Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for teknisk kybernetikk

Robert Strand
Stian Kold Huseby
Håvard Skansgård
Marcus Kristensen

Fremtidige PLS-baserte kontrollanlegg i vannkraftverk

Bacheloroppgave i Elektroingeniør
Veileder: Kåre Bjørvik

Mai 2021

NTNU
Norwegian University of
Science and Technology

Robert Strand
Stian Kold Huseby
Håvard Skansgård
Marcus Kristensen

Fremtidige PLS-baserte kontrollanlegg i vannkraftverk

Bacheloroppgave i Elektroingeniør
Veileder: Kåre Bjørvik
Mai 2021

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for teknisk kybernetikk

Forord

Følgende rapport er et tverrfaglig arbeid som konkluderer bacheloroppgave ved Norges teknisk-naturvitenskaplige universitet i Trondheim, våren 2021. Rapporten er bygget opp på en måte som innleder med teoretisk bakgrunn. Teoridelen har som mål om å gi forståelse av videre informasjon, uten særlig utgreiing. Det er antatt en grunnleggende basiskunnskap. Arbeidet med rapporten er gjort under tider av enestående karakter som har gitt implikasjoner for hvordan arbeidet har foregått, hvilken informasjon som har vært tilgjengelig og som har gitt studentene ekstraordinære utfordringer å håndtere.

Møtevirksomhet og samarbeid har foregått i stor grad på digitale plattformer og via korrespondanse som del av den nasjonale dugnaden for å stanse Covid-19 pandemien som nå herjer. Samtidig har arbeid med fysisk oppmøte i kraftstasjoner blitt avlyst, en del av oppgaven som er beskrevet som en forutsetning.

Studentene som inngår i bachelorgruppen har delte bakgrunner. Både med tanke på tidligere utdanning og når det kommer til spesialisert retning innen elektrolinjen ved NTNU. Her er to fra elkraftteknikk, og to fra automasjonslinjen. Dette har hjulpet å gi flere perspektiv på oppgaven.

Motivasjonen bak valg av denne oppgaven går til studentenes interesser og ønske om å utfylle utdanningsforløpets mangel på relevant kunnskap i henhold til faget. Studentene ønsket å lære mer om PLS styringssystemer, nettverksoppbygging, bruk av aktuell standardisering ved Norges mest sentrale produksjonssystemer i en virkelighetsnær setting.

Vi vil rette en stor takk til veilederne fra Statkraft, Pål Glimen og Safet Trto som har bidratt med sin kunnskap og brede erfaring under prosjektperioden. Deres engasjement smittet lett over og ga studentene inspirasjon til å fortsette å jobbe, til tross for lange dager hjemme i isolasjon. Videre takk gis til veileder Kåre Bjørvik og de mange ressursene som har satt av tid til intervjuer og delt sine erfaringer med oss. Takk til alle.

Bachelorgruppen
20. mai 2021

SAMMENDRAG

Kraftmarkedet og organisatoriske endringer, i tillegg til den akselererende teknologiutviklingen, påvirker hvilke investeringer som Statkraft må vurdere i tiden som kommer. Det lokale kontrollanlegget ved de 346 vannkraftverkene er grasrota, og optimalisering og økt kontroll ved disse vil gi ringvirkninger tilsvarende Statkrafts størrelse. Denne rapporten er en mulighetsstudie som vurderer hvordan fremtidige PLS-baserte kontrollanlegg ved vannkraftverk burde bygges.

Statnett, som er ansvarlig for sentralnettet, har satt presedens når det kommer til standardisering. Dette blir gjort for å oppnå en mer effektiv prosjektering og like anlegg. Det er sett på hvordan Statkraft kan benytte samme tankesett til å forenkle og på bedre vis samkjøre sin portefølje av kraftverk. Utenlandske aktører i Brasil, Canada og Italia tester bruken av IEC 61850 for sine kraftverk. Rapporten tar for seg hvilke muligheter dette gir og aktuelle deler av kontrollanlegget hvor denne standarden helst bør tas i bruk, og om en kan oppnå samme funksjonalitet på andre sett som er mindre inngripende i dagens anlegg.

Det sentraliserte styresystemet gjør at man alltid må vurdere nettverkssikkerhet og eksponering mot cyberangrep. Et problem som øker med stigende frekvens. Samtidig øker også nødvendigheten for datainnsamling og analyse. Rapporten ser på hvordan man kan ivareta sikkerheten og bevarer kontrollen i denne viktige delen av norsk infrastruktur.

Økt produksjonsregulering i fremtiden gir utfordringer for den tradisjonelle drifts og vedlikeholdsrutinen man har i dag. Større grad av regulering kan tenkes å medføre økt vedlikeholdskostnad og endret slitasjefrekvens. Dette medfører mer behov for instrumentering og logging av rådata til prediktivt bruk. Rapporten ser på måter en kan innføre slike system med minst mulig inngrep i dagens systemer.

ABSTRACT

The power market and the organizational changes, in addition to the accelerated development of technology, affect which investments Statkraft must consider in the future. The local control plant at the 346 hydropower plants is the foundation, and optimization and the increased control will have repercussions corresponding to Statkraft's size. This report is a feasibility study that assesses how future PLC-based control systems at hydropower plants should be built.

Statnett, which is responsible for the central grid, has set a precedent when it comes to standardization. This is done to achieve a more efficient design and equal facilities. The bachelor's group has studied how Statkraft can use the same mindset to simplify and better coordinate their portfolio of power plants. Foreign companies in Brazil, Canada and Italy are testing the use of IEC 61850 for their power plants. This report addresses the possibilities it provides and the relevant parts of the control system where the standard preferably should be used. Furthermore, whether one can achieve the same functionality in other ways that are less intrusive in today's facilities.

The centralized control system means that one must always consider network security and exposure to cyberattacks, an issue with increased frequency. At the same time, there is also a desire to increase data collection for analysis. The report looks at how to ensure security and how to maintain control in this critical part of Norwegian infrastructure.

Increased need to regulate production output in the future present challenges for the traditional operation and maintenance routine we have today. A greater degree of control may lead to increased maintenance costs and changed wear and tear frequency. This entails more need for instrumentation and logging of raw data for predictive use. This report looks at different ways in which such systems can be implemented, with as little intervention as possible in the current systems.

Ordliste

APCI	Application Protocol Control Information
ASDU	Application Service Data Unit
C2C	Controller to Controller
DCS	Distributed Control System
DDos	Distributed-denail-of-service
DMZ	Demilitarized Zone
DP	Decentralized Peripherals
ESD	Emergency Shut Down
ET	Ekstern Terminal
FB	Funksjonsblokk
HART	Highway Addressable Remote Transducer Protocol
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HW	Hardware
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IP	Internet Protocol
IRT	Isochronous Real-Time
IT	Information Technology
IIOT	Industrial Internet of Things
LME	London Metal Exchange
MCC	Motor Control Centre
MitM	Man in the Middel
MQTT	Message Queuing Telemetry Transport
MU	Merging Unit
NEK	Norsk Elektroteknisk Komite
OPC-UA	Open Platform Communications - Unified Architecture
OSI	Open Systems Interconnection
OT	Operational Technology
PA	Process Automation
PLS	Programmerbar Logisk Styring
PROFIBUS	Process Field Bus
PROFINET	Process Field Net
PTP	Precition Time Protocol
RBAC	Role Based Access Control
RDS	Reference Designation System
RT	Real-Time
SW	Software
SCADA	Supervisory Control And Data Acquisition
SCS	Station Control System
SDCI	Single-drop Digital Communication Interface

SDN	Software Defined Networking
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TIA	Totally Integrated Automation
UGW	Unidirectional Gateway
VFD	Variable-frequency Drive
VPN	Virtual Private Network
AES	Advanced Encryption Standard
RSA	Rivest–Shamir–Adleman
SHA	Secure Hash Algorithm
ECC	Elliptic-curve cryptography
PKI	Public key infrastructure

Figurer

Innhold

1 INNLEDNING

Vannkraftverk var tidligere uavhengige enheter med ansatte som driftet anlegget lokalt. Hver for seg hadde de sin måte å gjøre ting på og kjennskap til eget kraftverk var viktig for å raskt kunne håndtere diagnostisering og planlegge vedlikehold. Denne trenden har endret seg til en sentralstyrt modell med en mer sentralisert organisasjon enn tidligere. Samtidig har vi en endring i kraftmarkedet som er drevet i stor grad av prisen på karbon og den økende andelen uregulerbare energikilder. Selve prosessen som inngår i et vannkraftverk endrer seg lite, men man ser en endring i måten et vannkraftverk blir regulert.

Videre har Statkraft et ønske, som de fleste andre selskaper, om å holde tritt med teknologiutviklingen. Selv om prosessen som inngår endrer seg lite kan det være fordelaktig å ta i bruk nye systemer for å optimalisere og sikre drift. Samtidig er det et kostnadsaspekt. Kan bruk av ny teknologi korte ned tilbakebetalingstiden på nye kraftverk? Statkraft har tatt eierskap over flere kraftverk der en teknisk oppgradering står for tur. Denne studien har mål om å kaste lys over hvilken retning en burde vurdere som teknisk løsning i et slikt prosjekt, og prosjekteringsfasen som leder frem mot dette.

Bacheloroppgaven, som denne rapporten bygges på, kartlegger oppbygging av dagens lokale kontrollanlegg og ser på alternativer som bidrar til å bedre, og- eller tilpasser anlegget for å være bedre rustet til å møte fremtiden. Alternativene som vurderes kan være metoder som ikke er veletablert i dag blant Statkrafts energiverk, men som har basis for å kunne inkluderes i større grad på tvers av regioner. Et fokus på bruk av standardiseringsarbeid og hvordan dette kan gi fordeler er også vurdert. I denne sammenheng er det foretatt intervjuer med sentrale ansatte på tvers av kraftbransjen og på tvers av landegrenser med mål om å avdekke fokusområder, implementasjons- og effektiviseringsstrategier i tillegg til synspunkter på videre utvikling innen fagfeltet.

Problemstillinger som oppgaven belyser er viktig for at Statkraft skal kunne ta riktige beslutninger når fremtidige kontrollanlegg prosjekteres. Bacheloroppgaven har satt mål om å kunne foreslå løsninger fra et nøytralt ståsted og med uerfarne øyne.

Rapporten tar for seg en introduksjon av vannkraftproduksjon og oppbygging av et kraftverk og tilhørende komponenter. Med dette som basis vil man lettere kunne vurdere følgende drøftinger der detaljer rundt disse aspektene ikke er like fremhevet. Rapporten går videre inn på bruk av standarder og hvordan dette er brukt i dag. Intervju som er gjort i prosjektperioden fremlegges som basis for utviklingsideer og det drøftes endringer som kan gjøres. Til slutt gjøres en konkludering basert på prosjektdeltageres totale inntrykk.

2 METODE OG RESSURSER

2.1 Metode

Arbeidsmetoden brukt i bachelorprosjektet består av intervju med relevante aktører i kraftbransjen, og innsamling av resultater fra tidligere forskningsprosjekt på området. Store ressurser er benyttet til å oppdrive og studere forskningsrapporter. Av disse er relevant informasjon benyttet som innspill for oppgaven. Formålet har vært å hente erfaringer og benytte disse som grunnlag for et konkluderende svar, fra et nøytralt ståsted. Det er tatt hensyn til hvilke kilder som oppfattes som troverdige. Forutsetninger for oppgaven var i utgangspunktet god tilgang på dokumentasjon fra flere vannkraftverk, og befaringer for å gi grunnleggende forståelse av anleggene idag. Gitt omstendighetene med hjemmekontor, ble ikke dette gjennomførbart. Bachelorgruppen ble nødt til å skaffe relevant informasjon til oppgaven på alternative måter, som kan ha innvirkning på perspektivet i sluttresultatet. Gitt oppgavens omfang besluttet bachelorgruppen å fokusere på flere aspekt relevant for fremtidens kontrollanlegg. Det er vurdert hvilke utviklingsområder som kan være hensiktsmessig for Statkraft å følge med på.

2.2 Ressurser

Her listes de viktigste bidragsyterne som har medvirket til studien gjennom intervjuer.

Vattenfall AB:

Som Statkraft, er Vattenfall et statseid energiselskap med kunder over store deler av europa. De rundt 20 000 ansatte jobber innen ulike grener innenfor Vattenfalls' portefølje. Vattenfall har en diversifisert portefølje av energiverk som dekker atomkraft, vannkraft, vind og gass. I tillegg drifter de også forbrenningsanlegg til sentralvarme. Hensikten med intervjuet innen atomkraftsektoren var å undersøke hvilket fokus, og hva slags teknologi som ble innført samtidig som de opprettholdt den høye standarden for sikkerhet som de har i anleggene sine. Spesielt overvåkning og instrumenteringsdata har høy prioritet gitt konsekvensene et feilskjær i reguleringen medfører.

Voith Hydro AS:

Voith Hydro AS er et selskap under den tyske Voith gruppen med global virksomhet innen mange segmenter. Voith Hydro har over 140 års erfaring innen vannkraft og installasjon. [71] Votih Hydro leverer automasjons, service og vedlikeholdstjenester samt komplette anlegg mot vannkraftindustrien. Faktisk produseres så mye som $\frac{1}{4}$ av verdens vannkraft med teknologi fra Voith. Voith har vært leverandør til Statkraft i flere prosjekter og har unik innsikt i evolusjon i et vannkraftverks kontrollanlegg. Som stor bidragsyter til Statkrafts virksomhet vil Voith også måtte bli involvert i fremtidige endringer i struktur når det kommer til standardisering i leveranser og struktur i software.

Statkraft SF:

Statkraft SF er et statsforetak (SF) under Nærings og fiskeridepartementet. (NSD) Selskapet ble dannet -92, og har utviklet seg til å bli et ledende internasjonalt selskap med virksomhet i 17 land. Under Statkraft sin paraply ble det produsert 65,4 TWh i 2020, der 92% har opphav fra fornybare ressurser som vann, vind og solkraft. [43] Statkraft er oppdragsgiver i denne studien, og bidrar med teknisk kunnskap om anlegg og erfaring fra drift og vedlikehold. Statkraft bidrog med ressurspersonell fra Norge, Sverige og Tyskland som alle har forskjellige tilnærminger.

Statnett SF:

Statnett er de som har ansvar for forsyning og nett i Norge og samarbeider med andre nordiske nettansvarlige om balanse og flyt i nettet. Statnett kan man sånn sett si har den øverste regulerende makta over kraftverkene. Are Johan Hansen informerte om Statnetts tilnærming når det kommer til standardisering, anbudsprosesser og tankesett når det kommer til leverandørforhold.

Hydro-Quebec:

Er verdens fjerde største produsent av vannkraft og har røtter tilbake til 1945. Vår kontaktperson, Denis Francesconi, jobber med testing og implementering av IEC 61850 og bidro med å belyse rundt dette arbeidet.

Enyr:

Enyr leverer standardiseringstjenester for databehandling til kraftprodusenter. Selskapet spesialiserer seg på bruken av IEC 61850, skytjenester og data modellering. Giuseppe Rigadello som er modelleringsspesialist, informerte rundt standardiseringsarbeidet som de har bidratt til i Italia.

Siemens:

Siemens er en stor leverandør til Statkrafts kontrollanlegg. De har egen virksomhet for teknologiutvikling og har innsikt i hvilken retning markedet beveger seg. Ingeniør Leif Dahl informerte om system for vern og redundans med bruk av IEC 61850.

Marcos Mendes:

Marcos har skrevet en post-doktor rapport innen bruk av IEC 61850 og har dyp teoretisk forståelse for hensikten og fordelen bak dette tankesettet.

3 VANNKRAFTVERK

Dette kapittelet tar for seg generelle elementer innen vannkraft og er ment som et innførende kapittel med historisk utvikling, beskrivelse av produksjonsprosessen og vedlikeholdsarbeid som gjøres idag.

3.1 Historie

Vannkraft kommer fra vannfallsenergi som blir omgjort fra mekanisk energi til elektrisitet. Kraftproduksjon fra vannkraft har vært den viktigste energikilden i form av fornybar energi, og utgjorde rundt 16 prosent av verdens samlede kraftproduksjon.[57]

Vannkraften ble allerede tatt i bruk i antikken som vannhjul for å male korn. Teknologien spredte seg videre i Europa under den industrielle revolusjon på begynnelsen av 1800-tallet og var med å gi mekanisk energi til tekstil- og maskinindustrien. Produksjonen av elektrisk energi fra vannkraft startet først i 1870-årene, og elektrifiseringen som fulgte på i begynnelsen av 1900-tallet var basert på den typen kraftproduksjon.

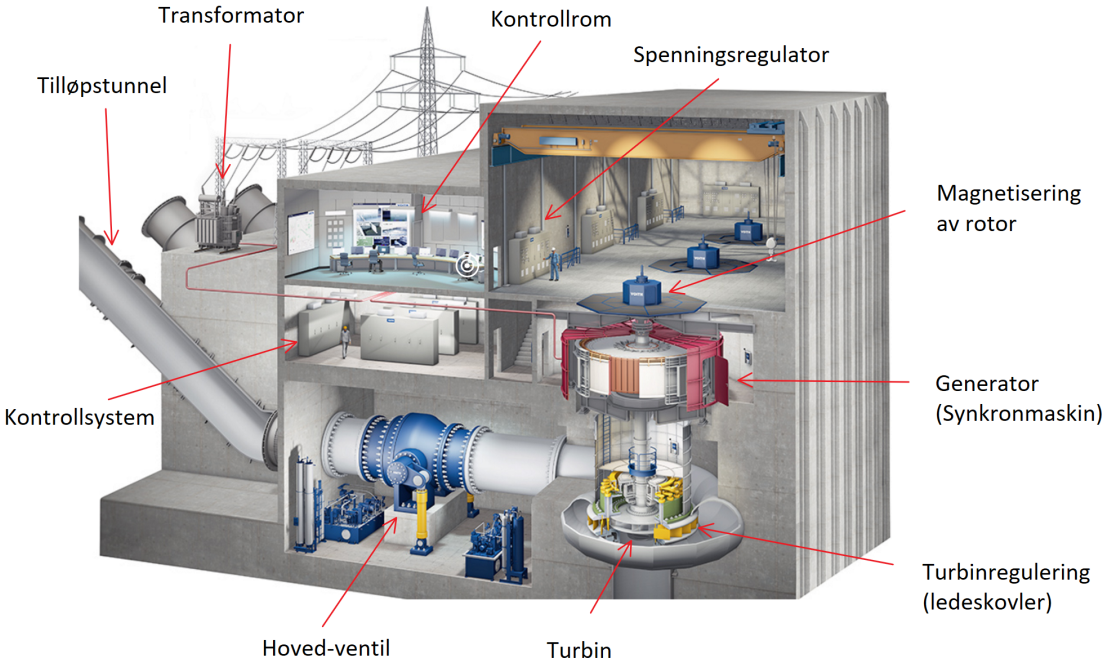
Vannkraftproduksjonen i Norge har vært enesteående på grunn av de spesielt gode naturgitte forutsetningene for utbygging av vannkraftverk. Mye nedbør og stor fallhøyde gjør det lett å utnytte vannfallet. Disse forholdene har gjort Norge til Europas største og verdens syvende største vannkraftprodusent, med totalt 976 vannkraftstasjoner i drift. Det meste av vannkraftpotensialet er allerede unyttet i Europa og Nord-Amerika, men i verdensdeler som Afrika, Asia og Sør-Amerika har det fortsatt et stort potensial av utnyttelse.

Figur 1: Venstre: Paulenfoss, statens første kraftverk fra 1895 [69].
Høyre: Oddatjørn-dammen, høyeste fyllingsdamkonstrukjonen i Norge som ble ferdigstilt i 1988 [42].

3.2 Hvordan fungerer et vannkraftverk

Vann som kommer ned fra fjell i form av nedbør og is- og snøsmelting blir demmet opp i vannmagasiner. Ved å plassere et kraftverk laverene enn demningen gir det vannet en potensiell energi som kan utnyttes ved å føre vannet ned til kraftverket via rør. Vannmagasinene gjør det mulig å regulere kraftproduksjonen etter behovet for energi og kraftverkene er konstruert slik at produksjonen kan skje hurtig og tilpasses forbruket.

Et typisk vannkraftverk består av følgende (se figur 2), og er hoveddelene av anlegget. Kraftverket har oftest flere turbiner og generatorer for å utnytte effekten av det tilgjengelige vannfallet.



Figur 2: Oversikt over oppbygning av et Vannkraftverk.[72]

En hoved-ventil åpner for at vann fra tilløpstunnelen kan strømme inn inn til turbinen. Vannet som strømmer inn igjennom turbien får den til å starte å rotere. En turbinregulator regulerer vannmengden inn til turbinen slik at turbinen får korrekt omløpshastighet i forhold til ønsket frekvens. Akslingen som er festet til turbinen vil få rotoren i synkronmaskinen til å rotere. Rotoren magnetiseres ved at den blir tilført en DC-spenning, og synkronmaskinen vil da fungere som en generator og indusere en AC-spenning. Spenningsregulatoren regulerer DC-spenningen for å gjøre generatoren enten overmagnetisert eller undermagnetisert ut ifra hvor mye reaktiv effekt som er ønskelig å produsere/forbruke. Strømmen fra generator går så til en transformator hvor den blir transformert opp til et høyere spenningsnivå for deretter bli sendt ut på hovednettet. Kontrollsystemet tar seg av alle start- og stoppsekvensene og overvåker systemet til enhver tid ved hjelp av sensorer og følere. I kontrollrommet kan alle prosessene styres ved hjelp av en datamaskin eller HMI. Kontrollrommet er koblet opp mot en driftssentral slik at stasjonen kan opereres uten at den nødvendigvis er bemannet.

3.3 Reguleringssystemer

Reguleringssystemet er en viktig komponent og del av et vannkraftverk. For at en generatoren skal kunne kobles til nettet må spenningen, frekvensen og fasen ut fra generatoren være helt lik som i strømnettet. Reguleringsystemene sørger for disse kriteriene før generatoren legges inn på nettet. Systemene er også med å levere en stabil spenning og frekvens etter den er tilkoblet nettet.

3.3.1 Spenningsregulering

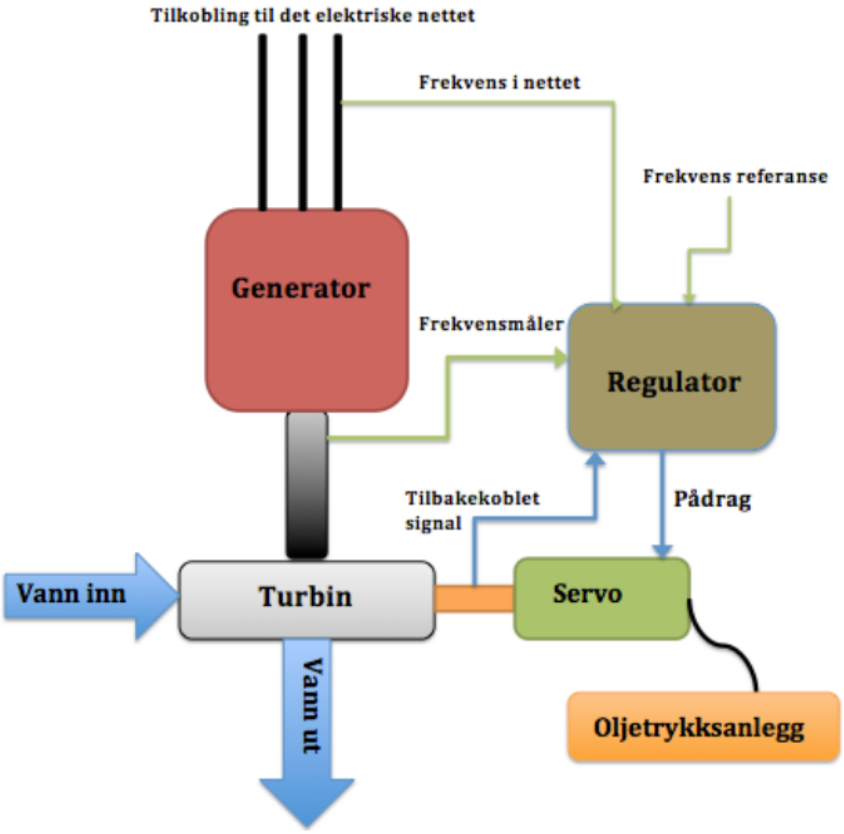
Belastningen i nettet varierer konstant og derfor er det nødvending med en regulator som kan stabilisere spenningen. En spenningsregulator gjør at spenningen ut fra en generator blir jevn og stabil. Det gjøres ved at regulatoren føler på spenningen ut fra generatoren hele tiden og kan detektere et spenningsfall som kan komme fra økt belastning i nettet. Ved et slikt fall i spenningen kan magnetiseringsspenningen til rotor øke som medfører at magnetfeltet blir sterkere som igjen øker generatorspenningen. [90] Magnetiseringsspenningen kan også redusere for å kompensere for en nedgang i belastning ved et mulig bortfall av last i nettet. Ved å kunne regulere magnetiseringsspenningen gir det muligheten for å gjøre generatoren enten over- eller undermagnetisert. En overmagnetisert generator vil være kapasativ og levere reaktiv effekt, mens en undermagnetisert er induktiv og forbuker reaktiv effekt.

3.3.2 Turbinregulering

Regulering av en vannkraftturbin går ut på å regulere omløpstallet/turtallet til turbinen [15]. Turtallet til turbinen blir regulert ved at vannmengden inn til turbinen reguleres ved hjelp av ledeskovler eller dyser. En turbinregulator består av olje-hydraulisk servomotorer som regulerer åpningen på ledeskovlene eller dysene. En digital regulator er en datamaskin som tar inn signaler fra målinger som videre sender signaler til servomotoren til å bestemme pådraget, altså åpningen eller vinkelen på ledeskovlene/dysene. For at en generator skal kunne tilkobles hovednettet må turtallet være i samsvar med den satte frekvensen nettet, som er 50Hz i Norge. Ved at generatorens rotor er festet til den samme akslingen som turbinen vil de ha det samme turtallet. I rotor er det plassert nord- og sørpoler, som får sin polaritet ut ifra magnetiseringsspenningen som blir påtrykt via kullbørster direkte på rotoren. Antall poler i rotoren bestemmes ut ifra det bestemete turtallet til generatoren og turbinen.

Formel: $poler = (120 * frekvens)/turtall$
Ut ifra denne formelen ser vi at lavere turtall gir flere poler for å opprettholde den samme frekvensen. I vannkraftturbiner er det vanlig med lavere turtall og flere poler sammenlignet med dampturbiner.

Figur 3: Turbinregulering med ledeskovler, lukket stilling til venstre og åpen stilling til høyre [99]



Figur 4: Prinsippfigur av et reguleringssystem [15]

3.4 Teknologisk evolusjon

Kontrollanleggene i vannkraftverk ble tidligere bygd opp som konvensjonelle anlegg. Kontrollsystemene var basert på releer, lamper, brytere, vendere og instrumenter. På 90-tallet ble PLS tatt i bruk og deler av det relebaserte anlegget byttet ut med en komponent som har mange releer innebygd i logikken. Dagens anlegg består av en blanding av PLS- og relebaserte kontrollanlegg, men hovedsaklig av PLS. Styring og overvåkning via brytere, lamper og instrumenter har blitt byttet ut med datamaskiner og skjermer. Grensenittet mellom datamaskin og mennesker er en skjerm med styring, denne kalles HMI. I dagens anlegg er det tilleggssystemer for datainnsamling og overvåkningskontroll, dette systemet kalles SCADA. Teknologien i kontrollsystemene utvikles hele tiden og i en enorm fart den siste tiden.

Reguleringsystemene også har utviklet seg stort siden vannkraftverk først ble bygd. Spenningsregulatoren var tidligere konstruert av en elektrisk motor som koblet inn eller ut elektriske motstandselementer for å regulere magnetiseringsspenningen. Nå benyttes statiske elementer som transformatorer, kondensatorer, likerettere og transduktorer. Denne typen regulator er i stand til å regulere spenningen mye raskere [90]. For å regulere vannstrømmen inn til turbinen ble det tidligere brukt luker og spjeld. Videre ble turbinregulatoren utviklet til en mekanisk løsing bestående av pendler og lodd for regulering av en ventil inn til turbinen. Utviklingen gikk videre og reguleringen ble de gjennomført med olje-hydrauliske servomotorer og PI- og PID-regulatorer. I ettertid tok elektroniske regulatorer over, disse bestod fortsatt med olje hydrauliske servomotorer men også med elektriske sensorer og regulatorer som ble digitale. Dette medførte at systemet var programmerbart, og det kunne settes opp konfigurasjoner og parametre gjennom PC. Kontinuerlig utvikling av elektronikk muliggjør forbedringer og endringer i reguleringssystemene i fremtiden [15].

3.5 Vedlikehold

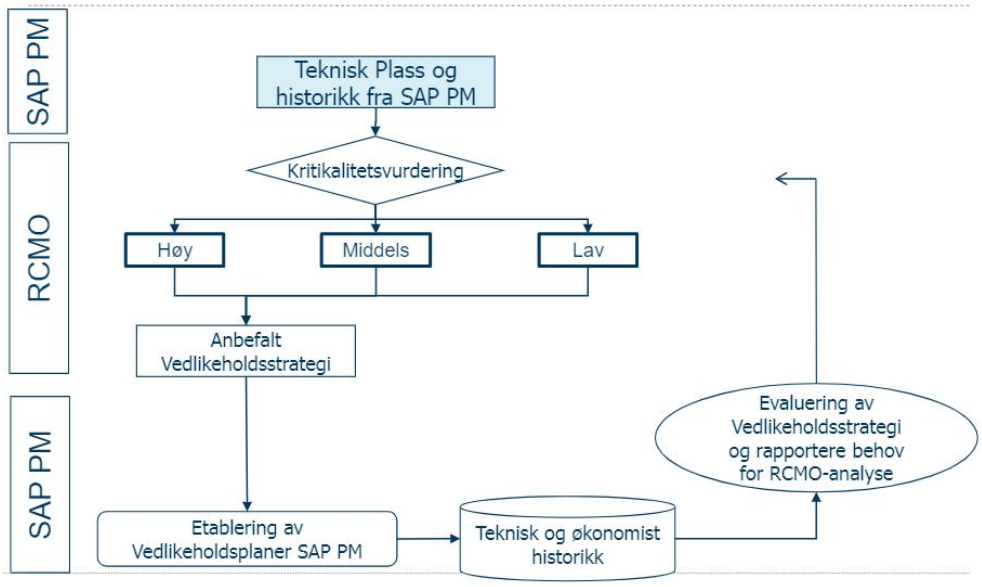
Det ligger store investeringer til grunn for å drifte et vannkraftverk. Derfor er det avgjørende med lang levetid ved anleggene for å skape fortjeneste. Det er ønskelig at et kontrollanlegg som helhet skal ha en teknologisk levetid på minst 20 år før en eventuell renovering. Derfor er det avgjørende at kraftverkseiere og leverandører av kontrollanlegg har rutiner for vedlikehold og service av HW og SW for å holde anlegget i drift. Kraftverkseiere har normalt en avdeling for drift og vedlikehold som følger opp anlegg i et avgrenset lokalområde. Leverandørene har ofte regionale eller nasjonalt stasjonerte servicearbeidere som reiser ut ved innleieservice.

3.5.1 Hardware

Kraftverkseierne følger leverandørenes anbefalinger for utskifting av HW. Dette er en deterministisk tilnærming til vedlikehold hvor for eksempel en komponent byttes ut hvert fem år eller etter hundretusen brukstimer, uavhengig av komponentens tilstand. Dette er en forebyggende tilnærming basert på forskning og erfaring som sikrer driften i anlegget. På grunn av serviceutgifter og tapt inntekt ved driftstans, er det ønskelig å utføre en planlagt stopp framfor uventet stopp som følge av havari på en eller flere komponenter [30]. Ved større rehabiliteringsarbeid planlegges stans til årstider med minst inntekttap, altså når strømprisen er lavest mulig.

Det siste tiåret har vært en overgang mot en ny vedlikeholdsfilosofi. Blant annet har Statkraft satt igang jevnlige tilstandskontroller ved vannkraftverkene, hvor det vurderes utskiftning av komponenter når risiko for kjøring er for høy [30]. Dette er en prediktiv tilnærming til vedlikehold, siden utskiftninger forekommer etter behov og risiko. For å vurdere vedlikehold tas betraktninger som påvirker lønnsomheten. Vurderinger som undersøkes er; tapt inntekt ved planlagt vedlikehold, tapt inntekt ved havari, og sannsynligheten for havari. Dette resulterer i en lønnsomhetsbetraktning som sammen med kvalitative kriterier avgjør om tiltak skal initieres [4]. Digitale verktøy som Vansimtap kan blant annet estimere tapt produksjonsinntekt som følge av havari eller vedlikehold [1]. Vansimtap brukes ved vurdering av større rehabiliteringsprosjekter hvor driftstans gir vesentlig tapt inntekt i vedlikeholdsprosessen.

Vedlikeholdssystemet hos Statkraft er en kombinasjon av SAP Plant Maintenance og RCMO [12]. RCMO er en analysemetode for valg av vedlikeholdsplan. Den benytter en prediktiv filosofi hvor påliteligheten til komponenter vurderes ut ifra jevnlige inspeksjoner med tilstandsvurdering. Komponenter eller anleggsdeler vurderes etter en karakterskala fra 1 til 4. Utslaget på skalaen indikerer hvilken oppfølging som er nødvendig. Karakter 1 viser til normaltilstand, karakter 2 kvalifiserer til tettere oppfølging, ved karakter 3 vurderes lønnsomhet for utbedring av tiltak i en skriftlig rapport, og karakter 4 krever skriftlig rapport og tiltak før start av aggregat [5]. SAP Plant Maintenance lagrer teknisk og økonomisk historikk ved kraftstasjonen, og benytter data fra RCMO for oppsett av vedlikeholdsplan basert på driftsstatistikk og tilstandsvurderingene [3].



Figur 5: Sturukturen i vedlikeholdssystemet i Statkraft [12].

Komponentsvikt kan likevel forekomme i forkant av rutinemessig utskiftning. Derfor har kraftverkene ofte reservedeler oppbevart ved kraftverket for å raskt sette anlegget i drift igjen, men mengder av lagervarer påvirker lønnsomheten. Ved mangel på reservedeler er man avhengig av at leverandør har tilgjengelige deler på lager. Dette varigerer mellom leverandørene og alderen på kontrollanlegget. Om anlegget er 15 år gammelt er det sannsynlig at komponenten ikke er i sortimentet lenger. Dette kan skape en dominoeffekt av utskiftninger siden nye komponenter ikke alltid er kompatible med de eldre. Derfor holdes ofte enkelte komponenter på lager ved kraftverket, siden tapet ved større utskiftinger er mere omfattende med tanke på kostnad og tid.

3.5.2 Software

Man kan si at SW testes hver gang kraftverket startes og stoppes, siden eventuelle feil skal gi varsel hos driftssentralen. Likevel kjøres kritiske funksjoner gjennom funksjonstester med jevne mellomrom. Det er ønskelig at alle funksjoner fungerer, slik at kontrollanlegget kjører en full funksjonstest ca. hvert 5. år.

SW vedlikeholdes av leverandøren på kontrollanlegget gjennom en serviceavtale. Bakgrunnen for at dette ikke håndteres av driftsavdelingen hos kraftverkseier er at feil eller endringsbehov i SW forekommer såpass sjeldent at det ikke er behov for eget personell på området. I tillegg bruker kraftverkene ofte ulike leverandører, slik at det er strukturelle forskjeller i programmene hos de ulike leverandørene. Siden kraftverkene er avhengig av leverandør for å holde driften oppe velges ofte leverandører som har vært i bransjen i flere titalls år for å sikre seg service i 20-30 år. Tar man Rødberg som eksempel må kontrollanlegget nå byttes etter bare 10 år på grunn av konkurs hos leverandør. Dette medfører store kostnader i ombygging, siden leverandører ikke er fortrolig med drift av andre leverandører sine anlegg.

Kretskort for PLS er et eksempel på en komponent som havarerer tilfeldig. Derfor er det viktig å ha reserve tilgjengelig, men den må også ha siste oppdatering for å oppnå lik funksjonalitet. Dette er et problem i dagens vedlikehold av SW, siden disse kretskortene ligger gjemt på et lager uten å bli oppdatert. Her står man ovenfor et dilemma om man skal lagre en utdatert backupløsning eller om man skal ha tillit til at leverandør sitter på reservedeler ved tilfeldig havari. Dette er det ulik praksis på blant kraftverkseierne.

