon i Norge er basert på at DMS skal benyttes for økt situasjonsforståelse, mens AMS HMI og SCADA HMI benyttes for direkte effektuering av endringer i kraftnettet. IDAS kan komme til å binde sammen separate systemer i fremtiden ved å få flere gjensidige koblinger samt å inneholde funksjonene til DMS, AMS HMI og SCADA HMI – enten ved å koble eksisterende systemer sammen eller å tilby et nytt holistisk system. I den grad nettselskapene har integrasjoner i dag, består dette primært av at AMS-head-end-systemet (vanligvis en ekstern skytjeneste) leverer data til DMS samt at SCADA leverer sensordata og bryterstatus til DMS.

[2] Det kan også diskuteres hvorvidt AMS også blir et driftskontrollsystem i et slikt scenario.

I resten av Europa fremstår det, basert på innspill fra workshop og samtale med bransjen, som om det allerede er en tettere kobling mellom DMS og SCADA ved at DMS kan effektuere endringer direkte. Det er rimelig å anta at tettere integrasjon også vil komme til Norge, gitt at de store utstyrsleverandørene opererer på internasjonal basis.



Figur 4 Høynivåbeskrivelse av integrasjonen mellom AMS, SCADA og DMS. De lilla pilene, samt den stiplede boksen som utgjør IDAS, viser den økte integrasjonen.

Figur 4 viser nå-tilstanden for drift av nett i Norge i tilfeller hvor nettselskapet har tatt i bruk DMS. Videre viser den lilla stiplete boksen hvor IDAS vil manifesteres, i form av tett integrasjon av enten systemer eller funksjonalitet. I tillegg viser de lilla pilene hvilke systemer IDAS vil kommunisere med. Her er integrasjon av data fra AMS mer automatisert og direkte, samtidig som IDAS tillates å kontrollere SCADA direkte. Dette øker angrepsflaten som følge av tettere kobling mellom systemer som tidligere var mer adskilt. I ytterste konsekvens kan man i praksis se for seg at man får et helhetlig IDAS-system som løser oppgavene til både DMS, AMS HMI og SCADA HMI. Tabell 3.1 forklarer de ulike interaksjonene i Figur 4.

Tabell 3.1 Kommunikasjon mellom systemer som vist i Figur 4. Nye interaksjoner ved økt integrasjon er markert med blå bakgrunn.

Grensesnitt	Komponenter		Beskrivelse av hva som overføres
	Fra	Til	
1	Smartmåler	HES	Smartmåleren sender jevnlig måleravlesning til HES, samt melding om evt. feil. Ved strømstans sendes "last gasp" og noen målere kan sende oppdateringer også etter avbrudd.
	HES	Smartmåler	HES sender kontrollmeldinger til smartmåleren. HES kan be om avlesning utenom planlagt intervall, koble ut

Grensesnitt	Komponenter		Beskrivelse av hva som overføres
	Fra	Til	
			bryteren, samt sette begrensning på tillat forbruk før bryter automatisk skal kobles ut (strupefunksjon)
2	HES	AMS HMI	HES tilbyr API for interaksjon. Nettselskapet kan enten bruke grensesnitt tilbudt i HES eller implementere sitt eget.
	AMS HMI	HES	
3	SCADA	DMS	SCADA overfører informasjon om status på brytere og kontrollpunkter i strømnettet til DMS
4	IDAS	SCADA	IDAS overfører kontrollsignaler til SCADA for å effektuere fysiske endringer i nettet direkte fra IDAS. Her kan brytere få endret tilstand
5	SCADA server	SCADA HMI	SCADA HMI er brukergrensesnittet til SCADA-kontrolleren. All tilstandsinformasjon sendes fra SCADA-server til SCADA HMI og kommandoer sendes fra SCADA HMI til SCADA-server
	SCADA HMI	SCADA server	
6	HES	DMS	HES sender over alarmer fra strømnettet slik at de kan settes i operasjonell kontekst i DMS
7	IDAS	HES	Styring av bryter og struping for hver enkelt smartmåler
8	Nettstasjon	SCADA server	Sensordata (fuktighet, temperatur, om døren er åpen/lukket, etc.), måling av belastning på trafo og tilstand på brytere
9	SCADA server	Nettstasjon	Kontrollsignaler for ut- eller innkobling av brytere
10	Eksterne, e.g. Yr	DMS	Overfører relevante oppdateringer fra eksterne kilder som værdata til DMS
11	DMS	Tilstandskart	DMS overfører relevante data (e.g. data som skal offentliggjøres)
12	DMS	NIS/GIS	DMS bygger på NIS/GIS-databasen. Følgelig vil endringer gjort i DMS-grensesnittet reflekteres i NIS/GIS-databasen og vice versa.
13	Montør/ Installatør	Manuell koblingsboks	Endrer manuelt tilstand på brytere

4 Trusselbilde

Mørketallsundersøkelsen for 2018 [8] gjengir noen generelle betraktninger rundt trusselbildet i Norge. Det er observert en økning i virksomheter som utsettes for phishing og dette er den vanligste formen for målrettede angrep ifølge NSM. Man ser også en økning i DDoS-angrep (Distributed Denial of Service), samt at 21 % av virksomhetene rammes av skadevare og virus. I følge mørketallsundersøkelsen er det i stor grad tilfeldigheter som avgjør om angrep oppdages, særlig gjelder dette virksomheter uten et velfungerende styringssystem for informasjonssikkerhet. Gjennom flere år har NSM observert en økning i antall målrettede angrep og innbrudd mot norske interesser. NSM har også sett at for eksempel statlige aktører har blitt mer avanserte i sine angrep og dermed vil være vanskeligere å oppdage. Også Telenor observerer at det stadig er innbrudd fra fremmede makter og at de ofte benytter epost som veien inn i systemer. Angripers mål er i disse tilfeller ofte spionasje og informasjonsakkvisisjon. Også Mnemonic har observert at angrepene blir mer målrettede enn før ved at de rettes mot en spesifikk organisasjon, gruppe, område eller industri.

