2018:00007 - Åpen

# Rapport

## Cybersikkerhet i digitale transformator-stasjoner

Forprosjekt

**Forfatter(e)**
Martin Gilje Jaatun, SINTEF Digital
Marie Elisabeth Gaup Moe, SINTEF Digital
Maren Istad, SINTEF Energi

**SINTEF Digital**
Cyber Security and Safety
2018-01-05

SINTEF Digital
Postadresse:
Postboks 4760 Torgarden
7465 Trondheim
Sentralbord: 73593000

info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

# Rapport

# Cybersikkerhet i digitale transformatorstasjoner

Forprosjekt

EMNEORD:
Sikkerhet
Konfidensialitet
Integritet
Tilgjengelighet
Smartgrid

**VERSJON**
1.0

**DATO**
2018-01-05

**FORFATTER(E)**
Martin Gilje Jaatun, SINTEF Digital
Marie Elisabeth Gaup Moe, SINTEF Digital
Maren Istad, SINTEF Energi

**OPPDRAGSGIVER(E)**
Statnett

**OPPDRAGSGIVERS REF.**
Innkjøpsordre 39471

**PROSJEKTNR**
102014960

**ANTALL SIDER OG VEDLEGG:**
33

**SAMMENDRAG**

Dette notatet beskriver konseptet digital transformatorstasjon, og skisser relevante cyber-relaterte sårbarheter og mottiltak. For grunnleggende sikkerhetsnivå (basisnivå) anbefaler vi at det gjennomføres risikoanalyse med henblikk på cyberangrep for en representativ digital transformatorstasjon, at det gjøres øvelser og trening basert på NVEs scenarioer for IKT-hendelser, at det innføres monitorering av nettverkstrafikk med anomalideteksjon, logging og logganalyse, konfigurasjonskontroll på fysiske og logiske komponenter, og at det etableres gode passord på alle komponenter. For utvidet sikkerhet anbefaler vi full-kryptering av all IEC 61850-trafikk i feltet (må veies mot ulempene kryptering medfører for monitorering), redundans av kritiske komponenter med failover, anomalideteksjon på sensormålinger (med ekstra sensorer for validering), etablering av "nødknapp" for enkel nettverks-segregering ved behov, og at det innføres tofaktor autentisering mot alle komponenter. Videre anbefaler vi at det foretas risikoanalyser med henblikk på cyberangrep for hver enkelt transformatorstasjon, og at det utarbeides nye scenarioer for cyber-hendelser spesifikt for digitale transformatorstasjoner.

**UTARBEIDET AV**
Martin Gilje Jaatun
SIGNATUR

**KONTROLLERT AV**
Christian Frøystad
SIGNATUR

**GODKJENT AV**
Maria Bartnes
SIGNATUR

| RAPPORTNR | ISBN | GRADERING | GRADERING DENNE SIDE |
|---|---|---|---|
| 2018:00007 | 978-82-14-06606-7 | Åpen | Åpen |

# Historikk

| VERSJON | DATO | VERSJONSBESKRIVELSE |
|---|---|---|
| 0.1 | 2017-01-20 | Dokument opprettet |
| 0.8 | 2017-06-23 | Sendt til QA |
| 0.9 | 2017-06-23 | Sendt til oppdragsgiver for godkjenning |
| 0.91 | 2017-12-07 | Oppdatert etter kommentarer fra Statnett |
| 1.0 | 2018-01-05 | Endelig versjon |

SINTEF

# Innholdsfortegnelse

SINTEF

**BILAG/VEDLEGG**

## Definisjoner og uttrykk

**CIA** – Confidentiality, Integrity, Availability (Konfidensialitet, Integritet, Tilgjengelighet)

**CIGRE** - Council on Large Electric Systems (fransk: Conseil International des Grands Réseaux Electriques)

**COO** – Controllability, Observability, Operability (kontrollerbarhet, observerbarhet, opererbarhet)

**CPU** – Central Processing Unit

**Cybersikkerhet** – konfidensialitet, integritet, tilgjengelighet av informasjon og utstyr

**DSAS** – Digital Substation Automation Systems

**GIS** – Geografisk InformasjonsSystem

**GTW – c**ommunication GaTeWay

**HMI** – Human Machine Interface

**IED** – Intelligent Electronic Device

**IKT** – Informasjons- og KommunikasjonsTeknologi

**Informasjonssikkerhet** – konfidensialitet, integritet, tilgjengelighet av informasjon

**Interoperabilitet** – evnen til to eller flere anordninger fra samme leverandør, eller ulike leverandører, til å utveksle informasjon og bruke informasjonen til korrekt samvirke. (Fra engelsk: **Interoperability** - is the ability of two or more devices from the same vendor, or different vendors, to exchange information and use that information for correct cooperation. IEC61850, 2010)

**IT** – InformasjonsTeknologi (Information Technology)

**LAN** – Local Area Network

**MU** – Merging Unit

**NIS** – Network Information System

**OT** – Operasjonell Teknologi (Operational Technology)

**Personsikkerhet** – forhold som berører liv og helse til personell og andre personer

**PMU** – Phasor Measurement Unit

**SAMU** – Stand Alone Merging Unit

**SCADA** – Supervisory Control And Data Acquisition. Kalles også driftssentralsystem eller driftskontrollsystem.

**SCU** – Switchgear Control Unit

**WACU** – Wide Area Control Unit

# 1 Introduksjon

Denne rapporten er basert på eksisterende litteratur med et mål om å lage en omforent definisjon av begrepet "digital transformatorstasjon" som er hensiktsmessig for Statnett og bransjen i Norge generelt. Videre har vi skissert hvilke cyber-relaterte sårbarheter som blir viktigere når man går fra konvensjonelle til digitale transformatorstasjoner. Til slutt anbefaler vi relevante tiltak mot cyber-trusler i digitale transformatorstasjoner.

## 2 Definisjon av begrepet "Digital transformatorstasjon"

> *"Transformatorstasjon er et elektrisk anlegg som transformerer (omformer) spenningen på strømnettet fra ett spenningsnivå til et annet, med tilhørende apparatanlegg bestående av kabler, samleskinner, effektbrytere, skillebrytere, overspenningsavledere, strøm- og spenningstransformatorer for måling og kontroll. I tillegg til dette har transformatorstasjonene et styre- og kontrollanlegg samt fjernstyringsutrustning. De fleste transformatorstasjoner er utstyrt med flere transformatorer, som over effektbrytere er koplet sammen via samleskinnene. På samme måte er de utgående kraftlinjer og/eller jordkabler tilknyttet samleskinnene. Dermed har man mulighet til å foreta omkoplinger både av transformatorer og linjer bare ved å kople brytere, noe som gjerne skjer via fjernstyring fra en driftssentral. Alt etter størrelse kan stasjonene være utført med flere sett samleskinner og flere grupper transformatorer."*
>
> Store Norske Leksikon [1].

Kildene som er benyttet i dette avsnittet er primært hentet fra CIGRE og IEEE. I tillegg er informasjon fra nettsidene til de største leverandørene av komponenter til transformatorstasjoner brukt. Det virker som om ABB og GE Grid Solutions er de mest ivrige aktørene innenfor "digital substation". Disse to leverandørene (og andre partnere) er også med i et forskningsprosjekt som heter "**F**uture **I**ntelligent **T**ransmission **NE**twork **S**ub**S**tation" (FITNESS) initiert av Scottish Power Energy Networks. Et kort sammendrag av dette prosjektet er vist i Figur 2-1. Informasjon om dette forskningsprosjektet er også innhentet fra prosjektlederen, Priyanka Mohapatra. Noen åpent tilgjengelige bransjemagasiner på nett er også benyttet.

SP Transmission (SPT), supported by project partners ABB, GE, Synaptec, and the University of Manchester, made a full proposal submission for the project, *Future Intelligent Transmission Network Substation (FITNESS)*, under the Network Innovation Competition (NIC) mechanism in 2015. Ofgem approved the proposal and issued the Project Direction on the 19th of December 2015. The project commenced in April2016 and is due to conclude in March 2020.

FITNESS brings together two of the largest vendors in the electrical industry to demonstrate the world's first multi-vendor next generation electricity substation using digital technology for full operation; from monitoring to control and protection. The project will also demonstrate the latest in the field of non-conventional instrument transformer (NCIT) technology and research, validating performance against today's Standards, informing and progressing the Standards as required, and also future proofing for potential wide-area control.

FITNESS will demonstrate a multi-vendor fully interoperable digital substation solution by deploying standardised and fully integrated substation protection, monitoring and control system based on the IEC 61850-9-2 Standard in a live substation, that will offer the following benefits:

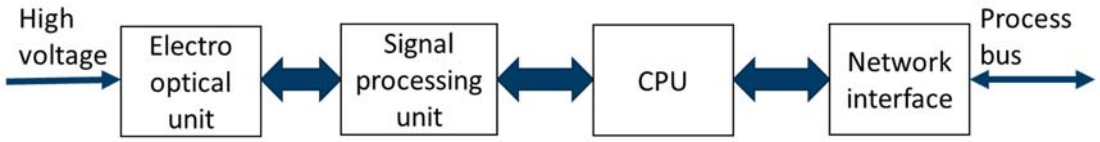
- **Reduce substation costs** – through reduced cabling and substation footprint
- **Improve system access** – secondary equipment decoupled from primary
- **Improve substation safety –** through reduced 'live' electrical conductors and use of optical sensors
- **Reduce environmental impact –** by reducing overall substation footprint, reduced concrete and copper requirements

**Figur 2-1 Kort sammendrag av prosjektet FITNESS [2].**

En transformatorstasjon har altså flere funksjoner, med nedtransformering og kobling/omkobling som sine viktigste oppgaver og slik vil det fortsatt være. Digital transformatorstasjon innebærer ingen endringer i oppgavene til en transformatorstasjon. Alle komponentene i en transformatorstasjon er knyttet til kontrollanlegget for transformatorstasjonen og videre til driftssentralen via SCADA. Noen av komponentene, eksempelvis transformatorer og effektbrytere, kan styres fra driftssentralen; brytere kan åpnes og lukkes og

transformatoren kan settes i drift, tas ut av drift eller omsetningsforholdet kan endres. I transformatoren måles eksempelvis temperatur og disse dataene går til SCADA. Spennings- og strømtransformatorer gir verdier på spenning og strøm til ulike kontroll- og styringssystemer. I kontrollanlegget er det også vern som ved en feil et eller annet sted i nettet skal beskytte komponentene og ledningene i transformatorstasjonen, for eksempel ved å koble dem ut ved behov ved lynaktivitet eller overlast.

Tradisjonelt har det vært elektrisk kontakt mellom komponentene, vern og kontrollutstyr i en transformatorstasjon. Hver måling og hvert signal har sin egen elektriske forbindelse. Med tiden har det kommet nye komponenter og ny måleutrustning som har redusert behovet for fysiske sammenkoblinger. Optiske spennings- og strømtransformatorer er et eksempel på ny måleutrustning. Figur 2-2 viser et eksempel på et blokkdiagram fra høyspenning til prosessbuss [3].