Ved feil eller mistanke om feil i SW har man i PLS kontrollanlegg muligheten for fjerndiagnose direkte fra leverandør. Fjernoppkoblingen foregår gjennom en VPN-tunell som krypterer data mellom kraftstasjon og leverandør. Dette sikrer at ingen andre på internett kan stjele eller påvirke informasjonen. Av sikkerhetsmessige grunner er oppkoblingen fra leverandør normalt gjennom en datadiode. Det vil si at leverandøren kun mottar informasjon fra anlegget uten mulighet for endringer. Dette gir leverandøren begrensninger, men muligheten for kundeservice opp imot kraftverkene. Enkelte kraftverkseiere har likevel mulighet til fjernendringer direkte fra leverandørens kontor. Dette gir mulighet for SW-oppdatering med endringer i funksjonalitet fra et kontor på andre siden av landet. Fjerndiagnose, men ikke minst fjernending i SW, gir derfor stor tidsbesparelse i vedlikehold og feilsøking. Likevel er det bare mindre endringer som kan utføres fjernt på grunn av krav for testkjøring ved betydlige endringer.

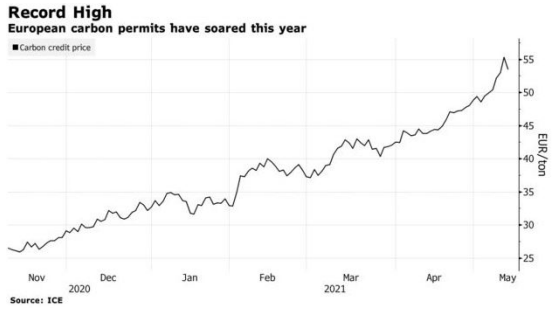
4 KRAFTMARKEDET

For å forstå reguleringsbehovene som Statkraft har i sine anlegg, er det viktig å ha en forståelse for hvordan markedet de opererer i fungerer. Rapporten tar her for seg en generell analyse om hvordan dynamikken i kraftmarkedet kan utvikle seg ved å se på globale hendelser som bachelorgruppen anser for å være indikative for fremtiden.

Markedet for fysiske kraftleveranser i Europa foregår på NordPool, en kraftbørs som opereres av Nasdaq. I 2020 ble så mye som 42TWh solgt i spotmarkedet, et day ahead marked som står for den største delen av fysiske kraftleveranser [52], og 19,9TWh solgt som en del av langsiktige kontrakter mot industrielle kunder.

I Norge er vannkraft den viktigste kilden til elektrisitet, og vil fortsette å være det i overskuelig fremtid.[66] Det skilles mellom regulerbar og uregulerbar produksjon der regulerbarheten defineres av leverandørens evne til å tilpasse seg markedets behov. To eksempler på dette innen vannkraft spesifikt vil være elvekraftverk og vannkraftverk med magasin. Elvekraftverket har høyere produksjon på våren under snøsmelting og produksjonen bestemmes i stor grad av økologiske forhold. Et vannkraftverk med magasinkapasitet vil være et mer allsidig anlegg. Her kan produksjonen reguleres etter markedsbehov og optimaliseres etter prisvariasjonene. Magasinene vil har tilsig av nye reserver gjennom året. [40] Magasinene kan også fylles opp igjen i tidsrom med lavere strømpriser, såkalt effektkjøring med et pumpekraftverk.

Spotmarkedet på kraftbørsen NordPool er allerede kjent for sin volatilitet, noe som vil forsterkes om man skal tro uttalelser fra Andreas Myhre til E24. Dette som følge av den ikke-regulerbare grønne energien som overtar når kull og gass fases ut de neste årene. [70] Prisen vil være volatil fordi en får mindre rom for justering av produksjon mot etterspørsel. Høyere forbruk vil derfor lede til høyere strømpris og vice versa. Endringen i markedet er drevet av et økende fokus på utslipp og at Parisavtalen skal nå sine mål. Samtidig blir prisen på karbon dyrere og dyrere og satte nylig ny rekord over 50 euro/tonn. Dette gjør miljøfiendtlige energikilder lite attraktive og overgang til de nevnte uregulerbare kildene mer bærekraftig. Faktisk har tyske kullkraftverk, som kan regulere produksjonen, i skrivende stund negative marginer og produserer med tap.



(a) Karbonpris [56]

(b) Tysk kullkraft har negativ margin [59]

En slik markedutvikling kan bringe Statkrafts potensielt økte reguleringsbehov nærmere på tidslinjen enn man kanskje kunne anta. Tilsvarende vil investeringshorisont og tilpasningsperiode for kontrollanleggene innskrenkes.

Om man ser til Japan, som kun har 4% vannkraft og 6% andel fornybare energikilder i sin totale energimix [50], så har de allerede nå adoptert et markedsproblem som Danmark tidligere har hatt som følge av stor andel uregulerbar vindkraft. Bloomberg kunne rapportere at spotprisen falt til 0,01yen/kWh i en periode på 6,5 timer som følge av lav etterspørsel i perioden samtidig som energi fra solcelleinstallasjoner hadde høy produksjon. Dagen etter kunne vi vitne en spotpris på 8,42 yen/kWh på grunn av overskyet vær senket den samme produksjonen. En utrolig svingning i markedet som konsekvens av været alene.

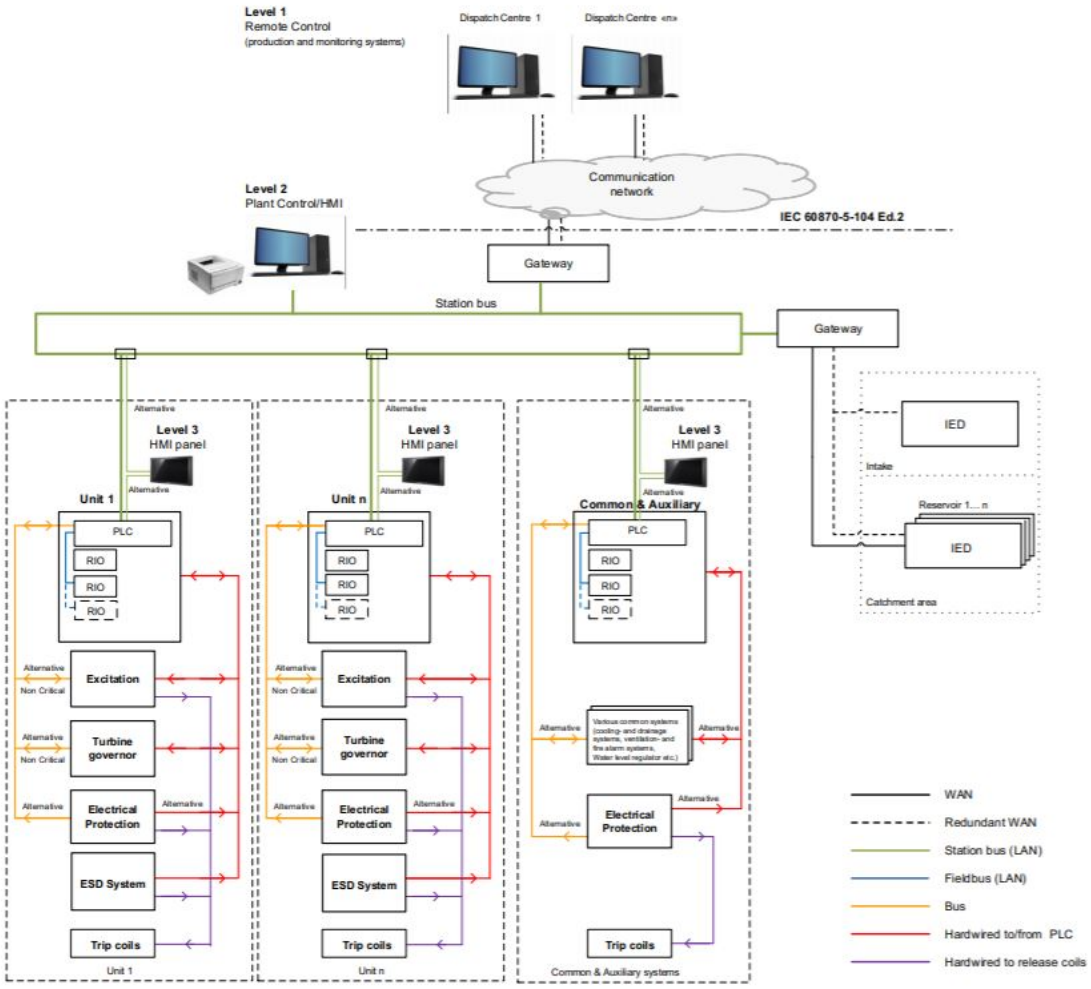
Figur 7: Japansk spotpris 11.April 2021 [68]

Slik ukontrollerbare påvirkninger i kraftproduksjon fra både sol og vind er noe markedet fremover kan se ut til å tilpasse seg til og noe man kan anta kommer til å endre det europeiske kraftmarkedet drastisk i årene som kommer. Dette kan som påpekt gi ringvirkninger som påvirker hvordan Statkraft sine kraftverk blir driftet og vedlikeholdt.

5 KONTROLLSYSTEM

Dette kapittelet tar for seg sentrale elementer generelt for kontrollsystemet. Det må gjøres en rekke valg under oppbygging av et kontrollanlegg som baseres på muligheter og begrensninger ulike løsninger kan gi. De mest brukte løsningene beskrives i dette kapittelet.

5.1 Topologi



Figur 8: Generell spesifikasjon [29] for oppbygging av kontrollanlegg.

5.1.1 Autonome enheter

Kontrollsystemet er delt inn i autonome enheter, som vil si at de er selvstyrende og ikke avhengig av hverandre. Dette gjøres for å begrense konsekvensene ved en mulig feil. Systemet skal også kunne differensiere mellom ukritiske og kritiske feil [29]. Hver av de autonome enhetene skal ha separat og uavhengig operatørgrensesnitt for lokal styring og et eget styreskap med uavhengig strømtilførsel. SCS blir minimum delt inn i 3 ulike autonome deler:

- Genererende enheter
- Normal- og tilleggssystemer
- Vannvei

Det skal være mulig å operere hver autonom enhet uavhengig av:

- Feil eller vedlikehold på andre autonome deler
- Feil på kommunikasjon av bus
- Feil på HMI styring og fjernstyring
- Ukritiske interne feil på SCS

5.1.2 Kontrollnivåer

Kontrollanlegget er delt inn i 4 kontrollnivåer, som er følgende:

1. Fjernstyring fra driftssentral
   Kraftverket er normalt styrt fra en driftssentral.

2. Kontrollrom
   Skal være mulig å operere og overvåke alle systemer i kraftverket fra kontrollrommet. Det er uavhengig av driftssentralen og skal kunne opereres selv om deler av SCS ser ute av drift

3. Lokalstyring
   Hver autonom enhet er tilkoblet HMI for lokal styring, hvor det skal være mulig operere og overvåke enheten. Alle målinger, indikatorer og feilmeldinger skal være tilgjengelige på panelet. Lokal styringen skal være uavhengig av driftssentralen og kontrollrommet.

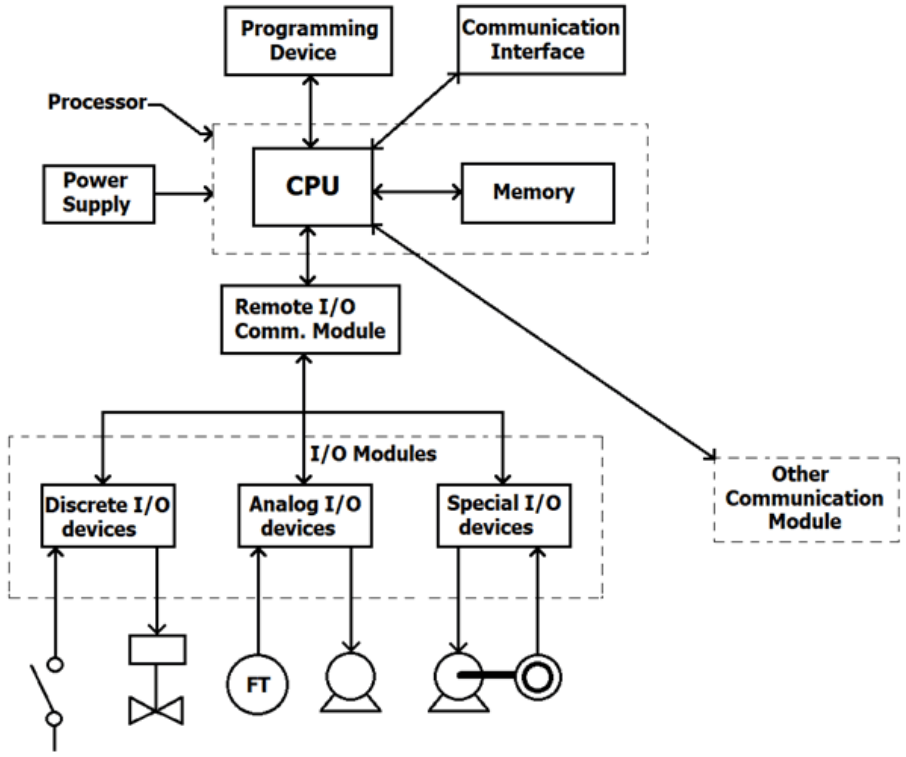
4. Direkte styring
   Systemene på dette kontrollnivået er normalt forsynt slik at de kan kontrolleres direkte og manuelt. Direkte styring brukes kun nå for service/vedlikehold eller i spesielle nødstilfeller og er uavhengig av alle kontrollnivåer (level 1,2 og 3).

5.2 PLS

PLS er en programmerbar datamaskin for automatisering i industrisammenheng. PLS erstattet mekaniske relé med databasert logisk styring og I/O-kort for håndtering av signaler. Dette medførte besparelser i strøm, plass og vedlikehold. En PLS kan programmeres gjennom 5 ulike strukturer og programmeringsspråk, mer detaljert informasjon blir omtalt i kapittel 6.11.1. Alle strukturene danner oversikt over funksjonen i PLS. Typisk bruksområde for en PLS er start og stopp av motor, åpne- og lukkefunksjoner for ventiler og brytere, og innhenting av sensordata.

PLS gjør at det er lettere å programmere og endre nåværende program i industrien i forhold til reléer, som gjør det tidkrevende og vanskelig å få til. Siden PLS har lite vedlikehold, fleksibilitet og gode evner for senere programmering, så er dette grunnen for at PLS er mest brukt i industrien i dag, når det kommer til kommunikasjon med ulike komponenter.

Når det kommer til industrien i dag og hvorfor det ikke blir brukt mikrokontrollere kontra PLS er uten tvil kostnadsforskjellen og robustheten til PLS. [94] PLS overholder industristandarden IEC 61131-3 som fremmer interoperabilitet mellom komponenter. PLS ble designet for å visuelt etterligne forbindelsene og skjemaene til relélogiske diagrammer og programmere med en av de 5 programmeringsspråkene. Mikrokontrollere bruker mer avansert programmeringsspråk som C og C++.



Figur 9: Eksempel av en intern arkitektur på en PLS[94]

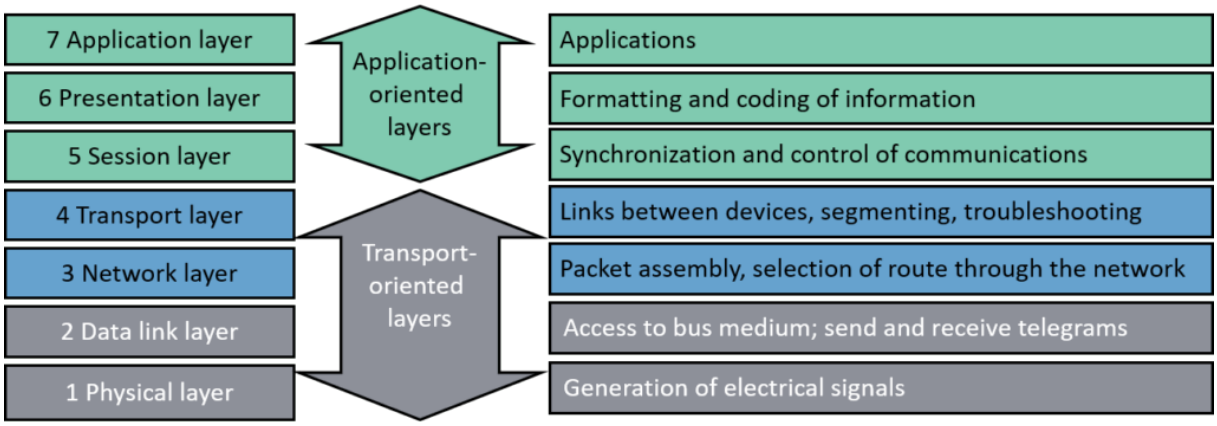
5.3 Kommunikasjon

Profibus og Profinet profilene er standardisert av IEC 61158 og 61784. Det er et industrielt nettverkssystem for sanntid distribuert kontroll, i tillegg er det en måte å koble sammen instrumenter i et produksjonsanlegg. Profibus ble introdusert på markedet i 1986 og Profinet ble introdusert i 2003.

Modbus er en industriell datakommunikasjonsprotokoll og blir brukt til tilkobling av industrielle enheter. Protokollen ble introdusert på markedet i 1979 av Modicon, som nå er Schneider Electric for å få kommunikasjon mellom PLS'er.[61] Modbus er en åpen protokoll, som også er avgiftsfri og regelmessig oppdatert av Modbus organisasjonen. Modbus er ofte brukt innen automasjon og SCADA produkter.

5.3.1 OSI-modell

Open Systems Interconnection eller OSI-modellen er en modell som beskriver de sju lagene i en grunnleggende nettverksarkitektur. Hvert lag i modellen bruker tjenestene som er tilbudt av laget under og karakteriserer og standardiserer kommunikasjonsfunksjonene mellom lagene. [93] Modellen fordeler datastrømmen i kommunikasjonsystemet, alt fra det fysiske laget og helt opp til de syvende laget som er applikasjonslaget. Mellom hvert lag, så er det et klasseskille mellom funksjonalitetene til både laget som er over og det som er under. Ved hjelp av standardiserte kommunikasjonsprotokoller så blir funksjonalitetene realiserbare i programvarene som blir tatt i bruk.



Figur 10: Sju lag av OSI-modellen til kommunikasjonsprotokollen til Profinet[86]

Lag 7 - Applikasjon
Applikasjonslaget bruker programvarer for å etablere forbindelse mellom hver av sidene. Dette går ut på og forberede og tolke data for bruk av de seks andre OSI-lagene som er under ved bruk av protokoller som for eksempel HTTP og E-post. [2]

Lag 6 - Presentasjon
Presentasjonslaget utfører data og protokollforhandlinger med og konvertere å sikre data som kan utveksles mellom hver av sidene og kan transporteres trygt over nettverket. Laget utfører også komprimering og kryptering om nødvendig. Dette blir definert ved bruk av data, programmeringstyper og kodeskjema for forskjellige tegnsett til et annet.

Lag 5 - Sesjon
Sesjonslaget er ansvarlig for å holde dialogen med transport laget, opprettholde kontroll og synkronisering av forbindelsene. [91] Laget er også ansvarlig for å administrere og etablere forbindelse mellom øktene til applikasjonene og nettverket.

Lag 4 - Transport
Transportlaget sørger for å kontrollere for at overføringen av data kommer frem på en ryddig måte. Transportlaget gjør korreksjoner, deteksjoner av feil, gjenoppretting og opprydding av data som er under overføringen mellom de to sidene. Transportlaget er den protokollen som ofte blir kalt for TCP protokollen.

Lag 3 - Nettverk
Nettverkslaget sørger for at datapakkene som blir transportert mellom sender og mottaker i nettverket kommer til rett mottaker i riktig rekkefølge. Dette går ut på og ta i mot forespørsler fra transportlaget og sende forespørsel til datalinklaget. IP er den protokollen som ofte er relatert til nettverkslaget.

Lag 2 - Datalink
Datalinklaget er ansvarlig for overføre og korrigere feilregistrert data. Laget korrigerer feilene i de fysiske laget og skaper forbindelse med de fysiske adressene. Ethernet er den protokollen som ofte relateres til datalinklaget

Lag 1 - Fysisk
Det fysiske laget er det laget som står for det elektriske systemet og den fysiske fremstillingen. Egenskapene til det fysiske laget er å koble sammen de ulike nettverkene og sende binære data gjennom en Ethernet kabel som et eksempel.

5.3.2 HART

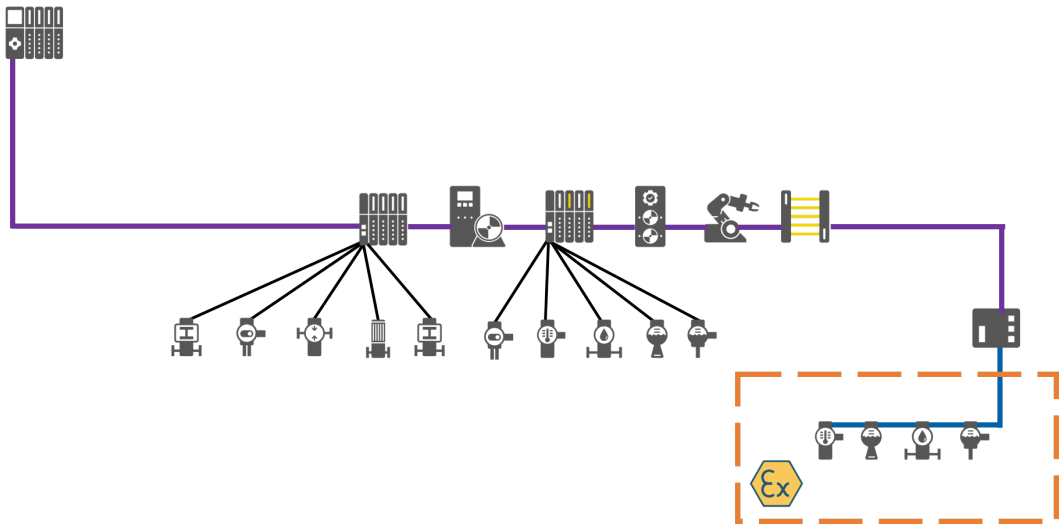
HART-protokollen står for Highway Addressable Remote Transducer Protocol og er en feltbuss-protokoll.[98] HART baseres på standardsignalet 4-20mA og blir brukt av operatører i industrien til å koble seg opp til feltinstrumenter. Ved bruk av en HART-kommunikator så kan man koble seg opp til instrumenter og kommunisere for å stille inn instrumentet manuelt. HART-protokollen forbindes med Profibus og de aller fleste feltinstrumenter med distribuerte kontrollsystemer.

5.3.3 Profibus

Profibus er en feltbuss basert automatiseringsstandard, som er modulært strukturert som en byggestein med kommunikasjonsprotokollen som kjernekomponent [65]. Profibus blir koblet opp via en busskabel som er basert på RS485 som videre blir koblet til kontrollere eller styringssystemer som har desentraliserte feltapparat som f.eks. aktuatorer eller sensorer på feltnivået. Dette gjør det mulig å få konsekvente datautvekslinger med overordnede kommunikasjonssystemer.

Profibus DP
Konsistensen av Profibus gjør det mulig og utnytte en standardisert applikasjonsuavhengig kommunikasjonsprotokoll som blir kalt for Profibus DP. Profibus DP støtter feltbuss løsninger både i fabrikk- og prosessautomatisering, bevegelseskontroller og sikkerhetsrelaterte oppgaver. Ved bruk av denne integrasjonen så er det enklere og planlegge, installere, igangkjøre å holde vedlikehold i systemet. Profibus DP benytter seg av RS485 kabel som både er brukervennlig og kostandseffektiv. RS485 blir brukt til systemer som krever høy overføringshastighet og ikke trenger eksplosjonsbeskyttelse.

Profibus PA
Profibus PA blir brukt til å kommunisere mellom måle- og prosessinstrumenter, som for eksempel PLS, prosesskontrollsystem eller aktuatorer [47]. Den blir også brukt til og overvåke måleutstyr via prosesskontrollsystemet i en PA applikasjon. Profibus PA blir brukt i miljøer innen prosessautomatiserte anlegg som vanligvis krever langsommere prosedyrer og kan da være preget av eksplosjonsfarlige områder, da den er egensikker. Selv om Profibus PA har en annen kappe som blir benyttet, så har den nøyaktig den samme protokollen som Profibus DP. Det er et avvik, da det er midlertidig at strøm og data blir transportert via samme kabel og dette fører til at regler angående nettverkstopologien må følges.



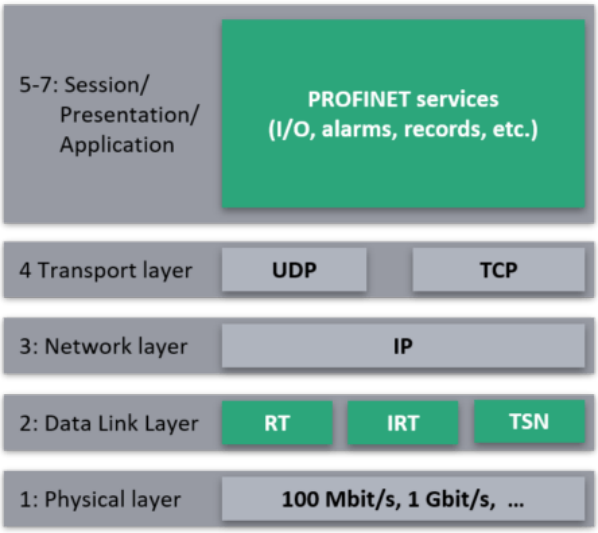
Figur 11: Profibus PA og Profibus DP har den samme protokollen, men Profibus PA har et annet fysisk lag som er brukt innforbi eksplosjonsfarlige områder. [89]

5.3.4 Profinet

Profinet er den mest anerkjente industrielle Ethernet løsningen vi har i industrien i dag og den er basert på internasjonale standarder som IEEE 802 i IEC 61158 og IEC 61784 [97]. Profinet er en åpen Ethernet løsning, som gjør at hundrevis av produsenter har utviklet flere Profinet-produkter som for eksempel PLS-er, I/O, diagnostisk utstyr, og mye mer for å øke kommunikasjonen mellom utstyret som blir tatt i bruk i industrien. [86] Profinet er en kommunikasjonsprotokoll som er designet for å distribuere data mellom kontrollere og enheter i automatiserte systemer i industrien.

Kommunikasjonen til Profinet kan både bli kjørt i syklisk og asyklisk form mellom komponentene og dette inkluderer forskjellige alarmer, diagnostikk, funksjonell sikkerhet og annen nødvendig tilleggsinformasjon som er koblet opp i nettverket. Profinet bruker en standard Ethernet kabel for å koble sammen alle komponentene til et felles nettverk, slik at andre Ethernet protokoller kan eksistere samtidig i samme infrastruktur. Ved siden av Profinet, kan du for eksempel bruke andre Ethernet baserte protokoller som OPC UA, SNMP, MQTT eller HTTP til å utfylle nettverket.

I industrien i dag krever det ofte høye hastigheter og deterministisk kommunikasjon. Siden ikke alle applikasjoner krever samme ytelse så er det avhengig av oppgaven at Profinet må sikre at data blir levert med riktig hastighet og determinisme. Kommunikasjonsprotokollen følger OSI-modellen, som vist under.

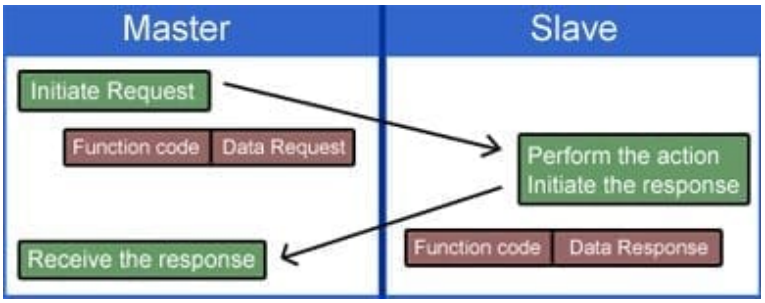


Figur 12: Beskrivelse av arbeidsfunksjonene i de ulike lagene til Profinet i OSI-modellen[86]

Profinet benytter seg av 3 kommunikasjonskanaler for å sikre en passende ytelse, som for eksempel TCP/IP, Profinet RT og Profinet IRT. Profinet har da mulighet for å bruke TCP/IP-kommunikasjon for oppgaver som ikke er tidskritiske, men for tidskritiske oppgaver så benytter Profinet en RT-kanal for å levere på en rask og deterministisk måte. Profinet RT har en syklus tid på mellom 250µs til 512ms og dette oppfyller kravene til de aller fleste tidskritiske applikasjoner som blir brukt, men om det ikke er godt nok så kan du bruke Profinet IRT. Profinet IRT oppfyller alle synkroniseringskrav og tillater deterministisk kommunikasjon ved å bruke variabel data til å eliminere forsinkelser og kjører sykluser helt ned til 31,25µs og opp til 1 av de forventede forsinkelsene og dette er også kjent som jitter.

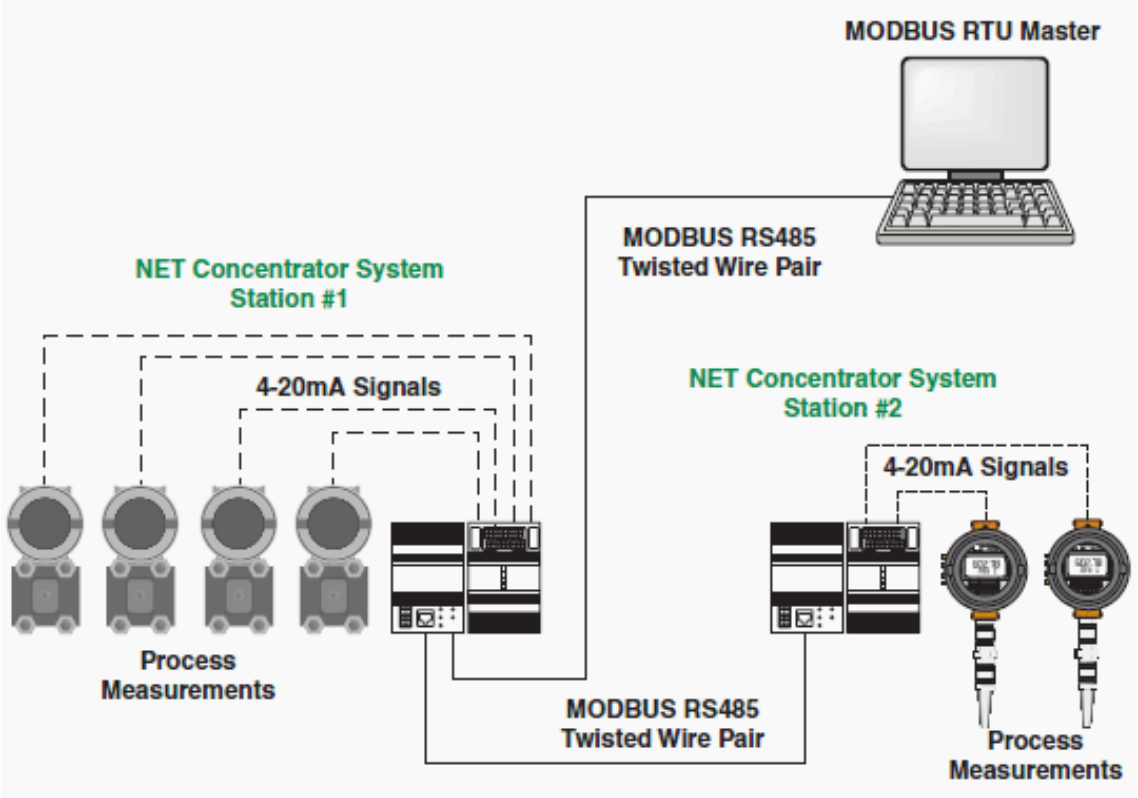
5.3.5 Modbus

Modbus er basert rundt master/slave arkitekturen og gir mulighet for enheter og utstyr til å kommunisere med hverandre. [60] Master/slave er en kommunikasjonsprotokoll, der en master har kontroll over en eller flere slaver. Kommunikasjonen mellom en master/slave går ut på datautveksling som består av forespørsler fra masteren, etterfult av svar fra slaven. Masteren er som regel en PLS, RTU, PC eller en DCS som sender ut data til slavens registre, der slaven registrerer tilsendt data og videreformidler informasjonen med å først gjenkjenne adressen for å så svare innen en tidsperiode, ellers vil masteren få feilmelding [49]. Slaven kan ikke sende fra seg informasjon på egenhand, men må bli bedt om det direkte fra masteren.



Figur 13: Kommunikasjon mellom Master/slave i et nettverk [46]

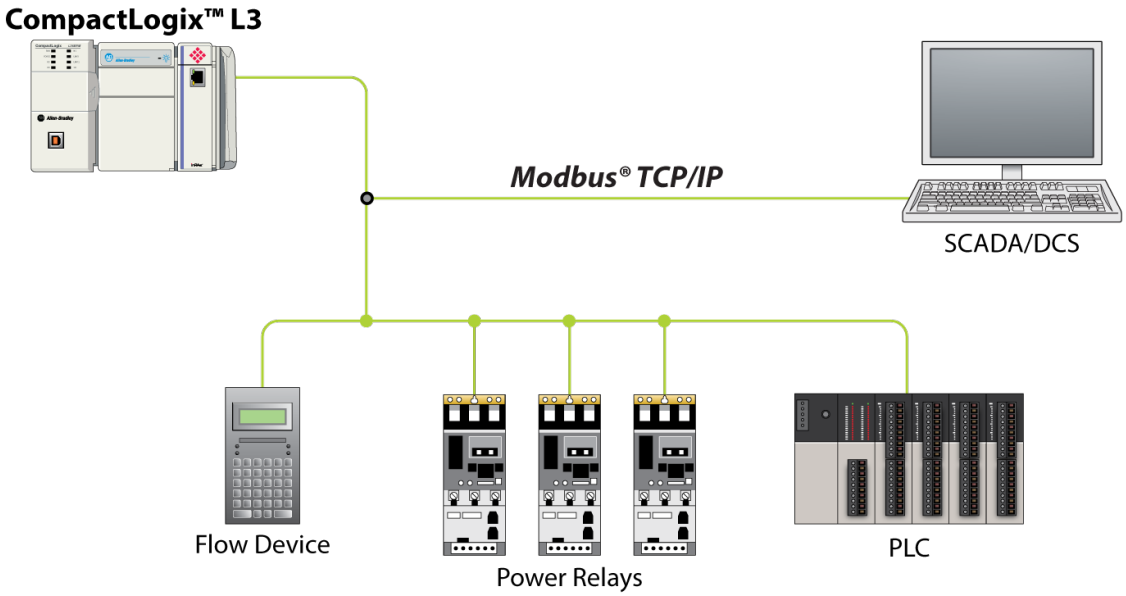
Det finnes flere forskjellige versjoner av Modbus som er av serielle porter og ethernet, men det vanligste er av typen RTU og TCP/IP. Det fysiske grensesnittet som blir mest brukt til RTU er av typen RS485 og ethernet til TCP/IP. I et Modbus RTU nettverk er det alltid en master og en eller flere slaver. Hver enkel slaveenhet har en unik 8-bits adresse eller nummer. Hver datapakke som masteren sender til slaven, enten om det er et forespørsel eller svar, så begynner pakken alltid med adressen til enheten eller slaven, som er etterfulgt av en funksjonskode og til slutt parameterne som definerer hva arbeidsoppgaven inneholder. RTU har en standard node adresse som er fra 1-255, der 0 er reservert for multicast meldinger [46]. Kommunikasjonen som RTU bruker er på applikasjons nivået på OSI-modellen og er ment for å være en forespørsel- og svarprotokoll som leverer spesifikt på funksjonskoder.



Figur 14: Modbus RTU som består av en PLC/DCS, som er en master og har x-antall slave enheter som er koblet sammen i et multi-drop nettverk [49]

Data blir lest og skrevet som et 16-bits register. Registeret består enten av et signert eller usignert 16-bits heltall. Om det krever 32-bits heltall eller et flytende punkt, så blir disse verdiene lest som et par registre istedenfor. Det fins fire forskjellige registre som heter, holderegister, inngangsregister, spoler og diskrete innganger. Holderegister og spoler er både lesbare og skrivbare, mens diskrete innganger og inngangsregisteret er lesbare. Spolen og de diskrete inngangene er basert på av og på funksjoner, der 1-bit er på og 0-bit er av. Inngangsregisteret har essensielle målinger og statuser, mens holderegisteret som er det mest brukte har de vesentlige konfigurasjonsverdiene i systemet.

Forskjellen på Modbus RTU og Modbus TCP/IP er at TCP/IP bruker en Ethernet kabel og RTU bruker en seriell port av typen RS485. Når Modbus TCP/IP ble introdusert ble det enklere å sende data forespørsler og få svar tilbake. Datapakken inkluderer fortsatt enhetsnummeret, men krever en IP-adresse og data overføres over et standard Ethernet nettverk. Modbus TCP/IP følger OSI-modellen i tillegg til at TCP/IP definerer presentasjon- og applikasjonslaget i OSI-modellen. Siden Modbus TCP/IP bruker Ethernet, så tillater dette punkt til punkt kommunikasjon og definisjonen til master/slave er mindre åpenbart. I et Ethernet nettverk har vi både klienter og servere, der master er klienten og slaven er serveren. Det kan være en eller flere klienter som kan få data fra en server. Dette betyr at man kan ha flere mastere, i tillegg til flere slaver og at det er systemdesignerens ansvar for å skape logiske assosiasjoner mellom master- og slavefunksjonalitetene i nettverket.