PST fremholder i sin åpne trusselvurdering for 2018 [9] at kritisk infrastruktur i Norge, deriblant kommunikasjonslinjer og energiforsyning, er attraktive mål for fremmede makter. Det må påregnes at det gjennomføres ulike former for kartlegging både digitalt og ved andre metoder.

Det har vært en rekke angrep mot prosesskontrollsystemer de siste årene. Mest kjent er trolig Stuxnet i 2010 som rammet prosesskontrollsystemer ved et iransk atomanrikelsesanlegg. Her kom man seg forbi forsvarsmekanismer som at systemene ikke var tilkoblet internett. I 2014 ble det gjennomført en stor kampanje for informasjonsinnhenting relatert til kraftindustrien, kalt Dragonfly [13]. Ved hjelp av enkle metoder, samt å bytte ut legitim programvare og oppdateringer med modifiserte og skadelige versjoner, kunne den som kontrollerte skadevaren fremskaffe informasjon om offeret. Dragonfly kunne også oppdateres slik at den teoretisk sett kunne gjøre skade også [14]. I 2015 ble BLACKENERGY 3 brukt til å oppnå kontroll over strømnettet til DSOer i Ukraina. Her ble DMS brukt til å koble ut deler av nettet og RTUer ble ødelagt [15]. Angrepet i 2015 ble utført manuelt, ved at uvedkommende logget seg på SCADA HMI via VPN-tilgang, ved hjelp av passord som var samlet inn ved hjelp av skadevare. I 2016 kom Industroyer, nesten samme angrepet som i 2015, men gjennomført med en modulær skadevare som snakket direkte med SCADA-komponentene heller enn med andre datasystemer [16].

I mars 2018 meldte US-CERT [10] at hackere hadde gjennomført målrettede angrep mot USAs energisektor. I 2017 ble det oppdaget et angrep direkte mot trygghetssystemer (*safety systems*) av typen Triconex fra Schneider Electric [17]. Angrepet er senere tilskrevet Russland [18].

I vår vurdering av uønskede hendelser har vi antatt at slike målrettede angrep kan komme til å skje. Ettersom andre land har blitt rammet tidligere, må man påregne at norske kraftsystem også kan bli utsatt.

5 Identifisering av verdier

SINTEF sin veiledning for risikoanalyse av AMS og tilgrensende systemer [2] anbefaler at før man identifiserer trusler og uønskede hendelser, bør man identifisere hvilke informasjonsverdier som finnes i systemet. I vår analyse har vi avgrenset fokus til verdien av *informasjon*, og sett bort fra verdien til systemet i seg selv. Man må derfor vite hva slags informasjon som skal beskyttes for å kunne bestemme passende sikkerhetsnivå og akseptabel restrisiko. Som diskutert i kapittel 3.4 medfører tettere integrasjon av AMS-DMS og SCADA at informasjon (bryteroperasjoner) pushes fra DMS til SCADA, noe som blir nytt sammenlignet med dagens situasjon. I tillegg blir informasjon om status på brytere i nettet et viktig grunnlag for beslutninger. I denne analysen har vi således valgt å fokusere på tre primære informasjonsverdier:

1) bryteroperasjoner i nettet
2) status på de enkelte bryterne i nettet, og
3) bryteroperasjoner i AMS.

Disse er beskrevet i Tabell 5.1.

I tillegg er det en rekke sekundære informasjonsverdier som må beskyttes, fordi angrep på disse kan ha påvirkning på de primære verdiene. Disse er beskrevet i Tabell 5.2.

Tabell 5.1 Primære verdier

Id	Primære verdier – informasjonsverdier	Konfidensialitet	Integritet	Tilgjengelighet	Lagres (varighet)	Prosesseres	Kommunikasjon
P1	**<u>SCADA-bryteroperasjoner</u>** Endring av tilstand på brytere i distribusjonsnett. Dette gjøres fjernstyrt ved å sende kommando som endrer tilstanden på bryteren. Bryteroperasjoner er viktige fordi de er grunnleggende i opprettholdelsen av nettet. Ved kontroll over bryteroperasjoner vil en aktør kunne koble ut hele eller deler av nettet, samt at det vil være vanskelig for den virkelige operatøren å fikse problemet uten å koble ut all fjernkommunikasjon og gå tilbake til manuell styring.	X	X	X	n/a	SCADA HMI + IDAS: Mottar beslutning fra LFK (eller muligens algoritmer i fremtiden). SCADA-server: mottar kommando fra SCADA HMI eller DMS og sender denne til riktig bryter i nettet. Fjernstyrte brytere: mottar kommando og endrer tilstand på bryteren.	Sendes fra IDAS eller SCADA HMI til SCADA-server før det går kablet eller trådløst ut til PLC.