**Figur 2-2 Blokkdiagram for optisk spennings – og strømtransformatorer med prosessbuss [3]**

Begrepet "Digital transformatorstasjon" har mange elementer i seg og ulike kilder fokuserer på ulike sider. Det er funnet kun en definisjon på "digital stasjon" i kildene [4]. En modifisert versjon av denne definisjonen er diskutert med Statnett og vil være definisjonen som brukes i dette prosjektet:

*En full-digital stasjon er en stasjon hvor så mye som mulig av dataene relatert til hovedprosessen til en stasjon (nedtransformering og kobling) digitaliseres øyeblikkelig*

- *Digitaliseringen omfatter måling, styring og statusmeldinger*
- *Utveksling av data mellom enheter skjer via digitale grensesnitt*
- *Funksjonalitet er først og fremst avhengig av programvare (software)*

Potensielle fordeler ved digital transformatorstasjon er i [4] oppsummert slik:

- Økt pålitelighet og tilgjengelighet – Digitale enheter som er selv-diagnostiserende og selv gir beskjed om at eksempelvis vedlikehold må utføres. Ved økt overvåkning av viktige skademekanismer kan degradering av komponenter overvåkes kontinuerlig og benyttes til å avgjøre når utskiftning bør gjøres
    - Redusert vedlikeholdskostnader – Overvåkning og analyse med tilhørende anbefalinger for vedlikehold
- Økte kommunikasjonsmuligheter – Datautveksling mellom intelligente enheter, internt og mellom stasjoner blir optimalisert gjennom Ethernetforbindelse. Smart lokal eller *wide area control units* (WACU) kan gjøre kommunikasjon mulig mellom spenningsnivåene i stasjonene og mellom stasjoner, uten å gå veien om kontrollrommet/driftssentralen, noe som reduserer responstid.

En dimensjon som er nevnt i det siste punktet over er de økte kommunikasjonsmulighetene både internt og mellom stasjoner. I distribusjonsnettet er mulighetene for kommunikasjon mellom stasjoner mye diskutert. Potensielle gevinster ved direkte kommunikasjon mellom stasjoner kan være raskere og automatisk gjenoppretting av forsyning etter feil (såkalt *self-healing*) og lokal kontroll og styring, eksempelvis med tanke på å lage et microgrid (lokalt nett med egen forsyning).

Kommunikasjon internt i stasjonen og kommunikasjon til driftssentralsystem (SCADA) er viktig. CIGRE har laget en rapport [5] som omhandler *Digital Substation Automation Systems* (DSAS). I innledningen til denne rapporten står det at en av de viktigste utviklingene innenfor DSAS har vært introduksjonen av Ethernet tek-

nologi og som en konsekvens en ny form for DSAS avhengig av LAN kommunikasjon (*local area network*). DSAS kan slik integrere enhver funksjon som trenger å kommunisere informasjon fra en IED (*intelligent electronic devices*) til en annen funksjon i et annet utstyr.

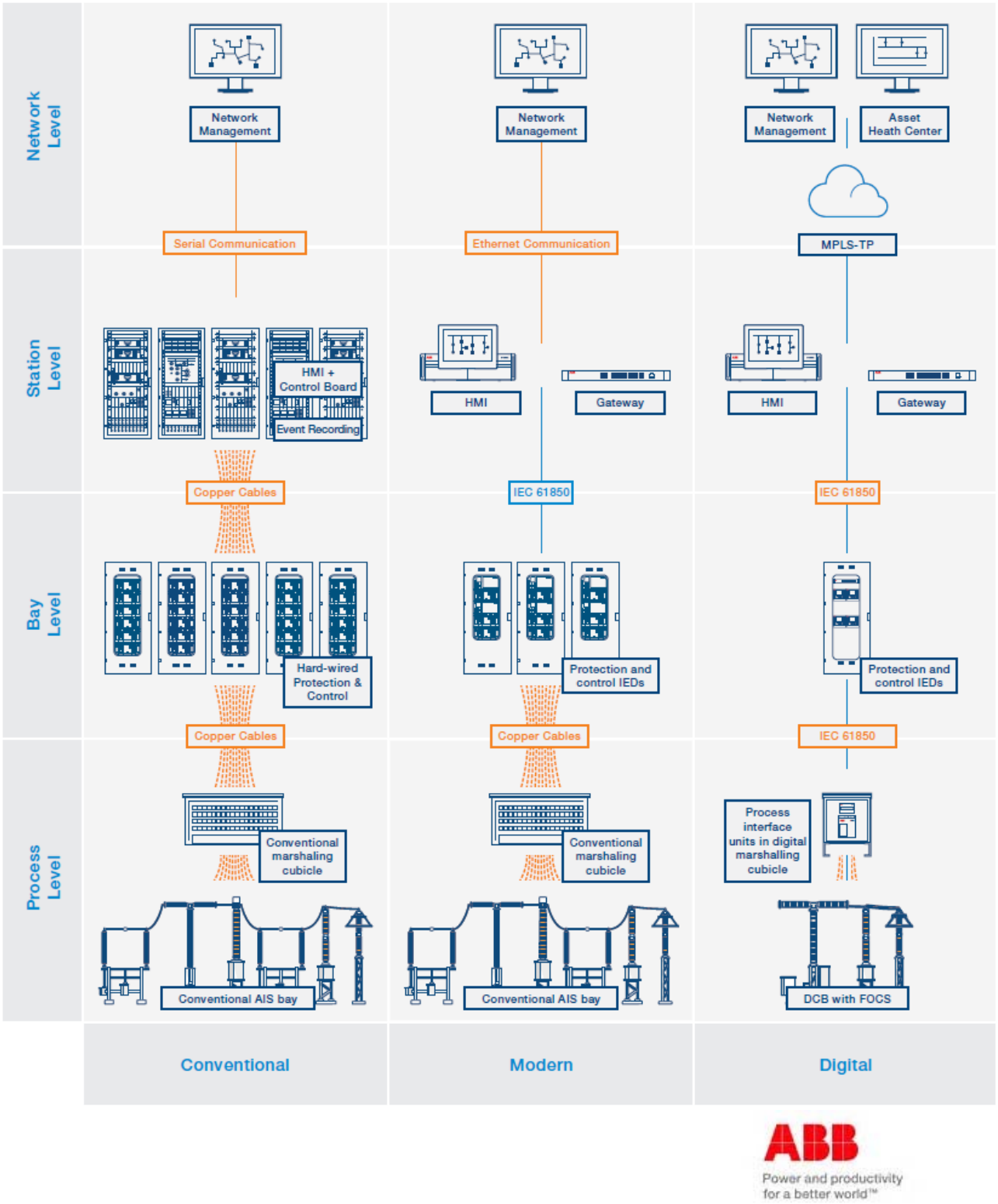
Et begrep som ofte nevnes i forbindelse med digital transformatorstasjon er IED. IED er ikke nytt, og mange IEDer er allerede i Statnett sine stasjoner, eksempelvis vern. IED er mikroprosessorbasert og kan motta informasjon og gi styringssignaler ved avvikende målinger, for eksempel for høy spenning. Det som er nytt i en digital stasjon er blant annet at IEDer ikke er "kablet fast" til bestemte komponenter/måleutrustning, men kan kommunisere med flere komponenter på prosessbussen. I en digital transformatorstasjon blir vernet "delt i to" ved at vernet mottar digitalisert informasjon fra måletransformatorene og ikke trenger å ha utstyr for å omforme analoge målesignaler til digitale, dvs at måletransformatorene, eventuelt *Merging Units* (se beskrivelse lengre ned i teksten) tar over en del av det som i dag inngår i vern [6].

Erfaringer med implementering av en full-digital transformatorstasjon er blant annet gjort i Danmark [7] og Russland [8]. Test av optiske instrumentransformatorer og prosessbuss er gjort i [9]. Disse kildene rapporterer så langt om gode resultater fra tester, men det er viktig å huske at artiklene er skrevet av leverandører av utstyr.

FITNESS-prosjektet [2] deler arkitekturen for en digital transformatorstasjon inn i tre nivåer med følgende komponenter i sin teststasjon Wishaw 275kV/132kV:

- Stasjonsnivå:
    - Human Machine Interface (HMI), Communication gateway (GTW), Wide Area Control Unit (WACU), phasor controller, routers and station level switches.
- Samleskinne (bay) nivå:
    - Protection Intelligent Electronic Devices (IEDs)
    - Control IEDs
    - Measurement IEDs
    - Phasor measurement units (PMU)
    - Disturbance recorder
    - Synaptec Interrogator
- Prosessnivå:
    - Switchgear Control Units (SCUs)
    - Merging Units (MUs)
    - Stand Alone Merging Unit (SAMU)
    - Analog acquisition unit
    - Synaptec Distributed measurement devices

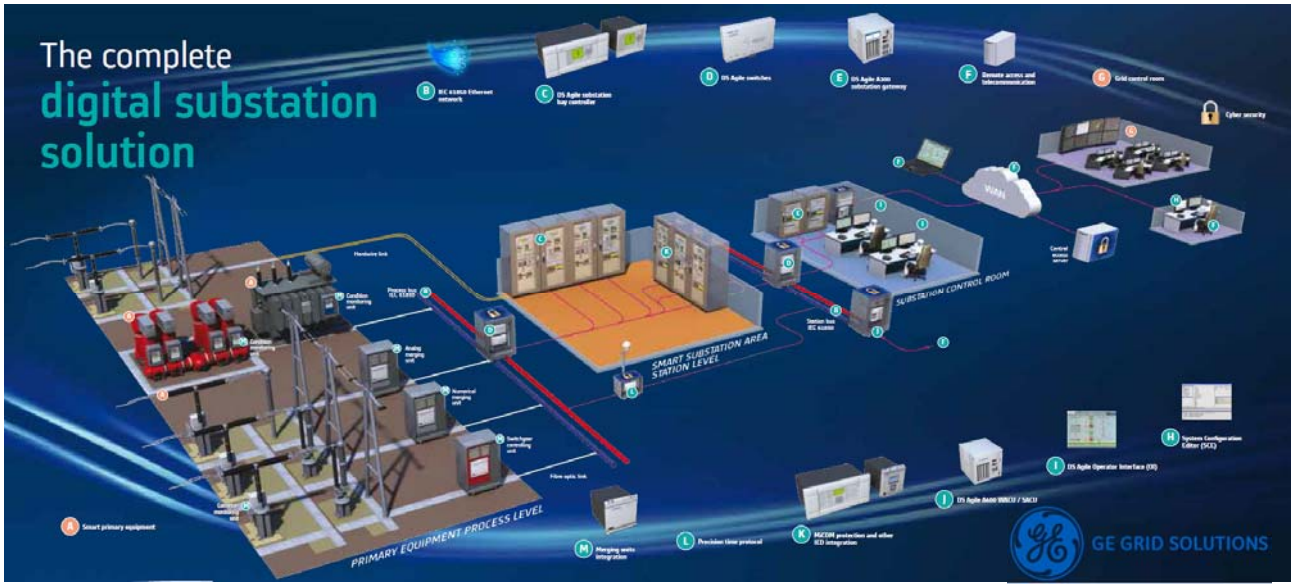
Synaptec er en utstyrsleverandør som er en del av FITNESS-prosjektet, sammen med ABB og GE. Interoperabilitet mellom utstyr fra ulike leverandører er et viktig aspekt ved FITNESS. ABB har en tilsvarende inndeling i fire med litt andre navn vist i Figur 2-3 [10], tillegg til de tre nivåene under har ABB et nettverksnivå over stasjonsnivå:




**Figur 2-3 Figur fra ABB som viser overgang fra tradisjonell til digital transformatorstasjon, figuren er trykket med tillatelse fra ABB og alle rettigheter til figuren tilhører ABB [10]**

I FITNESS brukes Ethernet til å implementere standarden IEC 61850 Edition 2 [39]. Kommunikasjonsprotokoller definert i IEC 61850-8-1 [40] er brukt for å utveksle digital og analog informasjon over stasjonsbuss og prosessbuss. Dette nivået er kontakten med omverden, først og fremst driftssentralen. I tillegg til driftssentralen kan data gå til et sentralt asset management system for analyse av blant annet tilstand og reinvesteringsbehov.