Figur 15: Eksempel struktur av et Modbus TCP/IP-nettverk [53]

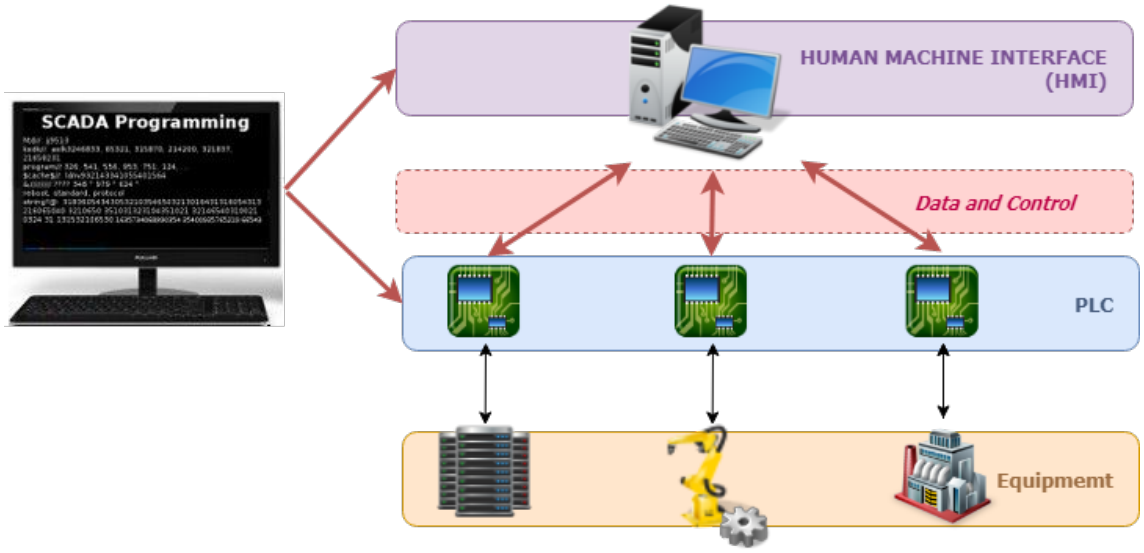
5.4 Skjermstyring

For å drifte et vannkraftverk er det viktig å samle nødvendige data og danne et oversiktsbilde for driftspersonell. Brukergrensesnittet er derfor en viktig del av kontrollanlegget. Som tidligere nevnt kan et kraftverk styres fra ulike kontrollnivåer i kontrollsystemet; direktekontroll, lokalkontroll, stasjonskontroll og fjernstyring. Disse styringene har ulike funksjoner og er satt opp i ulike brukergrensesnitt kalt OP-panel, HMI og SCADA.

5.4.1 SCADA

SCADA er et automatiersingssystem som er basert på programvare- og maskinvareelementer som gjør det mulig for organisasjoner innen industrien til å kontrollere prosesser både lokalt eller via driftssentraler [25]. SCADA-systemet opererer med signaler som kan kommunisere via de forskjellige kanalene som er tilgjengelig for å gi operatøren kontroll over funksjonene i et gitt system. Systemet kan også implementere en distribuert database eller en database av tag nummer som inneholder forskjellige koder i anlegget [45].

SCADA-systemet representerer er en enkel inngangs- eller utgangsverdi som blir overvåket og/eller styrt i kontrollrommet. Kodene som kommer opp blir loggført i databasen som har verdi-tidsstempelpar og kan benyttes kontinuerlig eller analysert på et senere tidspunkt. SCADA er mye brukt i industrien siden den har evnen til å samle, overvåke og behandle sanntidsdata for enheter som sensorer, ventiler, pumper og mer, for å så visualisere data gjennom en HMI. Systemet bidrar med å opprettholde effektivitet, behandle data for smarte beslutninger og kommunisere systemproblemer for å redusere nedetiden til prosessen.



Figur 16: Eksempel diagram av hovedkomponentene til et SCADA system.[87]

Det som er bak den grunnleggende SCADA-arkitekturen finst det fem viktige komponerende deler. RTU og PLS er små datamaskiner som kommuniserer med flere objekter i en prosess, ta for eksempel sensorer og pådragsorganer. Når PLS eller RTU har kommunisert med en sensor, så dirigerer den informasjonen fra disse objektene til datamaskiner med SCADA-programvare. RTU blir koblet opp mot sensorer og konverterer signaler til digital data og sender den til overvåkningssystemet der den blir lagret i en database. PLS blir brukt som felt innrettere fordi de er mer fleksible og økonomiske enn prosesspesifikk RTU. Fra hver tag HMI behandler så sender den informasjonen videre til en menneskelig operatør. Der operatøren kan kontrollere eller overvåke systemet.

Tilsynssystemet samler data som blir videresendes fra hver individuell kode og videre kommandoer eller operasjoner til prosessen. Til slutt så har vi kommunkasjonsinfrastrukturen som leverer tilkobling til overvåkningssystemet og videre til RTU og PLS for operatøren til å kommandere. For at SCADA-systemet skal fungere bra, så må kommunikasjonen mellom HMI, RTU og PLS være skikkelig. Det er fundamentalt at kommunikasjonen mellom det forskjellige komponentene kommuniserer med hverandre. Om det er noe galt som har skjedd, så varsler SCADA-systemet raskt en operatør om at det er noe galt. Operatøren har mulig til og gå gjennom dataen via en HMI for å finne årsaken til problemet og stoppe det om ønskelig. SCADA-systemets evne er å varsle operatørene om at det er et problem i prosessen og hjelpe operatøren med å løse det og forhindre ytterlige tap av produkt som produseres.

5.4.2 HMI

HMI er et brukergrensesnitt for samling og visualisering av data. I vannkraftverk er stasjonsdatamaskinen en HMI. Den befinner seg i kontrollrommet lokalt på vannkraftverket. Ved stasjonsdatamaskinen styrer man kraftverket som helhet, leser av informasjon, varslinger og trendkurver for prosessene.

5.4.3 OP-panel

Et operatorpanel, kalt OP-panel, er et lokalt brukergrensesnitt knyttet til og posisjonert ved mindre funksjonsenheter i vannkraftverket. Panelet er en liten HMI som ofte har enkle funksjoner, som for eksempel måleravlesning og enkel start eller stopp,. Ved et OP-panel har man begrenset eller ingen tilgang til endring av innstillinger knyttet til prosessen. Dette er det laveste kontrollnivået, hvor man har liten påvirkning på kontrollanlegget som helhet. Lokal PLS i funksjonsdelen samler I/O som sendes ut til et OP-panel for å strukturere dataene.

5.5 Sekvenser

Kontrollanlegget har en rekke kritiske overvåkninger å holde styr på under drift av vannkraftverket. For å enklere håndtere styringen og detektere feilsituasjoner lages en oversiktlig forståelse av prosessene som deles inn i sekvenser for start og stopp av produksjonen. Sekvensene består av flere steg, med kriterier for sekvensen, før neste sekvens kan aktiveres. Ved feil i sekvensene skal kontrollanlegget håndtere feilen, og om nødvendig stanse produksjonsenheten. Hvert enkeltsteg i sekvensen, og sekvensen som helhet overvåkes og har en tidsgrense for når det normalt skal være utført. Tidsoverskridelse av et enkeltsteg gir varsel. Derimot vil overskridelse av en sekvens resultere i stopp av anlegget. Type stopp avhenger av driftssituasjonen hvor feilen forekommer. Dette er beskrevet under gjeldende sekvens.

Før hver enkelt sekvens gjennomgås defineres kriteriene for stillstand. Vannkraftverket oppnår stillstand når følgende krav er oppfylt:

- Innløpsluke i lukket posisjon
- Hurtigstopp-luke i lukket posisjon
- Generatorbryter og/eller transformatorbryter i åpen posisjon
- Feltbryter i åpen posisjon
- Rotorhastighet lik 0 rpm

5.5.1 Start - Tomgang (umagnetisert)

Sekvensen 'Start - Tomgang (umagnetisert)' åpner vannveien for å oppnå ønsket hastighet på generatoren. Kriteriene for ferdigstilt sekvens er:

- Generatorspenning lik 0V
- Generatorbryter og/eller transformatorbryter i åpen posisjon
- Feltbryter i åpen prosisjon
- Rotorhastighet $>$ 90% av synkront turtall

Dette vil si at generatoren har oppnådd ønsket hastighet, er umagnetisert og ikke faset inn på nettet, altså kjøres i tomgang. Produksjonsenheten forblir i denne tilstanden til annen kommando er aktivert. Tomgangskjøring benyttes ikke under normal drift. Det kan være godt for testkjøring, feilsøking og revisjonsjobber.

5.5.2 Start - Tomgang (magnetisert)

Sekvensen 'Start - Tomgang (magnetisert)' kan aktiveres fra 'Stillstand' eller 'Start - Tomgang (umagnetisert)'. Feltbryteren lukker posisjon og magnetiserer, også kalt mater, rotor på generatoren med DC-spenning. Kriteriene for ferdigstilt sekvens er:

- Rotorhastighet $>$ 90% av synkront turtall
- Generatorspenningen er normal
- Innløpsluke er 100% åpen
- Generatorbryter eller transformatorbryter i åpen posisjon

Dette vil si at generatoren har oppnådd ønsket hastighet, er magnetisert og ikke faset inn på nettet. Produksjonsenheten forblir i denne tilstanden til annen kommando er aktivert. Tomgangskjøring benyttes ikke under normal drift. Det kan være godt for testkjøring, feilsøking og revisjonsjobber.

5.5.3 Start - Operasjon

Sekvensen 'Start - Operasjon' kan aktiveres fra 'Stillstand', 'Start - Tomgang (umagnetisert)' eller 'Start - Tomgang (magnetisert)'. Generatorbryter og transformatorbryter lukker posisjon og faser produksjonsenheten inn på nettet. Kriteriene for ferdigstilt sekvens er:

- Generatorbryter og transformatorbryter i lukket posisjon

Dette vil si at generatoren har oppnådd ønsket hastighet, er magnetisert og faset inn på nettet. Produksjonsenheten forblir i denne tilstanden til annen kommando er aktivert. I en normal driftsituasjon benyttes denne typen direkte start.

5.5.4 Frakobling

Sekvensen 'Frakobling' aktiveres ved midlertidig elektrisk eller mekanisk feil. Ved elektrisk feil kobler respektiv effektbryter generatoren ut fra nettet. Ved manuell aktivering åpner generatorbryter posisjon og faser produksjonsenheten ut fra nettet før feltbryter går til åpen posisjon, for å unngå rusing. Kriteriene for ferdigstilt sekvens er derfor 'Start - Tomgang (umagnetisert)':

- Generatorspenning lik 0V
- Generatorbryter og/eller transformatorbryter i åpen posisjon
- Feltbryter i åpen prosisjon
- Rotorhastighet $>$ 90% av synkront turtall

Produksjonsenheten forblir i denne tilstanden til annen kommando er aktivert.

5.5.5 QSD-E

Sekvensen QSD-E er en beskyttelsessekvens som aktiveres ved elektriske feil knyttet til generatorenheten eller ved aktivering av ESD. QSD-E åpner relevant effektbryter og feltbryter momentant. Samtidig aktiveres stenging av hurtigstopp-luke, inntaksluke og turbinregulator. På grunn av tidsavhengig stenging av stoppluken, vil generatoren oppleve rusing. QSD-E trigger en startblokk som gjør at generatorenheten må deblokkeres lokalt etter utbedring av elektrisk feil.

5.5.6 QSD-M

Sekvensen QSD-M aktiveres ved intern eller kritisk mekanisk feil i generatorenheten. QSD-M aktiveres kun lokalt gjennom trykknapp. QSD-M stenger hurtig-stoppluken, inntaksluken og turbinregulatoren. Farten på generatoren senkes før effektbryter faser ut fra nettet og til slutt kobles feltbryteren ut. Startblokk hindrer start før utbedring.

5.5.7 Normal stopp

Sekvensen 'Normal stopp' justerer ned produksjon av aktiv og reaktiv effekt, gjennom å henholdsvis justere vannmengde og magnetiseringsstrøm. Når justeringstiden er fullført, aktiveres QSD-M, med unntak av startblokkering.
Under stopp overvåkes tid for følgende funksjoner:

- Lukking av hurtigstopp-luke
- Lukking av ledeskovler
- Lukking av inntaksluke
- Utkobling av relevant effektbryter
- Utkobling av feltbryter
- Bremsetid for mekanisk brems

Tidsoverskridelse av én av disse stoppstegene medfører aktivering av ESD-systemet.

5.5.8 ESD

ESD-systemet er et redundant beskyttelsessystem som brukes for å stanse kritiske deler i produksjonsenheten ved uønskede hendelser [29]. Det fungerer som en reserve for hovedsystemet i det lokale kontrollanlegget og baseres på konvensjonell relestyring. ESD aktiveres i tilfeller ved feil i det databaserte kontrollsystemet, ved manuell aktivering eller ved kritiske forsinkelser under gjennomføring av en sekvens.

ESD-systemet har utløserspoler knyttet til effektbryter transformator, effektbryter generator og feltbryter for magnetisering. I tillegg utløses stenging av inntaksluke og stoppluke, og om nødvendig aktiveres mekanisk brems. Brannsikre kabler sikrer nedstenging ved brann i kraftverket. ESD-systemet har, som hovedsystemet, et identisk parallelt system fra alternativ 220V DC-kilde for å sikre tilførsel.

Under en kritisk feilsituasjon, etter at generatoren er magnetisert, må ESD-systemet benyttes framfor QSD-M for stopp av produksjonsenheten. Dette er på grunn av nødvendigheten for rask utkobling fra nettet. ESD-systemet faser produksjonsenheten ut fra nettet før feltbryteren for magnetisering kobles ut. Selv i en ESD-situasjon kan ikke vannvegen stenges momentant på grunn av kreftene som er involvert, slik at når feltbryteren kobles ut og turbinen forsynes med vann, resulterer dette i rusing av generatoren. Generatorene er dimensjonert for å tåle denne rusingen, men om nødvendig kan mekaniske bremser aktiveres for å motvirke noe av rusingen.

6 STANDARDER

6.1 Hva er en standard

En standard har som hensikt å gi ryddighet, forenkle samspill og gi en viss kvalitet. Vi har standarder for det meste. Alt fra ark i A4 format til avstand mellom stendere i et hus. Ved å anvende standarder innen prosjektering og utforming av et prosessanlegg vil man kunne oppnå besparelser inne tidsforbruk i selve prosjekteringsfasen, men også besparelser når det kommer til administrasjon av lager, vedlikeholdskostnader og drift. Under en anbudsprosess vil en spesifisert og grundig standard føre til et utjevnet spillefelt for de ulike aktørene. Gitt at pris er høyeste prioritet i valg av leverandør i et prosjekt, så vil man ikke kunne vinne anbud ved å anvende deler av lavere kvalitet enn konkurrentene. Grundige spesifikasjoner vil være både tid og kostnadsbesparende for anleggseieren. Vannkraftproduksjon er en sektor som, ifølge intervju med Voith, har lite å hente i form av optimalisering av prosessen. Evolusjon skjer i form av videreutvikling av teknologi som har eksistert siden 1800-tallet. For kontrollanleggets del vil dette si at det er en fin kandidat for standardiseringsarbeid.

6.2 Standardisering av PLS SW

Arbeid med å standardisere kontrollanleggets logiske virkemåte for å gi lik funksjonalitet uavhengig av leverandør vil være vanskelig uten at det grundig spesifiseres i bestillingen. Dette vil være en arbeidsom prosess og ressursbruket vil ikke kunne forsvares i enkeltprosjekter. Det spesifiseres derfor kun hvordan anlegget skal virke og hvilke funksjonaliteter det skal inneholde. Resten er opp til leverandør. I programmerbar logikk er det «mange veier til rom». Dette gjør at programmet man får vil avvike fra anlegg til anlegg og alt etter hvem som har programmert det. Selve «sluttproduktet» vil allikevel være det samme. Resultatet av dette kan være at man har vannkraftverk som styres av ulik logikk, reagerer på forskjellige måter på samme input og genererer alarmer på ulikt vis. Disse impulsene er samlet sentralt til driftssentralen. En bransje som har mange ulike anlegg og som har jobbet mye med standardisering, er norsk olje og gass. De har utviklet en standard kjent som IEC PAS 63131 (tidligere NORSOK I-005) som alle leverandører må forholde seg til.

6.3 NORSOK

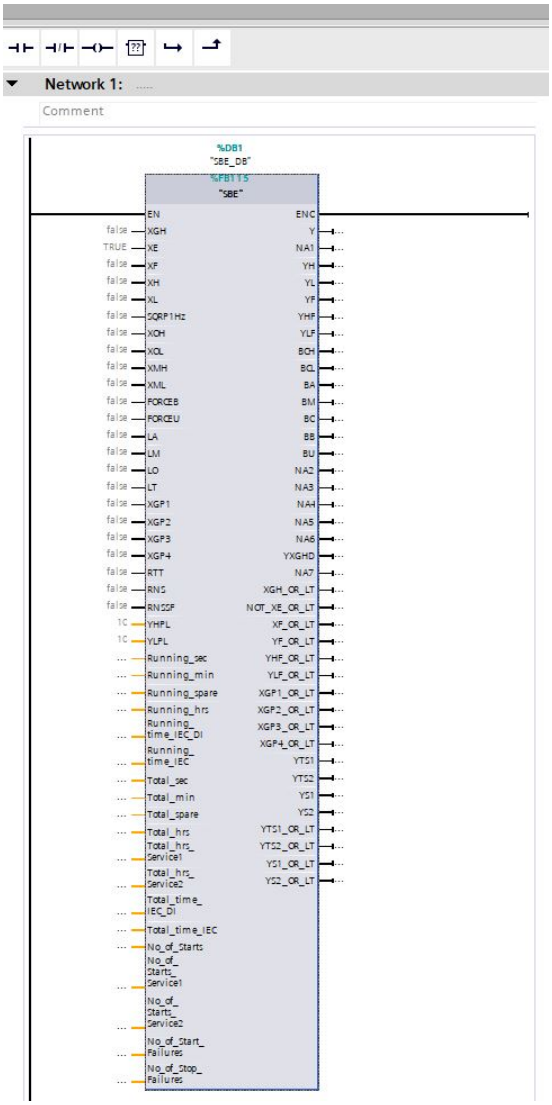
- Administreres av Standard Norge og er utviklet av den norske petroleumsindustrien med hensikt å redusere kost og sette en referanse.
- Er basert på internasjonale standarder, men med tillegg for å møte strenge norske krav.
- Standardene omfatter både funksjonell beskrivelse og normer for teknisk dokumentasjon.
- NORSOK er ment å dekke et anlegg gjennom hele sykelen fra prosjektering til idriftsettelse, drift og rammeverk for modifikasjoner.

Etter tips i intervju med Arild Hodne, ble det undersøkt muligheten for implementasjon av NORSOK standarden i PLS SW. I dag er ikke SW-strukturen for hverken PLS eller HMI spesifisert. Dette fører til at entreprenøren som vinner anbudsrunden har full råderett til å strukturere programmet etter eget skjønn innenfor spesifiserte funksjonsprosedyrer. Statkraft har i dag 346 ulike vannkraftverk, og det kan tenkes at et problem i anlegget hadde vært enklere å feilsøke for serviceingeniørene dersom en hadde hatt en viss kjent struktur. Ikke bare vil dette gi økt selvtillit under arbeid, men også potensielt lavere driftskostnader over tid. Et problem med dagens situasjon er at man er ofte nødt å ha kjennskap til anlegg og programstruktur. Slik lokalkunnskap vil være vanskelig å videreføre i en tid der man har mye utskifting av personell. Perioder med sårbarhet kan da oppstå. Både Siemens og ABB har NORSOK SW tilgjengelig og klar for bruk i sitt respektive programmeringsspråk.

NORSOK standarden introduserer predefinerte funksjonsblokker som skal virke veiledende og anvendes der det er mulig. Fordel med denne standarden er at SW får lik struktur og utseende på tvers av kraftverkene. Ved å anvende predefinerte funksjonsblokker vil logikken ha lik tilgjengelig funksjonalitet, selv om den ikke er i bruk. Dette vil igjen gjøre det lettere å gjennomføre like utvidelser på tvers av anlegg. Endringer i programmet i form av utvidelser og tilleggsfunksjoner vil kreve mye av de samme SW grepene og man beholder den gjenkjennbare strukturen. Det finnes 16 forskjellige FB som alle har en fast logikk og et gitt navn som beskriver blokkens hensikt og funksjonalitet.

For å illustrere bruksområdene og oppbyggingen vises her et utvalg fra det tilgjengelige biblioteket. Inn og utgangenes navn er bygget på et standardisert sett med koder, ikke ulikt tagsystemet som IEC 61850 introduserer for datamapping. Hva som skal påtrykkes og hvordan er beskrevet i dokumentasjonen sammen med klare instrukser om hvordan man tilpasser logikken og forutsetninger for drift og samkjøring med HMI.

SBE - Switching control by means of a binary control action of El. power Devices. En funksjonsblokk som består av 64 nettverk som brukes til å styre alle binære signal til for eksempelvis motorer, pumper og vifter.

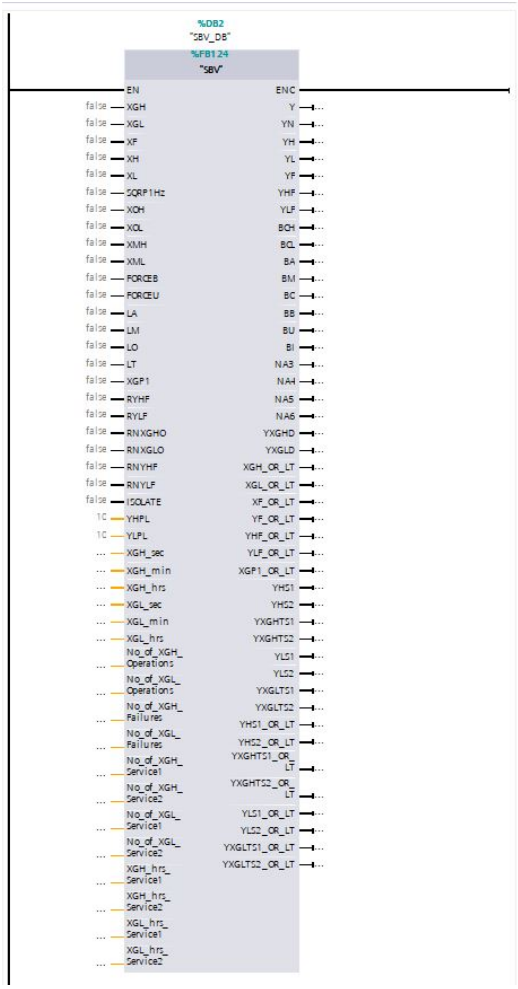


(a) Funksjonsblokkens utseende i Siemens S7 TIA

	SBE		
Inputs			Outputs
Pos. High feedback (MCC)	XGH	Y	Normal function output
External fault	XF	YF	Alarm Function failed
Function externally enabled (MCC)	XE	YH	Pulsed normal function output High
External priority 1 Set High	XP1H	YL	Pulsed normal function output Low
External priority 1 Set Low	XP1L	BCH	Output position High Confirmed
External priority 2 Set High	XP2H	BCL	Output position Low Confirmed
External priority 2 Set Low	XP2L		
External outside set High	XOH		
External outside set Low	XOL		
Operator Station:			Operator Station:
Select Auto mode			Fault annunciation
Select Man. mode			Status ON/OFF
Select outside			Auto / manual / Outside
Select On (high)			Status Blocked
Select off (low)			Status Suppressed
Blocking on			Status Disabled
Blocking off			Status Safeguard
Suppression on			Coincidence state
Suppression off			
Logic:			Logic:
Lock safeguarding Low	LSL	BA	Status Auto/Man mode
Force Safeguarding Low	FSL	BO	Status Outside mode
Force Disable transition High	FDH	BP1	Status Priority 1
Force Disable transition Low	FDL	BP2	Status Priority 2
Force suppression mode	FU	BS	Status Safeguarding mode
Force block mode	FB	BB	Status Blocked mode
Lock Auto mode	LA	BU	Status suppressed mode
Lock Manual mode	LM	BP1F	Priority 1 faulty
Lock Outside operation mode	LO	BP2F	Priority 2 faulty
Set priority 1 – Duty	SP1		
Set priority 2 – Standby	SP2		

(b) Oversiktstegning fra dokumentasjonen

SBV – Switching control by means of a binary control action of H/P power Devices (e.g. Valves). En funksjonsblokk som består av 69 nettverk som brukes til å styre binære signal til et flow elementer. Dette kan til eksempel være ventiler.



(a) Funksjonsblokkens utseende i Siemens S7 TIA

Inputs	SBV		Outputs
Position High feedback	XGH	Y	Normal function output
Position Low feedback	XGL	YF	Alarm Function failed
External fault	XF	BCH	Output Position High Confirmed
External set high	XH	BCL	Output Position Low Confirmed
External set low	XL		
External outside set high	XOH		
External outside set low	XOL		
Operator Station:			Operator Station:
Select Auto mode			Fault annunciation
Select Man. mode			Status Open/Closed
Select outside			Auto / manual / Outside
Select Open (high)			Status Blocked
Select Closed (low)			Status Suppressed
Blocking on			Status Disabled
Blocking off			Status Safeguard
Suppression on			Coincidence state
Suppression off			
Logic:			Logic:
Lock Safeguarding H	LSH	BA	Status Auto/Man mode
Lock safeguarding L	LSL	BO	Status Outside mode
Force Safeguarding H	FSH	BS	Status Safeguarding mode
Force Safeguarding L	FSL	BB	Status Blocked mode
Force Disable transition H	FDH	BU	Status suppressed mode
Force Disable transition L	FDL		
Force suppress mode	FU		
Force block mode	FB		
Lock Auto mode	LA		
Lock Manual mode	LM		
Lock Outside operation mode	LO		

(b) Oversiktstegning fra dokumentasjonen

Disse og tilsvarende FBer dekket i 2007 73% av logikken på Oseberg feltsenter [6] og 99% på Johan Sverdrup. [26] En forskjell her er at det da Oseberg ble prosjektert kun fantes 8 forskjellige FB'er. Nå som man har 16 stk. ser man helt klart utviklingen, og hvor flittig de blir implementert.

Programmeringen skal kun anvende «positiv logikk». Dette vil igjen si at for digital I/O, så har man høyt signal «1» som eksempelvis tilsier disse tilstandene:

- True på «ALL» terminalen til MA FB -> verdi er lavere enn bestemt grenseverdi
- True fra utgang «Y» på SBV FB -> Høy utgang
- True på terminal «LSL» på SBE FB -> Utgangen, Y, låses til «0»

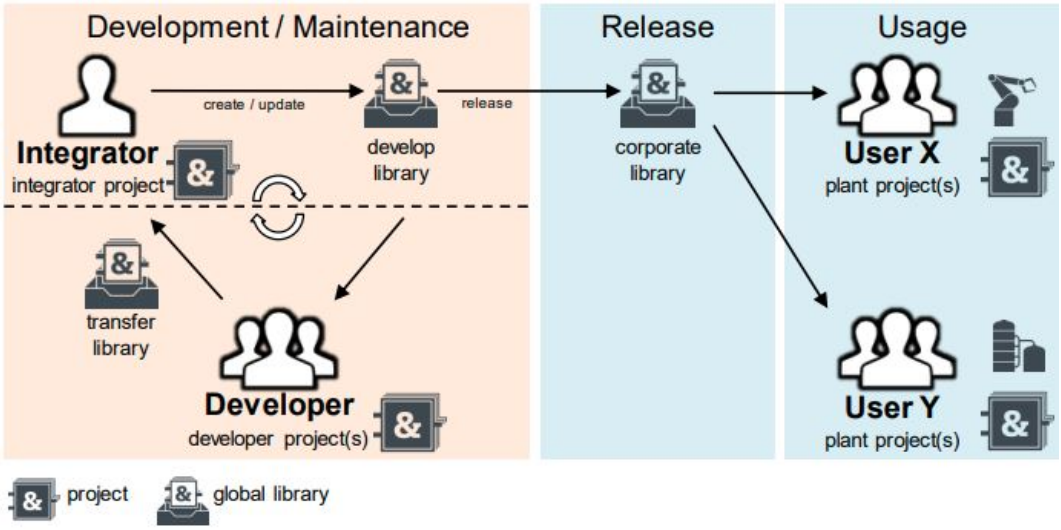
NORSOK standarden er utviklet spesielt mot petroleumsindustrien og det kan derfor tenkes at ikke alle templates vil passe seg like godt inn i vannkraftbransjen. Tankesettet med et standardisert bibliotek der man har spesifisert virkemåte og attributter på FBene som igjen kan samsvare med Statkrafts tagsystem, kan man derimot ta lærdom av. Bruk av standardiserte FBer vil også føre til at HMIer fra ulike kraftverk vil ha like funksjonaliteter. Alarmer vil genereres likt fra et kraftverk til et annet siden logikken bak er noenlunde lik. Dette kan bidra til å forenkle feilsøkingsarbeid.

6.4 UDT - User Defined Types

Tanken om en mer standardisert SW struktur, som i NORSOK, ledet studien til å undersøke hvordan dette kan opprettes og administreres på enklest mulig vis. Her vil anvendelse av UDTer bli vist og forklart med Siemens sin SW som utgangspunkt. Andre leverandører tilbyr også samme funksjonalitet for bibliotekbygging. De kan allikevel ha annen måte å oppnå samme funksjonalitet enn det som beskrives her.

Logikk som skal dupliseres og inneha lik funksjonalitet på tvers av prosjekter kan utvikles som en spesifisert «user defined data type». UDTer kan lagres i bibliotek og vil, i likhet med de 16 FB'ene som styrer oljeplattformene på norsk sokkel, gi gjenkjennbar struktur og raskere prosjektering med simplifisert oppbygging av logikken. I motsetning til Statkraft som tillater mye rom for egen tolkning, så er inntrykket som er dannet etter intervju med flere andre kraftselskaper at dette ikke er normen. Siden vannkraftverk har styresystem som i stor grad kan sies å være repeterbar, vil denne løsningen være meget anvendelig og det er utviklet system for utvikling og enkel distribusjon av dette til de aktuelle ingeniørselskapene som drifter kraftverkene.

6.4.1 Corporate Library

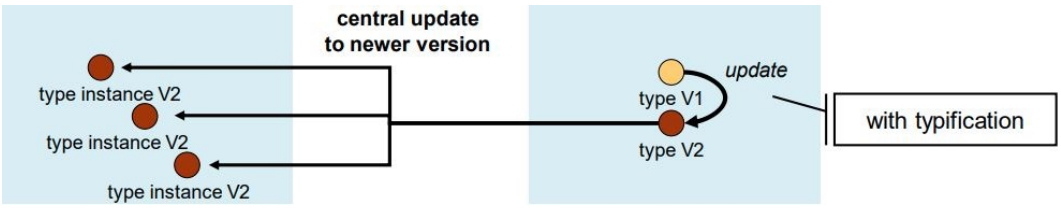


Figur 19: Tiltenkt arbeidsstruktur

Statkraft kan anvende UDT funksjonaliteten til å bygge seg et såkalt «Corporate Library». Arbeidsmetodikken bak dette baseres på at Statkraft som anleggseier setter opp en komite som beslutter hvordan de ønsker at deler av anlegget skal fungere. Disse får da rollen som «Integrator». Det er de som vet hvordan de ønsker anlegget skal fungere samtidig er det de som analyserer hendelser som forekommer og danner grunnlag for endringer i kraftverkenes virkemåte. Ønsket funksjonell virkemåte for en funksjonsblokk beskrives og sendes til den som har rollen som «Developer». En «Developer» sin rolle er å lage ny logikk i henhold til hva som er besluttet av Statkrafts overordnede ekspertkomite. En hendelse i ett kraftverk kan analyseres og brukes som forebyggende erfaring i de andre. Dersom man opplever noe som Statkraft føler PLS logikken burde reagert annerledes på eller man føler noe i prosessen burde generert en alarm kan man, etter å ha ha kommet frem til en bedre funksjonalitet, implementere denne ved at «Developer» oppdater funksjonene og laster revidert versjon opp til biblioteket.

Selve biblioteket vil være lagret på en server som en gruppe brukere har tilgang til og kan laste ned siste versjon fra. Her ser man en stor fordel i bruk av denne løsningen. Statkrafts endringer kan deretter enkelt implementeres i kraftverk fra Hylen vannkraftverk i Rogaland til Adamselv i Troms og Finnmark fylke av selskapene som har ansvar for anlegget. Tilleggsfunksjoner i logikken vil ikke alltid være aktuelle for alle anlegg og man kan naturligvis velge om man vil ta de i bruk.

Når det kommer til jobben med å oppdatere PLS programvaren, så er dette også forenklet i forhold til tradisjonell løsning. UDT'en som anvendes er en «instans FB» av UDT'en i biblioteket. Dette betyr at de er linket til den versjonen som ligger i prosjektbiblioteket. Når man oppdaterer denne, vil alle instansene av samme FB bli oppdatert. Man gjør endringen ett sted. De stedene der UDT'en brukes i programmet vil oppdateres ved kompilering etter at det lokale biblioteket er oppdatert med ny versjon.



Figur 20: Oppdatering av revidert UDT

Det man nå oppnår, er at man i tillegg til standardisert tagsystem, også har en standard for hvor taggene skal implementeres i PLS programmet og hvordan data behandles. Endringer man vil gjøre basert på erfaringer under drift implementeres lettere og kan også lett overføres til alle vannkraftverk under Statkrafts paraply. Samtidig vil programmet oppnå en mer gjenkjennbar struktur som tillater servicepersonell å jobbe på tvers av anlegg og uavhengig av hvem som har programmert anlegget. Anvendelse av en slik struktur baner igjen vei for standardisert struktur på HMI.

6.5 IEC 61850

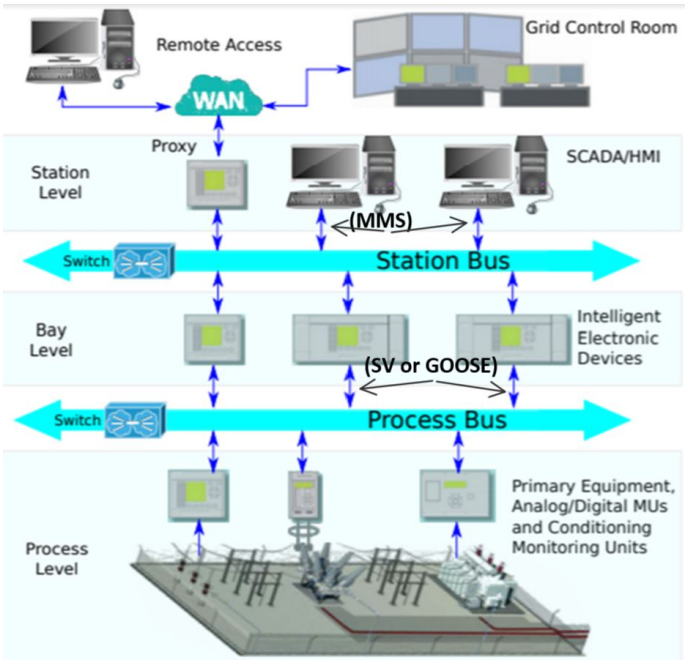
IEC 61850 er en internasjonal standard for kommunikasjonsnett og systemer for automatisering i energiforsyningen [20]. Formålet er et standardisert kommunikasjonssystem som baseres på optisk fiber og Ethernet, for rask interaksjon, som er operasjonelt på tvers av leverandører, og som enkelt kan implementeres med andre standarder. Dette skal resultere i effektivt drift og økonomisk bærekraftig for utvidelser eller rehabilitering. IEC 61850 er organisert som en åpen standard som muliggjør integrering av beskyttelse, styring, måling og monitorering av energisystemer [11].

6.5.1 Avgrensning

Bekrivelse og bruk av standarden er begrenset til det som oppleves relevant for kontrollanlegg ved vannkraftverk. Herunder kan seksjoner som IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410 og IEC 61850-7-510 nevnes som spesielt sentrale. IEC 61850-7-3 omhandler kommunikasjon og dataklasser, IEC 61850-7-4 omhandler kommunikasjon, logiske noder og dataobjekter, IEC 61850-7-410 omhandler kommunikasjon for styring og monitorering ved vannkraftverk, og IEC 61850-7-510 omhandler retningslinjer og stuktur for vannkraftverk.

6.5.2 Topologi

Topologien beskriver et forenkelt system for en overordnet forståelse av funksjonaliteten bak IEC 61850. Derfor vil ikke topologien det er henvist til være praktisk tilnærmet med tanke på redundans eller koblingspunkt. Topologien er ment til å være illustrativt behjelpelig for forståelse av strukturen i et kontrollanlegg med IEC 61850. Topologien deles inn i Stasjonsnivå, Kontrollnivå og Prosessnivå, som vist i Figur 21.