Id	Primære verdier – informasjonsverdier	Konfidensialitet	Integritet	Tilgjengelighet	Lagres (varighet)	Prosesseres	Kommunikasjon
P2	**<u>SCADA-bryterstatus</u>** Status på de enkelte bryterne i distribusjonsnettet. Dette er sanntidsinformasjon tilgjengelig for driftssentralen. Bryterstatus er viktig fordi 1) det kan brukes av andre for å kartlegge nettet, 2) feilaktig bryterstatus medfører at operasjoner på kontrollsenteret vil ødelegge eget nett istedenfor å vedlikeholde det og 3) mangel på oppdatert bryterstatus kan medføre at LFK iverksetter endringer som kan medføre unødvendige endringer eller endringer som medfører fare for liv og helse.	X	X	X	DMS (lagres frem til neste oppdatering). SCADA (lagres kontinuerlig).	Brytersensor: genererer og sender status for automatiserte brytere. SCADA-server: mottar signaler fra bryter-sensorer og tilgjengeliggjør disse før SCADA HMI. SCADA HMI og DMS: viser informasjon til operatør.	Går kablet eller over 4G til SCADA-server før tilgjengeliggjøring i SCADA-HMI og IDAS.

Id	Primære verdier – informasjonsverdier	Konfidensialitet	Integritet	Tilgjengelighet	Lagres (varighet)	Prosesseres	Kommunikasjon
P3	**<u>AMS-bryteroperasjoner</u>** To kategorier: bryter og struper. Hvis bryteoperasjoner kan manipuleres kan enkelte husholdninger kobles inn eller ut av uautorisert aktør. Hvis funksjonen ikke er tilgjengelig må noen ut for å koble ut manuelt. I et lengre perspektiv kan utilgjengelighet for eksempel lede til at alvorlige feil i enkelthushold ikke isoleres fra resten av nettet[3].		X	X	n/a	HES, IDAS, Smartmåler	Sendes fra HES til den enkelte smartmåler over 4G via masternode i maskenettverk eller mastnode. Radio lokalt, 4G til sentral. Kommunikasjonen er angivelig kryptert. Sende direkte adressert (kan ikke kringkastes).

[3] Dette er et eksempel på at når man i fremtiden gjør seg avhengig av en ny funksjonalitet medfører bortfall av funksjonaliteten problemer, til tross for at man ikke har disse problemene i dag.

Tabell 5.2 Sekundære verdier

Id	Sekundære verdier (informasjon, tjenester, programvare og nettverksforbindelser)	Konfidensialitet	Integritet	Tilgjengelighet	Lagres (varighet)	Prosesseres	Kommunikasjon
S1	**<u>Status AMS-bryter</u>** Rapporterer status på bryter i den enkelte smartmåler. Manipulering av status kan gi et feilaktig bilde av nettet og potensielt medføre at skadelige handlinger blir iverksatt i et mindre område. Støtter primærverdi: P3		X	X		Smartmåler, HES, DMS, IDAS	Sendes fra smartmåler til HES over 4G via enten maskenett med masternode eller dedikert masternode. Radio lokalt, 4G til sentral. Kommunikasjonen skal være kryptert.
S2	**<u>Sensordata</u>** Rapporterer status på ulike målepunkt i nettet. Dette kan være effektmålinger, temperatur, vind, fuktighet, slitasje på deler, etc. Forskjellige typer sensordata kan korreleres med bryterstatus for å detektere avvik. Manipulering av sensordata kan bidra til å skjule manipulering av primærverdiene. Støtter primærverdi: P1, P2, P3		X	X		Sensorer, SCADA-server, SCADA HMI, DMS, IDAS	Aggregeres i nettet og sendes via kabel eller 4G til SCADA-server som i tur tilgjengeliggjør for SCADA HMI og DMS.

Id	Sekundære verdier (informasjon, tjenester, programvare og nettverksforbindelser)	Konfidensialitet	Integritet	Tilgjengelighet	Lagres (varighet)	Prosesseres	Kommunikasjon
S3	**NIS/GIS-data** Representerer topologien til strømnettet gjennom ledningsdata om hvordan strømnettet er satt sammen, hvilke koblinger som ligger hvor, hvilke ledninger som ligger hvor og er koblet til hva, etc. Støtter primærverdi: P1, P2	X	X	X	Database i DMS-nettverket	DMS	NIS data importeres til DMS fra database.
S4	**AMS målerdata** Smartmålerne rapporterer kundens forbruk, alarmer, hendelser (e.g. jordfeil) til HES. Støtter primærverdi: P3	X	X	X		Smartmåler, HES, fakturasystem, [DMS]	Sendes fra smartmåler til HES over 4G via enten maskenett med masternode eller dedikert mastnode. Radio lokalt, 4G til sentral. Kommunikasjonen er angivelig kryptert. Hentes ut fra HES ved hjelp av API.

Id	Sekundære verdier (informasjon, tjenester, programvare og nettverksforbindelser)	Konfidensialitet	Integritet	Tilgjengelighet	Lagres (varighet)	Prosesseres	Kommunikasjon
S7	**<u>Autentiseringsinformasjon</u>** Administratorinformasjon på avveier kan medføre at uvedkommende får tilgang til å utforske systemet samt iverksette uønskede handlinger som kan medføre at strømnettet ikke lenger fungerer som tiltenkt. Støtter primærverdi: P1, P2, P3	X	X			Alle steder for innlogging og autorisasjon	n/a
S8	**<u>Krypteringsnøkler</u>** Krypteringsnøkler sikrer data i kommunikasjon, samt når de er lagret. Krypteringsnøkler på avveie kan medføre tap av sikkerhet i utvalgte kommunikasjonslinjer, eller i verste fall bortfall av all sikkerhet. I ytterste konsekvens kan dette medføre strømstans. Støtter primærverdi: P1, P2, P3	X	X	X		Smartmåler, HES, SCADA-server, PLC'er	n/a
S9	**<u>Systemdokumentasjon</u>** Detaljerte instruksjoner vedrørende kontrollsystemets fysiske sammensetning, benyttet maskinvare, programvare, sikkerhetskonfigurasjoner og bruksveiledning. Støtter primærverdi: P1, P2, P3		X	X		n/a	n/a