GE Grid Solution sin figur, Figur 2-4, viser et eksempel på en digital transformatorstasjon. Figuren viser viktige elementer i slike stasjoner.




**Figur 2-4 GE Grid Solution sin digitale stasjon, figuren er trykket med tillatelse fra GE Grid Solutions og alle rettigheter til figuren tilhører GE Grid Solutions [11]**

Figur 2-4 illustrerer noen av endringene som vil skje ved overgang fra konvensjonell til digital transformatorstasjon og dette kan oppsummeres slik:

- Nye primærkomponenter med flere sensorer integrert – dette gir mer data fra komponentene enn tidligere som kan benyttes i ulike typer analyser. Nye sensorer kan også ettermonteres på eksisterende komponenter, men slik montasje må være basert på en kost/nytte vurdering.
- *Merging units* – avmerket M i Figur 2-4. Disse enhetene tar seg av digital dataprosessering nødvendig for å oppfylle IEC 61850-9-2 standarden [11]. På sikte kan separate *merging units* sannsynligvis erstattes av prosessgrensesnitt integrert i høyspenningskomponenter [6]
- Prosessbuss
    - Data sendes fra primærkomponentene til eksempelvis vern via en prosessbuss og ikke kabler.
        - Dette medfører reduksjon i kabling ved bruk av prosessbuss (Ethernet/fiber)
    - IEC 61850 benyttes for kommunikasjon
- Vern- og kontrollutstyr er IED både i en digital og konvensjonell transformatorstasjon
    - I en konvensjonell stasjon har hvert felt i stasjonen sitt eget vern (trådbundet), men i en digital transformatorstasjon kan flere felt ha samme vern
        - Siden kommunikasjon gjøres ved protokoller skal utstyr på dette nivået være interoperatible, dvs. at det skal være enkelt å ha utstyr fra ulike leverandører
    - IEC 61850 benyttes for kommunikasjon
- Stasjonsbuss
    - Tidligere en SCADA buss. I en digital transformatorstasjon kan flere utveksle informasjon over stasjonsbussen, også mellom stasjoner
- Stasjonsnivå

    - Data fra alle sensorer i stasjonen er tilgjengelig for analyser og funksjoner som trenger dette på stasjonsnivå
- Nettverksnivå
    - Tradisjonelt kun kommunikasjon med driftssentral, i en digital transformatorstasjon kan kommunikasjon skje med andre stasjoner og andre systemer ved Ethernet/fiber kommunikasjon mellom stasjonene, eller via skyløsninger

For *asset management* kan fordelene med digital transformatorstasjon sammenlignet med en konvensjonell stasjon ligge i nye komponenter med mer overvåkning og mulighetene til å overføre store mengder data (ved bruk av fiber/Ethernet til ønsket analysested). Men tilgjengeligheten av dataene for *asset management* vil fortsatt avhenge av IKT-arkitekturen som velges internt i selskapene, eksempelvis om alle data går til et system som alle har tilgang til eller om man velger å ha ulike systemer med begrensede tilganger.

Viktige forskjeller mellom konvensjonell og digital transformatorstasjon er oppsummert i Tabell 2-1.

**Tabell 2-1: Forskjeller mellom konvensjonell og digital transformatorstasjon**

| Konvensjonell transformatorstasjon | Digital transformatorstasjon |
|---|---|
| • Kommunikasjon og styring vha både analoge og digitale signaler<br>  • Digitalt på vern og kontrollnivå, IEC 61850 benyttes på stasjonsbuss<br>  • På prosessnivå har hvert målesignal og utløsersignal sin kabel (prosessbuss er ikke digital)<br>• Kommunikasjon eksternt til SCADA<br>  • Fokus på drift<br>  • Alarmer og eventuelle aksjoner på driftssentralen<br>  • Statnett har et annet system i parallell med SCADA (som henter informasjon fra stasjonsbuss) med eget grensesnitt – server i Oslo som kan brukes til å utføre feilsøk, gjøre verninnstillinger og gi leverandører tilgang<br>• Annen bruk/analyser av dataene er "tungvint" (hente data fra SCADA) | • Kommunikasjon og styring vha. digitale signaler både internt i og ut av stasjonen til SCADA og andre systemer<br>  • Digital kobling mellom høyspennings-komponenter og vern- og kontrollsystem<br>  • IEC 61850 brukes for kommunikasjon mellom måleutstyr på komponenter, vern- og kontrollutstyr<br>• Kommunikasjon til SCADA og andre systemer<br>• Nye, smartere komponenter<br>  • Lokal intelligens og beslutningstagning (i.e. *self-healing*)<br>  • Optiske måletransformatorer<br>  • Nye komponenter med flere sensorer - økende antall målinger, også sanntids-målinger, som gir nye muligheter for analyser |

Følgende kulepunkter gir en oppsummering av gevinster ved digital transformatorstasjon funnet i [2], [10] og [11]. Digital transformatorstasjon er et "konsept" som spesielt GE og ABB selger, se [10] og [11]:

- Besparelser (tid og penger) ved:
    - Redusert installasjonstid pga. redusert tid til kabling og testing av riktig sammenkobling
    - Reduserte vedlikeholdskostnader ved å ha selvovervåkning på komponentene – noe som kan redusere behovet for forebyggende vedlikehold og også redusere korrigerende vedlikehold (færre feil)
    - Enklere å gjøre endringer og utvide transformatorstasjonene
        - Interoperabilitet mellom utstyr fra ulike leverandører ved bruk av IEC 61850
- Reduksjon av plassbehov

    - Det som er nytt i digital stasjon er blant annet at IEDer ikke er kablet fast til bestemte komponenter/måleutrustning, men kan kommunisere med flere komponenter på prosessbussen, dvs. at flere kan dele på samme IED
- Kommunikasjon
    - Bruk av fiber/Ethernet internt i stasjonene og fiber ut fra stasjoner gir "ubegrenset" overføringskapasitet
    - Kommunikasjon mellom stasjoner foregår i dag i distansevern (fiber). IEC 61850 [39] åpner for mer slik kommunikasjon
        - IEC101 brukes mellom ulike eiere av stasjoner, IEC61850 ansees som for åpen, IEC62850 er mulig å lukke med brannmur, men dette anses som for risikabelt
- Sikkerhet
    - Tradisjonelle strømtransformatorer kan potensielt forårsake skader om sekundærkretsen ved en feilhandling ikke kortsluttes midlertidig ved eksempelvis vedlikehold.
    - Tradisjonelle strøm- og spenningstransformatorer inneholder olje (isolasjonsmedium) og dermed er det en risiko for eksplosjon
- Drift
    - Dynamisk lastflytanalyse som gir muligheter for å drifte komponentene nærmere designgrensene
    - Selvovervåkning i komponentene sikrer at disse holder seg innenfor grenseverdier
- Kontroll
    - Digital prosessbuss kommuniserer med komponentene og sier fra om det er enheter som ikke virker – dette har ingen kontroll med i dag (vet ikke om det er ting som ikke fungerer før det skal brukes)
- Nye komponenter og nytt måleutstyr:
    - Flere målinger (eksempelvis CB Watch [12] fra GE Grid Solutions) gjør det mulig å vite mer om tilstanden til komponenter og tilpasse vedlikehold/reinvesteringer. Dette kan medføre mindre behov for fysiske inspeksjoner.
        - Komponenter som inkluderer selvdiagnose (logge eksempelvis antall brytninger og sammenligne med anbefalt antall brytninger – gi beskjed om at nå må "jeg" vedlikeholdes)
        - Dette muliggjør større grad av automatisering av oppgaver
    - Mer nøyaktige målinger med optiske måletransformatorer
    - Integrerte komponenter (eksempelvis effektbryter med integrert strømtransformator) som kan redusere plassbehovet i stasjonen

Under er utfordringer knyttet til digital transformatorstasjon oppsummert:

- *Merging unit* mellom elkraftkomponentene og vern. Det er viktig at alle enhetene kommuniserer med hverandre. Tidligere gikk måleverdiene fra komponentene direkte til vernet som behandlet måleverdiene og sendte ut styresignaler, nå vil det være merging unit som utfører funksjoner som vernet tidligere utførte. En ny sårbarhet av stor betydning kan vise seg å være merging unit og fungerende kommunikasjon mellom merging unit og vern
    - Kryptering av informasjon inne i stasjonen vil bli nødvendig. Vil denne komponenten vise seg å være et sikkerhetsmessig svakt punkt?
        - Eksempelvis må utganger som ikke er i bruk blokkeres
- Nye versjoner av software
    - Et alternativ er å fryse versjoner av programvare for å unngå oppdateringer, men dette kan medføre ulemper, eksempelvis ved utvidelser av stasjoner – hvordan skal dette håndteres? Det kan gå mange år mellom bygging av stasjonene og utvidelser. Et nytt felt må kunne kommunisere med resten av stasjonen. Det er derfor viktig å bygge et system som kan utvides.
    - Vil software medføre leverandøravhengighet?

- Testing
  - Tidligere ble testplugger (fysisk) benyttet for å sjekke at systemene fungerte. Nå må man ha simuleringsmodus tilgjengelig for testing. Dette representerer noe nytt for selskapene og nye prosedyrer for testing må lages
- Kryptering av kommunikasjon og deteksjon av inntrengere internt i stasjonen, i tillegg til informasjon som går ut fra stasjonen
  - Hvor skal krypteringen terminere? Nå er det kryptering fram til stasjonen. Må det krypteres mellom bryter og vern, internt i stasjonen? Vil det oppstå en konflikt mellom drift og cybersikkerhet?
- *Asset management*
  - Mer informasjon samles inn fra utstyret og dermed baseres prosesskontroll og vedlikehold på sensormålinger. Det er en risiko for å ta feil beslutninger om sensorinformasjonens integritet kompromitteres
- Kobling mellom stasjoner
  - Risiko ved fysisk tilgang i en stasjon
  - Kan hacking (uautorisert tilgang) av én stasjon være en inngangsport til prosesskontrollsystem i andre stasjoner?
- Mer SCADA-utstyr og nettverksutstyr ute i prosessnettet
  - Uautorisert utstyr kan være en trussel pga. lettere fysisk tilgang
- Nye versjoner av IEC 61850 [39]– hva må gjøres da?
- Har Statnett en spesiell sårbarhet knyttet til systemet de har i dag som er parallelt med SCADA (se avsnitt 6.2)?
  - Dette er annerledes enn andre velger å gjøre det, men dette vil trolig bli mer vanlig med digital transformatorstasjon
- Kompetanse på emner som ikke er tradisjonell elkraft
  - Overgang til at det er behov for mer softwarekompetanse framfor hardwarekompetanse?

# 3 Verdier

I dette avsnittet dokumenteres verdier (aktiva) som er til stede på en transformatorstasjon, og forskjeller mellom konvensjonell og digital transformatorstasjon fremheves.

- Forskjellige typer informasjon, forskjellig "gradering", beskyttelsesbehov
- Informasjonssystemet
- Infrastruktur

Tabellen under inneholder eksempler på aktiva og er ikke en komplett liste. Tabellen er heller ingen anbefaling om verdier som bør samles inn. Det kan være forskjeller mellom stasjoner i kraftsystemet. Av tabellen kan man se at svært mange aktiva er de samme i en konvensjonell og digital stasjon. Den store forskjellen er kommunikasjon og antallet komponenter og sensorer, både reduksjon og økning. Eksempelvis kan flere felt kan ha samme vern, men antallet sensorer for transformatorer og effektbrytere antas å øke.