Figur 21: Forenklet topologi for IEC 61850 implementert ved koblingsanlegg [36]

Stasjonsnivå
På stasjonsnivå finner man stasjonsdatamaskin, HMI og SCADA for lokalkontroll, i tillegg til brannmur som videre tillater ekstern tilkobling fra driftssentral og fjernoppkobling via gateway. Ekstern tilkobling og styring kan kommunisere over IEC 61850, men protokoller som benyttes idag, slik som IEC 104, kan om ønskelig mappes for kompatibilitet for et lokalt IEC 61850 system. I dette tilfellet er gateway erstattet med en RTU. Siden nettstasjonene allerede har gått over til IEC 61850, vil det være fordelaktig om forsyningssystemet som helhet benyttet samme standard med tanke på overstyringer knyttet til feil i forsyningsnettet. Dette diskuteres nærmere i kapittel 8.1.3.

Kontrollnivå
På kontrollnivå ligger IEDs, som kontrollanlegget i IEC 61850 baserer seg på. IED er en fellesbetegnelse for intelligente komponenter med funksjoner som måling, beskyttelse og styring. Alle IED's vil kunne kommunisere med hverandre basert på IEC 61850 standarden, slik at interoperabilitet mellom ulike leverandører vil være mulig. IEC 61850 åpner for en desentralisert inndeling, hvor IEDs plasseres i henhold til anleggsdelen den er tilkoblet for å spare kabling.

Prosessnivå
På prosessnivå ligger konvensjonelle måleinstrumenter tilkoblet MUs for omforming av måleverdier for IEC 61850 kommunikasjon. Disse kan deretter transporteres over optisk fiber eller Ethernet til Bay Level. MU-overgangen utgjør en mindre tidsforsinkelse på 2ms[79], og har derfor blitt modernisert til PMU. PMU er en microprosessor-basert intelligent enhet for målinger som kan kobles direkte mot Ethernet, og benyttes i IEC 61850. Denne vil derfor være ønskelig med tanke på rask overføring av tidskritisk informasjon.

Prosess- og stasjonsbuss
Nivåene i topologien er normalt sammenkoblet med Ethernet eller fiberoptisk kabel på det som kalles stasjons- og prosessbuss. IEC 61850 introduserer prosessbuss hvor en lokal svitsj styrer datatrafikk mellom MUs og IEDs. Sammenlignet med konvensjonelle kontrollanlegg er formålet med denne mellomkoblingen å redusere kabling ut til måleinstrumenter. Stasjonsbussen er der dataoverføringer mellom IEDs, stasjonsdata, HMI og gateway foregår. Svitsjer på bussene sammenkobler Ethernetkablene og styrer dataoverføringene. Dagens teknologi innen Ethernet er langt fremme, og fiber for prosess- og stasjonsbuss kan være 100Mbit/s eller 1 Gbit/s for å håndtere kapasiteten av dataflyt. Måten nettverket er sammenkoblet avhenger av ønske om redundans og hastighet i nettverket.

Redundans
Det er ønskelig med en enkel og redundant topologi for oversikt og pålitelighet i systemet. Der har IEC 61850 en fordel med bruk av Ethernet-svitsjer. På grunn av toveis kommunikasjon er ofte stasjonsbussen lagt i et ringnett. Dette sørger for at brudd i kabelen ikke hindrer kommunikasjon. Kablene kan også dubleres ut til komponentene og benytte dublerte svitsjer. En slik uavhengig dublering sørger for redundans ved feil i kabeltilkoblingen. Figur 40 viser forslag til redundant løsning.

I henhold til den generelle spesifikasjonen i Statkraft skal brudd i tilførselen aldri føre til tapte signaler [41]. Fra MODBUS RTU, som er mye brukt i kontrollanlegg, vet vi at kommunikasjonssvikt medfører tapte sekvenser. Serveren i IEC 61850 lagrer rapporter i bufferminnet slik at ved kortsiktige brudd i kommunikasjonen, vil klienten automatisk etterspørre sist mottatte fil når tilkoblingen er gjenopprettet. Klienten vil deretter motta filer lagret i bufferens køsystem, slik at ingen dataoverføringer går tapt [17]. Ved langvarige brudd vil nye rapporter overskrive de gamle slik at filene som overføres ved tilkobling vil inneholde siste registrerte hendelser. I dette tilfellet vil rapporten flagges som overskrivende, og man vet at data er tapt.

Kritiske komponenter kan dubleres for sikker drift ved komponentsvikt. I tillegg kan komponenter med lik funksjon være redundant for hverandre, og dele status om hverandres I/O i tilfeller med kommunikasjonssvikt mellom MU og IED.

6.5.3 Systemkonfigurasjon - SCL

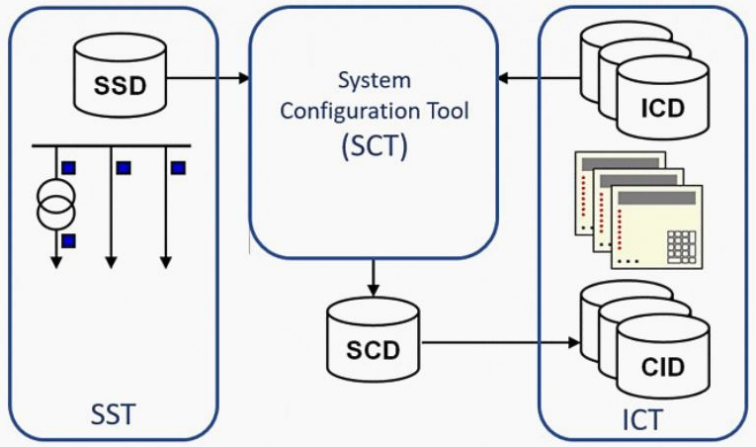
Interoperabilitet gjennom XML
IEC 61850 er et system for datakommunikasjon som baseres på IP-protokoll og benytter Ethernet eller optisk fiber for dataoverføring. Den standardiserte taggingen av signal gir mulighet for at ulike leverandører kan benytte samme kommunikasjonsspråk, og brukes om hverandre i anlegget. En IED kan motta data med en bestemt tag i et XML-format, oversette den til leverandøren sitt eget språk for intern prosessering, utøve nødvendige funksjoner for styring eller kommunikasjon, oversette fra leverandørspråket til IEC 61850, og sende dataene.

SSD
SSD gir beskrivelse av systemspesifikasjonen. Filen beskriver enlinjeskjemaet, spenninger, og nødvendige logiske noder for funksjonaliteten ved kraftverket og/eller koblinganlegget. Filen konfigureres i en System Spesification Tool (SST) ut ifra enlinjeskjema og funksjonsdiagrammer [48].

ICD
ICD gir beskrivelse av mulighetene i en IED. ICD lages av leverandøren i en IED Configuation Tool (ICT) og innholder logiske noder, data og kompatibilitet for andre systemer[48].

SCD
SCD gir beskrivelse av systemkonfigurasjonen. Her samles alle ICD filer fra konfigurerte IEDs og beskrivelse av kommunikasjonsprotokollene mellom dem. Filen konfigureres i System Configuration Tool (SCT) [48].

CID
CID inneholder IED konfigurasjon for hver IED individuelt og er et utdrag fra SCD-filen. Her kan parametre og innstillinger for hver enkelt IED konfigureres.



Figur 22: Konfigurering av filer [48]

Simuleringsverktøy for SW og HW
Det finnes en rekke SW for simulering og testing av konfigurasjonen, logikk, kommunikasjonsprotokoller og monitorering før HW i kontrollanlegget er montert. SW som 61850DOCTOR VIRTUAL IED kan simulere avanserte IED servere, endre innstillinger, kjøre fiktive sekvenser, GOOSE-protokoll, trip av effektbrytere og måleavlesninger. Funksjoner i IEDs med blokkfunksjoner fra IEC 61131 implementert kan testes. VIRTUAL IED gir en avansert simulering med visuell monitorering av datastrøm og reaksjoner på hendelser. F.eks. kan en IED for beskyttelse testes i en simulert feilsituasjon. Man kan oppnå tilsvarende testing i programmet Digital Twin, som benyttes av Siemens Energy for testing av SW.

Ved idriftsettelse av et nytt anlegg kan produkter fra Omicron Energy være til hjelp for testing etter at HW er montert. De tilbyr en rekke produkter med tilkobling til I/O og IEDs. Påførte strømmer kan simulere en normal driftssituasjon, og feilstrøm på input kan teste styre -og beskyttelsesfunksjoner.

6.5.4 Tagging av signal

Prefix
Siden IEC 61850 originalt ble utviklet for koblingsstasjoner med simple prosesser, benyttes prefiks kun som komponentnavn i IEC 61850. Det vil i kapittel 6.8 presenteres et tilleggssystem for organisering av tags for vannkraftverk, hvor blant annet navn på kraftverk og anleggsdel er henvist i taggingen. Med kun enkel prefiks fra IEC 61850 kan man ut ifra topologien bruke komponenten det er snakk om, for eksempel en IED, kalt IED1, som kan være et beskyttelsesrelé.

Logisk gruppe
IED1 består av én eller flere logiske enheter som kan ha ulik funksjonalitet i kontrollanlegget. Disse logiske enhetene kategoriseres etter overordnet funksjonalitet ved hjelp av en forbokstav.

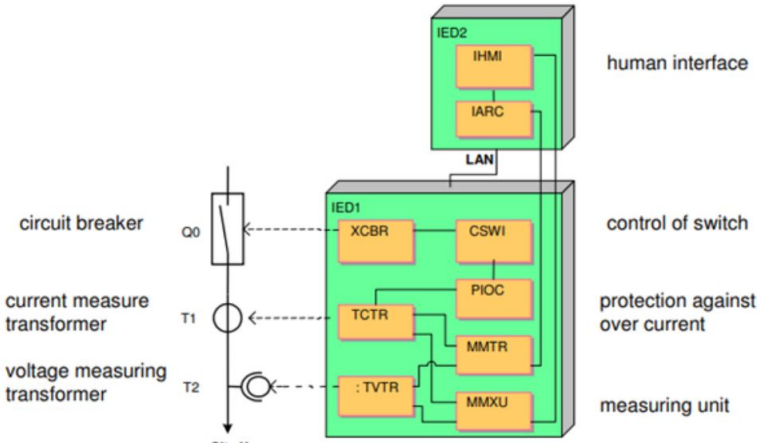
A	Automatisert kontroll
M	Måling
C	Monitorert kontroll
G	Generisk funksjon
I	Monitorering og arkivering
L	Logisk system-node
P	Beskyttelse
R	Beskyttelsesrelatert
S	Sensor
T	Instrument-transformatorer
X	Bryterfuksjon
Y	Effekt-transformatorer
Z	Andre funksjoner

En effektbryter vil være ha en bryterfunksjon og er derfor merket X etter standarden [21].

Logiske noder
IEDer består av én eller flere logiske noder. Logiske noder er standardiserte grupper data relatert til en systemfunksjon som er programmert av leverandør. Et utvalg logiske noder er:

XCBR	Effektbryter
IHMI	HMI
IARC	Arkivering
CSWI	Svitsj kontroller
PIOC	Overstrømsmåling
MMTR	Måling
TVTR	Spenningstransformator

En effektbryter har forkortelsen CBR, og inkludert logisk gruppe for bryterfunksjon merkes den XCBR. Figur 23 viser et simpelt system av logiske noder, og hvordan de er sammenkoblet for en automatisk løsning med monitorering, datainnsamling og styring. De logiske nodene TCTR og TVTR måler henholdsvis strøm og spenning. De er koblet til MMTR og MMXU for håndtering av målingen, som videre sendes ut av IED for beskyttelse til en annen IED med de logiske nodene IARC for arkivering og IHMI for monitorering. IED for beskyttelse har også direkte tilknyttet overstrømsmåling til strømtransformatoren, slik at oppnådd grense for overstrøm aktiverer effektbryter; XCBR, via svitsj styring; CSWI. Dermed har man et system inndelt etter funksjoner. Ved å dele signalene etter logisk node, kategoriseres også signaler på en oversiktlig måte når man har kunnskap om tilhørende node for sigalet.

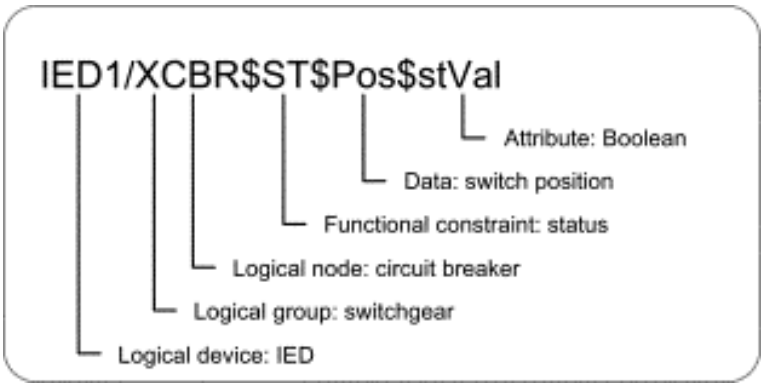


Figur 23: Logiske noder i IEDs [76]

Videre henviser hver logiske node viser til et dataobjekt.

Dataobjekt
Dataobjektet kan bestå av flere dataegenskaper etter behovet for datatyper. For å henvise til effektbrytere er dataobjektet en status, forkortet ST i taggingen, for åpen eller lukket posisjon. Deretter beskrives innholdet i statusen ved hjelp av datatyper.

Datatyper
Det er visse krav for datatyper som er obligatorisk merket innenfor hvert dataobjekt. Andre er valgfrie og kan utnyttes om nødvendig. Dette beskrives i konfigurasjonen inne i hver enkelt logisk node. IEC 61850 benytter funksjonelle begrensninger og standardiserte datatyper for systematisering av informasjon. For å bruke obligatoriske datatyper for effektbrytere som eksempel, har selve posisjonen en boolsk datatype for åpen/lukket. Dette er en statusverdi, forkortet StVal i taggingen. Alle signaler merkes også med et kvalitetsstempel (q). I tillegg har alle signaler et tidsstempel (t), slik at signalet kan dokumenteres til et eksakt tidspunkt.



Figur 24: Eksempel på strukturen for tagging av data [21]

6.5.5 Kommunikasjonsprotokoller

Kommunikasjon mellom nivåene foregår på stasjons- og prosessbussen. IEC 61850 benytter nettverkskommunikasjon slik at OSI-modellen skiller funksjonaliteten mellom protokollene.

MMS
Stasjonsbussen benytter en MMS-protokoll for et klient/server forhold [36]. MMS baseres på TCP/IP-protokoll hvor klienten etterspør data fra server, og server svarer med ønsket informasjon. MMS er den normale datakommunikasjonsmetoden som sikrer mottagelse av ønsket data. MMS brukes for å hente informasjon fra server om tilstander, trender og annet som er tilknyttet overvåkning og datainnsamling.

SV
Ved prosessbussen, mellom MUs og IED's, monitoreres tidskritiske prosesser som krever umiddelbar respons. Her benyttes protokollene SV og GOOSE som har strenge krav for tidsforsinkelser i kommunikasjonsprosessen. Protokollene baseres på publisher/subscriber forhold mellom IED's hvor muliticast-meldinger, av typen UDP, sendes og lagres i IED's. SV brukes for overføring av numeriske verdier, som strøm- og spenningsnivå [36]. SV-protokollen sender periodiske signal etter forhåndsinnstilt periode. For beskyttelse er standarden 4000 meldinger per sekund i et 50Hz system. Måleverdier sendes kontinuerlig for overvåkning, og baseres ikke på verifisering av mottagelse, slik som MMS.

GOOSE
GOOSE brukes for overføring av informasjon knyttet til overvåkning og kontrollfunksjoner, for eksempel bryterposisjon[18]. Protokollen sender ut multicast-melding ved tilstandsendring på en output. Tilstandsendringen sendes redundant med forsinkelse på 4, 16, 100 og 1000 ms, siden protokollen ikke baseres på verifisering av mottakelse, slik som MMS. Dette legger grunnlag for rask interaksjon mellom prosess- og kontrollnivå. Ved uendret tilstand sendes multicast-melding etter et forhåndsdefinert intervall fra 1 til 60 sekunders mellomrom. Om multicast-meldingen ikke registreres før tre ganger intervalltiden, vil tilsvarende IED registreres som ikke-kommuniserende, og forhåndsdefinert posisjon vil være tellende [18]. Her kan det tenkes å derfinere verst mulig tilfelle av sikkerhetsmessige grunner.

Fixed GOOSE
Det finnes en fjerde protokoll for tidskritisk kommunikasjon kaldt GSSE. Dette er en videreføring av gamle UCA2.0 som benytter et annet datasett enn tradisjonell GOOSE protokoll [32]. Derfor er GSSE blant enkelte IEDs en raskere kommunikasjonsprotokoll. GSSE ble ikke implementert i IEC 61850, og har derfor i praksis blitt erstattet av GOOSE som standard. I ettertid har GSSE blitt implementert som Fixed GOOSE i IEC 61850, hvor datasettet fra GSSE benytter GOOSE-protokollen, slik at Fixed GOOSE kan benyttes der hvor det er fordelaktig.

Prioritetsmelding
Under konfigurasjon av publisher/subscriber forhold defineres alle signaler etter prioritet i nettverket. Dette er for å sikre at kritisk informasjon, som for eksempel utløsersignal for effektbryter, ikke forsvinner i informasjonsflyten. Standarden har implementert IEEE 802.1Q for separering av båndbreddet innenfor et fysisk nettverk for å sikre prioritet etter rangering.

Hvis en SV multicast-melding defineres med høyere prioritet, tilbys kritisk informasjon førsteprioritet på båndbredden, og dermed sikrer man at proritete meldinger når frem. Forskning av SV-melding på prosessbussen viser at ingen data forsvant i tilfeller hvor meldingen hadde høyere prioritet enn annen trafikk [34]. Her ble nettverket overbelastet med hensikt om å teste prioritetsmeldingene i praksis.

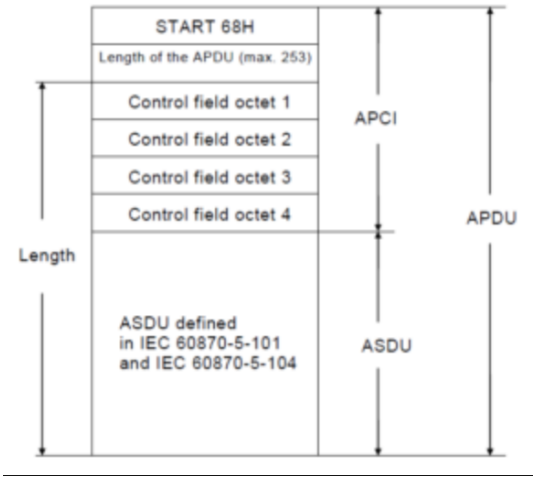
6.6 IEEE 1588 - Precision Time Protocol

I kritiske prosesser krever enheter for kontroll og monitorering en tidsstempling av signaler med presisjon på under mikrosekundet for å kunne operere nøyaktig. IEEE 1588 har en løsning som benytter GPS-basert teknologi direkte inn mot Ethernet ved hjelp av Precision Time Protocol (PTP). Leverandører av klokker basert på IEEE 1588 kan dokumentere en feilmargin på under $\pm 100ns$ [24]. Dette er en viktig tilleggsprotokoll for nøyaktig tidsstempling av data for analyse- og beskyttelsesfunksjoner i anlegg basert på IEC 61850 standarden. IEEE 1588 og har i praksis blitt implementert inn i IEC 61850 som en del av standarden. IEEE 1588 utnytter UDP-protokoll for effektiv interaksjon til nettverket.

6.7 IEC 60870-5-104 (IEC 104)

IEC 60870-5-104 er en kommunikasjonsprotokoll for fjernstyring av kraftverk eller transformasjonsstasjoner, og gir muligheten for å styre deres kontrollanlegg fra et sentralisert kontrollrom [51]. Protokollen kan også brukes for kommunikasjon intern i kraftverkets kontrollsystem. Ved å bruke en standardisert protokoll gjør det mulig å integrere automatiserte systemer fra forskjellige leverandører for å kunne kontrollere alle systemene uten protokoll-omformere eller tilpasninger.

IEC 104 er basert på IEC 60870-5-101 (IEC 101), som er en protokoll for telekontroll i automatiseringsapplikasjoner i kraftsystemer. IEC 104 gir nettverkstilgang til IEC 101, og dermed muliggjør for kommunikasjon mellom kontrollrom og en driftssentral via et standard TCP / IP-nettverk. Dette gjøres ved at IEC 104 fjerner den serielle overskriften og legger til de aktuelle overskriftene for bruk av TCP / IP-kanaler med full duplekskommunikasjon. IEC 101 venter på bekreftelse på hver melding som sendes, mens IEC 104 antar at kanalen er stabil, og et maksimalt antall K-meldinger kan sendes uten å vente på bekreftelse fra motsatt stasjon. IEC 104 fjerner den serielle toppteksten og legger til sin egen topptekst kalt APCI. De to første bitene i den første byten i APCI-overskriften brukes til å identifisere tre typer rammer:
U-ramme: Disse kontrollrammene administrerer trafikkutvekslingen over TCP-kanalen. De inkluderer en startmelding for å tillate trafikkflyten, en stoppmelding for å blokkere videre kommunikasjon og en testmelding for å sjekke om forbindelsen er i live.
I-ramme: Disse rammene transporterer applikasjonsdata (ASDU).
S-ramme: Tilsynsbildene viser motsatt stasjon nummeret til den siste rammen som ble mottatt riktig. De brukes som en bekreftelse på et sett med meldinger for å indikere at overføring av data kan fortsette.



Figur 25: APCI-topptekst i IEC 60870-5-104 [51]

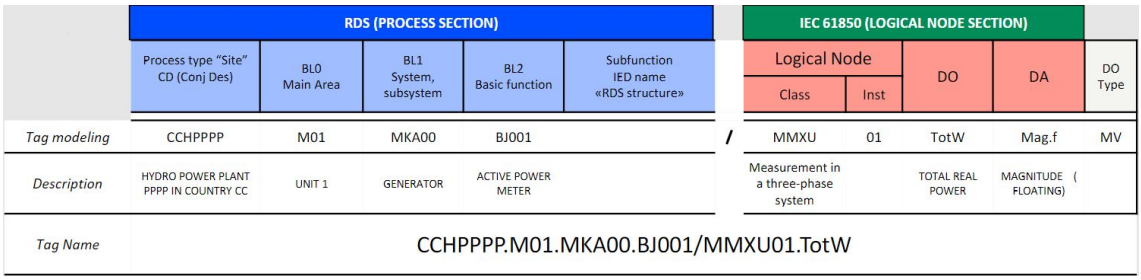
IEC 104 tillater definisjon av redundanskanaler over TCP / IP. Kontrollsenteret oppretter flere forbindelser samtidig (ved hjelp av forskjellige fysiske kanaler) og det aktiverer en av disse forbindelsene mens de andre er i "stoppet" tilstand og venter på å bli startet når kommunikasjonen i den aktive kanalen går tapt.

Ved at funksjonaliteten til IEC-104 er basert på TCP/IP viser det til en rekke sikkerhetsproblemer. Disse problemende blir forklart mer detaljert i delkapittel 10.3.

6.8 IEC 81346-10 - Reference Designation System

Som tidligere presentert i kapittel 6.5.4 har IEC 61850 en standardisering av tags i et lokal kontrollanlegg som er strukturert i flere lag basert på funksjon, logikk og datatyper. Dette gir en lokalt oversiktlig mapping, men som er lite praktisk opp imot et scada-system med mange vannkraftverk.

Som løsning kan den udefinerte prefiksen forran den lokale IEC 61850 taggen implementere en tag som sier noe om blant annet hvilket kraftverk, anleggsdel og komponent det er snakk om. Denne prefiksen vil være basert på IEC 81346-10 som er et system for strukturering av industrisystemer kalt Reference Designation System (RDS). Taggen som helhet vil ha en hierarkisk oppbygning. Som vist i eksempelbildet i figur , starter taggen med navn på kraftstasjon. Deretter kommer område og overordnet system. Til slutt kommer en beskrivelse av funksjonen og komponent. Det er her prosess-seksjonen fra RDS avluttes og taggen fra IEC 61850 fortsetter med logisk node, dataobjekt og datatype før selve informasjonskapselen.



Figur 26: Tags basert på RDS prefiks i et IEC 61850 tag [35]

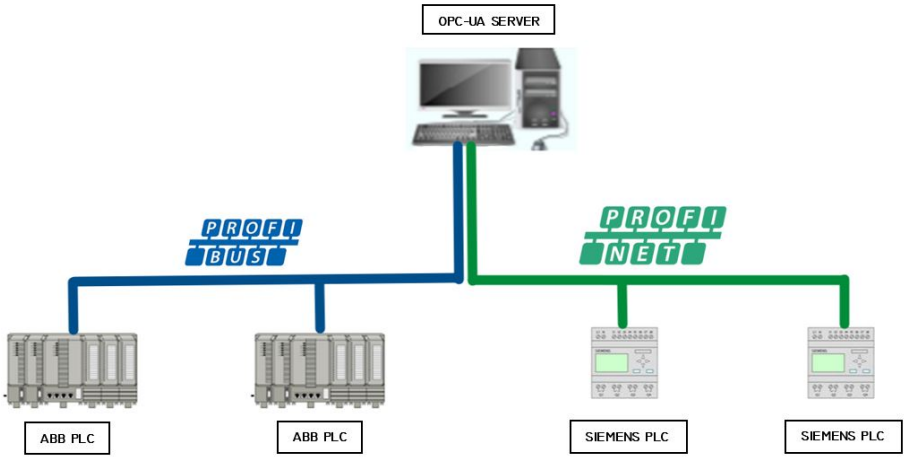
6.9 IEC 62439

I topologien er det implementert elementer fra IEC 62439 om redundans i nettverk. Dette skal hjelpe driftssikkerheten i kontrollanlegget. Viktige elemeter fra IEC 62439 er at komponentsvikt ikke skal hindre nettverksflyt. Derfor har topologitegningene dublert antallet komponenter i datanettverket. Mer detaljert er fiberkabler, svitsjer og rutere dublert i tilfelle feil.

En fordel med fiber er at kommunikasjon kan foregå begge veier i kabelen. For ekstra redundans kan derfor stasjonsbussen sammenkoble enhetene i et ringnettverk. Ved skade på kabelen kan data overføres motsatt veg i ringnettverket, og kommunikasjonen vil derfor ikke ta skade av kabelbrudd.

6.10 IEC 62541 OPC-UA

OPC-UA er en åpen maskin til maskin kommunikasjonsprotokoll for automasjon i industrien. Det består av en eller flere servere og klienter. Serveren definerer dataflyten og lagrer verdier, tidsstempel, kvalitet, hendelser og alarm-meldinger, i tillegg til variable tilstander innenfor et nettverk [62]. Serveren kan lastes inn i HW, som for eksempel en PLS eller datamaskin. Serveren lagrer data, fra ulike protokoller i industrien, som en OPC klient, for eksempel en HMI eller SCADA, kan etterspørre. OPC-UA har blitt høyt verdsatt i industrien, og leverandører etterkommer kravene for at komponenter skal være tilpasset standarden. Også datamaskiner, servere eller klienter, med tilknytning til OPC-UA er kompatible uavhengig av operativsystem eller versjon. Utdaterte versjoner av operativsystemet kan bli et problem når anlegget ikke lenger er nytt. Blant OPC-UA Servere på markedet idag, er disse kompatible til blant annet Windows XP, Vista, 7, 8 og 10 [33]. I tillegg vil nye operativsystemer tilpasses serveren. På denne måten kan OPC-UA samle industrielle komponenter fra ulike leverandører og tilkobles hvilken som helst datamaskin uten problemer med tanke på operativsystemer. En annen fordel med OPC-UA er at klienten kan være et automasjonsstudio. Her kan systemet simuleres og testes før bruk. OPC-UA erstatter MMS-protokollen fra IEC 61850 og er mer kompatibel, hvor MMS kun er operativ i et IEC 61850 nettverk. Erfaringer viser at MMS er en protokoll som ikke utvikles og tilpasses nye teknologier. OPC er derimot mer innovativ og kan by på flere muligheter i fremtidens kontrollsystem.



Figur 27: OPC-UA Server tilkoblet forskjellige leverandører og kommunikasjons-protokoller.

OPC-UA er også fordelaktig utenfor det lokale kontrollanlegget. Sammenlignet med IEC 60870-5-104 protokollen, som benyttes ut mot drifssentral i Statkraft og mange andre kraftverkseiere idag, gir OPC-UA muligheten for og automatisk populere data modellen i driftssentralen. Det betyr at driftssentralene alltid har siste registrerte data i sine systemer. Automatisk populering av datamodellen er også mulig gjennom IEC 61850 sine SCL-filer med mapping til IEC 60870-5-104, men dette er en mye mer krevende prosess. Om man får kontinuerlig oppdatering øker mulighetene for databehandling og hjelp av machine learning til å forutse feilsituasjoner og nødvendighet for vedlikehold.

Etterspørselen for Open Source plattformer som OPC-UA er økende i en tid med digitalisering og automatisering. OPC-UA er standardiserer interoperativitet mellom leverandører og gir enkle muligheter for hybride industri-løsninger mellom ulike leverandører. Dette kan skape konkurranse på komponentnivå, og potensielt skape billigere og driftssikre kontrollanlegg for fremtiden.

6.11 IEC 61131

6.11.1 IEC 61131-3

IEC 61131-3 er den tredje delen av standarden IEC 61131 og omhandler programvarearkitektur og programmeringsspråk for PLS [73][37][38]. Standarden definerer 3 grafiske og 2 tekstbaserte programmeringsspråk, og alle språkene deler IEC 61131 Common elements. Variablene og funksjonsanropene er definert av de vanlige elementene, så forskjellige språk i IEC 61131-3 standarden kan brukes i samme program.
De 5 programmeringsspråkene er:

- Ladder Diagram (LD)
  Ladder-logikk ble opprinnelig utviklet for å dokumentere design og konstruksjon av relé-baserte kontrollanlegg, der hver enhet ble representert med et symbol på

stige-diagrammet med forbindelser mellom enhetene. Logikken har utviklet seg til et programmeringsspråk som representerer et program ved hjelp av grafisk diagram basert på kretsdiagrammene til relélogisk HW. Språket brukes til å utvikle programvare for PLS-er som brukes i industrielle kontrollapplikasjoner. LD har vært populær på grunn av dens grafiske design.

- Function block diagram (FBD)
  Funksjonelt blokkdiagram er et grafisk språk for programmering av PLS, som kan beskrive funksjonen mellom inngangsvariabel og utgangsvariabel. En funksjon er beskrevet som et sett med elementære blokker. Inngangs- og utgangsvariabler er koblet til blokker ved hjelp av tilkoblingslinjer. En ikke formel versjon av FBD er continuous function chart (CFC), som er et mer fleksibelt kontinuerlig funksjonsdiagram. CFC er et super-sett av FBD og har to styrkeområder:

  - Blokkbasert funksjonell programmering
    Består av samlinger av forhåndsdefinert funksjonalitet som er koblet sammen for å gjennomføre boolsk logikk, matematiske beregninger eller en kombinasjon av de to. Informasjonsflyten kan være lett å forstå på grunn av at tilkoblingene er representert med linjer mellom funksjonsblokkene.
  - Hierarkisk design
    En praksis med å lage et design fra byggesteiner, som er bygget på enklere byggesteiner, som igjen er bygget på enklere byggesteiner. Byggesteinsteknikken er lettere å designe og forstå fordi den opprettholder et jevnt detaljnivå på hvert nivå i hierarkiet.

- Structure text (ST)
  Strukturert tekst er et tekstbasert høy-nivå språk som er blokkstrukturert og ligner syntaktisk på Pascal, som det er basert på. Språket støtter komplekse uttalelser og instruksjoner som:

  - Iterasjonssløyfer (REPEAT-UNTIL; WHILE-DO)
  - Betinget utførelse (IF-THEN-ElSE; CASE)
  - Funksjoner (SQRT(), SIN())

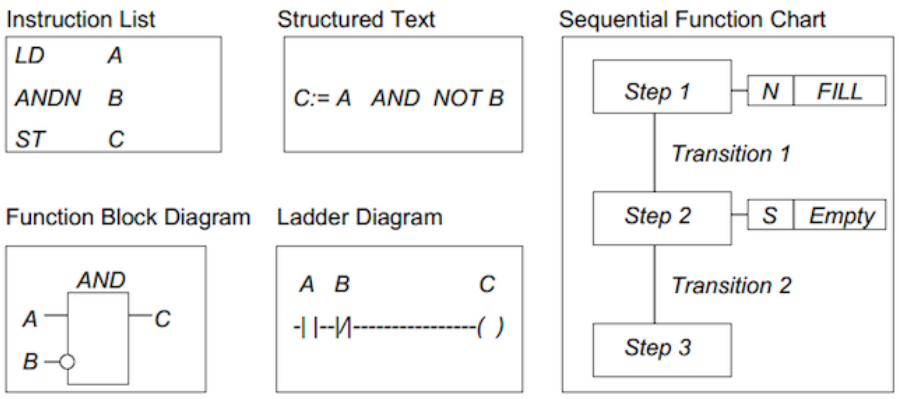
- Sequential function chart (SFC)
  Sekvensiell funksjonsdiagram er et grafisk programmeringsspråk som er definert som "Utarbeidelse av funksjonsdiagrammer for styringssystemer" og var basert på GRAFCET. Språket er brukt til å programmere prosesser som kan deles inn i trinn. Hovedkomponentene i SFC er:

  - Trinn med tilhørende handlinger
  - Overganger med tilhørende logiske forhold
  - Rettede koblinger mellom trinn og overganger

  Handlinger tilknyttet trinn kan være av flere typer, de mest relevante er Kontinuerlig (N), Sett (S) og Tilbakestill (R). SFC er enkel å designe fordi det tydelig beskriver tilstandene et system kan være i, hvordan systemet overgår mellom disse tilstandene og handlingene systemet skal ta mens de er i disse tilstandene. I løpet av kjøretiden

er det lett å se nøyaktig hvilken tilstand et system er i, hva det gjør i den tilstanden, og hva som får det til å flytte til neste tilstand.

- Instruction list (IL)
  Instruksjonsliste er et tekstbasert lav-nivå språk og ligner på montering. Språket ble avviklet i tredje utgave av IEC 61131. Filformatet er nå standardisert til XML av PLCopen.



Figur 28: De 5 forskjellige programmeringsspråkene i IEC 61131-3 [23]

6.11.2 IEC 61131-9

IEC 61131-9 er en del av en serie standarder for programmerbare kontrollere og tilhørende utstyr [80]. Delen spesifiserer seg mot kommunikasjonsteknologi for små sensorer og aktuatorer SDCI (IO-link). De utvider de tradisjonelle digitale inngangs- og digitale utgangsgrensesnittene som definert i IEC 61131-2 mot en punkt-til-punkt kommunikasjonslink. Denne teknologien muliggjør overføring av parametere til enheter og levering av diagnostisk informasjon fra enhetene til automatiseringssystemet. Teknologien er hovedsakelig ment for bruk med enkle sensorer og aktuatorer i fabrikkautomatisering, som inkluderer små og kostnadseffektive mikrokontrollere.

Denne delen spesifiserer SDCI-kommunikasjonstjenester og protokoll (fysisk lag, datalinklag og applikasjonslag i samsvar med ISO / OSI-referansemodellen) for både SDCI master og enheter. I tillegg inkluderer den også EMC-testkrav. Den dekker ikke kommunikasjonsgrensesnitt eller systemer som inneholder flere punkt- eller flere slippkoblinger, eller integrering av SDCI i systemer på høyere nivå som feltbusser.

7 INSTRUMENTERING I VANNKRAFTVERK

Et ressurskrevende og viktig område innen industriell datainnsamling i store anlegg, er industriell kommunikasjon og instrumentering. Dagens vannkraftverk er avhengig av en mengde sensorer for å overvåke og styre prosessen. Det anvendes trykkbryterer, initiatorer, strømningsmåling temperaturmålere, vibrasjonsmålinger mm. Nå som alt er sentralstyrt, er vi avhengig av at signalene blir logget og overført i sanntid for at de ansatte på driftssentralen skal kunne monitorere, og eventuelt agere. Som all annen teknologi, er det også innen dette feltet kommet nyvinninger når det kommer til hierarki og sensorteknologi som potensielt kunne blitt anvendt i et vannkraftverk.

Hierarkiske strukturer i et kontrollanlegg tilsier hvordan data innhentes og behandles. Her kan det inkluderes flere ulike kommunikasjonsprotokoller og tilnærminger for å oppnå anlegg med ønsket funksjonalitet og skalerbarhet, samtidig som man senker installasjonskostnader og gjør vedlikehold så enkelt som mulig. Nye ikke-proprietære protokoller tillater også kommunikasjon på tvers av leverandør.