Id	Sekundære verdier (informasjon, tjenester, programvare og nettverksforbindelser)	Konfidensialitet	Integritet	Tilgjengelighet	Lagres (varighet)	Prosesseres	Kommunikasjon
S10	**Software: HES** HES samler inn data fra smartmålere og sender styringssignal som kan medføre ekstramåling eller endring av brytere og strupefunksjon. Støtter primærverdi: P3		X	X		I leverandørens (sky)tjeneste	n/a
S11	**Software: SCADA-server** SCADA-server er hjernen i SCADA-oppsettet. Herifra sendes styringssignal til alle fjernstyrte brytere og hit samles alle sensordata fra nettverket. Støtter primærverdi: P1, P2		X	X		Servere hos nettoperatør	n/a
S12	**Software: IDAS** IDAS samler all styring av nettet i et system. Herifra kan man oppdatere NIS/GIS, gjøre endringer i nettet, styre smartmålere, samt ha innsyn i tilstander og rapporter. Støtter primærverdi: P1, P2, P3		X	X		Servere hos nettoperatør	n/a
S13	**Software: Skyintegrasjoner** Integrasjoner av IDAS og andre systemer mot nettskyen øker angrepsflaten		X				n/a

Id	Sekundære verdier (informasjon, tjenester, programvare og nettverksforbindelser)	Konfidensialitet	Integritet	Tilgjengelighet	Lagres (varighet)	Prosesseres	Kommunikasjon
S14	**<u>Programvare-/firmwareoppdateringer</u>** Oppdateringer er viktige for at systemet skal fungere på en sikker og trygg måte. Oppdateringer som distribueres og iverksettes feil har samtidig potensiale til å gjøre stor skade og være en enkel vei inn i ellers godt beskyttede systemer.		X	X	Hos leverandør	På enheter som oppdateres	n/a
S15	**<u>Nettverk: kommunikasjonsinfrastruktur</u>** For at styringssignaler skal nå frem til fjernstyrte brytere og data fra brytere skal nå kontrollsentralen, er man avhengig av kommunikasjonsinfrastrukturen – enten den er trådløs eller kablet. Forstyrrelse av kommunikasjonsinfrastrukturen kan få store følger for funksjonaliteten av systemet.			X	n/a	n/a	Trådløst eller kablet

6 Uønskede hendelser

En risikoanalyse inkluderer å kartlegge og vurdere mulige uønskede hendelser. Uønskede hendelser inkluderer hendelser som medfører brudd på informasjonssikkerhet, dvs. brudd på konfidensialitet, integritet eller tilgjengelighet relatert til identifiserte verdier.

Uønskede hendelser kan grovt deles inn i tre typer basert på årsak [2]:

- *Tilfeldige hendelser*: Dette er hendelser som skjer tilfeldigvis eller ved uhell. Eksempler kan være lynnedslag, svikt i strømforsyning, brann, diskkrasj, kommunikasjonsfeil og menneskelige feil.
- *Generelle angrep*: Disse skjer ved at man blir offer for et eller flere av de angrepene som til stadighet spres på Internett. Generelle angrep er ikke rettet spesielt mot AMS, DMS eller SCADA, men heller mot IKT-system generelt. Eksempler kan være HMI som rammes av virus, ekstern kommunikasjon som rammes av tjenestenekt mot kommunikasjonsleverandør.
- *Målrettede angrep*: Disse er rettet mot det spesielle systemet som vurderes i denne analysen, med mål om å ramme noen av organisasjonene som vil være involvert i driften, eller mot strømforsyningen i Norge generelt. 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. Egne ansatte kan også (bevisst eller ubevisst) være delaktige i slike angrep. Trusselbildet som ligger til grunn for målrettede angrep er blitt beskrevet i kapittel 4 av denne rapporten.

I denne rapporten er det primære fokuset uønskede hendelser av typen generelle og målrettede angrep som er relevante for de tre primære informasjonsverdiene: "SCADA-bryteroperasjoner", "SCADA-bryterstatus" og "AMS bryteroperasjoner" (se Tabell 5.1). Noen av hendelsene vil også ramme de sekundære verdiene.

Risiko er en kombinasjon av sannsynlighet og konsekvens. De uønskede hendelsene ble vurdert utfra hvilken konsekvens de har for nettselskapene, nettselskapenes kunder og det norske samfunnet og hvor sannsynlig det er at de vil inntreffe. I sannsynlighetsdimensjonen er det relevant å ta med hvor enkelt/vanskelig det er å gjennomføre angrepet, hvorvidt sikkerhetsmekanismer allerede er blitt implementert og hvorvidt slike angrep er blitt observert før. Valget av konsekvensdimensjon bestemmer hva man ønsker å vurdere risiko for. I energibransjen skal forsyningssikkerhet alltid inngå som konsekvensdimensjon. Andre relevante konsekvenser er personellsikkerhet og økonomi [7].

Skala for sannsynlighet og konsekvens som er blitt brukt i denne analysen finnes i vedlegg A og B.

Følgende matrise ble brukt for å klassifisere hendelser:

Sannsynlighet: høy	4	8	12	16
	3	6	9	12
	2	4	6	8
Sannsynlighet: lav	1	2	3	4
	Konsekvens: lav			høy

Risiko ble kalkulert som sannsynlighet * konsekvens der:

- Rød betyr høy risiko (verdi 12-16)
- Oransje betyr middels høy risiko (verdi 8-9)
- Gul betyr middels lav risiko (verdi 4-6)
- Grønn betyr lav risiko (verdi 1-3)

6.1 Forbehold

Merk at denne klassifiseringen i rød, oransje, gul og grønn er et forslag fra vår side i denne rapporten.