**Tabell 3-1: Aktiva i konvensjonelle og digitale transformatorstasjoner**

| Aktivum (verdi) | Konvensjonell | Digital |
|---|---|---|
| **Transformator** | | |
| Temperatursensor | ✓ | ✓ |
| Strøm | ✓ | ✓ |
| Styresignaler til trinnkobler | ✓ | ✓ |
| Gassmålinger (desolved gas analysis (DGA))<br>Eksempel på verdier:<br>Hydrogeninnhold<br>Karbonmonoksid<br>Acetylen<br>Ethylene | ✓ | ✓ |
| Overtrykksvern for trinnkobler | ✓ | ✓ |
| Buchholzreele (lokalt) | ✓ | ✓ |
| Overtrykksvern for tank (lokal) | ✓ | ✓ |
| PD-målinger | | ✓ |
| **Effektbryter** | | |
| Bryterbevegelse-sensor<br>• Lysbuetid<br>• Brytertid<br>• Åpningstid | | ✓ |
| Gasstrykk, temperatur og tetthet | ✓ | ✓ |
| Gassvakt | ✓ | ✓ |
| Styresignaler til bryter | ✓ | ✓ |
| Bryterposisjon (inne/ute) | ✓ | ✓ |
| Antall operasjoner | ✓ | ✓ |
| Temperaturmåling – kontakttemperatur | | ✓ |
| **Skillebryter** | | |
| Styresignaler til bryter | ✓ | ✓ |
| Bryterposisjon (inne/ute) | ✓ | ✓ |
| **Jordkniv** | | |
| Styresignaler til bryter | ✓ | ✓ |

| Aktivum (verdi) | Konvensjonell | Digital |
|---|---|---|
| Bryterposisjon (inne/ute) | ✓ | ✓ |
| **Spenningstransformator** | | |
| Spenning | ✓ | ✓ |
| Merging unit (optisk signal til IEC 61850) | | ✓ |
| **Strømtransformator** | | |
| Strøm | ✓ | ✓ |
| Merging unit (optisk signal til IEC 61850) | | ✓ |
| **Stand-alone merging unit (SAMU)** | | |
| SAMU | | ✓ |
| **Vern og kontroll** | | |
| Differensialvern | ✓ | ✓ |
| Vektormåling (PMU) | ✓ | ✓ |
| Ledningsvern | ✓ | ✓ |
| Objektmaskin | ✓ | ✓ |
| Feilskrivere | ✓ | ✓ |
| **På stasjonen** | | |
| Værmålinger<br>- Vindhastighet<br>- Temperatur<br>- Fuktighet | | ✓ |
| Tidssynkronisering | ✓ | ✓ |
| Lyn-aktivitet | ✓ | ✓ |
| Termografering | ✓ | ✓ |
| Energimåling | ✓ | ✓ |

Temperaturovervåkning for transformatorer gjøres i dag. Det finnes flere metoder for temperaturovervåking, og hvilken metode som brukes er til en viss grad avhengig av alder på transformatorene og tilgjengelig teknologi på tidspunktet transformatoren ble produsert. I nye transformatorer er det fiberoptisk temperaturovervåkning og flere målepunkter inne i transformatoren enn tidligere.

Gassmålinger (DGA) gjøres for transformatorolje i dag. Prøver av oljen tas ut og sendes til et laboratorium eller analyseres med bærbart utstyr, for eksempel Transport X Kelman/GE. DGA kan også gjøres kontinuerlig, for eksempel Hydran og Transfix, men i dag er dette typisk kun utført på utvalgte transformatorer. I noen tilfeller går det kun varsel om høyt gassnivå til driftssentralen og selve måleverdiene er ikke tilgjengelig. I en digital transformatorstasjon vil slike måleverdier fra gassmålinger være tilgjengelig for alle transformatorer.

Buchholzrelé og overtrykksvern for tanken til en transformator vil både varsle driftssentral og koble ut transformatoren.

*Merging unit* kan være en del av ukonvensjonelle strøm og spenningstransformatorer eller være separate enheter, *Stand-alone merging unit* (SAMU).

## 3.1 Informasjonsteknologi (IT) kontra operasjonell teknologi (OT)

I tradisjonell informasjonsteknologi (IT) er man gjerne opptatt av Konfidensialitet, Integritet og Tilgjengelighet (CIA på engelsk) av informasjon og systemer. I kraftbransjen (eller i prosesskontroll domenet generelt) gir ikke dette alltid mening, og prioriteringene er uansett vanligvis annerledes. En komplementær triade

har derfor blitt introdusert: Controllability, Observability og Operability. Vi har valgt å oversette dette til "Kan enheten styres?", "Kan enheten observeres?" og "Virker enheten?". I Tabell 3-2 har vi forøkt å klassifisere de identifiserte aktiva i henhold til alle seks egenskaper (der et valg ikke er relevant, er feltet fylt med svart).

Vi bruker følgende kvalitative rangering:

- H – det er mulig å påvirke egenskapen i stor grad, eller kan få store konsekvenser
- M – egenskapen kan påvirkes i noen grad med middels konsekvenser
- L – egenskapen kan påvirkes i liten grad med små konsekvenser

For å ta et konkret eksempel fra Tabell 3-2, så vurderer vi at manipulasjon av en temperatursensor kan få store konsekvenser (H) for observerbarhet (observability), ettersom det da ikke vil være mulig å lese av temperaturen. Legg også merke til at selv om sensoren isolert sett kan fungere, vil dette ikke ha noen verdi dersom den eller de som har bruk for informasjonen ikke kan lese (observere) den. Manipulasjon av sensoren vil også ha store konsekvenser (H) for opererbarhet (*operability*), ettersom den da ikke kan utføre sin funksjon, og dette kan i neste omgang få store konsekvenser (gasstanker kan eksplodere, etc.). På den annen side er konfidensialitet satt til L, ettersom det ikke anses som viktig å holde temperaturverdien skjult for uvedkommende. Ut fra samme argumentasjon som for Observerbarhet og Opererbarhet, er integritet satt til H, ettersom uautorisert endring av sensordata kan få samme konsekvens som om sensoren ikke kan kommunisere og/eller ikke virker. Tilgjengelighet settes til H av samme grunn.

**Tabell 3-2: Klassifisering av aktiva i digitale transformatorstasjoner**

| **Aktivum** | **Controllability "Kan styres"** | **Observability "Kan observeres"** | **Operability "Enheten virker"** | **C (K)** | **I** | **A (T)** |
|---|---|---|---|---|---|---|
| **Transformator** | | | | | | |
| Temperatursensor | | H | H | L | H | H |
| Lastmåler | **(kombinasjon av strøm og spenning; se under)** | | | | | |
| Strøm | | H | H | M | H | H |
| Spenning | | H | H | M | H | H |
| Styre trinnkobler | L | M | L | L | M | M |
| Gassmålinger | | L | L | L | L | L |
| Overtrykksvern for trinnkobler | H | M | H | L | H | H |
| Buchholtz-relé | H | M | H | L | H | H |
| PD-måling | | L | L | L | L | L |
| Trykkmåler | | H | H | L | H | H |
| **Effektbryter** | | | | | | |
| Bryterbevegelse (lysbuetid etc.) | | L | L | L | L | L |
| Gasstrykk, temp., tetthet | | M | H | L | H | M |
| Styresignal | H | | H | L | H | H |
| Antall operasjoner | | L | L | L | L | L |
| Temperatur | | L | L | L | L | L |
| Brytertilstand | | M | M | L | M | M |

| Aktivum | Controllability "Kan styres" | Observability "Kan observe-res" | Operability "Enheten virker" | C (K) | I | A (T) |
|---|---|---|---|---|---|---|
| **Skillebryter** | | | | | | |
| Styresignal | H | | M | L | H | M |
| Brytertilstand | | L | L | L | L | L |
| **Jordkniv** | | | | | | |
| Styresignal | H | | M | L | H | M |
| Brytertilstand | | L | L | L | L | L |
| **Spenningstrafo** | | | | | | |
| Spenning | | H | H | M | H | H |
| **Strømtrafo** | | | | | | |
| Strøm | | H | H | M | H | H |
| **Stand Alone Merging Unit (SAMU)** | | | | | | |
| Kombinert signal | | H | H | M | H | H |
| Input | H | M | H | M | H | H |
| **Vern** | | | | | | |
| Differensialvern | | H | H | L | H | H |
| PMU | | H | H | L | H | H |
| Feilskriver | | M | M | L | M | M |
| Ledningsvern | | H | H | L | H | H |
| Objektmaskin | | H | H | L | H | H |
| **Andre komponenter** | | | | | | |
| Tidssynkronusering | | H | H | L | H | H |
| Nettverkssvitsjer | H | M | H | L | H | H |

Vi har ikke funnet litteratur som har gjort forsøk på å summere opp klassifisering av IT og OT, og det følgende må derfor vurderes kritisk, men ved å gi hver egenskap en verdi fra 1-3 basert på kvalitativ vurdering L-H og deretter summere, kan man prioritere de forskjellige aktiva innbyrdes. Et eksempel som korresponderer med aktiva i Tabell 3-2 vises i Tabell 3-3. NB: De valgte verdiene i Tabell 3-2 må kvalitetssikres med Statnett før Tabell 3-3 brukes til prioriteringer. Dette kunne gjerne være tema for en egen workshop.

**Tabell 3-3: Cyber Score for aktiva i digital transformatorstasjon**

| Aktivum | Cyber Score |
|---|---|
| SAMU Input | 16 |
| Transformator Overtrykksvern for trinnkobler | 15 |
| Transformator Buchholtz-relé | 15 |
| Nettverkssvitsjer | 15 |
| Transformator Strøm | 14 |
| Transformator Spenning | 14 |
| Spenningstrafo Spenning | 14 |
| Strømtrafo Strøm | 14 |
| SAMU Kombinert signal | 14 |
| Transformator Temperatursensor | 13 |
| Transformator Trykkmåler | 13 |
| Effektbryter Styresignal | 13 |
| Differensialvern | 13 |
| PMU | 13 |
| Ledningsvern | 13 |
| Objektmaskin | 13 |
| Tidssynkronusering | 13 |
| Effektbryter Gasstrykk, temp., tetthet | 11 |
| Skillebryter Styresignal | 11 |
| Jordkniv Styresignal | 11 |
| Transformator Styre trinnkobler | 9 |
| Effektbryter Brytertilstand | 9 |
| Feilskriver | 9 |
| Transformator Gassmålinger | 5 |
| Transformator PD-måling | 5 |
| Effektbryter Bryterbevegelse | 5 |
| Effektbryter Antall operasjoner | 5 |
| Effektbryter Temperatur | 5 |
| Skillebryter Brytertilstand | 5 |
| Jordkniv Brytertilstand | 5 |

Etter at verdiene i Tabell 3-2 er kvalitetssikret med Statnett (og evt. andre interessenter) kan man bruke en oppdatert versjon av Tabell 3-3 til prioriteringer av tiltak. Dette impliserer at det aktivumet med høyest Cyber Score evalueres først med hensyn på beskyttelsesmekanismer som ivaretar COO-CIA. Det er viktig å bemerke at Cyber Score slik den er definert her kun tar høyde for potensielle konsekvenser, og tar i utgangspunktet ikke hensyn til eksisterende sikkerhetstiltak. Det kan følgelig godt hende at et aktivum med høy Cyber Score ikke krever ytterligere tiltak, dersom det allerede er godt sikret.