7.1 Distribuert I/O

På «gamlemåten» måtte man lage trase og trekke kabler til hvert enkelt instrument fra PLS'ens inngangskort. Tilsvarende fra utgangskortet til et pådragsorgan. Etter hvert som behovet for datainnsamling har økt og anleggene har vokst, har det blitt utviklet strukturer som reduserer hvor arbeidsintensivt det er å implementere den økende overvåkningen av et industrielt anlegg. Den generelle løsningen er å flytte inn- og utgangskortene fra tavlerommet, og ut til anlegget for å korte ned instrumenteringskablingen og samle den totale dataflyten på en enkelt kabel. Siden man med det effektivt bytter ut mange kabler med en enkelt, er det lett å se rasjonale. Særlig gitt inflasjonen i kobber som vi har sett den siste tiden som har doblet prisen det siste året. Dette har kommet som følge av enorme investeringer i infrastruktur og fornybare energikilder.

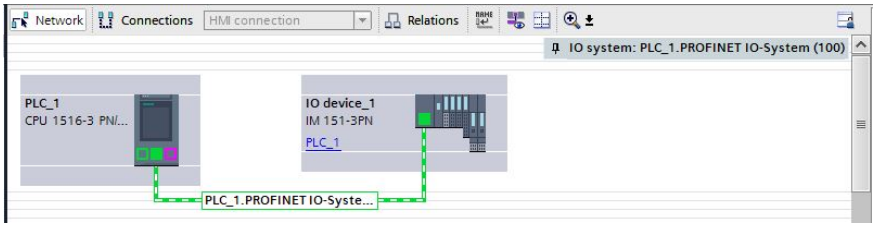
Figur 29: 3 måneders future kontrakt for kobber som omsettes på LME

Denne prisøkningen vil produsentene overføre til kunden, som vil være Statkraft.

Samtidig som man sparer arbeidstimer og kost vil man også redusere eksponering mot støy i signalkabler. Man oppnår da høyere nøyaktighet på målingene som er avhengig av analoge signal. Bachelorgruppen har sett på et mangfold av løsninger som finnes for datainnsamling og distribuert topologi, både veletablerte og nyere og kompilert informasjon om de som kan tenkes å være mest aktuelle.

7.1.1 PLS med master - slave topologi eller ET

Den mest kjente løsningen for å distribuere I/O er å implementere en såkalt ET som linkes opp mot PLS via buss. Dette er noe som flere leverandører har benyttet seg av i sitt respektive system. Siemens sine ET'er tilkobles på enten Profibus DP eller Profinet som har kommet i ettertid. En ET er kun en forlengelse av selve PLS'en som står for den overordnede logikken og besitter ikke egen logikk. Selve ET terminalen er modulbasert og kan utvides alt etter behov. For å installere en ET i anlegget trenger man kun kommunikasjon fra PLS via busskabel eller Profinet, i tillegg til 24VDC tilførsel. Selve tilkoblingen i SW gjør man i PLS'ens HW-konfigurasjon. Dette gjør alternativet attraktivt fra et kostnadsperspektiv.



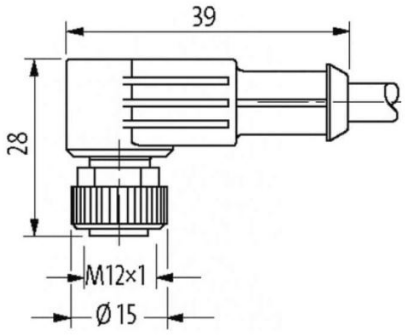
Figur 30: Profinet konfigurering i PLSens HW konfigurasjon

I et profibus nettverk gis ET'en et nodenummer. For Profinet gis den en IP da dette er en ethernetbasert protokoll. Denne type topologi tillater bruk av ET terminaler fra flere leverandører. IP-adresser må koordineres av IT avdelingen slik at man ikke får flere enheter med samme identitet på nettet. Forskjellen på en topologi med I/O og et med et master - slave oppsett er logikkplassering. Har man en slave, så vil logikken sitte her og master står for routing mellom enheter på bussen. En ET har ingen CPU og er bare en ren forflytning av I/O-kort. Slave-PLS'en er derfor å anse som en «IED».

Figur 31: Modulsetup i PLSens HW konfigurasjon. Her konfigurert med 2 I/O-kort

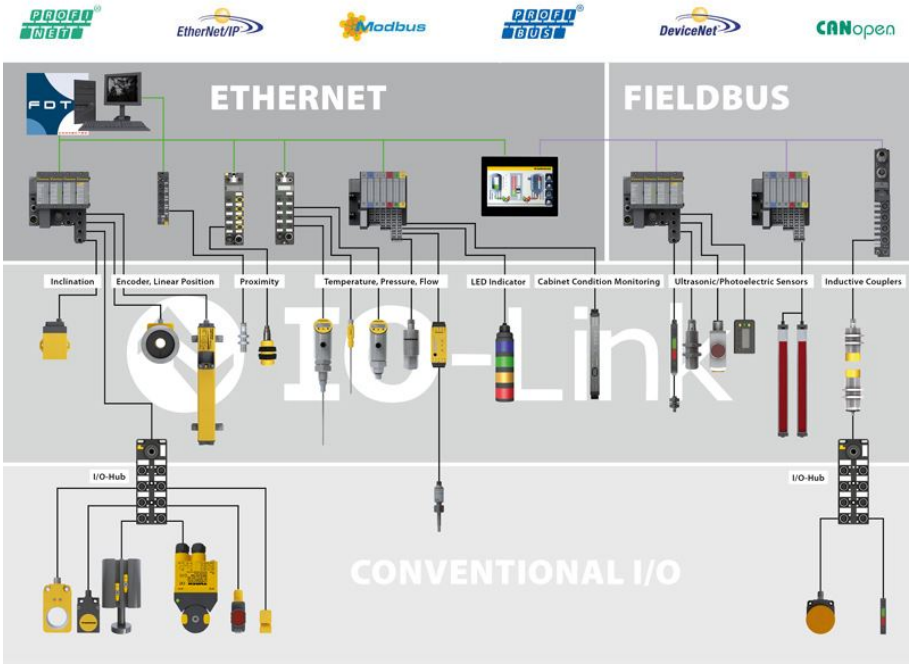
7.1.2 IO-Link

IO-link, også kjent som SDCI, tilbyr en instrumenteringsløsning som tar i bruk en primitiv form for distribuert automasjon og standardiserer tilkoblingene til instrumenteringen med en M12 plugg. Som flere andre nykommere innen industriell kommunikasjon, tilbyr IO-Link en overføringsprotokoll som tillater instrumenteringen fra ulike leverandører. Etablerte selskaper som Siemens, Turck og Sick har utstyr som støtter denne løsningen.



Figur 32: M12 plugg [64]

IO-Link topologien baserer seg på at man har et felles knutepunkt for instrumenteringen, en såkalt IO-Link master, som er tilkoblet PLSens bussprotokoll.



Figur 33: IO-Link topologi [22]

Det er i denne komponenten man kan programmere en logikk for instrumentering som den administrerer. Denne masteren kan på allsidig vis kobles til Profibus, Profinet, Modbus nettverk blant andre. En IO-link master har et utvalg inn og utganger man kan konfigurere etter bruk. Dette gjøres ved å sette innstilling i henhold til sensor som skal kobles til. Skal man gjøre endring i anlegget, kan man tilpasse denne til instrumentet som kobles til. Instrumentering herfra, som kan være alt fra temperatur eller trykk sensorer til aktuatorer, kobles til via standardisert ferdigterminert 3 til 5-wire kabling som består av 24VDC tilførsel og signal, og danner et punkt-til-punkt stjernenettverk. Løsningen er tiltenkt områder med mye signalinnsamling på lite areal der man ønsker enkel og

hurtig installasjon. Kabling fra master til instrument er begrenset til 20m. Fra master til instrument har man dataflyt i begge retninger i henhold til IEC 61131-9 som er omtalt i kapittel 6.11.2. Dette vil effektivt fjerne antall enkeltermineringer i anlegget som igjen gir mindre rom for feilkoblinger og reduserer behov for lange rekkeklemmelister i styre eller krysskoblingsskap. Dette gjør installasjon mer effektivt. Den standardiserte kablingen gjør også potensielle utskiftinger av komponenter enklere. Her også da uten behov for terminering. Feilkobling eller vakkelkontakt ved idriftssettelse blir dermed et ikke eksisterende problem. IO-link masteren kan inneha muligheter over overvåking og diagnostikk av sensorene og funksjonalitet for å kontrollere hysterese. For Siemens sin del anvendes samme SW som for PLS programmering, TIA. Dersom man logger inn på supportsiden til Siemens kan man laste ned et bibliotek av ferdigkonfigurerte funksjonsblokker. Dette tillater hurtig engineering av anlegget og en standardisert struktur for denne del av programmet.

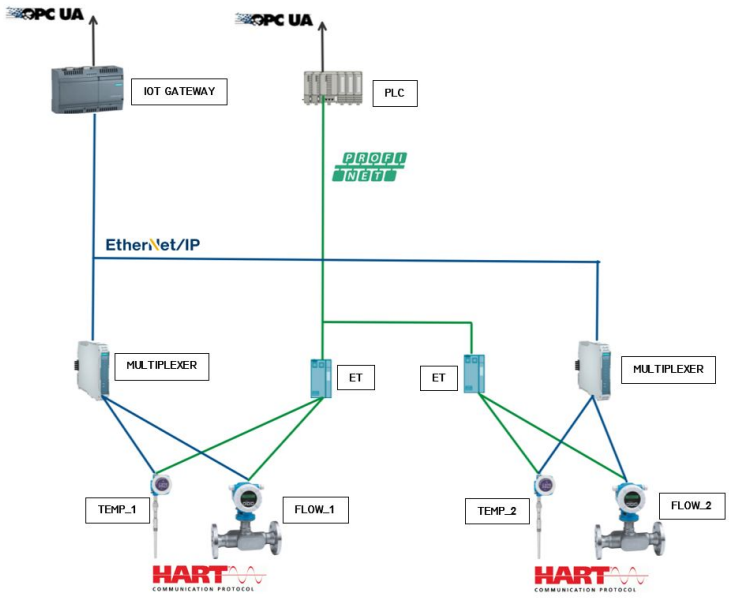
7.1.3 IIOT

Man kan ikke komme utenom å vurdere bruken av følere som opererer i et IoT-nettverk. Et IoT-nettverk vil i praksis si at instrumenteringen kan monitorere sine respektive områder, i tillegg til at de samkjører data blant hverandre på eget nettverk. Såkalt C2C eller horisontal topologi som det også kalles. Siemens tilbyr en IoT gateway som gjør at data fra HART-basert instrumentering (versjon 5, 6 og 7), som man normalt finner i prosessanlegg i dag, kan benyttes til å kjøre algoritmer designet for å analysere og diagnostisere prosessen. Man kan ta dette i bruk i et parallelt nettverk som er separat fra selve styringslogikken. Ved at man holder PLS styrings logikken for seg, og diagnose logikken separat, tillater man en direkte rute for denne datatrafikken og unngår å komplisere den etablerte styringa. Signalene splittes ut ved å seriekoble en multiplexer som skiller ut data fra HART sløyfen og ruter disse til gateway'en uten å påvirke 4-20mA signalet i målesløyfen. Denne har egen OPC server og kommuniserer videre til anleggets OPC klient. Herfra kan de tas i bruk i SCADA systemet eller tas ut for fjerndiagnostikk og vedlikeholdsplanlegging. Muligheten for å ta i bruk denne teknologien med en allerede etablert serverplattform som OPC UA, gjør dette lettere å implementere enn man skulle tro og kan derfor dele plattform med den mer tradisjonelle hierarkiske strukturen som PLS nettverket danner.

Figur 34: Siemens MX300 multiplexer [55]

Figur 35: SiemensCC240 IOT gateway [54]

Et eksempel på bruk kan være logging av temperatur i en transformator. Man er ikke lengre kun avhengig av å belage seg på simple H og HH alarmer. Alternativt for logging av vibrasjoner i lager for vedlikeholdsestimering. Ved å bruke logget rådata, som lastes opp i en fastsatt samplefrekvens, kan man tidlig oppdage dersom noe skulle begynne å endre karakter og undersøke opphavet til denne endringen før det får konsekvenser. Den loggede rådataen kan man så senere bruke til å ta lærdom når det oppstår hendelser man ønsker å finne forklaring til, og utvikle algoritmer som detekterer og forhindrer dette fremover. Fordi dette er separat, kan man benytte dette mer aktivt uten å gripe inn i kraftverkets daglige drift. Det at det er HART baserte signaler som løsningen baseres på, gjør også at man oppnår leverandøruavhengighet når det kommer til valg av instrumentering.



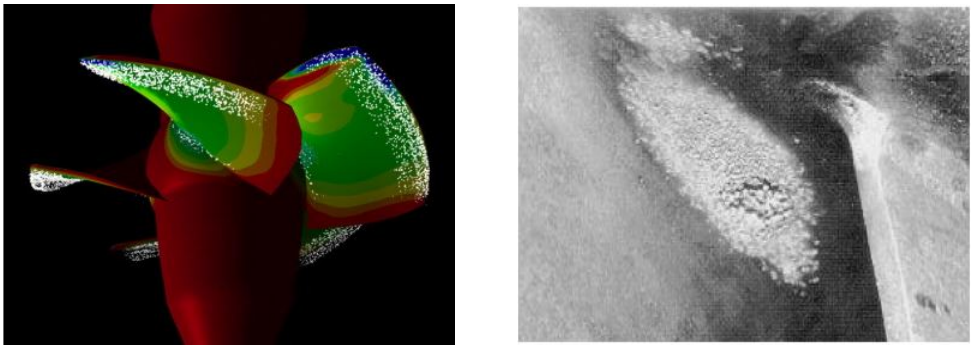
Figur 36: Eksempel på utskilling av HART data med SiemensCC240 IOT gateway i PLS anlegg.

7.1.4 Turbininstrumentering

Analysen som bachelorgruppen har gjennomført av kraftmarkedets utvikling i kapittel 4 viser til at behov for regulering av produksjon vil øke fremover. Det spekuleres i at reguleringsbyrden, som per i dag ligger hos de største kraftverkene, vil måtte fordeles videre på mindre kraftverk. På bakgrunn av dette ble det undersøkt om dette kan ha påvirkning for den strukturelle integriteten til komponentene som inngår i et vannkraftverk. I arbeidet med å få oversikt over potensiell påvirkning dette vil ha, ble flere tidligere forskningsstudier funnet og gjennomgått. Disse viser til at endringer i trykk på opp og nedstrømsside av en turbin gir redusert virkningsgrad over tid som følge av skader på skovlenes overflate på grunn av kavitasjon.

Skader påført av kavitasjon skjer som følge av bobledannelser som kolliderer med turbinen. De gassfylte boblene blir dannet ved trykkfall til under damptrykket. Fenomenet utsetter det spesifikke området på turbinen for høy belastning. Den mest brukte turbinen er Francis turbinen og er sårbar for trykkendringer og burde helst kjøres jevnt ved full last. Dette

er optimalt, men kan allikevel ikke vise seg å ikke være et alternativ. Overvåkning i form av ekstra instrumentering vil kunne sees på som en nødvendighet for å avdekke skadevirkninger.



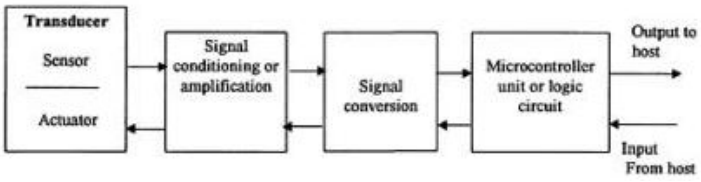
Figur 37: Venstre: Modellert kavitasjonsvirkning på Kaplanturbin [10]
Høyre: Kavitasjon på turbin [10]

Vibrasjonsmåling
Studier viser at ved å måle vibrasjonsmønster på lager, trykk på turbinbladene og analysere disse data i en historisk trend, kan man oppdage skadevirkninger og estimere behov for inspeksjon og vedlikehold. Lagerovervåking for roterende maskineri er ikke noe nytt fenomen, men det kan tenkes at bruk av data til å modellere endringer i væremåte under forskjellige laster ikke er tatt i bruk i stor grad. Statkraft krever at leverandører er veletablerte for å kunne sikre service og tilgang på deler. En slik leverandør som kan være aktuell er Baker Hughes som leverer tilsvarende overvåkingssystemer til anlegg over hele verden. Trykksensorene for montasje på skovler er etter det bachelorgruppen vurderer fortsatt på forskningsstadiet. En rapport utarbeidet av U.S department of energy fra 2016 [19] tilsier derimot at problemstillingen har vært forsket på i flere år allerede. Arbeid med å finne utstyr som annonseres til kommersielt bruk er derimot ikke en del av normale leveranser per i dag etter det bachelorgruppen kan se. Dette kan tyde på at teknologien ikke er klar helt ennå. Den økte CPU kraften som kreves dersom man implementerer en del mer instrumentering i et eksisterende anlegg, vil kunne utløse krav om HW utskiftinger for å kunne holde grensenivåene som er satt i Statkrafts spesifikasjoner. Som det foreslås tidligere, mener bachelorgruppen at ekstra datastrømming legges separat for å unngå komplikasjoner i eksisterende anlegg samtidig som det på enklere vis kan installeres. Når det kommer til datasikkerhet, vil det også gi fordeler om man har enveis transmisjon av data. Man får økt datastrøm ut, men tilgang til kontroll av anlegget forblir det samme.

7.1.5 Smarte sensorer

Smarte sensorer vil si instrumentering som innehar egen logikk og egen måleomformer som digitaliserer signalet. Bruk av smarte sensorer vil i praksis fungere som å en distribuert automasjonsløsning der logikken er flyttet ett hakk nærmere prosessen. En sensor er smart dersom den har mulighet til å:

- Måle prosessmediet
- Vurdere og prosessere måledata
- Monitorere sin egen tilstand
- Kommunisere i et horisontalt hierarki gjennom TCP/IP, som IoT



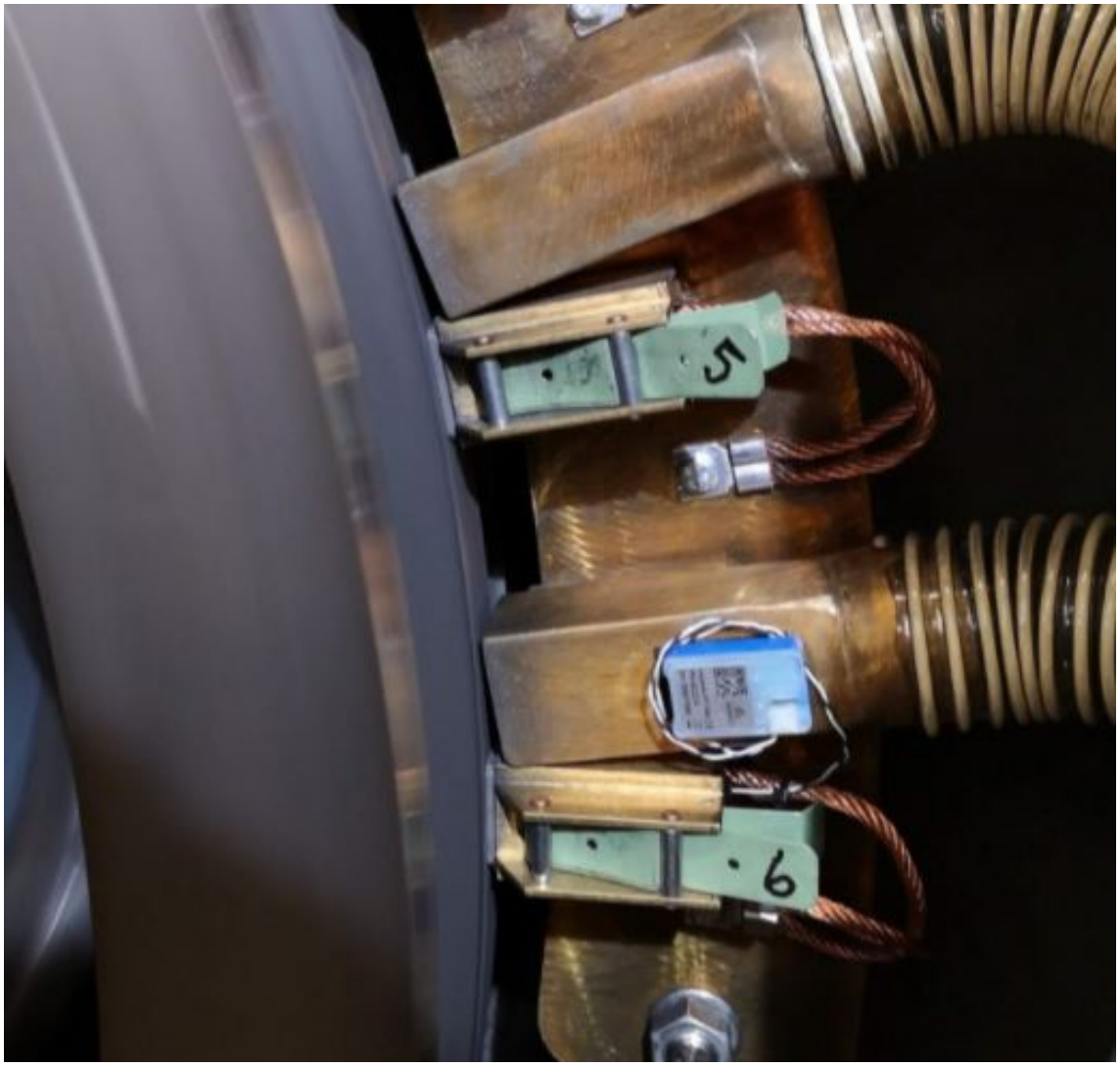
Figur 38: Smart sensor funksjonalitet [10]

Dette er et er måte å tenke på innen det som kalles Industri 4.0 der komponentene opptrer som autonome enheter og har mulighet for selvlæring og kunstig intelligens.
Sensorene kommuniserer på to måter:

- Multicast
  Noden sender data med en «felles» adresse som bare de nodene som abonnerer på denne oppfatter.
- Client-Server
  Tilsvarende som tradisjonelle request/send kommunikasjonsstrukturer.

Ved Pikerfoss elvekraftverk kan man lese at det er tatt i bruk trådløse temperatursensorer for overvåkning av slepebørstene på generatoren allerede tilbake i 2019 [31]. Med kontinuerlig logging og analyse av disse temperaturene kan en oppdage skeivslitasje, endringer en anser som uvanlige og lage plan for vedlikehold og inspeksjon. Temperaturen i disse korrelerer også med belegg fra kullstøv som igjen kan lede til overslag og børstebrann.

Siden sensorene er trådløse, er montasjearbeid mindre omfattende relativt til tradisjonelle PT100 elementer. Signaler fra samtlige trådløse sensorer samles til en gateway som viderefører data til server eller analyseverktøyet man ønsker å benytte. Det finnes trådløs instrumentering for temperatur, trykk, lekkasjeovervåking og tradisjonelle initiatorer der alle kommuniserer over samme protokoll. En nedside med trådløse sensorer er at de belager seg på batteridrift som tilførsel. Dette er noe som inngår i den smarte sensorens monitorering av egentilstand. Temperatursensorene som er nevnt i Pikerfoss er oppgitt til å ha levetid på rundt 15 år, men siden de kun står for overvåking og alarmgivning vil ikke uforutsette utfall påvirke drift.



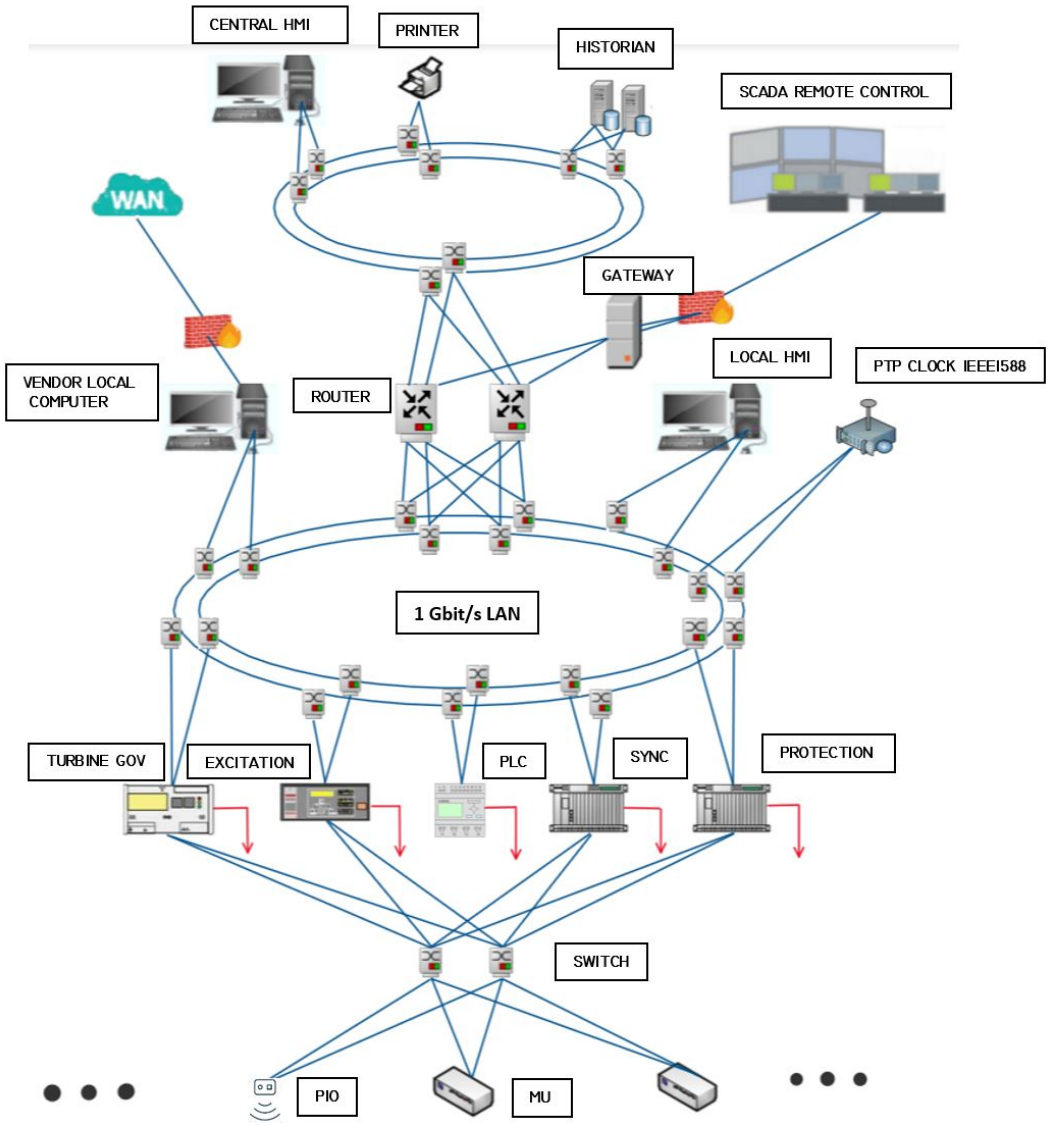
Figur 39: Trådløse PT100 elementer som monitorerer børstetemperatur [31]

8 TOPOLOGIER OG PROTOKOLLER

Det er viktig med en god struktur i kontrollanlegget med tanke på funksjonelle inndelinger, men ikke minst redundans i tilfelle en feilsituasjon skulle oppstå. Bachelorgruppen har undersøkt implementering av IEC 61850 for standardisering og som kommunikasjonsprotokoll i kontrollanlegget, og gjort vurderinger på implementering av andre teknologier. Løsninger er blitt vurdert etter robusthet, kostnad, erfaring, fordeler og ulemper.

8.1 Kontrollanlegg basert på IEC 61850

8.1.1 Topologi



Figur 40: Topologi for kontrollanlegg basert på IEC 61850

8.1.2 IED

I anlegg som finnes idag benyttes ET for distribuert I/O i kraftverk. Dette er en god løsning som minker kabling opp til PLS. IEC 61850 introduserer konseptet distribuert automasjon ved hjelp av IEDer. Distribuert automasjon er en forenkelt semiautomatisk metode for å forenkle oversikten for logikk og kommunikasjon ved å oppdele funksjoner i IEDer [13]. Målet med distribuert automasjon er enkel fjernstyring og overvåkning fra SCADA, med interoperative IEDer i et større smart grid system. Distribuert automasjon gir en oversiktlig funksjonsinndeling i kontrollanlegget hvor IEDer kan være redundante for hverandre.

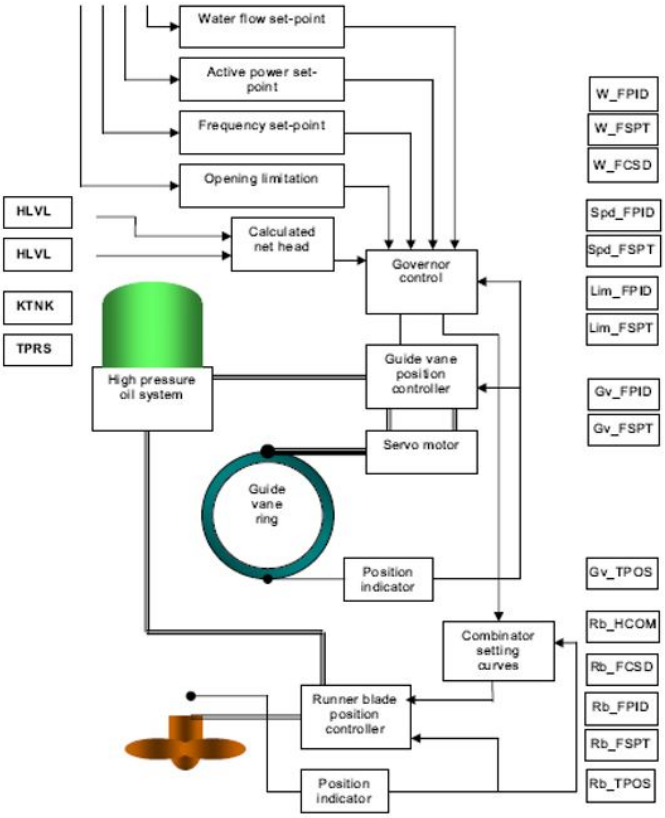
PLS
PLS er en IED i et IEC 61850 kontrollanlegg, men den vil ha minimalt med ansvar for drift. PLS kan stå ved hver produksjonsenhet som redundans for kritiske funksjoner slik som:

- Start/stopp sekvenser
- Bremsesystem
- Magnetisering
- Turbinregulering
- Kjølesystem
- Pumpesystem
- Lukesystem
- Synkronisering
- Alarmsystemer

Turbinregulator
Turbinregulering består av elektronisk regulator, servomotorer, elektronisk hydraulikk og oljetrykk for regulering av produsert effekt. Reguleringen foregår i respektiv IED, hvor kritiske innganger for IED er turbinfart, effektbrytere og servovinkel for ledeskovlene. Turbinregulator er en kritisk styreenhet i kraftverket, og derfor kan det tenkes at individuell hardwire-tilkobling til disse sensorene burde vurderes.

I tilfelle feilsituasjoner eller endringer utenfor turbinregulatoren, burde IED abonnere på data fra høyspentbrytere, enhetsfrekvens, nettfrekvens og produsert effekt for rask interaksjon om regulering trengs. Fra IEC 61362 skal turbinregulatoren har en redundant løsning ved utfall av én IED. Som nevnt er PLS foreslått som reserve.

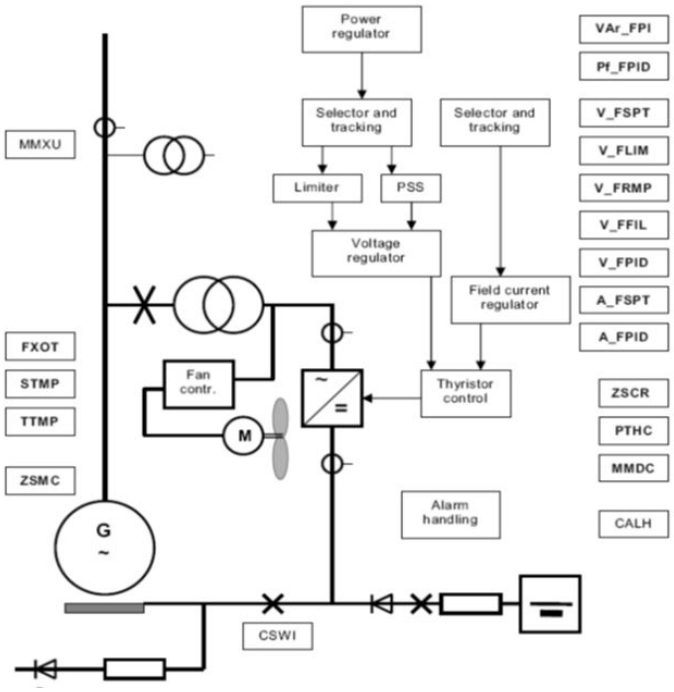
Figuren nedenfor viser logikken for turbinregulatoren med tilhørende logiske noder.



Figur 41: Logikk for turbinregulator med tilhørende logiske noder [78]

Navngiving i bildet ovenfor inkluderer en prefix i henhold til anleggsdel. Denne foreslås å byttes ut med en prefiks ut ifra RDS-systemet beskrevet i kapittel 6.8. Siste fire bokstaver beskriver den logiske noden. Logisk gruppe er F for funksjonsblokk, T for sensor, K for mekanisk utstyr og H for vannkraft. Sentrale logiske noder for turbinreguering er FPID for PID-regulator og HCOM for kombinator.

Magnetisering
Magnetisering i en IED holder busspenningen stabil og mater rotor for parallelle enheter med DC-strøm, også om det oppstår feil i strømnettet. IED skal abonnere på informasjon om statorspenning, statorstrøm og feltstrøm. Magnetisering har flere funksjoner og består hovedsaklig av effektregulator, systemstabilisator, automatisk spenningsregulator (AVR) og feltstrøm-regulator. I tillegg settes en limiter med parametere for undermagnetisering, overmagnetisering, forhold mellom spenning og frekvens, og maks feltstrøm. Figuren nedenfor viser logikk for magnetisering med tilhørende logiske noder.



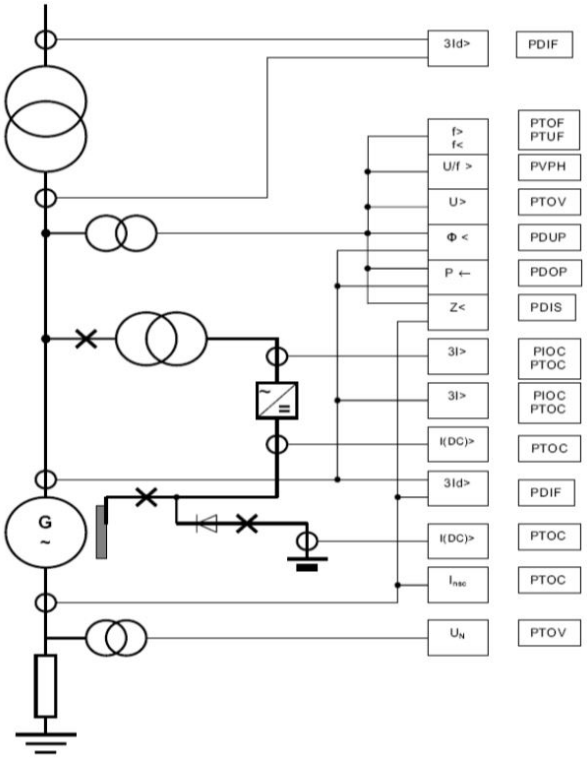
Figur 42: Logikk for magnetisering med tilhørende logiske noder [78]

Sentrale logiske noder i magnetiseringen er ZSCR for thyristor styring, ZSMC for synkrongenerator og FPID for PID-reguator.

Beskyttelse
Beskyttelse skiller mellom mekanisk og elektrisk beskyttelse. Dette har med prosedyrene for reaksjon på feil som oppstår. I IEC 61850 kan beskyttelse som en IED håndtere både elektrisk og mekanisk beskyttelse.

Elektrisk beskyttelse oppnås gjennom målinger av elektriske signaler. Ved indikasjon på feil kutter IED ut komponenter med elektriske feil for å skape sikker drift raskest mulig.

Mekanisk beskyttelse overvåker feil i temperatur, oljenivå, hastighet og vibrasjoner. Ved nivåer utenfor forhåndsdefinerte grenser kan IED utløse alarmer, og om nødvendig stoppe generatorenheten med mekanisk feil.



Figur 43: Logikk for beskyttelse med tilhørende logiske noder [78]

Den logiske gruppen P tildeles beskyttende logiske noder. Sentrale logiske noder innen beskyttelse er PTOV for overspenning, PIOC for overstrøm og PDIF for differensialvern.