Bransjen må selv ta stilling til hvilken risiko de anser som uakseptabel, og dermed trenger å gjøre noe med i form av tiltak.

6.2 Identifisering og vurdering av uønskede hendelser

Tabell 6.1 presenterer de uønskede hendelsene identifisert gjennom workshop med bransjen og påfølgende dokumentstudier ([1][2][3][5][7][12]). Tabellen inneholder ikke alle mulige hendelser; vi har valgt å fokusere på hendelser som har direkte konsekvens for primærverdiene identifisert i denne analysen og som er innenfor oppdragets ramme.

Hendelser som medfører bortfall av funksjonalitet vil ha forskjellige alvorlighetsgrad avhengig av hvor lenge hendelsen varer. I vår analyse har vi i de fleste tilfellene antatt at bortfallet varer så lenge at det medfører behov for å sende ut personell for manuell håndtering av hendelsen.

Tabell 6.1 Uønskede hendelser som har direkte konsekvens for primærverdiene

ID	Uønsket hendelse	Primærverdi	Konfidensialitet	Integritet	Tilgjengelighet	Konsekvens	Alvorlighet	Sannsynlighet	Risiko
H1	Avlytting av kommandoer som endrer tilstand på brytere samt statusmeldinger fra fjernstyrte brytere i distribusjonsnett.	SCADA-bryteroperasjoner (P1), SCADA-bryterstatus (P2).	X			Kan kartlegge topologien av nettet, samt oppnå forståelse av kommunikasjonsmønster.	1	3	3

ID	Uønsket hendelse	Primærverdi	Konfidensialitet	Integritet	Tilgjengelighet	Konsekvens	Alvorlighet	Sannsynlighet	Risiko
H2	Uvedkommende sender falske kommandoer med bryteroperasjoner til fjernstyrte brytere i distribusjonsnettet.	SCADA-bryteroperasjoner (P1).		X		Kan koble ut hele eller deler av nettet, samt utøve skade på utstyr og nett som medfører større og langvarig strømbrudd. I verste fall kan dette medføre utkobling av store områder inklusivt sykehus og annen samfunnskritisk infrastruktur.	4	3[4]	12
H3	Tjenestenektangrep som rammer kommunikasjonslink til en enkelt eller noen få fjernstyrte brytere i et begrenset område i distribusjonsnettet.	SCADA-bryteroperasjoner (P1), SCADA-bryterstatus (P2).			X	Får redusert innsikt i status, samt forsinkelse i mulighet til å effektuere endringer i nettet som følge av å måtte sende ut personell.	1	2[5]	2

[4] Observert gjennomført i Ukraina i tilfellet fullintegrert DMS og SCADA
[5] De viktigste selskapene i Norge har krav til redundant kommunikasjon i driftskontrollsystemet, slik at feil i én kommunikasjonslinje ikke medfører funksjonssvikt [11].

ID	Uønsket hendelse	Primærverdi	Konfidensialitet	Integritet	Tilgjengelighet	Konsekvens	Alvorlighet	Sannsynlighet	Risiko
H4	Målrettet angrep mot SCADA-server slik at tilstand på brytere i distribusjonsnettet ikke kan fjernstyres.	SCADA-bryteroperasjoner (P1), SCADA-bryterstatus (P2).			X	Vesentlig redusert innsikt i eget nett samt evne til å effektuere endringer i nettet som følge av å måtte sende personell til samtlige brytere for både tilstand og endring.	2	2	4
H5	Angrep mot sentral kommunikasjonsinfrastruktur som hindrer kommunikasjon med fjernstyrte brytere.	SCADA-bryteroperasjoner (P1), SCADA-bryterstatus (P2), (Denne hendelser rammer også den sekundære verdien Kommunikasjonsinfrastruktur.)			X	Vesentlig redusert innsikt i eget nett samt evne til å effektuere endringer i nettet som følge av å måtte sende personell til samtlige brytere for både tilstand og endring.	2	3	6
H6	Rapportering av falsk bryterstatus til SCADA-server.	SCADA-bryterstatus (P2).		X		Kan iverksette endringer i nettet som kan forårsake skade på nettet og folk heller enn å stabilisere.	3	3[6]	9

[6] Observert i f.eks. Stuxnet

ID	Uønsket hendelse	Primærverdi	Konfidensialitet	Integritet	Tilgjengelighet	Konsekvens	Alvorlighet	Sannsynlighet	Risiko
H7	Uvedkommende utfører endring i DMS-delen av IDAS som medfører at uhensiktsmessige SCADA bryteroperasjoner effektueres.	SCADA-bryteroperasjoner (P1), SCADA-bryterstatus (P2). (Denne hendelser rammer også den sekundære verdien IDAS.)		X		Kan koble ut hele eller deler av nettet, samt utøve skade på utstyr og nett som medfører større og langvarig strømbrudd. I verste fall kan dette medføre utkobling av store områder inklusivt sykehus og annen samfunnskritisk infrastruktur.	4	3[7]	12

[7] Dersom man tar dagens DMS uendret inn i IDAS vil sannsynligheten være større som følge av at DMS har flere kontaktpunkter mot omverden og har lavere krav om sikring.