# 4 Sårbarheter

Overordnet beskrivelse av hvordan nye avhengigheter og kobling av systemer for vern, styring og overvåking kan påvirke cybersikkerheten (nye sårbarheter) for en digital transformatorstasjon.

## 4.1 Organisatoriske

Vi har ikke identifisert noen spesielle organisatoriske sårbarheter med hensyn til ansvar og myndighet for digitale transformatorstasjoner. Den økte interoperabiliteten mellom leverandører kan imidlertid medføre at en transformatorstasjon har utstyr fra flere leverandører enn før, noe som vil kreve mer koordinering og administrasjon av leverandørtilgang. Dette vil f.eks. være relevant når det gjelder fjerntilgang i forbindelse med sikkerhetsoppdatering av programvare på enkeltkomponenter.

## 4.2 Fysiske

En digital transformatorstasjon vil ha samme grad av behov for gjerder, låser, overvåkning og alarm som en konvensjonell transformatorstasjon, men lav/manglende bemanning vil være en faktor. Det vil potensielt være en større grad av IP-trafikk ute i feltet, og tilgjengelig dokumentasjon tyder på at det også kan være trådløse forbindelser. Konfigurasjonskontroll (*asset management*) vil være avgjørende, ettersom man må forhindre at utenforstående som baner seg fysisk adgang til feltet introduserer egne enheter til erstatning for, eller i stedet for, eksisterende enheter.

## 4.3 Regulatoriske

NVE publiserte nylig rapporten "Regulering av IKT-sikkerhet" [21], som gir en grundig gjennomgang av regelverket for IKT-sikkerhet innen energisektoren nasjonalt og internasjonalt, samt internasjonale standarder og kommer med anbefalinger til krav som bør stilles til IKT-sikkerhet i et fremtidig, oppdatert regelverk. Rapporten er en oppfølging av Lysne-utvalgets anbefalinger om en gjennomgang av sektorregelverket og beredskapsforskriften.

NVE anbefaler at regelverket oppdateres slik at beredskapsforskriften også stiller krav til informasjonssikkerhet i form av *grunnsikring av digitale informasjonssystemer som har anlegg eller system av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme i energiforsyningen.* Krav til logging og logganalyse, hendelseshåndtering, samt krav til sikkerhet ved tjenesteutsetting, leverandørkjeder og fjernaksess inngår i anbefalingen. NVE har tatt for seg digitale strømmålere særskilt og kommer med spesifikke anbefalinger for disse. Digitalisering av driftskontrollsystemer har ikke fått samme særskilte oppmerksomhet i NVEs gjennomgang, i rapporten anbefales det at sikkerhetsnivåene for disse systemene følger systemenes klasser, som i dag, med mulig mindre endringer i ordlyden i kravene.

Begrepet "forsvarlig sikkerhet" er sentralt i klassifiseringsregimet og krav til driftskontrollsystemer, ifølge NVE [21] kan dette begrepet forstås som *en rettslig standard der sikkerhetsnivået i første rekke bygger på virksomhetenes risiko- og sårbarhets (ros)-analyser, utført i tråd med kravene til slike analyser, og markedspraksis i bransjen*. I tillegg kommer minstestandard i henhold til gjeldende regelverk.

Beredskapsforskriften opererer med begrepet driftskontrollsystem (DKS) som favner videre enn ISO/IEC 27019 [42] sin definisjon av prosesskontrollsystem. Virksomheten er selv ansvarlig for å definere hva som inngår i driftskontrollsystemet (ifølge veilederen til beredskapsforskriften , § 7-1 [41]). I en digital transformatorstasjon vurderer vi det slik at stort sett alle komponenter, bortsett fra de rene elektromekaniske komponentene vil falle innenfor definisjonen av driftskontrollsystem, og man må derfor følge kravene til sikring av driftskontrollsystemer, som beskrevet i beredskapsforskriften kapittel 7. NVE anbefaler [21] at ordlyden slik den er i dag med detaljerte krav i beredskapsforskriften kapittel 6 og 7 bør forenkles og oppdateres slik at det

i større grad brukes begreper fra internasjonale standarder. ISO-standardene 27001/2 og den tekniske rapporten ISO TR 96 27019 (som nå er erstattet av ISO/IEC 27019 [42]) trekkes fram av NVE i denne sammenhengen.

Så vidt vi kan bedømme er ikke personopplysningsloven relevant for digitale transformatorstasjoner og transmisjon. Energiloven [43] stiller overordnede krav til informasjonssikkerhet, med fokus på sikring av tilgang til sensitiv informasjon om kraftforsyningen. Dagens sikkerhetslov stiller detaljerte krav til informasjonssikkerhet for *skjermingsverdige objekter*, men ingen virksomheter innen energisektoren har i dag utpekt objekter som faller inn under denne lovgivningen. Om forslaget til ny sikkerhetslov (presentert av Traavik-utvalget i 2016 [44]) vedtas derimot, vil dette medføre endringer i regelverket for klassifisering av skjermingsverdige objekter og sikringstiltak, og kraftforsyningen vil bli underlagt sikkerhetsloven med NSM som sikkerhetsmyndighet. Skjermingsverdige objekt og infrastruktur innen energisektoren vil dermed bli regulert i henhold til klassifiseringsgrader som skiller seg fra dagens regelverk.

## 4.4 Teknologiske

Potensialet for informasjonsinnhenting er større, dersom en inntrenger får tilgang på interne nett vil det i større grad enn før være mulig å foreta rekognoseringsaktiviteter som å "skanne" nettet og foreta "enumeration" (lage liste over tilgjengelige enheter).

Økt bruk av digitale komponenter medfører at angrepsflaten øker, og erfaringer tilsier at feil konfigurasjon av brannmurer etc. medfører at langt flere komponenter er tilgjengelige fra forskjellige nettverk (ikke nødvendigvis internett) enn det systemeieren kanskje tror. Ofte har det vist seg at nettverk som har vært antatt isolert fra omverdenen likevel har en forbindelse.

Det finnes en egen søkemotor kalt Shodan [34] hvor man enkelt kan få informasjon om industrielle komponenter som er koblet til internett. Første gang NSM ble varslet om åpne SCADA-systemer i Norge var i 2011 [35]; amerikanske sikkerhetsmyndigheter sendte en liste over 38 IP-adresser som måtte sjekkes ut. I 2013 fant Dagbladet 2500 norske styringssystemer offentlig tilgjengelig ved hjelp av denne søkemotoren. I 2016 fant sikkerhetsfirmaet Kaspersky i størrelsesorden 200 000 tilgjengelige ICS-komponenter på verdensbasis [36]. Dette indikerer at sikker konfigurasjon av SCADA-systemer fortsatt er en utfordring for mange operatører.

## 4.5 Personellmessige

Digital transformatorstasjon vil gi bedre personsikkerhet, ettersom behovet for fysisk intervensjon vil reduseres. For leverandører kan det muligens være en utfordring at det ikke lenger er nok å ha oversikt over egen løsning, og at det følgelig vil være et behov for økt kompetanse hos hver enkelt leverandør. I praksis betyr dette at alle leverandører til en gitt transformatorstasjon må etablere økt samhandling og informasjonsutveksling for å unngå uønskede sikkerhetskonsekvenser. Dette er det imidlertid vanskelig å kontrollere på forhånd.

Det vil videre være behov for økt bestillerkompetanse på digitale løsninger, spesielt med tanke på trusselbildet. Grensesnittet mellom IT og OT i organisasjonen må vies spesiell oppmerksomhet, og internopplæring må ta høyde for dette.

# 5 Trusselbilde

Digitaliseringen gjør tradisjonelt lukkede systemer mer åpne, noe som kan føre til flere utnyttbare sårbarheter, samtidig er trusselbildet i endring. I følge PSTs sikkerhetsvurdering for 2017 [32] er systemer innen kraftsektoren spesielt utsatt for etterretningsoperasjoner med formål om å *hente ut informasjon om selve infrastrukturen samt å legge til rette for å kunne manipulere data eller forberede sabotasje, dersom det oppstår en tilspisset utenriks- eller sikkerhetspolitisk situasjon*. Med økende tilkobling av utstyr til internett og

økende systemkompleksitet og mellomkoblinger, øker også faren for at utenforstående kan forstyrre systemet. Samtidig gjør de samme faktorene at man raskere kan oppdage at uvedkommende forstyrrer systemene. Slike eksterne trusler kan være av fysisk art mot stasjoner og anlegg, men kan også være av digital art. Hvilke trusler og aktører som er relevante for en digital stasjon vil en risikovurdering kunne tydeliggjøre, men det er gjentatte eksempler på at truslene og aktørene er reelle.

Sårbarheter i driftskontrollsystemet kan utnyttes av en angriper som ønsker å få uautorisert tilgang for å forårsake et større strømbrudd; dette kan f.eks. oppnås ved:

- Å sende kommandoer direkte til SCADA-utstyret
- Fjerntilgang til Menneske-Maskin-grensesnittet (HMI)
- Å endre GIS/NIS databasen
- Menneske-i-midten-angrep på protokoller
- Forfalske sensor-input til FLISR

Hver uke rapporteres det om cyberangrep i form av datainnbrudd og store datalekkasjer, og for hver av de som rapporteres kan vi trygt anta ti eller hundrevis av urapporterte hendelser. Rapporten "2015 Information Security Breaches Survey" [26] hevder at ni av ti virksomheter har vært utsatt for informasjonssikkerhetshendelser gjennom det foregående året. Den samme undersøkelsen oppgir også at seks av ti respondenter forventet flere sikkerhetshendelser i de følgende året sammenlignet med det foregående. De påløpte kostnadene av en sikkerhetshendelse øker også raskt, og måles nå i skalaen millioner, heller enn tusenvis, av euro.

Det første offentlig kjente cyberangrepet rettet mot industrielle prosesskontrollsystem var Stuxnet [27] som spredte seg over hele verden i 2010, men med en markert konsentrasjon i Iran i en tidlig fase. Det benyttet seg av fire nulldags-sårbarheter og infiserte PCer som styrer Siemens Simatic PLS-systemer. Herifra kontrollerte Stuxnet sentrale deler av kraftverket. Sentrifugene ble, i hurtig etterfølgende sekvenser, spunnet opp og ned. Falske data til kontrollrommet gjorde at operatørene ble lurt til å tro at alt var normal. Dette medførte at flere sentrifuger for foredling av uran ble ødelagt. Etter at Stuxnet ble avslørt, kom det frem at en tidligere versjon (Flame) hadde vært brukt til informasjonsinnhenting i flere år. De klarte også å forbli uoppdaget frem til skaden var gjort.

Sommeren 2014 rapporterte Nasjonal sikkerhetsmyndighet om et målrettet og koordinert cyberangrep mot en rekke virksomheter i olje- og energisektoren [33]. Eposter med virusinfiserte vedlegg ble sendt til over 50 mottakere, viruset inneholdt funksjonalitet som søkte etter og hentet ut informasjon om programvare som brukes for fjernpålogging til industrielle kontrollsystemer. Dette angrepet var en del av en større kampanje kalt ”Dragonfly”, der den samme trusselaktøren hadde utført målrettede cyberangrep mot vestlige selskap og leverandører innen kraftbransjen og annen kritisk infrastruktur siden 2011. Dragonfly [28] benyttet metoder som spam, exploit kits og byttet ut legitime drivere og oppdateringer på nettstedene til leverandører av kontrollsystemer med trojanske versjoner. Skadevaren inneholdt også mulighet for å utnytte det de fant ved hjelp av å fjernoppdatere skadevaren.