Prosessbuss
Ved full utnyttelse av Ethernet-kablet prosessbuss, spares over 50% av kabler sammenlignet med konvensjonelle anlegg [8]. Bruk av Ethernet åpner også for implementering av industri 4.0, hvor vannkraftverk kan benytte smarte sensorer. Tidligere har sensorer vært transdusere som skaper elektriske signaler som parametere for å indikere temperatur, trykk og vibrasjoner. Derimot har smarte sensorer en mikroprosessor med logikk for omforming til digitale verdier, de kan være åpen for kommunikasjonsprotokoller, og selvdiagnostisere ved interne feil. Disse kalles Programmed Input/Output, forkortet PIO. Ved videreføring av konvensjonelle transdusere kan MUs være mikroprosessoren som overfører målingene til ønsket protokoll, og deretter overføres via Ethernet.

ESD system
Løsningen for kontrollanlegget fokuserer på det primære systemet. Likevel for sikkerhetsmessige grunner er det nødvendig med et ESD-system, også i kontrollanlegg basert på IEC 61850. ESD systemet skal fungere uavhengig av kontrollanlegget, og oppgaven er nedstenging av kraftverket ved en feilsituasjon. For kraftverk med installert generatorytelse over 250MVA krever kraftberedskapsforskriften også dublering av viktige styrekomponenter [14].

VLAN - Virtual Local Area Network
Virtuelle lokale nettverk (VLAN) deler fysiske nettverk i mindre logiske nettverk for å øke ytelsen, forbedre håndterbarheten og forenkle nettverksdesign. Dette er en vanlig og grunnleggende funksjon i administrerbare svitsjer for Ethernet. Hvert VLAN består av et enkelt domene som isolerer trafikk fra andre VLAN. Ved å bruke VLAN begrenser det domenet, i tillegg tillater logiske undernett for å strekke seg over flere fysiske steder.
Bruk av VLAN anbefales på det sterkeste i IEC 61850-kompatible systemer [16]. VLAN tilbyr en metode for å redusere ledningsnett, dermed redusere installasjonskostnader, og forbedre totalbeskyttelsen av moderne høyhastighets Ethernet-kommunikasjonsnettverk. VLAN tillater mer effektiv datatrafikk innen bestemte grupper av enheter, ved filtrering i svitsjen slik at IEDer ikke får data fra VLANer som de ikke er koblet til. Dermed trenger ikke enkelte IEDer å behandle data som er beregnet på andre IEDer.

8.1.3 Muligheter og utfordringer

Standardisert system i energiforsyningen
IEC 61850 er allerede i bruk ved koblingsanlegg av netteierne i Norge idag. Også nye anlegg planlegges etter IEC 61850 standarden. I og med at netteieren har ansvaret for belastning og utkoblinger ved feilsituasjoner, er det fordelaktig om energiforsyningen som helhet, inkludert kraftverkene, er basert på den samme standarden for kommunikasjon. Det vil gjøre det enklere for systemene som helhet ved å ha overlappende funksjoner med overstyring i feilsituasjoner. Leverandører vil kunne tilby flere komponenter for systemer med IEC 61850 om også kraftverkene benyttet dette. Likevel er det en problemstilling rundt en integrasjon av produksjon og høyspentnett. Energiloven §4-6 og §4-7 krever funksjonell adskillelse mellom produksjon- og nettvirksomhet [58]. Dette vil i praksis si at SCADA-systemer for nett og produksjon vurderes som sårbart ved sammenslåing, men muligheten ligger i en avgrenset funksjonalitet for utkobling av hovedstrøms effektbryter i feilsituasjoner.

Effektiv innsamling, tilgang og analyse av data
Et bærelager for én generatorenhet vil normalt ha 12 signaler opp imot SCADA-systemet. Siden navngiving av signalene i hver enkelt vannkraftverk er gjort ulikt, resulterer dette i over 400 ulike navn i SCADA-systemet (i Statkraft) som beskriver disse 12 målingene ved ulike kraftverk. Dette skaper unødig kompleksitet i datasystemet, og overflødig arbeid for datainnsamling. Ett av målene med standardiserte signaler er muligheten for ett system som håndterer datasamling for alle kraftverk. Derfor er standardisert tagging av signaler en viktig brikke når systemer skal digitaliseres.

Ved at all informasjon er tilgjengelig over internett-protokoll, kan data samles i en skyløsning hvor man kan få tilgang til enkelte måleverdier. Overføring av data kan skje via en UGW opp i skyen, og dermed kobles imot systemer for analyse og visualisering av data. Leverandører kan sikre at den fysiske lagringen av skyen er sikker mot misbruk av data. Det er disse mulighetene etter tagging og IEC 61850 standardisering som gjør løsningen attraktiv for fremtidlige kontrollanlegg. Digitalisering og automatiske løsninger kan utgjøre stor forskjell i lønnsomhet og sikker drift av vannkraftverk.

Gjennom en fast struktur på taggingen, forenkler dette et tverrfaglig samarbeid ved å tilgjengeliggjøre datalister internt. Standardisert laginndeling og tilnærmet like signallister på tvers av kraftverk skaper et generelt grunnlag for tverrfaglig forståelse.

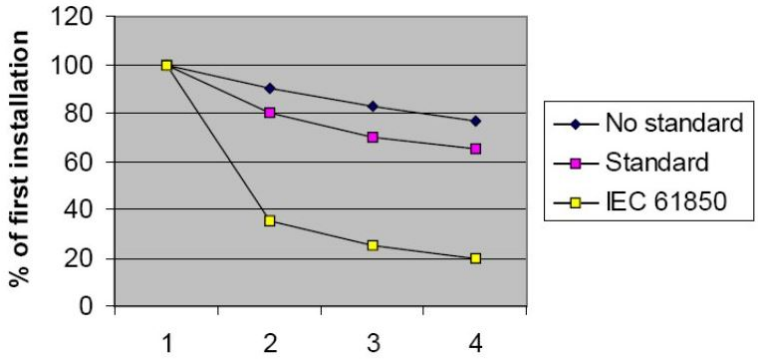
Analyse og databehandling
Siemens Energy har utviklet en SW for visualisering kalt SOGO Digital. SOGO er ment til å utnytte datainnsamlingen for trender og overvåkning som ikke er direkte knyttet til prosessen, som driftsentralene overvåker. IEC 61850 sine evner til å samle data i skyen, muliggjør systematisk overvåkning av viktige parametere. For eksempel kan temperaturer, vibrasjoner og trykk plottes i et aksesystem over tid for visualisering. Videre kan SW implementere smarte systemer for Big Data Analysis og maskinlæring for vedlikehold og varslinger i faresituasjoner. Dette minker muligheten for menneskelig feil.

Montasje og vedlikehold
IEC 61850 introduserer en rekke elementer som skal forenkle montasje og vedlikehold av kontrollanlegget. Under montasje av HW og konfigurering av SW har mange anlegg tilnærmet like funksjoner i respektive IEDer. Dermed kan anlegg etter de første implementeringene kopieres til nye anlegg, med mindre spesifikke endringer. Prosessbussen og stasjonsbussen utnytter oppkobling mot Ethernet og svitsjer, noe som minker mengden kabler, og dermed skaper raskere og billigere montasje.

Implementering av IEC 61850 er en stor overgang med tanke på vedlikeholdsprosessen. Sammenlignet med eldre kontrollanlegg gir simpelheten i konvensjonelle komponenter en fordel med tanke på enkle utskiftingen. Det vil forekomme noen ekstra steg i vedlikeholdsprosessen i et IEC 61850 system. Dette har med konfigurasjonen av SCL-filen for korrekt navnsetting, parametere og testing. Likevel kan utskiftninger og vedlikehold av SW gjøres effektivt og sikkert. SW kan simuleres for feilsøk, og i tillegg tillater internetprotokollen for fjernoppdatering av mindre SW-detaljer, slik som parametre. Siden konfigurasjon for hver enkelt IED samles i SCL-filen kreves kun én opplastning for oppdatering av hele kontrollanlegget. Ved større endringer enn endring av parametre eller liknende er det normalt med en servicegjennomgang lokalt på anlegget for testing.

Et system under utvikling
Erfaring viser at vannkraftens komplekse prosesser krever avansert logikk og mer omfattende kontrollanlegg enn koblingsanleggene som IEC 61850 opprinnelig ble utviklet for. Derfor jobbes det per idag med nye utgaver av IEC 61850 for implementering i vannkraftverk. Få anlegg er bygd og testet, men Enel har idag vannkraftverk basert på IEC 61850.

Investering og omstilling
En overgang til IEC 61850 iverksettelser store tiltak med tanke på tagging og opplæring av nye systemer. Idéen bak standardiseringen som kommer med IEC 61850 er at dette er en investering som over tid vil gjør anleggene billigere, både å bygge og drifte. Bakgrunnen for dette er et detaljert standardisert anlegg hvor metoden for nye anlegg får en klipp-og-lim effekt over seg. Dette medfører en stor jobb med de 2-3 første anleggene, som i praksis blir en læringsprosess og investering for senere anlegg. Figuren nedenfor viser hvordan prisutviklingen av nye anlegg svekkes betraktelig med IEC 61850 sammenlignet med andre løsninger.

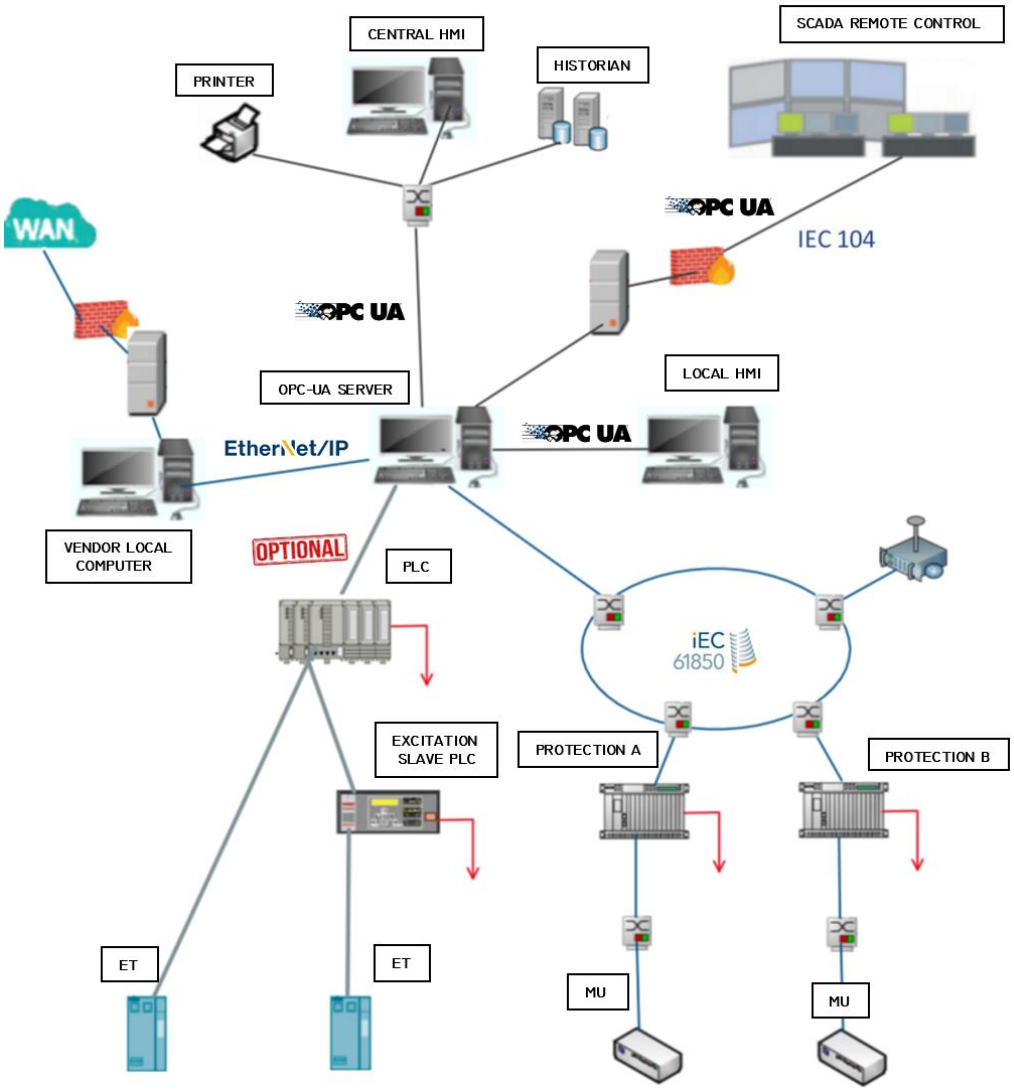


Figur 44: Investeringsbilde for IEC 61850 og standardisering [81]

Generell standardisering ser ut til å hjelpe, men som figuren viser har IEC 61850 større fordeler i en samlet standard enn andre løsninger har [81].

8.2 Delvis implementering av IEC 61850 ved hjelp av OPC-UA

Standardiseringen som ligger i IEC 61850 er en viktig brikke i fremtidens kontrollanlegg. Likevel trenger ikke hele kontrollanlegget å benytte kommunikasjonsprotokollene fra IEC 61850. Dagens løsninger for styring av generatorenheten er fullt fungerende, slik at en overgang til IEC 61850 kan være mer bry enn fordelaktig. Store endringer kan være kostbart og påvirker lønnsomheten for vannkraftverket. Derfor vurderes muligheter for delvis implementering av IEC 61850 for prosesser som har nytte av fordelene, og som er godt testet for implementering. Én av fordelene med IEC 61850 er distribuert automasjon med intelligent overvåkning og GOOSE meldinger for tidskritiske funksjoner, noe som passer beskyttelsesvern.



Figur 45: Topologi for delvis implementering av IEC 61850

Når det gjelder nødvendige funksjoner i kontrollanlegget for styring av generatorenheten kan tradisjonell PLS med valgfri kommunikasjonsprotokoll mot I/O benyttes. Om det er snakk om rehabilitering av et kontrollanlegg kan PLS og protokoll mot I/O fortsette. Én ulempe man ikke utnytter med IEC 61850 blir da ekstra kabling ute mot I/O, men dette finnes det løsninger for idag, med for eksempel en ET, som samler I/O for samlet transport opp mot PLS. I denne situasjonen minsker man kablingen og utnytter fungerende komponenter og kabler fra anlegget i videre drift. Ved bruk av protokoller som Profinet eller MODBUS TCP, oppnår man like fordeler som ved IEC 61850, da disse også er IP-baserte. TCP- og UDP-overføringer tillater tilbakemelding og multicast-meldinger over Ethernet. Ved å ikke bruke IEC 61850 mister man muligheten for hurtig GOOSE-kommunikasjon, men Profinet har en tilsvarende protokoller for hurtig kommunikasjon kalt Profinet RT og Profinet IRT. Dette viser at enda en fordel med IEC 61850 allerede benyttes idag.

Kontrollanlegget håndterer flere protokoller ved hjelp av en OPC-UA Server. Grunnen til at PLS og beskyttelse er adskilt via OPC-UA Server er fordi dette er to uavhengige systemer. Det kan tenkes at tidkritiske reguleringer drar nytte av IEC 61850 protokollene, men i en hybridløsning vil dette skape problemer siden OPC-UA Server gir noe tidsforsinkelse. OPC-UA blir en viktig SW om denne løsningen skal være gjennomførbar. Alternativet er en gateway med mapping fra valgfri protokoll til IEC 61850 for en hybridløsning, men dette krever induviduell mapping for hver protokoll, hvor OPC-UA allerede håndterer mange protokoller. En annen fordel med OPC-UA serveren er å få OPC-protokoll opp mot driftssentral, historian og HMI. OPC-UA skaper kompatibilitet i kontrollanlegg. De tidskritiske målingene via MUs på IEC 61850-siden av hybridløsningen har fremdeles tilkoblet GPS-klokke for nøyaktighet. Derimot tidstemples andre målinger gjennom OPC-UA serveren.

En slik løsning benytter gjenbruk og er en mykere overgang mot IEC 61850. Samtidig utnyttes fordeler av IEC 61850 der hvor det er hensiktsmessig og godt testet idag ved koblingsanlegg og transformatorstasjoner.

Denne løsningen gjør at styre- og beskyttelsessystemet må konfigureres på ulike vis, siden IEC 61850 har et eget system for konfigurasjon. Samtidig skaper dette muligheter for kopiering av konfigurasjon for vern for kommende implementeringer, siden det grunnleggende beskyttelsessystemet fungerer likt på tvers av kraftverkene.

8.3 Kontrollanlegg uten IEC 61850

Kontrollanlegg som benyttes idag er fullt operative for effektiv drift. Derfor kan det tenkes at større endringer, som krever investeringer, skaper overflødig ekstraarbeid og unødvendig omstilling. Idéene bak en omstilling mot IEC 61850 er fordelene man oppnår i lengden, men implementering av annen teknologi kan gjenskape mange av de samme fordelene, uten store inngrep i dagens kontrollanlegg.

Som flere kraftverkseiere påpeker kommer de største fordelene med IEC 61850 på entreprisenivå med implementering av smarte applikasjoner med blant annet maskinlæring for vedlikehold og kostnadsoptimalisert produksjon. Dette ligger utenfor det lokale kontrollanlegget slik at en løsning for digitalisering og systemer for signalbehandling enkelt kan åpne for disse fordelene, uten bruk av IEC 61850 i kontrollanlegget. Likevel er det fordelaktig i signalbehandlingen om alle signaler fra alle vannkraftverk standardiseres slik at tredjeparts programmer ikke må detaljprosjekteres forskjellig på tvers av vannkraftverk. En løsning på dette er å kun implementere IEC 61850 tagging av signaler. Selve kontrollsystemet trenger ikke å være IEC 61850 for å navngi signalene etter standarden. På denne måten kan man utnytte standardiseringen fra IEC 61850 uten endringer i dagens kontrollanlegg.

På statsjonsnivå er IEC 104 idag foretrukket og av leverandører og kraftverkseiere, og kan dermed fortsette som protokoll. På sikt ser OPC-UA ut til å gi flere muligheter som en åpen protokoll under stadig utvikling.

På prosessnivå vil Ethernet-baserte protokoller være fordelaktig. Herunder kan kjente protokoller som Profinet og MODBUS TCP benyttes. Ethernet-protokoller gir en rekke fordeler. De muliggjør implementering av IEEE 1588 og PTP, prioritering av meldinger, potensielt 50% kortere kabelforbindelser ved hjelp av svitsjer, oppdeling i VLAN, og UDP-kommunikasjon tillater multicast meldinger for I/O-kommunikasjon. Internettbaserte protokoller er også åpne protokoller som tillater HW innen instrumentering fra ulike leverandører, noe som åpner valgfrihet mellom I/O-løsninger [7].

En annen fordel med IEC 61850 er leverandøruavhengighet gjennom den åpne kommunikasjonsprotokollen og XML-filer. Dette åpner muligheten for å bygge kontrollanlegg med IEDer fra ulike leverandører. Ved koblingsanlegg utnyttes dette ved å dublere kritiske IEDer med bruk av 2 forskjellige leverandører. Når det kommer til vannkraft er det kun kraftverk med samlet generatorytelse større enn 250MVA som krever dublering av de viktigste styrekomponentene [14]. Erfaring viser at en slik leverandørdublering er simpelt for koblingsanlegg, men vurderes som upraktisk for vannkraftens komplekse systemer. En slik dublering av flere IEDer setter igang en tidkrevende og lite praktisk oppdeling av anbud for kontrollanleggene. Per idag er det normal å forholde seg til én leverandør, som sikrer funksjonaliteten i hele kontrollanlegget. Ved innblanding av flere leverandører risikerer kravtverkseier at enkelte funksjoner faller mellom leverandøreres ansvar, og risiko for feil og konflikter øker. Av den grunn vurderes leverandøruavhengighet i det lokale kontrollanlegget som overflødig om kun én leverandør benyttes.

8.4 Konklusjon av løsning for topologi og protokoller

Siden prosesser i vannkraftverket er optimalisert gjennom hundrevis av år, ligger de største fordelene framover i digitalisering og effektiv databehandling for predikert vedlikehold og optimalisert kjøring av vannkraftverket.

Sentralt for alle løsninger som er presentert er et standardisert tagsystem med IEC 61850 på signalnivå og RDS for lokalisasjon. Dette er et ferdigutviklet system, tilpasset vannkraft gjennom IEC 61850-7-410 og IEC 61850-7-510. Standardiserte signal åpner for effektiv analyse og maskinlæring for smart styring av prosesser.

Dagens IP-baserte protokoller, slik som Profinet, er bedre testet for vannkraft og kan gi lik funksjonalitet som IEC 61850, som kommunikasjonsprotokoll, siden begge baseres på Ethernet. IEC 61850 foreslår også en oppdeling av funksjonalitet i flere IEDer, noe som gir økt kostnad basert på flere installerte komponenter og kabler i anlegget. Ved bruk av IP-protokoller og ET, for distribuert I/O, med dagens PLS-løsning for styring, forenkles installasjonen og kostnadene minker for kontrollanlegget. Samtidig er løsningen godt testet og kan enkelt implementeres i eksisterende anlegg.

OPC-UA Server er en sentral SW i alle løsninger som er presentert. OPC-UA gir grunnlag for hybride systemer og leverandøruavhengighet. I tillegg åpner SW løsninger for cybersikkerhet, kompatibilitet med utdaterte og ulike operativsystemer, og ulike kommunikasjonsprotokoller. OPC-løsninger kan simuleres, og derfor testes grundig før implementering. Standarden har stor interesse i industrien, og det forutsettes at OPC-UA utvikles som en sentral brikke i digitalisering av industrien.

9 PILOTPROSJEKT RØDBERG

Bachelorgruppen fikk mot tampen av prosjektperioden mulighet til å ta fatt, og se på hvordan man kunne bygge om et spesifikt anlegg basert på teknologi som studien hadde undersøkt. Rødberg Kraftverk ble ferdigstilt i 2009, men er kandidat for ombygging på grunn av manglende service og supportmulighet fra leverandør. Utstyr og hardware vil derfor, i så stor grad som mulig, vurderes å brukes videre basert på kriterier som Statkraft selv har satt når det kommer til sikkerhet, leverandøruavhengighet og pålitelighet mm. Eventuelt kan det suppleres for å oppnå ønsket konfigurasjon og egenskaper. Denne tilnærmingen vil ikke bare være bærekraftig, men også være med på å vise hvordan ny teknologi kan tas i bruk i eksisterende anlegg uten behov for massive ombygginger. For å klare dette på optimalt vis, ble det avsatt arbeidstimer for å kartlegge funksjonalitet til, det hittil, ukjente kontrollanlegget. Bachelorgruppen vil dokumentere og se på forskjell fra dagens til en alternativ løsning. For Rødberg spesielt, gitt kraftverkets fysiske størrelse, vil ikke alle forslag være økonomisk forsvarlig. Poenget er heller å bruke denne plattformen til å kunne inkludere ny teknologi som et pilotprosjekt som senere kan tas i bruk i større skala. Under drift kan en også få videre erfaringer og kunnskap som vil komme til gode i ettertid.

Det er gjort undersøkelser av komponenter som er tilgjengelige ved Rødberg. Flere måleinstrument og relé for elektrisk beskyttelse av typen VAMP ved Rødberg er allerede kompatibel med IEC 61850 og kan enkelt tas ibruk med en ny konfigurering opp imot IEC 61850. Dette gjelder:

- 4 stk multimeter (VAMP 96)
- 1 stk spenningsrelé ved samleskinne (VAMP 135)
- 2 stk overstrøm- og kortslutningsvern ved samleskinne og transformatorbryter (VAMP 140)
- 1 stk generatorvern (VAMP 210)
- 1 stk differensialvern ved transformator (VAMP 265)

Fordeler med overgang fra MODBUS TCP til IEC 61850 ved disse komponentene er rask interaksjon ved hjelp av SV- og GOOSE-protokoll ved prosessbussen, og publisher/subscriber forhold mellom vern med lik utløserfunksjon, slik at man oppnår redundans.

Redundans gjennom publisher/subscriber kan oppnås for generatorutkobling mellom:

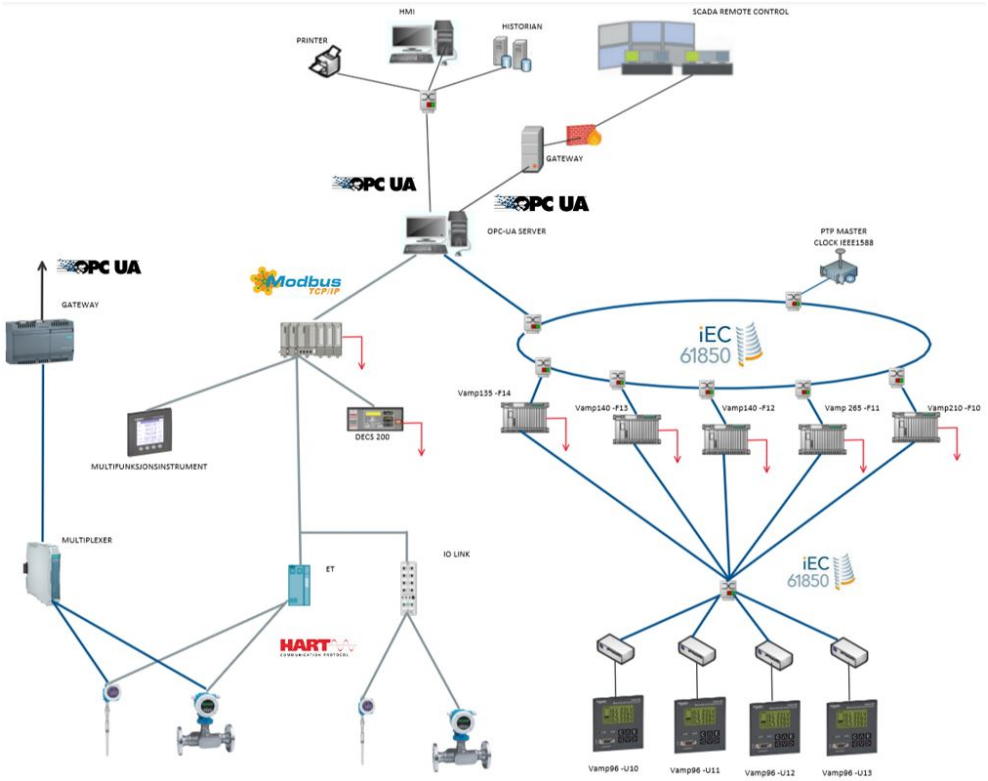
- VAMP 135
- VAMP 210
- VAMP 265

Redundans gjennom publisher/subscriber kan oppnås for effektbryter utkobling mellom:

- VAMP 135
- VAMP 140

Når det gjelder styresystemet i kontrollanlegget er det idag en PLS fra ABB med en forenklet spenningsregulator for magnetisering. Styresystemet benytter Modbus TCP som kommunikasjonsprotokoll. Dette tilsvarer tidligere presentert løsning for hybrid, med delvis implementering av IEC 61850. IP-protokollen gir en rekke fordeler som tidligere er nevnt.

For sammenkobling av det hybride kontrollanlegget skal en OPC-UA Server håndtere mapping mellom protokollene. OPC-UA kan også derfor testes som kommunikasjonsprotokoll opp imot driftssentral.



Figur 46: Topologi for nytt kontrollanlegg ved Rødberg

Kontrollanlegget bygges parallelt, så langt som mulig, med eksisterende styring for å holde anlegget i drift under pilotprosjektet. Dette er for å sikre driften og utnytte kraftverket som inntektskilde. En generator på 3,2MW tilsvarer i teorien 28GWh i årsproduksjon ved konstant kjøring. På grunn av tider med stopp i produksjonen var årsproduksjonen ved Rødberg i 2020 15GWh [74]. Med gjennomsnittlig spotpris for 2020 på 20,7 øre/kWh antas årsinntekten ved Rødberg i 2020 å være rundt 3,1 millioner kroner [75]. Det er et småkraftverk, men relestyringen kan gjøre pilotprosjektet mindre kostbart ved å produsere strøm under utprøving av nye systemer.

Ved testing av det nye kontrollanlegget kan forriglinger sammenkoble styring fra rele og det nye kontrollanlegget. Releanlegget kan overstyre det nye om feil skulle oppstå. Og omvendt kan stoppsekvenser blokkeres av fra det nye under bygging og testing. Blokkering kan oppheves ved stopptest. Når det gjelder vern, kan disse simuleres ved hjelp av SW-løsninger presentert tidligere, og idriftsettes umiddelbart.

10 CYBERSIKKERHET

Verden blir mer og mer sammenkoblet og digitalisert, og det skaper en del utfordringer når det kommer til OT- og IT-sikkerhet. Cybersikkerhet rundt kraft og energisektoren blir bare viktigere ettersom den er utsatt og svært sårbar for nettangrep. Et mulig angrep på et kontrollsystem til et kraftverk kan føre til alvorlige konsekvenser. Dagens systemer må designes slik at det sikrer all kommunikasjon og data. De viktigste målene for å sikre informasjonssystemene bør være: konfidensialitet, integritet og datasikkerhet. Oppbygningen og designet av kommunikasjonsnettverket i et kontrollsystem vurderes nøye for å få det best mulig sikret mot et cyberangrep. Anlegg må være i henhold til "forskriften om sikkerhet og beredskap i kraftforsyningen (kraftberedskapforskriften)", som har følgende formål: "*Innenfor formålene i energiloven § 1-2, skal forskriften sikre at kraftforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene*" [27]. Oppbygging av anlegget bør være henhold i IEC 62443 og IEC 62351. IEC 62443 er standard designet for å sikre OT-systemene, og brukes i alle operative tekniske systemer fra kraftstasjoner og produksjonsanlegg til sykehus og offentlig transport. IEC 62351 er den standarden som er utformet for å gi en veiledning for å ivareta sikkerhet i systemer og operasjoner før byggingen har startet, slik at slipper å sette igang nye sikkerhetstiltak etter at systemene er implementert.

Typiske angrep mot et industrielt kontrollsystem er [77]:

- Ransomware
  En skadelig programvare i form av løsepengevirus, utpressingsprogramvare eller gisselvare som krypterer deler av en infisert datamaskin slik at det er utilgjengelig for eieren for så å utpresse for løsepenger.
- Malware
  Et begrep som brukes for beskrive skadelig programvare som spionprogramvare, løseprogramvare, virus og ormer. I kontrollsystemsammenheng kan en slik trussel forstyrre visse komponenter og gjøre et system ubrukelig.
- Phishing
  En praksis for å sende falske kommunikasjoner som ser ut til å komme fra en anerkjent kilde med mål om å stjele sensitiv data som for eksempel passord.
- DDos
  Et sofistikerte angrep designet for å oversvømme nettverket med overflødig trafikk, og kan medføre i svekket nettverksytelse eller direkte avbrudd.
- Zero-day exploit
  En null-dagers utnyttelse treffer etter at et nettverksproblem er kunngjort, men før en oppdatering eller løsning er implementert. Angripere retter seg mot det avslørte sårbarheten i løpet av dette tidsvinduet.

Et eksempel er cyberangrep i Ukraina i 2015, hvor de tok kontroll over kritisk infrastruktur [39]. Hackerene klarte å komme seg helt inn i kjernen av systemet og tok kontroll over både SCADA-systemet og HMI. I cyberangrepet kom hackerene seg inn i 3 forskjellige kraftleverandører og kontrollsystemet deres som førte til at over 250 000 mennesker var uten strøm.

Et annet eksempel var da Norsk Hydro ble utsatt for et omfattenede cyberangrep mot flere av selskapetes forretningsområder [28]. Hydro ble utsatt for var et Ransomware-angrep kombinert med et angrep mot Active Directory (AD), hvor IT-nettverket til 35 tusen ansatte fordelt på 40 forskjellige land ble berørt. Angrepet skal ha kostet Hydro rundt 300 til 350 millioner kroner.

Det finnes en rekke ulike løsninger for sikre systemer for cyberangrep, hvor de kan kombineres og brukes på forskjellige områder. I dette kapittelet vil det legges vekt på en del løsninger for cybersikkerhet, hvordan de fungerer og hvordan de kan kombineres for å sikre kontrollanlegget på best mulig måte.

10.1 Kommunikasjon mot tredjepart

Ved at verden blir bare mer og mer digitalisert inkludert kontrollsystemene til kraftverk gjør at bruk av data fra disse blir mer populært. For optimalisering av drift og vedlikehold og diagnosering er det viktig å få ut data og informasjon fra kraftverket. For å åpne tilgjengeligheten av denne informasjonen kommer det en del utfordringer knyttet til sikkerthet. Dette er på grunn av at en tredjepart tilkoblet kraftverkets OT- og IT-nettverk kan være svært risikofult, ved at en tredjepart kan være et svakt ledd og deremed bakveien inn i nettverket. Dette delkapittelet baserer seg på å sikre kommunikasjonen og fjernstyringen til en tredjepart på den mest optimale og sikreste måte.

10.1.1 Brannmur: Blacklisting/Whitelisting

En brannmur er en mekanisme som brukes til å kontrollere tilgang til og fra et nettverk og beskytte tilknyttet datamaskiner for uautorisert bruk [9]. Brannmuren håndhever en tilgangspolicy ved at den bruker mekanismer som enten blokkerer eller tillater (blacklisting/whitelisting) visse type trafikk, og dermed regulerer strømmen av informasjon. Ved bruk av whitelisting blokkeres all trafikk bortsett fra f.eks. IEC 61850, IEC 104 eller andre protokoller som har fått godkjennelse. Blacklisting derimot blokker kun trafikk fra gitte protokoller. Brannmuren blokkerer vanligvis trafikk fra utsiden av et beskyttet område til innsiden av et beskyttet område, brukere på innsiden tillater å kommunisere med eksterne tjenester. Hovedoppgavene til en brannmur er å begrense data til/fra OT-nettverket, logge vellykkede/mislykkede transaksjoner gjennom brannmuren og samhandle nettverk som ikke er designet for å gjøre det.

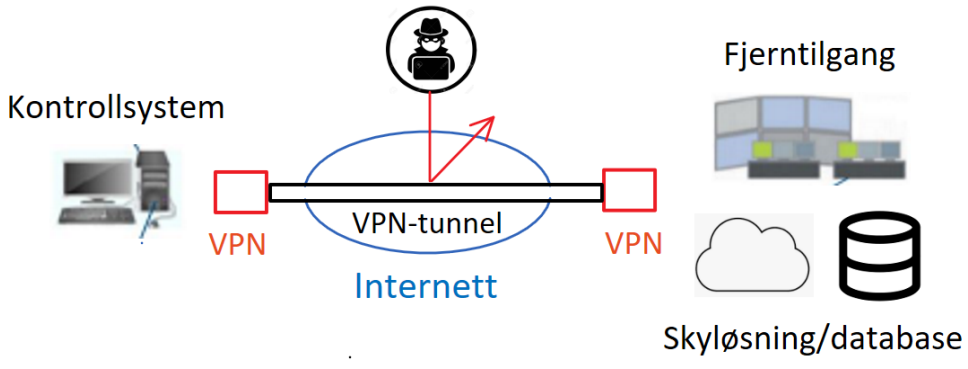
En brannmur er ikke løsingen på alle innbruddsproblemer i et industrielt kontrollanlegg. Svakhetene ved en brannmur er at den ikke er designet for alle applikasjoner i et kontrollanlegg og kan dermed gjøre det vanskelig å skreddersy filtreringen for optimal sikkerhet. Brannmurer har også utviklet seg veldig mye og kan kreve spesial kompetanse for å designe. Bruk av brannmur i sammenheng med kontrollsystem bør starte med å sette opp brannmurkonfigurasjonen for å nekte all trafikk, og deretter se på trafikken som kreves og bare tillate det eksplisitt.

10.1.2 VPN - Virtual Private Network

Virtuelt privat nettverk [9] er et datanettverk som overfører data i punkt-til-punkt forbindelser som en slags tunnel, og kapslet inn i en form av kryptering. Denne løsningen beskytter data fra det offentlige internettet og er en god beskyttelse for typiske MitM-angrep. VPN er mye brukt for å sikre fjerntilgang til kontrollsystemet og sikre data fra OT-nettverket til IT-nettverket. VPN består av tre sikkerhetskomponenter: Autentisert og autorisert, integritet og konfidensialitet. Ved disse komponentene fastslår gyldigheten av en overføring for å verifisere personens autorisasjon, beskytter mot uautorisert modifikasjon av informasjon og forsikrer at informasjon ikke blir levert til uautoriserte personer eller enheter.
Det finnes tre klassifiseringer for VPN:

- Sikkerhetsport til sikkeretsport: Sender data fra et pålitelig nettverk til et annet pålitelig nettverk, mens VPN sikrer trafikken via det usikrede nettverket. Denne typen VPN kalles LAN-LAN VPN.
- Vert til sikker Gateway: Den ene enden består av en vertskomputer og den andre enden er et sikkert nettverk, VPN sikrer trafikken via det usikrede nettverket. Det kalles ofte for VPN for ekstern tilgang.
- Vert til vert: Hvert endepunkt i VPN-tunnelen er en vertkomputer og VPN sikrer kommunikasjonen via det usikrede nettverket.