ID	Uønsket hendelse	Primærverdi	Konfidensialitet	Integritet	Tilgjengelighet	Konsekvens	Alvorlighet	Sannsynlighet	Risiko
H8	Tjenestenektangrep som rammer kommunikasjonslink ut til en eller flere kunder i nettet.	AMS-bryteroperasjoner (P3). (Denne hendelser rammer også den sekundære verdien Status AMS-bryter.)			X	Bryter og struping i AMS påregnes å bli brukt forholdsvis sjeldent per kunde, men bortfall av kommunikasjonslink kan medføre redusert innsikt i eget nett. Forsinkelse for nettselskap med utbedring som følge av å måtte benytte manuell arbeidskraft til å utføre endringer i husstanden. Situasjonen er identisk med slik privathusholdninger driftes i dag, men med potensielt redusert arbeidsstokk vil dette kunne være belastende for nettselskapet.	1	4[8]	4
H9	Uvedkommende får kontroll over AMS - bryterfunksjonalitet på et hus.	AMS-bryteroperasjoner (P3).		X		En enkelt husstand utkoblet.	1	2	2

[8] Med bruk av sammensatt kommunikasjonsteknologi med radio, mobilnettverk, kobber og liknende, vil utfall av kommunikasjon måtte påregnes.

ID	Uønsket hendelse	Primærverdi	Konfidensialitet	Integritet	Tilgjengelighet	Konsekvens	Alvorlighet	Sannsynlighet	Risiko
H10	Uvedkommende utfører bryteroperasjoner på en gruppe av husstander.	AMS-bryteroperasjoner (P3).		X		Vilkårlig mange husstander utkoblet.	4	2[9]	8
H11	Uvedkommende setter vilkårlig mange smartmålere ut av spill ("bricking").	AMS-bryteroperasjoner (P3). (Denne hendelser rammer også den sekundære verdien Status AMS-bryter.)		X	X	Mister innsikt i nettet og mister evne til å koble ut husstander med alvorlige feil på sitt strømnett. Påfører nettselskapet merkostnader i reparasjoner og manglende rapportering av forbruk. Måling i nettstasjon vil gi aggregert informasjon, og avhjelpe litt på problemet med manglende data for enkeltkunder.	2	2	4

En oversikt over risiko av disse hendelsene finnes i Tabell .2.

[9] Lavere sannsynlighet å finne mange nøkler for gruppeutkobling av mange husstander enn å finne nøkkel for én. Dog trolig ikke tilstrekkelig redusert sannsynlighet til at det rettferdiggjør verdien 1. Det finnes ikke noen funksjon for gruppeutkobling i AMS, men det fremstår enkelt å lage sin egen på bakgrunn av tilgjengelig informasjon

Tabell 6.2 Risiko av de uønskede hendelsene identifisert i Tabell 6.1

Sannsynlighet: høy	H8			
	H1	H5	H6	H2, H7
	H3, H9	H4, H11		H10
lav				
	Konsekvens: lav			høy

6.3 Hendelser med høy risiko

To hendelser er vurdert til å ha høy risiko (rød). Disse er:

- H2: Uvedkommende sender falske kommandoer med SCADA bryteroperasjoner til fjernstyrte brytere i distribusjonsnettet.
- H7: Uvedkommende utfører endring i DMS-delen av IDAS som medfører at uhensiktsmessige SCADA bryteroperasjoner effektueres.

Disse hendelsene er av tilsvarende alvorlighet som hendelsene i Ukraina i 2015 og 2016 [15]. Dette vil medføre utkobling av store deler av kraftnettet, med alvorlige konsekvenser for liv, helse og viktige samfunnsfunksjoner.

Observer: klassifiseringen av alvorlighet av risiko i rød, oransje etc. er et forslag fra SINTEF – se forbehold i avsnitt 6.1.

6.4 Hendelser med middels høy risiko

To hendelser er vurdert til å ha middels høy risiko (oransje). Disse er:

- H6: Rapportering av falsk bryterstatus til SCADA-server
- H10: Uvedkommende utfører bryteroperasjoner på en gruppe av husstander

Disse hendelsene vil få konsekvenser for nabolag og potensielt større områder. Effekten vil være mer indirekte enn en angripers mulighet til å direkte effektuere endringer i nettet som beskrevet over.

6.5 Hendelser med middels lav eller lav risiko

Resterende hendelser ble vurdert til å ha enten middels lav risiko (gul) eller lav risiko (grønn). For disse er det ikke nødvendig å redusere risiko, men som diskutert i neste kapittel så er det noen anbefalte tiltak som vil ytterligere redusere risiko også for disse.

6.6 Andre uønskede hendelser som bør hensyntas ved implementasjon av et konkret system

Vi har vurdert et tenkt, fremtidig system som enda ikke er implementert. Ettersom vi da ikke har detaljerte implementasjonsdetaljer, har vi fokusert på trusler og vurderinger knyttet til de identifiserte primærverdiene i denne analysen. Likefullt er det vurderinger som må gjøres opp mot sekundærverdiene. Disse vurderingene vil være tett koblet til konkrete systemer, og vi anbefaler at dette gjøres i den faktiske planleggingen og utbyggingen av systemene når den tid kommer. Dette innebærer bl.a. å fylle ut de grå feltene i Tabell 6.33 – merk at tabellen ikke er ment å være uttømmende.

Tabell 6.3 Uønskede hendelser som må vurderes for konkrete systemer og implementasjoner.