Såkalt ”spearphishing”, der eposter med infiserte vedlegg sendes ut til utvalgte mål, var også en viktig komponent i cyberangrepet som førte til strømbrudd for over 230 000 mennesker i Ukraina i desember 2015 [23]. Eposter med infiserte vedlegg spredde en skadevare som automatisk skannet de infiserte systemene etter påloggingsinformasjon, noe som gjorde at trusselaktørene fikk tak i passord slik at de manuelt kunne logge seg på prosesskontrollsystemene i tre Ukrainske kraftselskap via fjernaksessløsninger. Etter at de hadde hatt tilgang i en periode på flere måneder hadde de opparbeidet seg nok kunnskap om systemene til å kunne utføre et angrep der de tok over kontrollen og stengte ned minst 27 transformatorstasjoner ved å gi kommandoer som åpnet brytere. Bryterstillingene ble manipulert via SCADA HMI på arbeidsstasjonene, hvor operatørene kunne observere angrepet ved å se en "spøkelsesmus" klikke rundt på skjermen. Samtidig ble gjenopprettelse forsinket av at skadelig programvare var lastet opp til enhetene som oversatte mellom seriell- og ethernet-

kommunikasjon. Den skadelige programvaren forhindret operatørenes arbeidsstasjoner fra å utstede fjern-kommandoer, og det var følgelig heller ikke mulig for dem å vekke nettstasjonene til live.

For å gjenopprette strømbruddet i Ukraina var man nødt til å erstatte *Remote Terminal Units* (RTUer) som var satt ut av spill, og i mellomtiden var det avgjørende at operatøren var i stand til å få nettverket på fote igjen ved å gå over til manuell kontroll.

SCADA-protokoller har tradisjonelt hatt dårlig sikkerhet [24]. Selv der hvor sikrere alternativer er tilgjengelige, medfører den lave oppdaterings- og erstatningstakten i bransjen at SCADA-systemer forblir sårbare. Den fremherskende sikkerhetsløsningen til driftskontrollsystemer har følgelig vært å plassere en brannmur som et "hardt skall rundt et mykt senter" [25]. Problemet med en brannmur er at i de fleste tilfeller er man nødt til å lage hull i den for å få arbeidet gjort.

Mens det første cyberangrepet mot strømnettet i Ukraina i 2015 fremstod som velkoordinert og effektivt i tilnærming, til tross for å være forholdsvis enkelt teknisk, fremstår det andre cyberangrepet i 2016 [29] langt mer automatisk og omfattende i sin tekniske tilnærming. Angrepet påvirket transmisjonsstasjonen Pivnichna i Kiev og resulterte i ca. en time med strømstans 17. desember 2016. Dette angrepet hadde likhetstrekk med angrepet i 2016, men man benyttet denne gangen "Industroyer" – en modulbasert skadevare som kommuniserer direkte med SCADA-systemer. Heller enn å basere seg på personer som tar over kontrollterminaler for å gjøre manuell endringer, hadde man utviklet angrepskode som kunne kommunisere direkte med industrielt utstyr utplassert i nettverket og dermed effektivt ta over som kontrollnode. Industroyer støttet flere vanlige kommunikasjonsprotokoller for industrielle prosesskontrollsystemer [29]: IEC60870-5-101, IEC60870-5-104, IEC 61850, OLE for Process Control Data Access (OPC DA).

I løpet av 2017 har man sett økt aktivitet i det som er blitt omtalt som Dragonfly 2.0 [30]. Denne har vært i effekt siden desember 2015 og retter seg spesielt mot USA, Tyrkia og Sveits. Den har en tilsvarende tilnærming som den originale Dragonfly, men benytter litt andre verktøy og ser eksplisitt etter kontrollsystemer i sin informasjonsinnsamling.

Våren 2016 satte GCHQ [31], etterretningstjenesten i Storbritannia, foten ned for den pågående utrullingen av smarte strømmålere i Storbritannia. Argumentet var at i sin daværende forfatning var prosjektet en fare for rikets sikkerhet. Problemet var at til tross for at smartmålerne benyttet kryptering av data måleren sendte og mottok, var nøkkelen den samme for alle målerne. Dermed ville en angriper som fikk kontroll over nøkkelen til en måler ha full tilgang til alle målere. GCHQ viser til skalaen av angrep som er mulig når de uttrykker sin bekymring.

*“The guys making the meters are really good at making the meters, but they might not know a lot about making them secure. The guys making head-end systems know a lot about making them secure, but not about what vulnerabilities might be built into them”* – Dr. Levy [31]

GCHQ påpeker også hva som skulle til for at de var komfortable med å rulle ut strømmålerne:

*"The resilience is gained by needing three independent exploits or failures to happen to cause any large-scale effect."* – Dr. Levy [31]

# 6 Løsninger for cybersikkerhet i digital transformatorstasjon

Dette avsnittet gir en oversikt over tilgjengelige og anbefalte sikkerhetstiltak for å styrke cybersikkerheten i en digital transformatorstasjon. Tiltakene er listet opp i tabellen under med henvisning til hvilket avsnitt beskriver løsningene, og med kobling til kategori av tidligere identifiserte sårbarheter.

| Tiltak ↓ Sårbarheter → | Organisatoriske | Fysiske | Regulatoriske | Teknologiske | Personellmessige |
|---|---|---|---|---|---|
| Brannmur | | | Se under | 6.1 | |
| Anti-skadevare | | | | 6.1 | |
| IDS | | | | 6.1 | |
| Hvitelisting | | | | 6.1 | |
| Konfigurasjonsstyring | | | | 6.5 | |
| Endring av standard passord | 6.6 | | | 6.6 | |
| Multi-faktor autentisering | 6.6 | | | 6.6 | |
| Nettverkssegregering | | 6.1 | | 6.1 | |
| Fjerntilgangsstyring | 6.2 | | | 6.2 | 6.2 |
| Nødknapp | | 6.3 | | 6.3 | |
| Testmiljø | | | | 6.4 | |
| Risikoanalyse | 7.1 | 7.1 | | 7.1 | 7.1 |
| Hendelseshåndtering | 7.2 | | | | 7.2 |
| Beredskapsplanlegging | 7.3 | | | | 7.3 |
| Øvelser | 7.3 | | | | 7.3 |
| Asset management | | 6.5 | | 6.5 | |
| Sårbarhetsskanning | 7.1 | 7.1 | | 6.4, 7.1 | 7.1 |
| Patching | | | | 6.4 | |
| Inntrengingstesting | | | | 6.1, 6.4, 7.1 | |

Løsninger som har med forebygging og beredskap å gjøre, behandles separat i avsnitt 7. Som det framgår av tabellen, har vi ikke identifisert løsninger som adresserer regulatoriske sårbarheter. Dette må ikke forstås dithen at det ikke kan finnes relevante regulatoriske tiltak, men snarere at relevante myndigheter gjennom forskrifter, veiledninger etc. kan bidra til at de andre tiltakene vi foreslår implementeres av bransjen.

## 6.1 Nettverkssikkerhet

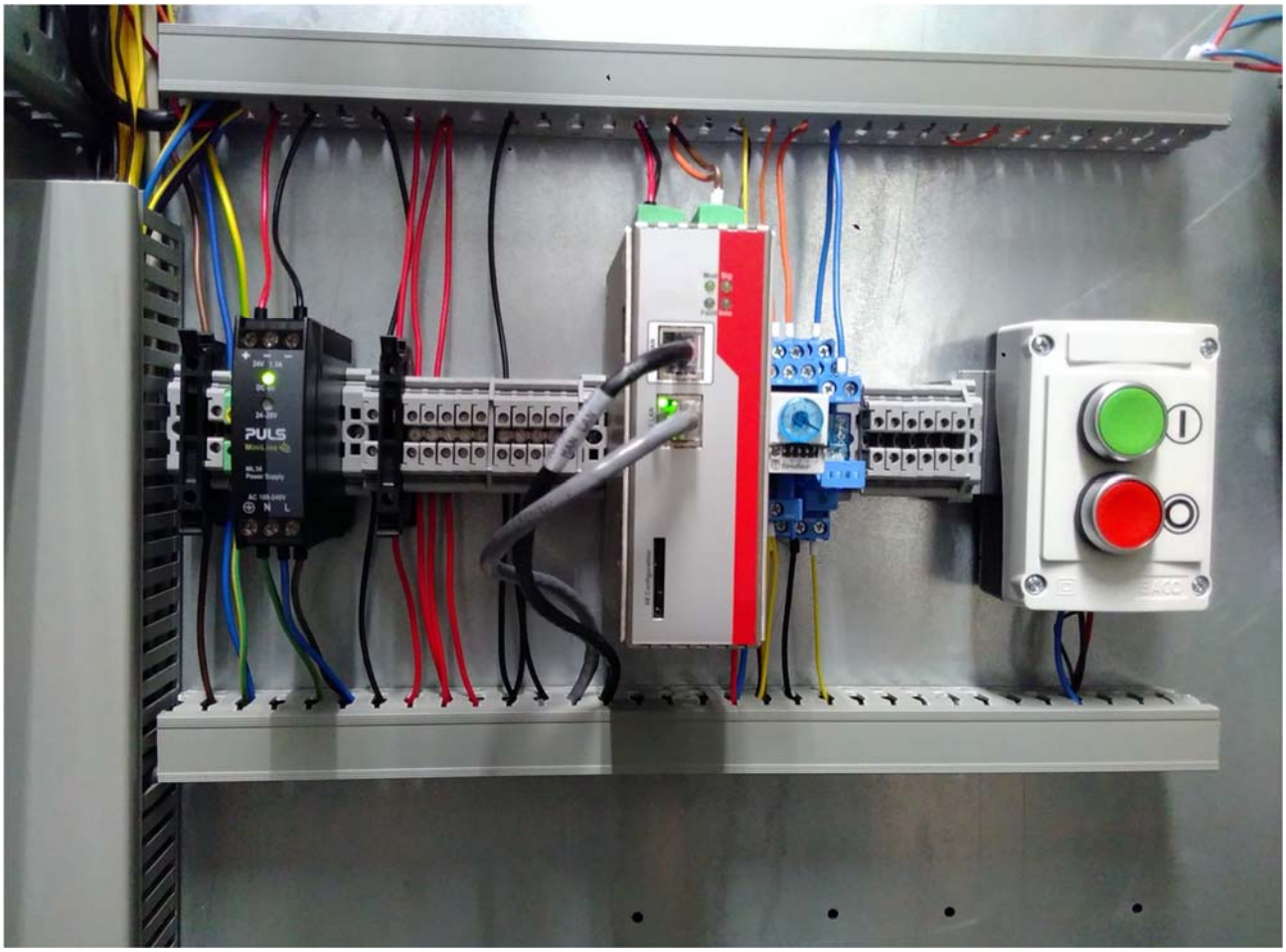
Ettersom stadig større deler av kommunikasjonen i en digital transformatorstasjon blir vanlig IP-trafikk, vil det være aktuelt med sikkerhetsmekanismer som hittil har vært brukt i kontornettverk, som f.eks. brannmurer, anti-skadevare og inntrengningsdeteksjon; sistnevnte både regelbasert og anomalibasert. Anomalibaserte systemer må trenes på typisk trafikk i digital transformatorstasjon.