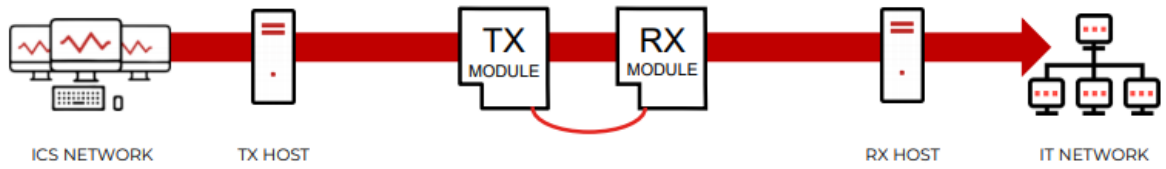
Ved at VPN er SW-basert løsning har den en del sårbarheter og kan være utsatt for cyberangrep. En tredjepart som er tilkoblet for ekstern tilgang kan være svært risikofylt med tanke på cyberangrep, ved at en hacker kan komme seg inn via tredjeparten. Hvis en hacker først har kommet seg inn, beskytter VPN ingenting for at en hacker kommer seg videre til andre systemer som er koblet til samme VPN. Den krypterer like lett et angrep som annet data. På grunn av dette kan VPN fungere som en bakdør inn til OT- og IT-nettverket via en tredjepart.



Figur 47: Prinsippfigur av VPN-tunnel

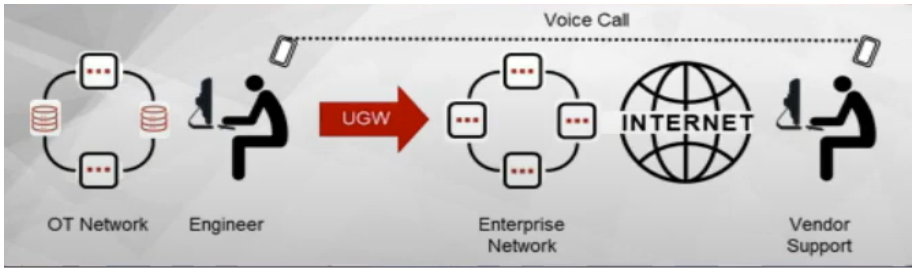
10.1.3 UGW - Unidirectional Gateway

Waterfall Security leverer en løsning kalt Unidirectional Gateway [85] som er en ensrettet gateway hvor data kun kan sendes i én retning. Løsningen består av både HW- og SW-komponenter. HW-komponentene består av en TX-modul som inneholder en fiberoptisk sender, en fiberoptisk kabel og en RX-modul som innholder en fiberoptisk mottaker. SW'en består av TX-host som samler data fra de industrielle serverene og komponentene i kontrollsystemets OT-nettverk, og en RX-host som replikerer og emulerer et data fra industrielle servere, enheter og protokoller til IT-nettverket. Ved et mulig cyberangrep vil kun IT-nettverket bli påvirket og ikke OT-nettverket. En hacker kommer seg kun inn i en database og ikke kraftstasjonen i seg selv, som gjør at kraftstasjonen vil fungere som normalt uten noen form for trussel. Denne løsningen gir 100 prosent beskyttelse mot cyberangrep, ved at der er fysisk umulig å sende data tilbake fra internettet til det industrielle nettverket inne i et kraftverk. Det vil si den gir kun tilgang til data fra systemet og ikke direkte tilgang til systemet.



Figur 48: Prinsippfigur på en Unidirectional Gateway [85]

Remote Screen View
Remote Screen View [84] er en skjermdelings-løsning innenfor UGW og er nytting om en driftsoperatør inne i kraftstasjonen støter på et problem hvor det behøves assistanse fra en leverandør eller tredjepart. Driftsoperatøren skrur på skjermdeling, ringer til supporttekniker hos leverandøren via en mobiltelefon og ber han koble seg til. Skjermdelings-tjenesten tar video av driftsoperatørens skjerm og sender til supportteknikerens skjerm gjennom en UGW. Supportteknikeren kan kun se hva som se på driftoperatørens skjerm men ikke gjøre endringer, han blir nødt til å veilede igjennom mobiltelefonen. Dette skaper en form for sikkerhet ved at driftsoperatøren vet hvilke endringer som blir gjort i systemet ved at han gjør de selv.



Figur 49: Prinsippfigur på en skjermdeling [84]

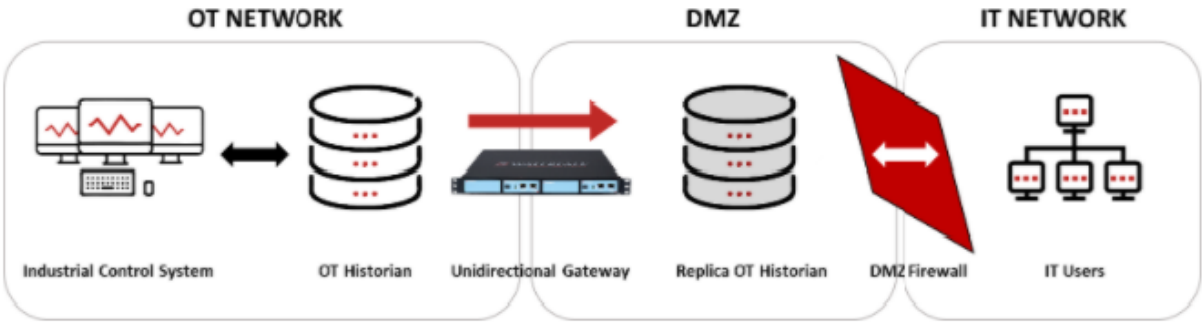
Secure Bypass

En Secure Bypass [83] er en løsning som kan brukes i parallell med en UGW for å gi en sikker kommunikasjon inn til det industrielle nettverket i en kraftstasjon. Den fysiske løsningen gir kontroll over når aktørere utenfor kraftverket kan koble seg opp mot kraftverkets nettverk. Enheten gir en fysisk kobling med elektromagneter som aktiveres ved å vri om en nøkkel. Når nøkkelen er vridd om i aktivert posisjon åpnes det for datakommunikasjon i begge retninger. Løsningen er tiltenkt å brukes til nødstilfeller hvor det trengs at kraftstasjonen må kobles opp mot support for å fikse et problem via fjernstyring, og kun opp mot klarerte supportteknikere. Etter det nødvendige er gjort vris nøkkelen tilbake og den fysiske kontakten blir brutt. Modulen kan også programmeres slik at den bryter kontakten etter et gitt tidsrom. UGW fungerer som normalt mens Secure bypass-modulen er aktivert.

Figur 50: Prisippfigur på en Secure Bypass [83]

10.1.4 DMZ - demilitarized zone

DMZ er en demilitarisert sone, også kjent som omkretsnettverk eller et skjermet subnettverk. Det er i hovedsak et nettverk mellom et nettverk, og i vårt tilfelle et nettverkslag mellom OT, ICS eller SCADA mot det mot det mindre sikrede IT-nettverket [95]. Moderne industriell DMZ fungerer som et sone- og ledningssystem som beskytter fysiske prosesser og skiller nettverk i henhold til deres forskjellige formål, krav og risiko. En måte å designe en DMZ er å plassere to brannmurer, en mellom OT-nettverket og DMZ-nettverk, og en mellom IT-nettverket og DMZ-nettverket. Ved å designe det på denne måten reduseres sannsynligheten for at det åpnes en angrepsvei rett inn i kontrollsystemets nettverk ved en mulig SW-feil i brannmuren. Fra et angrepsperspektiv kan det være enkelt å stjele et brannmur-passord eller et passord på IT-nettverket som er klarert for OT-nettverket og en angriper kan komme seg rett inn i systemene i DMZ. I dette tilfelle hjelper det ikke å ha to brannmurer. En mer moderne måte er å beskytte den ene siden av IT/OT DMZ med å sette inn en Undirectional Gateway for å replikere OT-systemet til IT-nettverket. En OT-database replikeres og sendes via det ensrettede nettverket hvor den lagres på en replika-server inne i DMZ, der IT-nettverket får tilgang til serveren igjennom en brannmur. Dette blir langt mer sikker løsning da to brannmurer i seg selv ikke er en tilstrekkelig løsning for sikring av angrep inn til OT-nettverket.

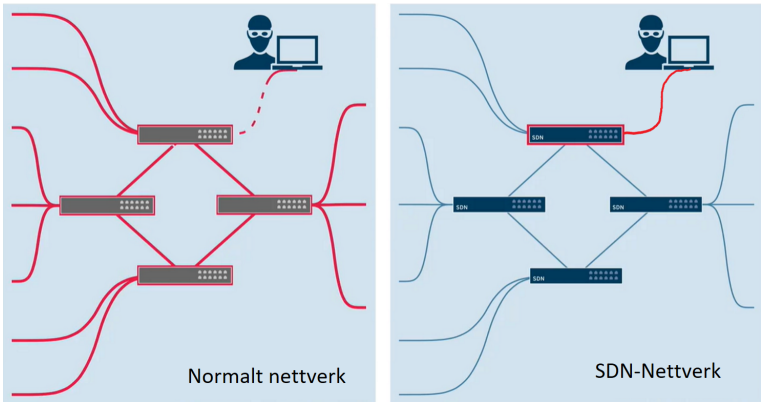


Figur 51: Prisippfigur på DMZ med en Undirectional Gateway [95]

10.1.5 SDN - Software Defined Networking

En programdefinert nettverksteknologi er en tilnærming til en nettverksadministasjon som muliggjør for dynamisk og effektiv programmerbar nettverkskonfigurasjon. Et IEC 61850-basert system trenger et robust nettverk for å sikre uavbrutt beskyttelse. SDN er en løsning som eliminerer en del begrensninger til et tradisjonelt Ethernet-nettverk. Systemet kan reparere seg selv ved brudd i løpet av få millisekunder, håndtere store mengder datatrafikk og øke cybersikkerheten, sammenlignet med et konvensjonelle Ethernet-svitsjer [82]. SDN styrker også cybersikkerheten ved å benytte en deny-by-default-arkitektur der kommunikasjon bare blir videresendt hvis de samsvarer med et strengt sett med forhåndsdefinerte regler. Dette gir et ekstra lag med forsvar som forhindrer skadelig programvare eller annen uautorisert trafikk i å reise innenfor nettstasjonen. Ved et mulig cyberangrep forhindrer SDN at trusselen sprer seg til andre enheter som er koblet til samme nettverk.

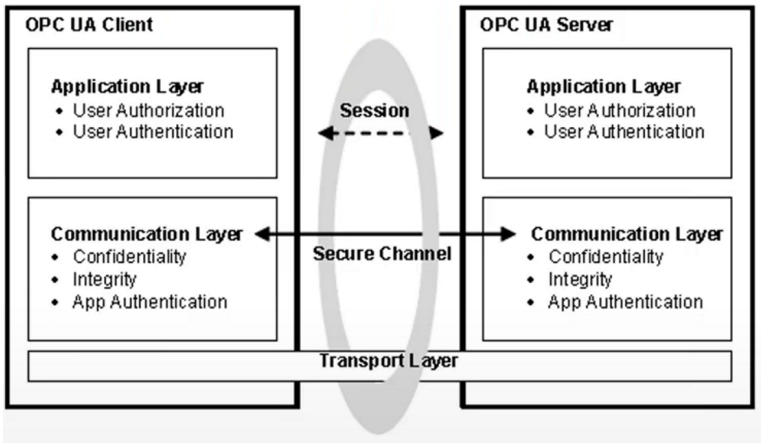
Sintef har gått sammen med NTNU i et prosjekt som kalles SDN microSense [67]. Prosjektet dreier seg om utprøving av SDN baserte metoder for å sikre elektriske nett og kraftproduksjon. Ved å ta i bruk SDN-basert teknologi vil prosjektet utvikle en trelags sikkerhetsarkitektur ved å distribuere og implementere risikovurderingsprosesser, selvhelende egenskaper, store distribuerte deteksjons- og forebyggingsmekanismer, i tillegg til et ekstra lag for beskyttelse av personvern. Målsetningen med prosjekte er å kunne tilby en rekke verktøy mot cyberangrep som sikerer normal drift av kraftverk, og integriteten og konfidensialiteten til kommunikasjonen.



Figur 52: Prisippfigur for cyberangrep mot SDN, angrepet blir stoppet i første punkt. [82]

10.1.6 OPC UA

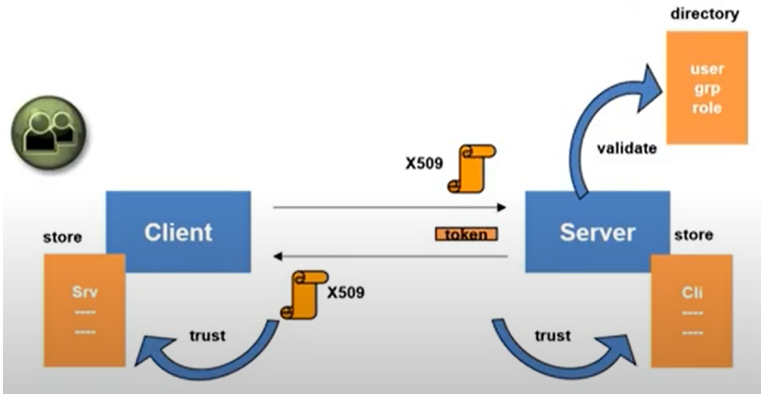
OPC UA er en protokoll som brukes mellom komponenter i driften av industrianlegg fra flere nivåer [63]. Prokollen vil bli distribuert i varierte valg av operasjonelle miljøer med varierende tilgjengelighet og trusler. OPC UA gir derfor et sett med fleksible sikkerhetsmekanismer. Den nye OPC UA-teknologien integrer sikkerhet på forskjellige måter og gir sikkerhet i designet. Kjernearkitekturen til OPC UA baserer seg på sikkerhetsprinsipper som klarert informasjon i form av konfidensialitet, integritet og tilgjengelighet. I tillegg prinsipper for adgangskontroll som autentisering, autorisering og loggføring. Dette skilles mellom to lag for sikkerhet, et applikasjonslag og et transport -og kommunikasjonslag.



Figur 53: Lagfordeling i OPC UA [63]

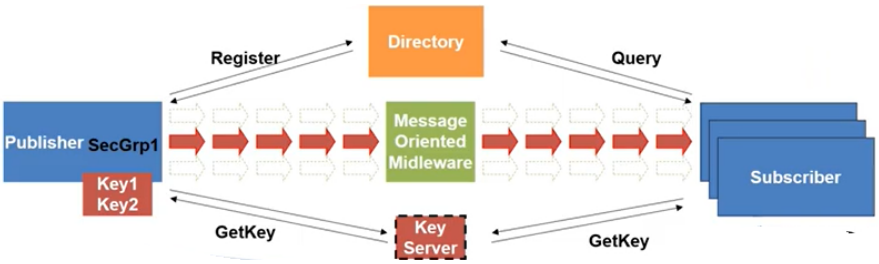
Applikasjonslaget inneholder flere sikkerhetsmekanismer. Brukere eller operatører av et program/system kan indentifiseres med bruk av brukernavn og passord eller et brukersertifikat. Tilgangsnivået kan justeres for hver enkelt node, og dermed kontrollere brukertilgangen. For eksempel kan en bruker bare få tilgang til å se verdier, mens en annen bruker med høyere tilgangsnivå har tilgang til redigering eller gjøre endringer, og en gjest kanskje ikke har tilgang til noden i hele tatt. I tillegg er det revisjonsmekanisme som loggfører hvilken bruker som endret hvilke verdier på det tidspunktet. Funksjonene er integrerte deler av spesifikasjonen og sikkerheten vil derfor ikke være valgfri.

Transport -og kommunikasjonslaget i OPC UA baseres seg på forsvar i dybdekonsept, som vil si flere sikkerhetsmekanismer, demilitariserte soner og brannmurer [63]. OPC UA har innbakt end-to-end sikkerhet som er basert på allerede etablerte standarder som AES, RSA, SHA og ECC. For sikkerhet i kommunikasjon og transport mellom klient/server kan det brukes Public Key Infrastructure (PKI) og asymmetrisk algoritme-utvekslings nøkler. Nøklene brukes til kommunikasjon med symmetriske algoritmer og de blir ofte rotert. For autentisering brukes x509-sertifikater. OPC UA servere identifiserer hvilke kryptiske algoritmer de støtter, og klienter velger hvilke de ønsker å bruke når de kobler seg til serveren.



Figur 54: Prinsippfigur for klient/server [44]

Publish/Subscribe (PubSub) er en end-to-end sikkerhetsmetode som brukes i OPC UA som baserer seg på krypteringsnøkler. Nøkler blir delt mellom utgivere og abonnenter, og blir administrert av en sikkerhetsgruppe. Nøkkelfordelingen gjøres med OPC UA klient/server-sikkerhetsprosedyre, og det skjer en autentisering og autorisering under tilgang til nøkkelserveren. PubSub kan utplasseres i to miljøer, ett hvor det eksisterer en megler og hvor ett som er meglerfri [63]. I et meglerløst PubSub-kommunikasjonsmodell oppnåes konfidensialitet og integritet ved bruk av symmetrisk kryptering og signaturalgoritmer, og de nødvendige nøklene distribueres via en Security Key Server (SKS). Når det brukes en megler så brukes samme det samme modellen som en meglerfri, men også kommunikasjonen til megler kan sikres i henhold til regler som blir definert for megleren.



Figur 55: Prinsippfigur for PubSub [44]

10.2 Adgangskontroll

Adgangskontroll bør vurderes for å ha kontroll på utførelse av kontrolldrift av autorisert operatører, og for å unngå feil drift, ulovlig drift, og ulovlig datatilgang. Generelt bør brukeren identifiseres og autentiseres for å få tilgang til systemet. Adgangskontroll basert på autorisasjon av roller bør brukes for å definer forskjellige kontrollområder og tilordne personers roller i henhold til deres arbeidsbehov.

10.2.1 RBAC - Role Based Access Control

I store organisasjoner og bedrifter finnes det hundrevis av brukere og tusenvis av tillatelser til forskjellige operasjoner. Da er det viktig å ha en god struktur på tilgangskontroll for å bevare sikkerheten. Rollebasert tilgangskontroll er en tilnærming for å begrense systemtilgangen til autoriserte brukere, og kan brukes til å sikre nettverk og applikasjoner i kontrollanlegget til blant annet kraftverk. Systemet designes slik at det opprettes roller for ulike jobbfunksjoner, og tillatelser til å utføre visse operasjoner blir tildelt de ulike rollene [88]. Ansatte eller medlemmer tildeles bestemte roller og gjennom rollene skaffes de tillatelsene som er nødvendig for å utføre operasjonene. Et problem med rollebasert tilgangskontroll er interferens når flere brukere har dynamisk tilgangsnivåer. Det kan føre til ustabilitet i krypteringsnøkkel, som kan utnyttes av en ekstern bruker med uautorisert tilgang. Dette problemet kan løses ved å ha nøkkel-delingsapplikasjoner i dynamiske virtuelle miljøer.
Tre hovedregler for RBAC:

1. Rolletildeling: Et emne kan kun utøve en tillatelse hvis emnet har valgt eller fått rolle.
2. Rolletillatelse: Fagets aktive rolle må godkjennes for faget. Regel 1 sikrer denne regelen for at brukere bare kan ta på seg roller de er autorisert for.
3. Tillatelsesautorisasjon: Et emne kan kun utøve en tillatelse hvis tillatelsen er autorisert for fagets aktive rolle. Med regel 1 og 2 sikrer denne regelen at brukere bare kan utøve tillatelser der autorisert for.

RBAC kan også bygges opp med ytterlige regler, hvor roller kan kombineres i et hierarki der roller på høyere nivåer overtar tillatelser som eies av underroller.

10.3 Kommunikasjon mot driftssentral

Et kraftverk er koblet opp mot en driftssentral for å kunne driftes og fjernstyres uten bemanning av stasjonen. For fjernstyring av kraftverk og transformatorstasjoner brukes kommunikasjonsprotokollen IEC 60870-5-104 (IEC 104). IEC 104 er basert på IEC 60870-5-101 (IEC 101), som er en protokoll for telekontroll i automatiseringsapplikasjoner i kraftsystemer. IEC 104 gir nettverkstilgang til IEC 101, og dermed muliggjør for kommunikasjon mellom kontrollstasjon og en driftssentral via et standard TCP / IP-nettverk. Mer detaljert beskrivelse er forklart i delkapittel 6.7. Kommunikasjonen overføres via TCP/IP nettverk og for sikkerhetsårsaker blir overføring gjort på et dedikert lukket nettverk (ref møte med Voith og Statkraft Tyskland). Det dedikerte nettverket vil være et eget fysisk lukket nettverk med galvanisk skiller. Sikkerhetstrusselen mot en driftssentral og kommunikasjonskanalen til et kraftverk vil være svært lav på grunn av det lukkede nettverket, og en driftssentral er godt sikret.

Generelt er det en rekke sikkerhetsproblemer ved funksjonaliteten til IEC-104 er basert på TCP/IP. IEC 104 definerer ingen sikkerhet som passord for tilgang, autentisering eller kryptering. Dette danner en alvorlig sårbarhet mot IEC 104-kommunikasjon, spesielt når den overføres over usikkert IP-lag.

Mulige angrep på IEC 104-kommunikasjon kan omfatte:

- Endre verdien av en ASDU overført i IEC 104-pakken.
- Sette inn falske ADSU-meldinger i nettverket.
- Gi DDoS-angrep.
- Avlytting av de overførte dataene.

På grunn av disse sårbarheten og mulige angrep egner ikke IEC 104 i et usikret nettverk. Det er mulig å redusere disse truslene med kommunikasjonen og autentisering ved å implementere End-to-End VPN og brannmurer.

10.4 Sikkerhetssoner

Figur 56 brukes som en modell til å vurdere cybersikkerheten til automatisering- og kontrollsystemet. Figuren bryter ned arkitekturen til soner og sammenkoblinger [16]. Kontrollsystemet brytes ned i fem hovedsoner: Prosesskontroll-sone, sentralisert driftssone, utenforliggende driftssentralsone, mellomliggende sone og informasjonssone. Prosesskontroll-sonen er igjen delt opp i tre soner: Utstyrssone, lokal kontrollsone, sentralisert kontrollsone og transformatorens kontrollsone. Den utenforliggende driftssentralsonen og transformatorens kontrollsone ligger utenfor omfanget for dette kontrollanlegget. Sonene er klassifisert etter tre sikkerhetsnivåer: Høy, middels og lav.

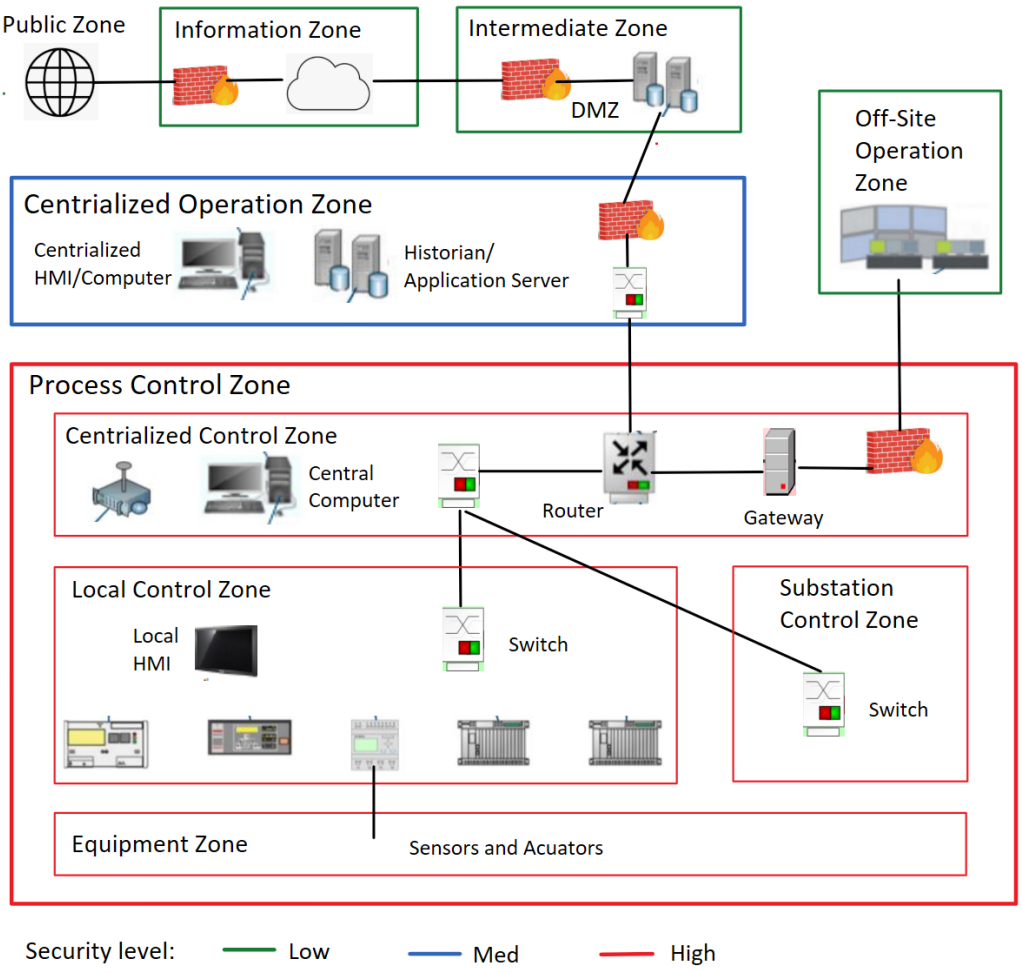
Prosesskontroll-sonen har det tidskritiske nettverket som kobler sammen automatiseringskomponenter, stasjonsdatamaskin og lokal HMI. Sonen er i den industrielle delen av kraftstasjonen og alle de tre sonene går under denne sonen siden de har samme sikkerhetsnivå. Sonen er klassifisert sikkerhetsnivå høy, på grunn av konsekvensene er drastiske ved tap av datakommunikasjon og automatiseringsfunksjoner.

Den sentraliserte kontrollsonen har nettverket som kobler sammen automasjonssystemet til historikkdatabase, applikasjonsserveren og operasjonskonsoller (HMI). Denne sonen har normalt fysisk adgangskontroll, som kun autoriserte personal har adgang til. Sonen er som regel plassert på kraftstasjonen, for eksempel et operasjonsrom eller utsendelsesrom. Den klassifiseres med sikkerhetsnivå middels.

Utenforliggende driftssentralsonen ligger utenfor kraftstasjonen og er utenfor omfanget. Denne sonen er beregnet som lav risiko på grunn av den er godt sikret og kommunikasjonen går igjennom et dedikert lukket nettverk.

Den mellomliggende sonen inneholder en database og blir en industriell demilitarisert sone (DMZ), og klassifisert som lav risiko.

Informasjonssonen har bedriftens nettverk og har forbindelse med den mellomliggende databasen for utveksling av data. Sonen er plassert i kraftstasjonen, og vanligvis i den administrative delen hvor fysisk adgang kontrolleres. Klassifiseres med lavt sikkerhetsnivå fordi en mulig trussel kan kun få adgang til IT-nettverket.



Figur 56: Sikkerhetstruktur for soner og sammenkoblinger

10.5 Konklusjon av cybersikkerhet

For høyest mulig sikkertet vil det mest optimale være å kombinere løsninger som vil fungere som flere sikkerhetsbarrierer. kombinasjonen av HW-løsninger, brannmurer, VPN og andre SW-løsninger kan øke sikkerheten for kontrollanlegget betraktelig. Strukturen vises i figur 57. Det konkluderes med at en leverandør eller tredjepart skal ha tilgang via VPN til selve OT-nettverket og fjernstyring av kontrollanlegget til enhver tid er en svært stor risiko. Dette på grunn av at svakheten ligger i en mulig inntrenger kan komme seg inn via tredjepartsleddet. En leverandør eller tredjepart har stor nytte av få tilgang til data fra en kraftstasjon for å kunne kjøre diagnose eller innhente informasjon fra stasjonen.

En sikker løsning for å muliggjøre dette er en UGW som fungere som en ensrettet gateway og sender kun data en vei. I tillegg muliggjør det med denne løsningen at en supporttekniker fra leverandøren kan hjelpe en driftsoperatør ved feil, via en skjermdelingstjeneste. Supportteknikeren vil ikke ha noen tilgang til systemet, men klarer å veilede driftsoperatøren. Dette blir også en sikrere løsning ved at driftsoperatøren også vet nøyaktig hvilke endringer som gjøres. Samtidig kan UGW kombineres med en Secure Bypass for nødstilfeller, hvor en tredjepart må gjøre endringer systemet og/eller fjernstyre selve kontrollsystemet. Ved at den har en fysisk nøkkel som bryter kommunikasjonen gjør at den kan opprettholde sikkerheten. En VPN-tunnel bør uansett brukes når tredjeparten skal gå inn i systemet via en Secure Bypass. En ulempe med bruk av UGW er du blir bundet til å bruke en Secure Bypass i tillegg, eller så blir det fysisk umulige å få tilgang inn til kontrollsystemet for en tredjepart.

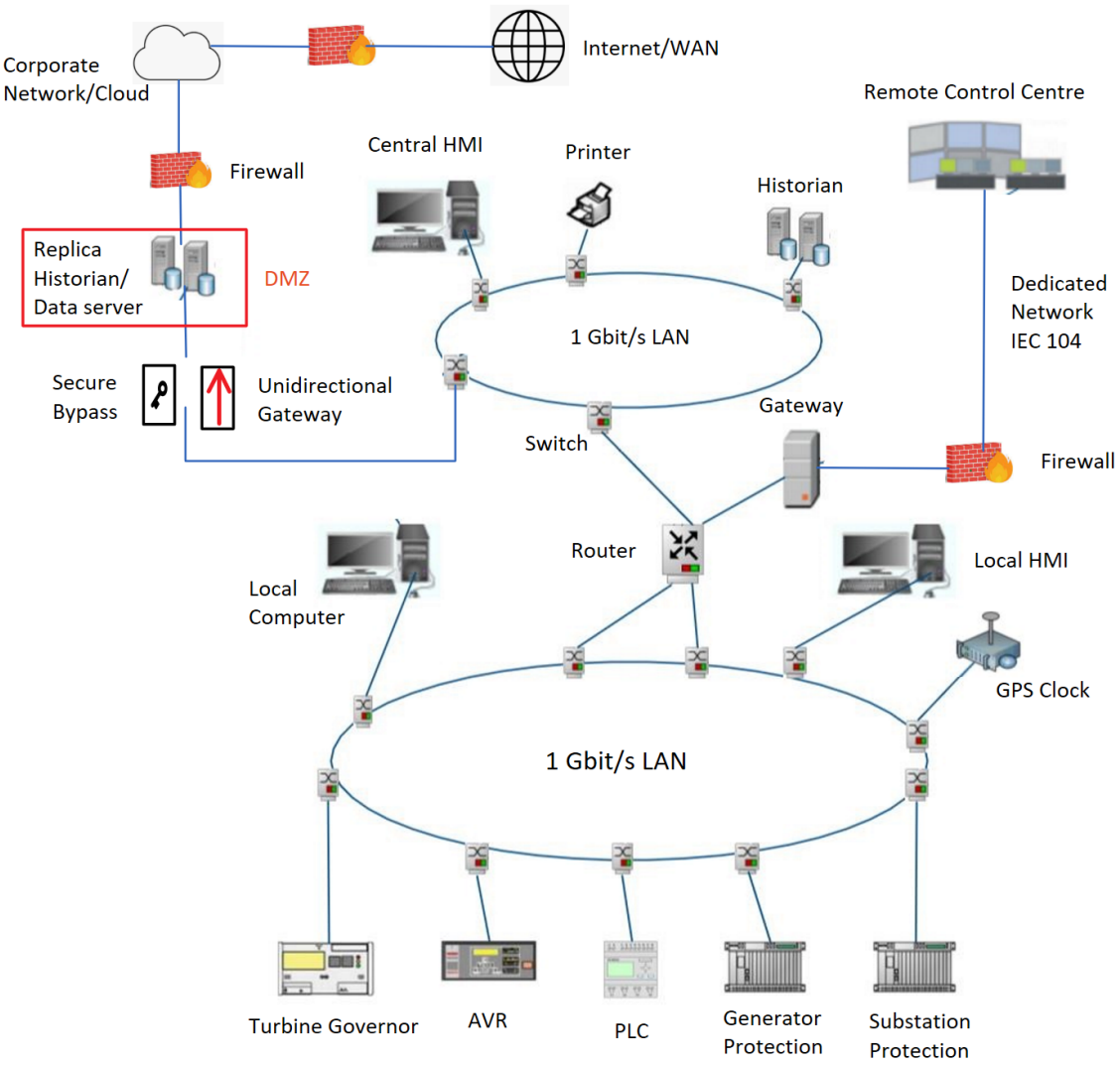
SDN-teknologien virker som ha å potensiale innen sikring av drift og kommunikasjon i et kraftverk. På grunn av at teknologien enda er i utviklingsfasen vil den ikke vurderes som en god nok løsning. Ved gode resultater på testingen og utvikling rundt denne teknologiuen kan det være et godt alternativ for fremtiden.

En god sikkerhetsstrategi vil være å plassere databaser og servere på utsiden av UGW og en i demilitarisert sone (DMZ) mellom OT-nettverket og IT-nettverket til bedriftsnettverket. En kopi av historikk-databasen er å anbefale å plassere i DMZ og denne blir tilgjengelig igjennom en brannmur. Adgangskontroll ved hjelp av RBAC er et godt alternativ for å begrense adgang og tilgjengelighet basert på roller og ansvarsområder.

OPC UA er en mulig løsning med tanke på den har gode sikkerhetsmekanismer for å bevare konfidensialitet, integritet og tilgjengelighet. I tillegg dekker adgangskontrollen i form av autentisering, autorisering og loggføring. Selv om protokollen dekker en del sikkerhetsfunksjoner så anbefales bruken av UGW for sikring av at inntrengere inn i OT-nettverket og kontrollsystemet.

Kommunikasjonen mellom kraftverk og driftssentral anses som svært sikker på grunn av det dedikerte nettverket. Bruken av IEC 104 protokollen for kommunikasjon vil fungere godt så lenge overføringen skjer på et lukket nettverk.

Inndelingen av sikkerhetsoner og klassifisering av sikkerhetsnivåer er viktig for å kunne vurdere sikkerheten i kontrollanlegget. Det blir tydelig hvor de mest kristiske delene av anlegget ligger, og sikkerhetsstrategier kan bygges opp deretter.



Figur 57: Topologi for sikkerhet av nettverk i kontrollanlegg

11 SPESIFIKASJON

Når du skal inngå en ny investering, vil du ofte forholde deg til en spesifikasjon. Dette gjelder når leverandører spesielt skal levere et eller flere anlegg til en kunde. Spesifikasjonen utarbeides av kunden og er en planlagt måte og beskrive noe i detalj. Noe som betyr å beskrive kravspesifikasjonene som kunden ønsker på prosjektene.

Spesifikasjonen blir levert ut til aktuelle leverandører i en anbudskonkurranse. Her beskriver kunden kravene på en detaljert måte som mulig, sånn at leverandøren forstår kravspesifikasjonene rett og at det blir utført på riktig måte. Leverandørene som ønsker å levere et pristilbud til kunden må sørge for at det de leverer er i henhold til kundens kravspesifikasjoner.

Når kunden velger ut leverandørene, så inngår spesifikasjonen som en del av kontrakten med leverandørene. Bruken av en spesifikasjon gjør det mulig for å poengtere hva slags struktur og andre ønsker kunden vil ha fra leverandøren.

Kapittelet er basert på opparbeidet informasjon gjennom prosjektperioden. Informasjonen er fra møter med forskjellige aktører i ulike selskaper som har vært intervjuet. Det er også gitt personlige meninger med egne erfaringer og diskuterte løsninger med bachelorgruppen.

Figur 58: Spesifisert dokumentasjon mellom leverandør og kunde.

11.1 Valg av leverandør

Det er flere kriterier som spiller inn når det kommer til valg av riktige leverandører. Det er ofte 3 hoved kriterier som inngår og det er kompetanse, kvalitet å pris. Kunden ønsker god kvalitet, kompetanse og ikke minst en god pris som fører til lang levetid i vannkraftverket.

Siden selskaper er underlagt loven om offentlig anskaffelser så må de følge anskaffelsesforskriften som dem er lovpålagt å følge. Dette medfølger at dem må gå gjennom en anbudskonkurranse eller en begrenset anbudskonkurranse, som f.eks. har konkurransegrunnlag, kvalifikasjonskrav og kravspesifikasjoner i anbudene.[92]

Det er her kriteriene blir satt på prøve til de ulike leverandørene og kunden finner frem til de beste tilbudene som er tilgjengelig via vekting av all dokumentasjon fra vær av leverandørene.