ID	Uønsket hendelse	Sekundærverdi	Konfidensialitet	Integritet	Tilgjengelighet	Konse-kvens	Alvorlighet	Sannsynlighet	Risiko
H12	Uvedkommende kan avlese målerverdier fra smartmåler	AMS målerdata (S4)							
H13	Manipulering av målerverdier								
H14	Avlytting av meldinger som inneholder bryterstatus	Status AMS-bryter (S1)							
H15	Rapportering av falsk bryterstatus til HES								
H16	Field Area Network (FAN) aksess brukt til å bryte inn i sentrale systemer (HES og mer) hvilket medfører uautorisert modifikasjon av HES	Software: HES (S10)							
H17	Uautorisert avlytting av sensordata	Sensordata (S2)							
H18	Uautorisert manipulering av sensordata								
H19	Uautorisert tilgang til NIS/GIS	NIS/GIS-data (S3)							
H20	Uautorisert manipulering av NIS/GIS								
H21	Uautorisert adgang som følge av autentiseringsinformasjon på avveie	Autentiseringsinformasjon (S7)							
H22	Uautorisert adgang som følge av for svak autentisering								
H23	Krypteringsnøkler på avveie	Krypteringsnøkler (S8)							
H24	Brutt kryptering som følge av for svak kryptering								

7 Anbefalinger om tiltak

Dette kapittelet gir forslag på tiltak som bør vurderes gjennomført. Disse er sammenfattet i Tabell 7.1 som viser en oversikt over tiltak, knyttet til hendelser. Det er viktig å påpeke at dette ikke er ment som en uttømmende liste, og tiltakene må vurderes opp mot bransjens egen vurdering av akseptabel risiko.

Tabell 7.1 Anbefalte tiltak.

ID	Tiltak	Gjelder hendelse
T1	Autentisering, integritets- og konfidensialitetsbeskyttelse av alle SCADA-meldinger (SCADA-bryteoperasjoner: primær verdi P1 og SCADA-bryterstatus: primær verdi P2). Dette kan implementeres gjennom oppsett av sikre sesjoner mellom de kommuniserende entiteter. For forbindelsesløs kommunikasjon må hver enkelt melding beskyttes.	H1, H2, H6
T2	Sikre AMS bryterfunksjonalitet (AMS- bryteoperasjoner: Primær verdi P3) iht. veileder utgitt av NVE [12]	H9, H10
T3	Definere og håndheve prosedyrer og kriterier for tilgangskontroll til systemer og utstyr i IDAS (DMS, AMS-HMI og SCADA HMI).	H7
T4	Uavhengige redundante kommunikasjonslinjer, gjerne over ulike bærere (trådløs/fiber/etc.) levert av ulike leverandører	H3, H5, H8
T5	Herding, dvs. fjerning av unødvendige tjenester og konfigurering av gjenværende tjenester til høyeste sikkerhetsnivå, av SCADA-server	H4, H6
T6	Segmentering av SCADA-nettet, dvs. oppdeling av nettet i forskjellige sikkerhetssoner.	H3, H4, H5
T7	Brannmur mellom IDAS og omverdenen	H3, H4
T8	Inntrengningsdeteksjonsmekanismer tilknyttet SCADA-server	H4
T9	Innføre regime for signering av all programvare og oppdateringer som skal installeres på SCADA-komponenter, kun tillate installering ved korrekt signatur	H11
T10	Gjennomfør kontinuerlig sårbarhetsskanning på de ulike delene av systemet – inkludert eksterne avhengigheter	Alle
T11	Gjennomfør penetrasjonstesting og bruk "Red Team"[10] på de ulike delene av systemet – inkludert eksterne avhengigheter	Alle
T12	Bare tillat tilkoblinger fra hvitelistede kilder/aktører/systemer	Alle
T13	Benytt sertifikater for sikring av kommunikasjon og besørg at sertifikatene er tilstrekkelig godt sikret, samt at utbytting og oppdatering av sertifikater skjer på en sikker måte	H1, H2, H6, H9, H10, H11

[10] "Red Team" er en gruppe ansatte som påtar seg rollen som angriper for å forsøke å finne flest mulig feil/problemer å utbedre

8 Konklusjon

Økt integrasjon av SCADA, DMS og AMS medfører at systemer som opprinnelig ble designet for å være selvstendige, kobles sammen og blir avhengige av hverandre. Spesielt interessant blir dette når systemer som tidligere har vært konstruert for å unngå å falle under kategorien driftskontrollsystemer, kobles sammen med eksisterende driftskontrollsystemer.

Denne rapporten har primært sett på uønskede hendelser knyttet til følgende verdier:

- SCADA-bryteroperasjoner
- SCADA-bryterstatus
- AMS-bryteroperasjoner

I vår vurdering av uønskede hendelser har vi antatt at målrettede angrep kan komme til å skje. En rekke hendelser viser at andre land har blitt rammet tidligere, og man må derfor påregne at norske system også kan bli utsatt for slike målrettede angrep.

Følgende uønskede hendelser er vurdert til å ha høy risiko:

- H2: Uvedkommende sender falske kommandoer med SCADA bryteroperasjoner til fjernstyrte brytere i distribusjonsnettet.
- H7: Uvedkommende utfører endring i DMS-delen av IDAS som medfører at uhensiktsmessige SCADA bryteroperasjoner effektueres.

Det er risiko ved økt integrasjon, men rapporten presenterer også en rekke tiltak som kan redusere risikoen for de uønskede hendelsene. Bransjen oppfordres til å bruke disse som et utgangspunkt, men utvide både risikovurderingen og tiltakene i tråd med det konkrete systemet de utvikler. Det er også tjenlig om bedriftene gir en ansatt i oppgave å ha et spesielt fokus på uforutsette hendelser som potensielt kan få store konsekvenser om de inntreffer; såkalte *svarte svaner*.