## 6.2 Fjerntilgang fra leverandører

Vi har forstått at Statnett bruker en egen løsning for å gi leverandører tilgang til vern o.l. i sin pilotinstallasjon av digital transformatorstasjon. Vi har ikke hatt tilgang til detaljert informasjon om denne løsningen, men basert på omtalen tolker vi det dithen at løsningen er tilsvarende andre løsninger som tidligere er benyttet for samme formål i oljeindustrien [22]. Vi legger til grunn at slike løsninger har gitt akseptabel sikkerhet i andre bransjer det er naturlig å sammenligne seg med.

## 6.3 Nødknapp for nettverks-segregering

Koblingen mellom prosesskontrollsystemet internt på den digitale transformatorstasjonen og omverdenen (driftssentralen og eventuelt andre koblinger til leverandør) er et kritisk punkt og man kan i krisesituasjoner ha behov for å fullstendig koble av prosesskontrollsystemet i anlegget fra nettet å la det fortsette å kjøre som en selvstendig enhet. Et mulig beredskapstiltak er å klargjøre anlegget og legge opp nettverksarkitekturen på en slik måte at det er en enkel kobling til omverdenen som en tekniker enkelt kan koble fra om det oppstår en situasjon som gjør dette nødvendig. Et eksempel på en slik situasjon kan være skadevare som spres mellom systemer eller feiltilstander som forårsaker korrupte datapakker på nettet. En enkel løsning kan være å installere en "nødknapp" inne i koblingsskapet for å enkelt segregere nettverkene. Dette vil gjøre det enkelt for en tekniker å frakoble prosesskontrollsystemet fra nett uten å måtte identifisere hvilke nettverkskabler som må trekkes ut inne i koblingsskapet. Datapakker fra diverse sensorer kan lagres i et buffer, og settes på vent om nødknappen trykkes inn, slik at driftssentralen kan få nødvendig data tilsendt når nettverkene kobles sammen igjen. Prosedyrer for bruk av nødknappen må beskrives i gjeldende beredskapsplaner og personell må få opplæring og trening i bruken.




**Figur 6-1: Den store, røde bryteren, en nødknapp for å enkelt koble stasjonen fra omverdenen. Eksempel på installasjon ute i felt.**

## 6.4 Patching

Funksjonaliteten i digitale transformatorstasjoner er først og fremst avhengig av programvare (*software*), og tradisjonelt SCADA-utstyr kompletteres av stadig større grad av "konvensjonelt" nettverksutstyr ute i prosessnettet. Mye mer data samles inn, men man gjør seg også mer avhengig av tilgjengelige og korrekte data. Trusselbildet er stadig mer dynamisk, og utvidelser av installasjoner bidrar også til at det hyppigere blir behov for sikkerhetsoppdateringer. Når en ny sårbarhet oppdages, vil det være et tidsvindu for eksponering fram til sikkerhetshullet tettes, og i denne perioden vil man være spesielt sårbar for cyberangrep. Utfordringen er at i prosesskontrollmiljø vil det være avgjørende å teste at sikkerhetsoppdateringer ikke medfører negative konsekvenser, og det kan derfor være vanskelig å rulle ut oppdateringer så raskt som ønskelig.

Det er derfor behov for bedre løsninger for "software patching" for fremtidens digitale transformatorstasjoner, og vi trenger nye, innovative løsninger for testing av sikkerhetsoppdateringer. Dette vil kunne redusere risikoen for hacking og cyberangrep mot kraftnettet.

Vi har foreslått et forskningsprosjekt i samarbeid med Statnett og norske industriaktører med sikte på konseptutvikling for representasjon av styringssystem-komponenter som virtuelle enheter basert på "*Hardware in the loop*" (HIL) testing. Prosjektet vil utføre design av løsning for virtualisering av komplett styringssystem, inklusiv simulering av det styrte systemet, og foreta implementasjon av en demonstrator for et avgrenset system.

## 6.5 Konfigurasjonsstyring / Asset management

En måte å håndtere kompleksiteten til digitale transformatorstasjoner er å ha gode rutiner for konfigurasjonskontroll og styring av informasjonsverdier og fysiske komponenter (*asset management*). Dette gjør en i stand til å ha oversikt over hvilke enheter man har i stasjonen, hvilken programvareversjon de bruker, og hvilke oppdateringer er installert. Når nye sårbarheter blir kjent, vil man da umiddelbart vite hvilke enheter man trenger å oppdatere.

## 6.6 Autentisering

Mye utstyr leveres fortsatt med et velkjent standardpassord, eller uten passord i det hele tatt. Det er derfor viktig å umiddelbart sette nytt passord på alle komponenter som installeres, samt sørge for at passordene har tilstrekkelig kvalitet mhp. kompleksitet og lengde. Dette kan også inngå som en del av konfigurasjonsstyringen (se 6.5)

Der det er mulig, bør man introdusere multifaktor autentisering slik at det ikke er nok å vite (gjette) passordet for å få tilgang. Aktuelle løsninger omfatter bl.a. passord+kodebrikke og passord+mobilapp. SMS regnes ikke lenger for en sikker andre faktor [37][38].

# 7 Forebyggende tiltak og beredskap for cybersikkerhet i digital transformatorstasjon

Forebygging av hendelser gjøres ved å implementere tiltak som står i forhold til trusselen. Generell kunnskapsoppbygging er viktig her, men dette omfattes ikke av denne rapporten. Imidlertid er det viktig å gjennomføre risiko- og sårbarhetsanalyser som også tar høyde for informasjonssikkerhet (*cyber security*) for å kunne vurdere trusselen objektivt. Videre er det fundamentalt å innse at det ikke er mulig å beskytte et system mot alle mulige cyber-trusler, og det er derfor avgjørende at man vet hvordan man håndterer cybersikkerhetshendelser når de oppstår. Øvelser og opplæring av ansatte er viktig i denne sammenhengen, vi vil derfor skissere scenarioer og test-caser som kan brukes til dette formålet.

## 7.1 Risiko- og sårbarhetsanalyser

Tøndel et al. [13] gir et overordnet bilde av SINTEFs rapport som gir råd om gjennomføring av risikovurdering i Avanserte Måle og Styresystemer (AMS) [15]. I en digital transformatorstasjon er det rimelig å anta at

det vil være et mindre fokus på personvern enn det vil være i forbruker-nære AMS-installasjoner, men den øvrige metodikken anses for å være relevant.

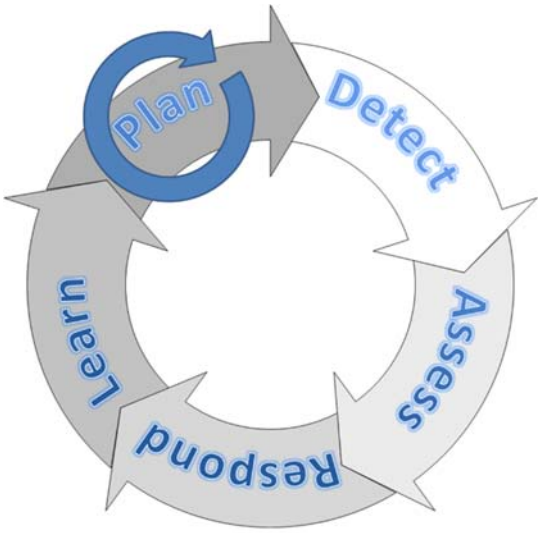
Ved gjennomføring av en risikoanalyse for en konkret digital transformatorstasjon anbefaler vi følgende [13]:

- Inkluder de riktige menneskene med den riktige kompetansen.
- Sett av to halve dager framfor en hel, for å få tid til innhenting og bearbeiding av informasjon mellom arbeidsmøtene
- Benytt sjekklister eller andre, tidligere utførte, risikoanalyser for å komplettere diskusjonen i analysegruppa.
- Bruk tid på å diskutere sannsynlighet og konsekvens. Ta tak i eventuelle uenigheter. Der man har uenighet i gruppa, vil man ofte ende opp med grundigere vurderinger.
- Man kan gjerne leie inn ekstern fasilitator eller annen kompetanse som mangler. Det er imidlertid viktig at representanter for virksomheten selv er aktive i arbeidet. Det å delta i risikoanalyser gir en økt bevissthet om sikkerhet. Prosessen i seg selv kan ofte være vel så viktig som sluttrapporten.
- Tekniske feil og angrep er viktige å vurdere, men informasjonssikkerhet er ikke kun et teknisk anliggende. Mennesker og prosesser i organisasjonen er også viktige, og disse aspektene bør tas inn i analysen.
- Vær klar på hva analysen dekker. Fokuser gjerne på mindre deler av systemet om gangen. Slik blir arbeidet mer overkommelig, og man får mulighet til å gå mer i dybden. Samtidig er det nyttig også å gjøre overordnede analyser for å få det store bildet, og øke forståelse for hvordan sikkerhet ett sted påvirker sikkerhet andre steder i systemet.

## 7.2 Hendelseshåndtering

Kulturforskjellene som eksisterer mellom ansatte med elkraft- eller prosess-bakgrunn og IT-folk er en utfordring når det gjelder håndtering av cyber-hendelser i denne bransjen [16][19]. Det er derfor viktig å være bevisst på at det er nødvendig å kunne håndtere cyber-hendelser også i prosessnett, og man må sørge for å trene også på denne type hendelser (se avsnitt 7.3).

Innen tradisjonell IT henviser man til standarder som ISO/IEC 27035 og retningslinjer som NIST SP 800-61, og vi har tidligere gjort forsøk på å lage tilpassede rutiner for prosessorienterte bransjer. Imidlertid har vi kommet til [20] at det i utgangspunktet ikke er noe i veien for å basere hendelseshåndtering i kraftbransjen på ISO/IEC 27035, som illustrert i Figur 7-1.




**Figur 7-1: ISO/IEC 27035 Hendelseshåndteringssyklus**

Arbeidet er delt inn i fem faser (fritt oversatt):

1. Planlegging
2. Detektering
3. Vurdering
4. Behandling
5. Læring

Alle fasene er like viktige, men de tre midterste oppleves kanskje som mest selvsagte; man må på ett eller annet vis oppdage at noe har skjedd, så må man vurdere situasjonen, og deretter iverksette tiltak. Imidlertid er det i planleggingsfasen at man kan legge grunnlaget for en vellykket håndtering når noe skjer, og dette er en fase som aldri avsluttes, men inngår som en del av virksomhetenes arbeid med kontinuerlig forbedring. I denne forbindelsen er læringsfasen også veldig viktig, ettersom det her er mulig å trekke lærdom fra erfaringene med en konkret hendelse. For at dette skal være gjennomførbart, må planleggingen av fasene 2-4 også ta høyde for at informasjon som understøtter denne læringen kan samles inn under veis.

## 7.3 Øvelser

Kraftbransjen har lang tradisjon for gjennomføring av beredskapsøvelser, men det har inntil nylig ikke vært vanlig å inkludere cyber-aspektet i slike øvelser [16]. NVE har i sin rapport fra 2015 [18] dokumentert fire eksempler på IKT-relaterte (cyber) øvelses-scenarioer, men de første to er rene "kontor"-scenarioer, det tredje er muligens relevant (tyveri av sensitiv informasjon), og det siste er klart relevant (angrep på SCADA-infrastruktur). Øvelser basert på det siste scenarioet ble studert av Bartnes, Moe og Heegaard [17], og de konkluderte med at flere slike scenarioer burde utarbeides for kraftbransjen. I fortsettelsen av dette kan vi framføre at det også burde utarbeides egne scenarioer spesielt for cyber-angrep på transformatorstasjoner, som en del av prosessen med kontinuerlig forbedring. KraftCERT tilbyr koordinering av trening og øvelser med flere aktører i bransjen.

# 8 Oppsummering og anbefaling

Denne rapporten har beskrevet hva vi oppfatter som definisjon av hva en digital transformatorstasjon er, og videre dokumentert hvilke cyber-trusler denne kan utsettes for. Vi har kommet med forslag til løsninger for cybersikkerhet, samt innspill om forebyggende tiltak og beredskap. Vi har dokumentert sikkerhetsrelevante aktiva i digitale transformatorstasjoner, og lansert et forslag for prioritering av aktiva som tar hensyn til både OT- og IT-klassifiseringer.

I det følgende gjentar vi stikkordsmessig anbefalinger til Statnett, fordelt på grunnleggende (basis) tiltak og ytterligere tiltak (utvidet sikkerhetsnivå). Til slutt kommer vi med forslag til videre arbeid.

## 8.1 Grunnleggende sikkerhetsnivå (basisnivå)

- Gjennomfør risikoanalyse med henblikk på cyberangrep for en representativ digital transformator-stasjon
- Øvelser og trening basert på NVEs scenarioer for IKT-hendelser
- Monitorering av nettverkstrafikk med anomalideteksjon
- Logging og logganalyse
- Konfigurasjonskontroll på fysiske og logiske komponenter
- Gode passord på alle komponenter

## 8.2 Utvidet sikkerhet

- Fullkryptering av all IEC 61850-trafikk i feltet (må veies mot ulempene kryptering medfører for mo-nitorering)
- Redundans av kritiske komponenter med failover
- Anomalideteksjon på sensormålinger, med ekstra sensorer for validering
- "Nødknapp" for enkel nettverks-segregering ved behov
- Foreta risikoanalyser med henblikk på cyberangrep for hver enkelt transformatorstasjon.
- Utarbeidelse av nye scenarioer for cyber-hendelser spesifikt for digitale transformatorstasjoner
- Tofaktor autentisering mot alle komponenter

## 8.3 Videre arbeid

Klassifiseringene i avsnitt 3.1 bør kvalitetssikres av representanter for bransjen. Vi ser for oss at dette kunne løses praktisk i en workshop med bred deltagelse fra norsk kraftindustri. SINTEF bidrar gjerne til en slik workshop.

Det er en rekke muligheter for sikkerhetsforskning i EUs forskningsprogram H2020, og det er viktig at norsk kraftbransje deltar på denne arenaen for å bidra til forsking som kan gi sikrere digitale transformatorstasjo-ner, også for å lære av andre europeiske aktører.

## Referanser


[1] Store Norske Leksikon - https://snl.no/transformatorstasjon

[2] Future Intelligent Transmission Network Substation (FITNESS), "Project Progress Report", December 2016, p.4, tilsendt på epost fra Priyanka Mohapatra, prosjektleder for FITNESS

[3] G. Igarashi et al. "Development of a Digital Optical Instrument Transformer with Process Bus Interface According to IEC 61850-9-2 Standard", 2015 IEEE PES Innovative Smart Grid Technologies Latin America (ISGT LATAM), p. 893-897

[4] S. Richards et al. Feedback on In-Service Deployment of the Fully Digital Substation, CIGRE 2014, paper no. B5-110

[5] Documentation Requirements Throughout the Lifecycle of Digital Substation Automation Systems, CIGRE Brochure 628

[6] N. Hurzuk et al. "Digitale stasjoner i transmisjonsnettet", NEF Teknisk Møte 2017 Informasjonsteknologi og elektroteknikk – Det digital energiskiftet, ISBN 978-82-594-3772-3, p.250-261

[7] S. Richards, et al. "Feedback on In-Service Deployment of the Fully Digital Substation", CIGRE 2014, paper B5-110-2014

[8] Y.I. Morzhin, et al. "First "Digital Substation" 110 kV, using the IEC 61850 (-8-1 and-9-2LE) for measurement, protection and control switching devices in Russia", CIGRE 2014, paper B3-110-2014

[9] D. Chatrefou, et al. " DIGITAL SUBSTATION – Tests of Process Bus with GIS Non Conventional Instrument Transformers", CIGRE 2012, paper B3-108-2012

[10] ABB brochure, "We are bridging the gap - Enabling Digital Substations", p. 13 https://library.e.abb.com/public/c3f8221f76db46b38d9ae6f8ec6475b2/ABB_Digital%20Substation%20Brochure_1.0.4.pdf

[11] GE Grid Solutions brochure, "Agile digital substations - Releasing the potential of digital technologies", p. 2-3 http://www.gegridsolutions.com/alstomenergy/grid/Global/Grid/Resources/Documents/Products/Agile%20digital%20substation%20solution.pdf

[12] GE Grid Solutions, CB Watch 3, http://www.gegridsolutions.com/md/catalog/CBWatch3.htm

[13] Inger Anne Tøndel, Maria B. Line, Gorm Johansen og Martin G. Jaatun "Risikoanalyse av AMS knyttet til informasjonssikkerhet og personvern", NEF Teknisk Møte 2014, p 315-323 http://www.sintef.no/contentassets/8f3be4a5285b4a7a85a2987a9d397615/rapporter/7.2_tondel_-line_johansen_jaatun---risikoanalyse-av-ams-knyttet-til-informasjonssikkerhet-og-personvern.pdf

[14] Maria Bartnes Line "UNDERSTANDING INFORMATION SECURITY INCIDENT MANAGEMENT PRACTICES: A case study in the electric power industry", doktorgradsavhandling, NTNU 2015 http://hdl.handle.net/11250/2359707

[15] Maria Bartnes Line, Inger Anne Tøndel, Gorm Johansen, Hanne Sæle "Informasjonssikkerhet og personvern: Støtte til risikoanalyse av AMS og tilgrensende systemer", SINTEF Rapport A24258, August 2014 https://infosec.sintef.no/wp-content/uploads/2014/09/St%C3%B8tte-til-gjennomf%C3%B8ring-av-risikovurdering-v1.1.pdf

[16] Maria B. Line, I. A. Tøndel and M. G. Jaatun, "Information Security Incident Management: Planning for Failure," *2014 Eighth International Conference on IT Security Incident Management & IT Forensics*, Munster, 2014, pp. 47-61.

[17] Maria Bartnes, Nils Brede Moe, Poul E. Heegaard: "The future of information security incident management training: A case study of electrical power companies", Computers & Security, Volume 61, 2016, Pages 32-45, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2016.05.004.

[18] Ann-Kristin Larsen: "Øvelser: En veiledning i hvordan planlegge og gjennomføre øvelser innen energiforsyningen", NVE Rapport 39/2015 http://publikasjoner.nve.no/rapport/2015/rapport2015_39.pdf

[19] MG Jaatun, M Bartnes and IA Tøndel: "Zebras and Lions: Better Incident Handling Through Improved Cooperation", presented at I4CS, Vienna, Innovations for Community Services, Volume 648 of the series Communications in Computer and Information Science pp 129-139

[20] MB Line, IA Tøndel and MG Jaatun: "Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations", International Journal of Critical Infrastructure Protection, vol 12, pp 12-26, https://doi.org/10.1016/j.ijcip.2015.12.003
[21] Janne Hagen, Ola Hermansen, Øyvind Toftegård, Jon-Martin Pettersen, Roger Steen, Synnøve Lill Paulen: "Regulering av IKT-sikkerhet - Et helhetlig og fremtidsrettet sikkerhetsregime for forsyningssikkerhet i en digitalisert energisektor", NVE Rapport nr. 26/2017 http://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf
[22] MG Jaatun, TO Grøtan, and MB Line, "Secure Remote Access to Autonomous Safety Systems: A Good Practice Approach", Int. J. of Autonomous and Adaptive Communications Systems, Vol. 2, No 3, 2009
[23] Conway, T., Lee, R. M. og Assante, M. J. (2016), "Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case", SANS ICS and E-ISAC white paper. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[24] Nordbø, P.E. (2013), "Cyber security in Smart Grid stations", in 22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013), Stockholm, 1-4
[25] Cheswick, B. (1990), "The Design of a Secure Internet gateway", in USENIX Summer Conference Proceedings.
[26] A. Miller, et al., "2015 INFORMATION SECURITY BREACHES SURVEY", 2015, https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf
[27] David Kushner, "The Real Story of Stuxnet", https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet, Last-Checked: 15.11.2017, Last-Updated: 23.02.2013
[28] Symantec Security Response, "Dragonfly: Western Energy Companies Under Sabotage Threat", https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat, Last-Checked: 15.11.2017, Last-Updated: 30.06.2014
[29] Anton Cherepanov and Robert Lipovsky, "Industroyer: Biggest threat to industrial control systems since Stuxnet", https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/, Last-Checked: 15.11.2017, Last-Updated: 17.07.2017
[30] Symantec Security Response, "Dragonfly: Western energy sector targeted by sophisticated attack group", https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks, Last-Checked: 15.11.2017, Last-Updated: 20.10.2017
[31] Pilita Clark and Sam Jones, "GCHQ intervenes to secure smart meters against hackers", https://www.ft.com/content/ca2d7684-ed15-11e5-bb79-2303682345c8, Last-Checked: 15.11.2017, Last-Updated: 18.03.2016
[32] Politiets sikkerhetstjeneste "Trusselvurdering 2017", http://www.pst.no/media/82648/pst_trusselvurd_2017_no_web.pdf
[33] "Varsler om datainnbrudd", https://www.nsm.stat.no/aktuelt/varsler-om-datainnbrudd/
[34] Shodan, https://www.shodan.io/
[35] Eireann P. Leverett: "Quantitatively Assessing and Visualising Industrial System Attack Surfaces", Masteroppgave, University of Cambridge 2011, https://www.cl.cam.ac.uk/~fms27/papers/2011-Leverett-industrial.pdf
[36] Kaspersky Lab Discovers Vulnerable Industrial Control Systems Likely Belonging to Large Organizations https://usa.kaspersky.com/about/press-releases/2016_kaspersky-lab-discovers-vulnerable-industrial-control-systems-likely-belonging-to-large-organizations
[37] Thomas Fox-Brewster : "All That's Needed To Hack Gmail And Rob Bitcoin: A Name And A Phone Number" Forbes, 17/9 2017 https://www.forbes.com/sites/thomasbrewster/2017/09/18/ss7-google-coinbase-bitcoin-hack/
[38] NIST: "Digital Identity Guidelines: Now Available" https://pages.nist.gov/800-63-3/
[39] IEC 61850:2017 SER - Series - Communication networks and systems for power utility automation - ALL PARTS https://webstore.iec.ch/publication/6028

[40] IEC 61850-8-1:2011, Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3 https://webstore.iec.ch/publication/6021
[41] Ingvild Vaggen Malvik (red): Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredsskapsforskriften), NVE Veileder nr 1-2013, Norges vassdrags- og energidirektorat, http://publikasjoner.nve.no/veileder/2013/veileder2013_01.pdf
[42] ISO/IEC 27019:2017, Information technology -- Security techniques -- Information security controls for the energy utility industry, https://www.iso.org/standard/68091.html
[43] Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven), https://lovdata.no/dokument/NL/lov/1990-06-29-50
[44] Kim Traavik (leder): Samhandling for sikkerhet, Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid, NOU 2016:19, https://www.regjeringen.no/contentassets/03960058f3f94fbe9d290593bee22c1a/no/pdfs/nou20160160019000dddpdfs.pdf

Teknologi for et bedre samfunn

**www.sintef.no**