9 Referanser

[1] ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management (3rd edition)

[2] Informasjonssikkerhet og personvern: Støtte til risikoanalyse av AMS og tilgrensende systemer. SINTEF rapport A24258, 2014

[3] Risikovurdering av AMS. Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS. SINTEF rapport A22318, 2012.

[4] Lovdata: Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften), Kapittel 7: Beskyttelse av driftskontrollsystem. https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157#KAPITTEL_7

[5] Inger Anne Tøndel, Martin Gilje Jaatun og Maria Bartnes Line: "Security Threats in Demo Steinkjer" SINTEF Report A23351, September 2012, https://brage.bibsys.no/xmlui/handle/11250/2382059

[6] Inger Anne Tøndel, Martin Gilje Jaatun og Maria Bartnes Line (2013) "Threat Modeling of AMI", In: Hämmerli B.M., Kalstad Svendsen N., Lopez J. (eds) Critical Information Infrastructures Security. CRITIS 2012. Lecture Notes in Computer Science, vol 7722. Springer, Berlin, Heidelberg

[7] Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen. Norges vassdrags- og energidirektorat, 2010

[8] Mørketallsundersøkelsen 2018, Næringslivets sikkerhetsråd, 2018

[9] Trusselvurdering 2018, PST, 2018

[10] Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, US-CERT, Mars 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A, Sist sett: 22.10.2018

[11] NOU 2015:13 Digital sårbarhet – sikkert samfunn.

[12] Frank Skapalen, Bjørn Jonassen. Veileder til sikkerhet i avanserte måle- og styringssystem. Norges vassdrags- og energidirektorat, 2012.

[13] Dragonfly: Western Energy Companies Under Sabotage Threat. 30 juni 2014. https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat-energetic-bear Sist sett: 24.10.2018

[14] Dragonfly: Western energy sector targeted by sophisticated attack group. 20 oktober 2017. https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks Sist sett: 24.10.2018

[15] Analysis of the Cyber Attack on the Ukrainian Power Grid. E-ISAC, March 18, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[16] WIN32/INDUSTROYER: A new threat for industrial control systems. Anton Cherepanov, ESET. Version 2017-06-12. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

[17] TRISIS, 14.12.2017, Dragos, https://dragos.com/blog/trisis/ Sist sett: 30.10.2018

[18] TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers, 23.10.2018, FireEye, https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html Sist sett: 30.10.2018

A Skala for sannsynlighet

1 = Usannsynlig

a) Sjeldnere enn hvert tiende år
b) Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten
c) Tiltakene kan kun omgås/brytes av egne medarbeidere med gode ressurser, og god/fullstendig kjennskap til tiltakene.
d) Eksternt personell kan ikke omgå/bryte tiltakene. Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap.
e) Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.
f) Det finnes ikke noen kjente eksempel på slike angrep.

2 = Mindre sannsynlig

a) Årlig
b) Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten.
c) Tiltakene kan likevel omgås/brytes av egne medarbeidere med små til normale ressurser, som i tillegg har normal kjennskap til tiltakene.
d) Eksternt personell trenger gode ressurser, og god/fullstendig kjennskap til tiltakene for å omgå/bryte disse.
e) Utenforstående må opptre med overlegg og ha noe kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene
f) Lignende angrep har forekommet i andre sammenhenger og kan i teorien også ramme kraftbransjen.

3 = Mulig

a) Flere ganger i året
b) Sikkerhetstiltak er ikke fullt etablert, eller fungerer ikke etter hensikten.
c) Egne medarbeidere trenger kun små til normale ressurser for å omgå/bryte tiltakene, det er ikke nødvendig med kjennskap til tiltakene.
d) Eksternt personell trenger normal kjennskap til tiltakene (eksempelvis til hvilke rutiner som gjelder, eller hvordan sikkerhetsteknologi er implementert), i tillegg til små/normale resurser. Inngrep forutsetter forsett (bevisst eller aktivt) for å bryte sikkerhetstiltakene
e) Slike angrep er blitt observert i kraftbransjen før.

4 = Sannsynlig

a) Flere ganger pr. måned
b) Sikkerhetstiltak er ikke etablert, eller kan omgås/brytes av egne medarbeidere og eksternt personell med små til normale resurser.
c) Det er ikke nødvendig med kjennskap til tiltakene.
d) Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående.
e) Slike angrep er vanlig forekommende i kraftbransjen.

B Skala for konsekvens

1 = Ubetydelig

- Ubetydelig eller liten konsekvens for privatabonnenter.
- Ikke avbrudd i strømforsyning.
- Ingen skade på utstyr
- Ubetydelig økonomisk tap

2 = Moderat

- Noen lokale konsekvenser for privatabonnenter.
- Et begrenset antall kunder mister strømmen under kortere tid.
- Mindre skader på utstyr
- Gjenopprettelig økonomisk tap

3 = Alvorlig

- Alvorlige konsekvenser i infrastruktur og lokalsamfunnet.
- Lengre avbrudd hos et begrenset antall kunder.
- Skader på nettet og/eller skader på personell.
- Alvorlig økonomisk tap

4 = Kritisk

- Samfunnsviktige funksjoner som liv og helse, samt viktig infrastruktur rammet / satt ut av funksjon
- Store deler av netter utkoblet under lengre tid.
- Meget store skader på utstyr eller tap av liv.
- Uopprettelig økonomisk tap

SINTEF

Teknologi for et bedre samfunn

www.sintef.no

NVE

Norges vassdrags- og energidirektorat

MIDDELTHUNSGATE 29
POSTBOKS 5091 MAJORSTUEN
0301 OSLO
TELEFON: (+47) 22 95 95 95

www.nve.no