11.2 Kompetanse

For at leverandøren skal bevise kunden at de har kompetansen innenfor det relevante arbeidet som skal utføres, så må de vise frem dokumentasjon som f.eks, CV'er, bemanningsplan, prosjektorganisasjon, erfaring fra tidligere opprustninger, dedikerte ressurser og en rammeavtale om kunden ønsker dette.

Leverandøren skal kommentere hvordan det skal behandle eventuelle oppsigelser eller ansettelser i rollene som bemanner kundens prosjekt. Det skal også bevise kunden at leveranseevnen ikke skal bli påvirket av dette og de skal sikre at leveranseevnen ikke blir svekket av eventuelle hendelser som kan forekomme i prosjektet.

Teknologien som finnes i dag har en eksponentiell vekst, noe som gjør at større bedrifter har flere fordeler med tanke på kapasiteten de kan bruke til videreutvikling av nye produkter, enn hva de små bedriftene har mulighet til. Det kan være en fordel og prioritere bedrifter som har vært i bransjen i lang tid, sånn at de minker sjansen for at dem forsvinner i løpet av vannkraftverkets livstid.

Det betyr ikke at kraftselskapene ikke burde ta i bruk andre bedrifter, siden det er sentrale til enkelte arbeidsoppgaver i prosjektene. Når det kommer til IEC 61850 standarden, så skal det i teorien være mulig å implementere dette i vannkraftverk i dagens samfunn. Det er bare en mangel på etterspørsel fra kunden og at bedriftene skal begynne å produsere produkter som er spesifikt laget til vannkraftverk som omhandler standarden.

11.3 Kvalitet

Når det kommer til kvalitet, så vil kunden vurdere hva leverandørene tilbyr. Vurderingen som blir utført går ut på hva kunden har i sine krav til spesifikasjoner som det har laget og om det er opprettholdt av leverandøren. Leverandøren skal vise frem kompetanse og dokumentasjon som er relevant for tilbudet. Leverandøren skal gå gjennom tekniske løsninger, serviceintervaller, lagervarer og leveransetider, i tillegg til responstid på henvendelser og leveranser.

Kvaliteten som kunden ønsker, minker når leverandørene har frie tøyler til hvordan det går frem med kvaliteten på produktene og programmene som blir brukt. Kunden bør lage klare krav til spesifikasjonene i anlegget som skal bygges og ha det i fokus hele tiden. Med dette så får kunden strukturen de ønsker og i tillegg til hvordan produktene å programmene skal installeres.

Med dette så er leverandøren låst på hvordan det kan gå frem, med tanke på og følge krav som f.eks. ha en struktur i programmene som en kan kjenne seg igjen i uavhengig hvilket kraftverk man befinner seg i. Det er hensiktsmessig og oppdatere spesifikasjonene jevnlig, sånn at dem ikke blir utdaterte og kan føre til store forbedringer i vannkraftverk framover.

11.4 Pris

Det vil alltid være risiko og usikkerheter som er forbundet med nye investeringer. Med tanke på eksponentiell teknologisk utvikling som gjør at produktene blir byttet ut med nye, som kan føre til at vannkraftanleggene blir utdaterte i løpet av få år. Det kan bety at produktene kan få en kortere levetid og føre til at konkurransene blir stadig hardere for leverandørene.

Leverandørene må være smarte når det kommer til leveringen av et anlegg som burde fungere i 15-20 år frem i tid, uten spesielle oppgraderinger i senere tid. Med tanke på energiprisene fremover så kan det få store betydninger for fremtidige beslutninger når det kommer til det grønne skifte vi er under i dag. Planleggingen og investeringsutgiften kan variere når det kommer til om det er verdt og lage et nytt anlegg, ha en hybrid løsning eller bare beholde det samme anlegget noen år til.

Med tanke på pris så spiller kompetanse og kvalitet en viktig rolle. Kvaliteten på anlegget trenger ikke og være av høyeste kvalitet for å oppnå samme resultat som et anlegg som er billigere. Når gjelder kompetanse, så bør leverandøren installere anlegget riktig første gang sånn at kunden ikke bruker mer penger på å fikse feilene etter dem. Dette spiller en viktig rolle når det kommer til pris i senere tid, ettersom systemet ved en feil kan bli koblet ut og føre til unødvendig vedlikehold, som igjen er tap av penger. Her kan man bruke en lineær beregningsmodell for å finne fram til rett kvalitet og pris. Med tanke på totalkostnaden på et anlegg så er det mye som ligger bak de estimerte prisene. Det er prismatrise, eksempelstasjoner, timepriser, planlegging, produkter, og mye mer.

Den estimerte prisen er teoretisk sett nesten lik den reelle planlagde prisen på anlegget når tilbudet er gitt. Minst mulig delelager fører til bedre likviditet, men ventetiden på en ny del kan fort koste mer enn forventet, ettersom anleggene ikke produserer penger når det er under stans. Med betraktning til deler med kortere levetid enn andre, så kan kunden ha et sentralt varelager som er nært de ulike anleggene i området. Ved bruk av rammeavtaler som gjør anleggene like, så kan det tenke seg at det har en økonomisk fordel.

11.5 Rammeavtale

Rammeavtale er en avtale som er inngått mellom kunde og leverandører. Når kunden og leverandøren går sammen om en rammeavtale så må kunden være fornøyd med avtalen som er inngått. Avtalen som er mellom partene har til formål å fastsette vilkårene for kontraktene som blir tildelt i løpet av rammeavtalens periode.

Det bør være en serviceavtale i rammeavtalen som fastslår hvor lenge avtalen skal være og hvordan arbeidet skal gjennomføres. Rammeavtaler har som hovedregel en maksimal varighet på fire år og det finnes tre forskjellige rammeavtaler.

Den første er basert rundt en enkel leverandør og de to andre gjelder flere leverandører med ulike vilkår. Den ene har fastlagte vilkår, altså parallelle rammeavtaler der det er et krav om minst tre leverandører og den andre er at ikke alle vilkår er fastlagt. [96]

Det kan være bra og ha rammeavtale siden anbudsrunder er tidkrevende og kan føre til mye forandringer rundt fremtidige anlegg. Det bør vær en låst teknisk løsning i rammeavtalen, sånn at anleggene som skal bygges i løpet av avtalen med leverandørene blir mest mulig like. En låst teknisk løsning er at f.eks. at standarden og fremgangsmåten er lik på det ulike anleggene som skal bygges og at den varer i fire år

Kan fokusere på første anlegget som blir laget for å fikse feil og eventuelle mangler, sånn at det går raskere og bygge de andre anleggene. Det skal også være en fabrikktest etter avtale med leverandøren før utstyret blir tatt i bruk.

Hovedgrunnen for å bruke rammeavtaler er basert på mye utbygginger med kjente leverandører og at anleggene som er fra samme tidsperiode ser relativt like ut. Dette gjør at det kan bli mindre leverandøravhegig med tanke på at det er enkelt for drift å holde kontroll og ha en enkel oppfølging med få interne personer.

Rammeavtalen er stort sett ferdig priset, med unntakk fra indeksjustering på priser hvert år. Det kan diskuteres ved venting til neste rammeavtale med endringer om nyere teknologi og andre løsninger som kan være relevante til vannkraftverk.

11.6 Konklusjon av spesifikasjoner

Det vil alltid være risiko og usikkerheter ved nye investeringen. For å få riktige leverandører og at vannkraftverkene skal ha en levetid på 15-20 år eller lengre, så må leverandørene bevise riktig kompetanse og ha bra kvalitet på produktene de leverer.

Kunden går gjennom en anbudskonkurranse og legger frem kravene sine. Det kan være hensiktsmessig og prioritere større bedrifter som har tidligere erfaringer og kan legge frem relevant dokumentasjon til kunden i anbudet. Dette minker sjansen for tidligere ombygginger av at det kan risikere at bedriften forsvinner i anleggets levetid.

Kunden bør fastsette vilkårene for kontraktene som inngår i rammeavtalen. Rammeavtalen bør ha en periode på fire år, ettersom dette er det maksimale de kan ha uten spesielle omstendigheter. Det bør avtales en serviceavtale med leverandørene som er tildelt rammeavtalen. Grunnen til og ha en rammeavtale med leverandørene er for å spare tid og penger med tanke på anbudsrunder.

Spesifikasjonene bør ha en løsning som innebærer en teknisk låst standard, som gjør at anleggene får en slik struktur som kunden ønsker og at det skal være mulig å kjenne seg selv igjen om du er på et annet anlegg. Det bør være klare krav til spesifikasjonene som leverandørene skal holde seg til, ettersom dem er låst på hvordan de kan gå frem.

Det kan gå utover kvaliteten på anlegget om leverandørene får fri tilgang til hvordan de går frem i planleggingen til et nytt eller renovert anlegg, med tanke på og ha en bra struktur i anlegget og programmene som blir installert. Når man har en låst teknisk standard i rammeavtalens periode, så kommer det ikke nye endringer i perioden.

Det er hensiktsmessig og holde spesifikasjonene jevnlig oppdatert og forbedret når rammeavtalen er over. Kunden kan avtale en ny rammeavtale med de samme leverandørene og legger til de spesifikke endringen med ny teknologi og andre relevante løsninger som gjør at vannkraftverket vil fungere bedre. Dette gjør det positivt og bruke rammeavtaler med kjente leverandører og fører mest sannsynlig til at anleggene i en gitt tidsperiode ser relativt like ut med tanke på mye utbygginger og opprustninger i eldre anlegg.

12 KONKLUSJON

Mulighetsstudien kan konkludere med at datainnsamling for analyse fra instrumentering burde legges i parallell med dagens kontrollanlegg for å unngå å komplisere styringen. Samtidig vil den økte datastrømmen ut være separat, som er positivt fra et cybersikkerhetsstandpunkt. Bruk av UGW for utsending av data mot tredjepart vil være den sikreste løsningen på grunn av den fysiske sikkerheten det gir. I tillegg vil det være hensiktsmessig å kombinere UGW med en Secure Bypass slik at muligheten for at en tredjepart skal kunne koble seg inn på OT-nettverket, men kun via en Gateway sikret med en fysisk nøkkelbryter. For å sikre data vil den beste løsningen være å plassere en kopi av historikk-databasen i en DMZ, som kun blir tilgjengelig for en tredjepart gjennom en brannmur.

Et kontrollanlegg med OPC klient/server forhold ser ut til å være den logiske løsningen for fremtidige kontrollanlegg. Løsningen gir fordelene til IEC 61850 når det kommer til leverandøruavhengighet, uten å måtte gjøre omfattende utskiftinger i eksisterende anlegg. Bachelorgruppen konkluderer med IEC 61850 standarden som et alternativ for vernsystemet ved vannkraftverk. OPC-UA og IO-Link, som tillater leverandøruavhengighet, kan åpne opp for kostbesparende sentrallager og geografisk uavhengig serviceansatte. Dette kan redusere bemanningsbehov. Ved bygging av nye anlegg kan bruk av Ethernet-baserte kommunikasjonsprotokoller være fordelaktig med tanke på hurtig kommunikasjon og enkel installasjon.

Standardisering har klare fordeler over tid når det kommer til prosjektering, kostnadseffektivisering, kvalitetssikring og lagerbeholdning. Tankesettet kan innføres i mange områder slik som standardiserte funksjonsblokker, tagging og rammeavtaler for bygging av nye kontrollanlegg. Standardisering av tags fra ulike kontrollanlegg muliggjør enklere løsning for databehandling og analyse, fremfor individuelle tilpasninger på tvers av vannkraftverkene. Tags burde standardiseres etter IEC 61850 og RDS-strukturen, som er ferdig utviklet idag.

Ved bygging av nye anlegg bør Statkraft fastsette vilkårene for kontraktene som inngår i en begrenset rammeavtale på 4 år. Spesifikasjonen bør ha en teknisk låst standard som gjør at anleggene bygges likt, og at det er klare krav til hvordan leverandørene er fastlåst i fremgangsmetoden for kontrollanlegget.

Videre arbeid:

- Rapporten gir grunnlag for videre studier innen cybersikkerhet, databehandling og videreutvikling av instrumentering som trengs for å kunne regulere etter fremtidens markedskrav og den ekstra påkjenningen dette vil påføre, som avdekt i rapporten.
- Cyberkriminalitet har en sterkt økende trend og man har egne organisasjoner som beriker seg på spredning av ransomware. Kunder innen krisisk infrastruktur er spesielt utsatt da betalingsvillighet og mulighet ikke minst er stor. Videre arbeid for å kartlegge sikkerheten rundt den økende datastrømmingen som trengs burde settes i fokus.
- Data som samles inn burde samles og analyseres i en algoritme som kan gjenkjenne og forutse behov for vedlikehold. Et prosjekt som arbeider med utvikling og optimalisering av en slik AI burde prioriteres.
- For å senke fremtidige vedlikeholdskostnader og sikre anleggets integritet, burde det innføres smart instrumentering. Arbeid med å kartlegge hensiktsmessige medier å overvåke og samkjøring mellom disse kan være aktuelt å undersøke.

13 VEDLEGG

Fremtidens PLS-baserte kontrollanlegg i vannkraftverk

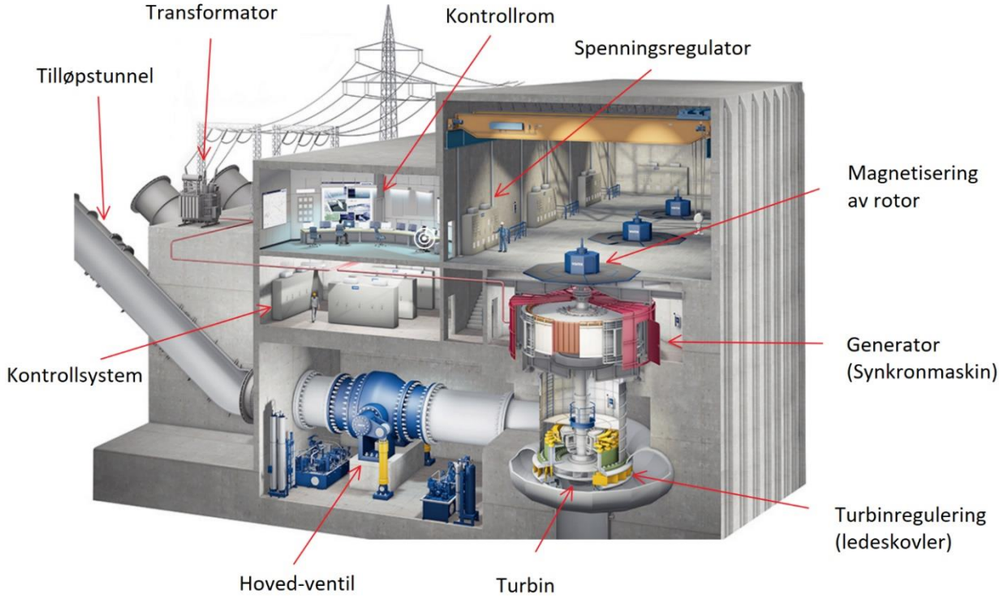
Håvard Skansgård, Marcus Kristensen, Robert Strand og Stian Kold Huseby

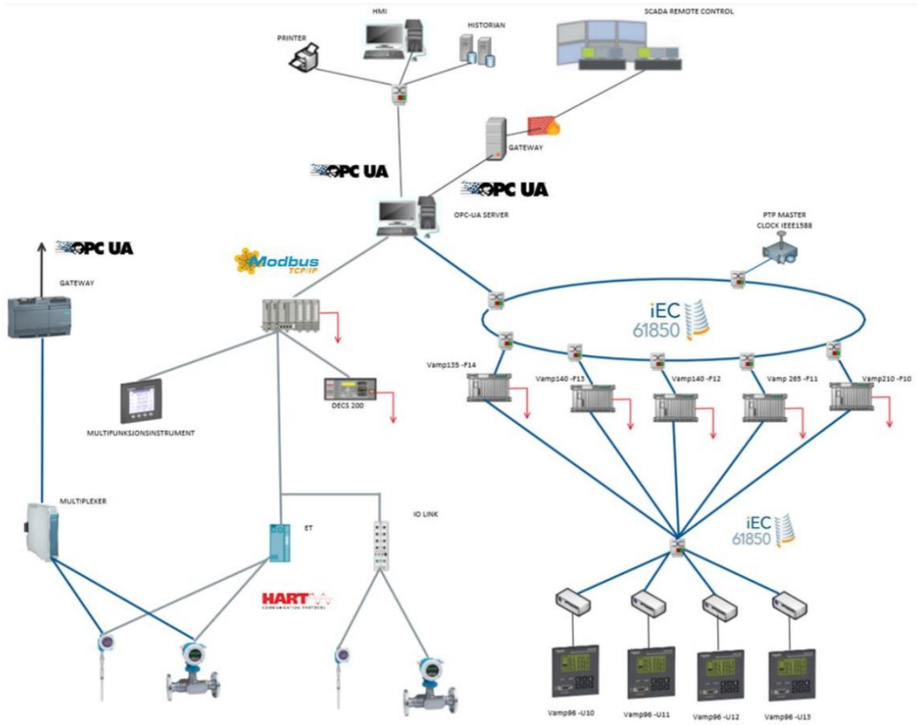
Bakgrunn

Statkraft har et ønske, som de fleste andre selskaper, om å holde tritt med teknologiutviklingen. Selv om prosessen som inngår endrer seg lite kan det værefordelaktig å ta i bruk nye systemer for å optimalisere og sikre drift. Statkraft har tatt eierskap over flere kraftverk der en teknisk oppgradering står for tur. Denne studien har mål om å kaste lys over hvilken retning en burde vurderesom teknisk løsning i et slikt prosjekt.

Oppgaven

Bacheloroppgaven, som denne rapporten bygges på, kartlegger oppbygging av dagens lokale kontrollanlegg og ser på alternativer som bidrar til å bedre, og- eller tilpasser anlegget for å være bedre rustet til å møte fremtiden. Alternativene som vurderes kan være metoder som ikke er veletablert i dag blant Statkrafts energiverk, men som har basis for å kunne inkluderes i større grad på tvers av regioner. Et fokus på bruk av standardiseringsarbeid og hvordan dette kan gi fordeler er også vurdert. I denne sammenheng er det foretatt intervjuer med sentrale ansatte på tvers av kraftbransjen og på tvers av landegrenser med mål om å avdekke fokusområder, implementasjons- og effektiviseringsstrategier i tillegg til synspunkter på videre utvikling innen fagfeltet. Hvorfor er det viktig å ta tak i denne oppgaven Problemstillinger som oppgaven belyser er viktig for at Statkraft skal kunne ta riktige beslutninger når fremtidige kontrollanlegg prosjekteres. Bacheloroppgaven har satt mål om å kunne foreslå løsninger fra et nøytralt ståsted og med uerfarne øyne.





Omfang

Rapporten omhandler:

- Oppbygning av dagens kontrollanlegg
- Instrumentering i kraftverk
- Standarder knyttet til kontrollanlegg
- Oppbygning av kontrollanlegg basert helt og delvis på IEC 61850 og OPC UA
- Forslag til oppbygning av nytt kontrollanlegg til Rødberg kraftverk
- Løsninger innen cybersikkerhet og sikring av kontrollsystemet
- Utforming av teknisk spesifikasjon

Konklusjon

Mulighetsstudien kan konkludere med at datainnsamling for analyse fra instrumentering burde legges i parallell med dagens kontrollanlegg for å unngå å komplisere styringen. Utsending av data bør skje igjennom en ensrettet Gateway og innsending av data eller fjernstyring bør skje gjennom en Secure Bypass for best mulige sikring mot cyberangrep.

Et kontrollanlegg med OPC klient-server forhold ser ut til å være den logiske løsningen for fremtidige kontrollanlegg. Løsningen gir fordelene til IEC 61850 når det kommer til leverandøruavhengighet, uten å måtte gjøre omfattende utskiftinger i eksisterende anlegg. I kombinasjon med OPC-UA og IO-Link, som tillater leverandøruavhengighet, kan disse åpne opp for kostbesparende sentrallager og geografisk uavhengig serviceansatte.

Standardisering har klare fordeler over tid når det kommer til prosjektering, kostnadseffektivisering, kvalitetssikring og lagerbeholdning. Tankesettet kan innføres i mange områder slik som standardiserte funksjonsblokker, tagging og rammeavtaler for bygging av nye kontrollanlegg. Standardisering av tags fra ulike kontrollanlegg muliggjør enklere løsning for databehandling og analyse, fremfor individuelle tilpasninger på tvers av vannkraftverkene. Tags burde standardiseres etter IEC 61850 og RDS-strukturen, som er ferdig utviklet i dag.

Referanser

[1] Sintef. *Optimalt vedlikehold av vannkraftverk*. 2002. URL: https://www.sintef.no/globalassets/project/beslutningsstotte_vannkraft/oh_eso.pdf.

[2] Acromag Incorporated. *INTRODUCTION TO MODBUS TCP/IP*. 2005. URL: https://www.prosoft-technology.com/content/download/11984/233509/file/intro_modbustcp.pdf.

[3] Sintef. *Beslutningsstøtte for vedlikehold og rehabilitering innen vannkraft*. 2005. URL: https://www.sintef.no/globalassets/project/beslutningsstotte_vannkraft/brukermote-kontrollanlegg.pdf.

[4] Sintef. *Vedlikehold og rehabilitering innen vannkraft*. 2005. URL: https://www.sintef.no/globalassets/project/vrv/brosjyre.pdf.

[5] Sintef. *Vedlikehold og rehabilitering innen vannkraft*. 2005. URL: https://www.sintef.no/globalassets/project/vrv/brosjyre.pdf.

[6] Idar Pe Ingebrigtsen. *Databasert dokumentasjon - SCD*. 2007. URL: https://www.itk.ntnu.no/fag/TTK4175/forelesningsnotater/2007/NTNU%5C%20Databasert%5C%20dokumentasjon%5C%202007.pdf.

[7] EE Times. *Understanding Ethernet-based industrial communication protocols*. 2007. URL: https://www.eetimes.com/understanding-ethernet-based-industrial-communication-protocols/#.

[8] Harold Fischer. *Revised Engineering and Testing Practices Resulting From Migration to IEC 61850*. 2008. URL: https://selinc.com/api/download/3509/.

[9] NEK IEC. *IEC 62433-3-1*. 2009.

[10] R.P.Saini Pardeep Kumar. *Study of cavitation in hydro turbines*. 2009. URL: https://www.globalspec.com/reference/60189/203279/chapter-47-smart-transducers-sensors-or-actuators-interfaces-and-networks.

[11] General Electric. *Leading the industry in IEC 61850 implementation*. 2010. URL: https://www.gegridsolutions.com/multilin/iec_innovations.htm.

[12] Asbjørn Lilleb. *Erfaringer i bruk av SAP som FVD-system i Statkraft*. 2011. URL: https://docplayer.me/1071242-Erfaringer-i-bruk-av-sap-som-fdv-system-i-statkraft.html.

[13] Salman Mohagheghi. *Applications of IEC 61850 in distribution automation*. 2011. URL: https://www.researchgate.net/publication/252000959_Applications_of_IEC_61850_in_distribution_automation.

[14] Lovdata. *Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften)*. 2012. URL: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157.

[15] Jon Harald Skare. *Mateoppgave: Regulering av turbiner i vannkraftverk - En litteraturstudie*. 2014.

[16] Marcos Foneseca Mendes. *Modern Automation of Hydroelectric Power Plant*. Tekn. rapp. 2015.

[17] LD for Protection og Control. *61850-102 l IEC 61850 Introduction v1*. 2015. URL: https://www.youtube.com/watch?v=ahd0V8qwbPY.

[18] LD for Protection og Control. *61850-102 l IEC 61850 Introduction v1*. Youtube. 2015. URL: https://www.youtube.com/watch?v=ahd0V8qwbPY.

[19] SF Harding. *Experimental Pressure Measurements on Hydropower Turbine Runners*. 2016. URL: https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-26061.pdf.

[20] Lars Ihler. *NEK IEC 61850-serien*. 2016. URL: https://www.nek.no/manedens-standard-april-2016-nek-iec-61850-serien/.

[21] ScienceDirect. *Logical Node*. 2016. URL: https://www.sciencedirect.com/topics/engineering/logical-node.

[22] Turck. *IO-Link$_T$echnology*. 2017. URL: https://www.turck.de/static/img/IO-Link_Technology_2017_11_800x600_EN.jpg.

[23] MILES BUDIMIR. *What are IEC 61131-3 and PLCopen?* 2018. URL: https://www.motioncontroltips.com/iec-61131-3-plcopen/.

[24] Mingyu Ha. *IEEE 1588 Time Synchronisation Performance for IEC 61850 Transmission Substations*. 2018. URL: https://www.research.manchester.ac.uk/portal/files/82086612/Elsevier_v4.4.pdf.

[25] Inductiveautomation. *What is SCADA?* 2018. URL: https://www.inductiveautomation.com/resources/article/what-is-scada#:~:text=Supervisory.

[26] Idar Pe Ingebrigtsen. *Automated code generation by means of the IEC PAS 63131*. 2018. URL: https://www.automationml.org/o.red/uploads/dateien/1548668479-15_Drath_Oil-Gas-IEC-63131.pdf.

[27] Lovdata. *Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften)*. 2019. URL: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157.

[28] SaaS Security. *Hydro utsatt for et omfattende nettangrep*. 2019. URL: https://saassecurity.no/Ressurs/Dagens-trusler/ArticleId/38/hydro-utsatt-for-et-omfattende-nettangrep.

[29] Statkraft. *Technical Specification Station Control Systems Hydro Power Plants*. 2019.

[30] Statkraft. *Vedlikehold: Sikrer vannkraften evig liv*. 2019. URL: https://www.statkraft.no/nyheter/nyheter-og-pressemeldinger/arkiv/2019/vedlikehold-sikrer-vannkraften-evig-liv/.

[31] El-Watch. *NEURON sensors tar tempen på vannkraften*. 2019. URL: https://www.el-watch.com/neuronsensors-pikerfoss/.

[32] Wikipedia. *Generic Substation Events*. 2019. URL: https://en.wikipedia.org/wiki/Generic_Substation_Events.

[33] Undefined Automation. *OPC UA Servers – Downloads*. 2020. URL: https://www.unified-automation.com/downloads/opc-ua-servers.html.

[34] Peter Crossley. *Interoperability Performance Assessment of Multivendor IEC61850 Process Bus*. University of Manchester. 2020. URL: https://core.ac.uk/download/pdf/204192054.pdf.

[35] Enel. «Enel Green Power DM». Enel powerpoint presentasjon. 2020.

[36] Energies. *Real-Time Analysis of Time-Critical Messages in IEC 61850 Electrical Substation Communication Systems*. 2020. URL: https://www.mdpi.com/1996-1073/12/12/2272/pdf-vor.

[37] P.E. GARY L. PRATT. *Which IEC 61131-3 Programming Language is best? Part 2*. 2020. URL: https://www.controleng.com/articles/which-iec-61131-3-programming-language-is-best-part-2/.

[38] P.E. GARY L. PRATT. *Which IEC 61131-3 Programming Language is best? Part 2*. 2020. URL: https://www.controleng.com/articles/which-iec-61131-3-programming-language-is-best-part-2/.

[39] Norsk Elektroteknisk Komite. *Beskytter vi kritisk infrastruktur godt nok?* 2020. URL: https://www.nek.no/beskytter-vi-kritisk-infrastruktur-godt-nok/.

[40] NVE. *Vannkraft*. 2020. URL: https://www.nve.no/reguleringsmyndigheten/stromkunde/om-kraftmarkedet-og-det-norske-kraftsystemet/.

[41] Statkraft. «General Technical Requritements - Low voltage Electrical and Automation equipment». 2020.

[42] Statkraft. *Ulla-Førre - en av de siste store*. 2020. URL: https://www.statkraft.no/om-statkraft/historien-var/#1970-1992/1988.

[43] Statkraft. *Årsrapport 2020*. 2020. URL: https://www.statkraft.no/globalassets/1-statkraft-public/05-investor-relations/4-reports-and-presentations/2020/q4/statkraft-as-arsrapport-2020.pdf.

[44] TheOPCFoundation. *20200622 03 OPC UA Security Overview*. 2020. URL: https://www.youtube.com/watch?v=2mPGeddA65E.

[45] Answerexpress. *En introduksjon til SCADA.systemer*. 2021. URL: https://no.answersexpress.com/an-introduction-scada-systems-99185#menu-1.

[46] Real Time Automation. *MODBUS RTU*. 2021. URL: https://www.rtautomation.com/technologies/modbus-rtu/.

[47] Nelly Ayllon. *WHAT IS THE DIFFERENCE BETWEEN PROFIBUS DP AND PA?* 2021. URL: https://us.profinet.com/what-is-the-difference-between-profibus-dp-and-pa.

[48] Christian B. *Functional testing of IEC 61850 based Substation Automation Systems*. 2021. URL: https://electrical-engineering-portal.com/functional-testing-iec-61850-based-substation-automation-systems.

[49] Crushtymks. *Bruke MODBUS for prosesskontroll og automatisering (1)*. 2021. URL: https://crushtymks.com/no/industrial-automation/1093-using-modbus-for-process-control-and-automation-1.html.

[50] eia. *Japan*. 2021. URL: https://www.eia.gov/international/analysis/country/JPN.

[51] ENSOTEST. *Introduction to the IEC 60870-5-104 standard*. 2021. URL: https://www.ensotest.com/iec-60870-5-104/introduction-to-the-iec-60870-5-104-standard/.

[52] Arild Helseth. *Multimarkedsplanlegging*. 2021. URL: https://www.sintef.no/ekspertise/sintef-energi/multimarkedsplanlegging/.

[53] Prosoft Industries. *Modbus TCP/IP Enhanced Communication Module*. 2021. URL: https://www.prosoft-technology.com/Products/Rockwell-Automation-In-chassis/Platform/CompactLogix/Modbus-TCP-IP-Enhanced-Communication-Module.

[54] IOTgateway. *SITRANS Cloud Connect 240*. 2021. URL: https://new.siemens.com/global/en/products/automation/process-instrumentation/digitalization/sitrans-cloud-connect-240.html.

[55] IOTgateway. *SITRANS MX300*. 2021. URL: https://mall.industry.siemens.com/mall/en/hu/Catalog/Product/7MP2200-1AD10-2AA0.

[56] Ewa Krukowska. *Germany Signals Record EU Carbon Price Rally May Slow Down*. 2021. URL: https://www.bloomberg.com/news/articles/2021-05-13/germany-signals-record-eu-carbon-price-rally-may-slow-down.

[57] Store Norske Leksikon. *Vannkraft*. 2021. URL: https://snl.no/vannkraft.

[58] Lovdata. *Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven)*. 2021. URL: https://lovdata.no/dokument/NL/lov/1990-06-29-50.

[59] Elchin Mammadov. *The margins of coal-fired power stations are collapsing*. 2021. URL: https://twitter.com/elchinmamedov/status/1390416445570433024?s=20.

[60] Control Solutions Minnesota. *Modbus 101 - Introduction to Modbus*. 2021. URL: https://www.csimn.com/CSI_pages/Modbus101.html?fbclid=IwAR39dluXfCLD1sdoC6O4Z59bEJQOJ9tDEUJKQpT9fteTf4kHs40Ah2Wt6sg.

[61] Modbus. *Modbus FAQ: About the Protocol*. 2021. URL: https://modbus.org/faq.php.

[62] OPC Organization. *OPC UA Online Reference*. 2021. URL: https://reference.opcfoundation.org/#Core.

[63] OPC Organization. *OPC UA security architecture*. 2021. URL: https://reference.opcfoundation.org/Core/docs/Part2/4.5.1/.

[64] Sensor Partners. *PVC 5-wire M12 connection cable*. 2021. URL: https://www.sensorpartners.com/en/product/murr-elektronik/pvc-connection-cable-5-wire-m12/.

[65] PROFIBUS. *Overview*. 2021. URL: https://www.profibus.com/technology/profibus/overview.

[66] Knut Samdal. *Vannkraft*. 2021. URL: https://www.sintef.no/felles-fagomrade/vannkraft/#/.

[67] Sintef. *SDN microSense*. 2021. URL: https://www.sintef.no/prosjekter/2019/sdn-microsense/.

[68] Stephen Stapczynski. *Strong solar power output made Japan's wholesale electricity price basically free for 6.5 hours today.* 2021. URL: https://twitter.com/SStapczynski/status/1381052128458809346?s=20.

[69] Statkraft. *Starten på krafteventyret.* 2021. URL: https://www.statkraft.no/om-statkraft/historien-var/#1895-1945.

[70] Svein Olav Sæther. *Kraftforvalter venter mer uforutsigbar strømpris.* 2021. URL: https://e24.no/det-groenne-skiftet/i/dlqnBj/kraftforvalter-venter-mer-uforutsigbar-stroempris-blir-veldig-hopp-og-sprett.

[71] Voith. *About-us.* 2021. URL: https://voith.com/corp-en/about-us/company.html?90664%5B%5D=1.

[72] Voith. *Hydro control system.* 2021. URL: https://voith.com/corp-en/hydropower-components/automation.html?xtor=AD-[VH418]-[HyCon_2020_SoMeKampagne_1]-[LinkedIn_1]-[0]-[http_voith_com_corp_en_hydropower_components_automation_html_125277]-[0]-[0]&fbclid=IwAR1uXW4zA7xawGdHPSK9RJPM7S7AVyJ2kBRfwUNefyoTEeHjxKlskhGiTGI#125277.

[73] Wikipedia. *IEC 61131-3.* 2021. URL: https://en.m.wikipedia.org/wiki/IEC_61131-3.

[74] Wikipedia. *Liste over vannkraftverk i Norge.* 2021. URL: https://no.wikipedia.org/wiki/Liste_over_vannkraftverk_i_Norge.

[75] THOMAS AANENSEN. *Veldig lav strømpris i 2020.* 2021. URL: https://www.ssb.no/energi-og-industri/artikler-og-publikasjoner/veldig-lav-strompris-i-2020.

[76] Electric Axis. *Modern Substation Automation Hierarchical Control.* URL: http://www.electricalaxis.com/2020/11/iec-61850-logical-nodes-and-data.html.

[77] Cisco. *What Are the Most Common Cyber Attacks?* URL: https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html.

[78] KEMA. *IEC 61850 Extensions.*

[79] Stefan Meier. *OP060 – Performance considerations in digital substation applications.* ABB.

[80] PLCopen. *IEC 61131-9.* URL: https://plcopen.org/iec-61131-9.

[81] Richard Schimmer. *IEC 61850 Overview.* PDF; accessed 29.01.21. KEMA.

[82] SEL. *Software-Defined Networking (SDN).* URL: https://selinc.com/mktg/132609/.

[83] Waterfall. *Remote Access, PHYSICAL CONTROL OVER REMOTE SUPPORT.* URL: https://static.waterfall-security.com/Waterfall-for-Secure-Bypass.pdf?hsCtaTracking=39bf110c-166a-4e94-8cc1-9341d92fc77b%5C%7C2d56eba1-5436-40d5-bdf1-430e14a9e8e0.

[84] Waterfall. *Remote Screen View.* URL: https://waterfall-security.com/static/Waterfall-for-Remote-Screen-View.pdf.

[85] Waterfall. *Uniderctional Security Gateway*. URL: https://static.waterfall-security.com/WF-500_Datasheet.pdf?hsCtaTracking=de7f3971-ba60-4d29-918a-319451161614%5C%7Ce6e74d0d-e22d-4d4a-b8a7-42a98a33db17.

[86] Nelly Ayllon. *WHAT IS PROFINET? – PROFINET EXPLAINED*. 10.02.2021. URL: https://us.profinet.com/profinet-explained/#:~:text=.

[87] dpstele. *How Do SCADA Systems Work?* 10.06.2020. URL: https://www.dpstele.com/scada/how-systems-work.php.

[88] Wikipedia Encyclopedia. *Role-based access control*. 20 Februar 2021. URL: https://en.wikipedia.org/wiki/Role-based_access_control.

[89] Carl Henning. *THE DIFFERENCE BETWEEN PROFIBUS AND PROFINET*. 10.06.2020. URL: https://us.profinet.com/the-difference-between-profibus-and-profinet/.

[90] Store Norske Leksikon. *spenningsregulator*. 6. september 2019. URL: https://snl.no/spenningsregulator.

[91] Ivar M. Liseter. *OSI*. 18.06.2020. URL: https://snl.no/OSI.

[92] Lovdata. *Forskrift om offentlige anskaffelser (anskaffelsesforskriften)*. 19.02.2020. URL: https://lovdata.no/dokument/SF/forskrift/2016-08-12-974?q=anskaffelsesforskriften.

[93] Patrick McClanahan. *10-A.1: TCP/IP Fundamentals*. 27.04.2021. URL: https://eng.libretexts.org/@go/page/40102.

[94] Emmanuel Odunlade. *Microcontroller vs PLC: A Detailed Comparison*. 3.10.2018. URL: https://circuitdigest.com/article/microcontroller-vs-plc-detailed-comparison-and-difference-between-plc-and-microcontroller.

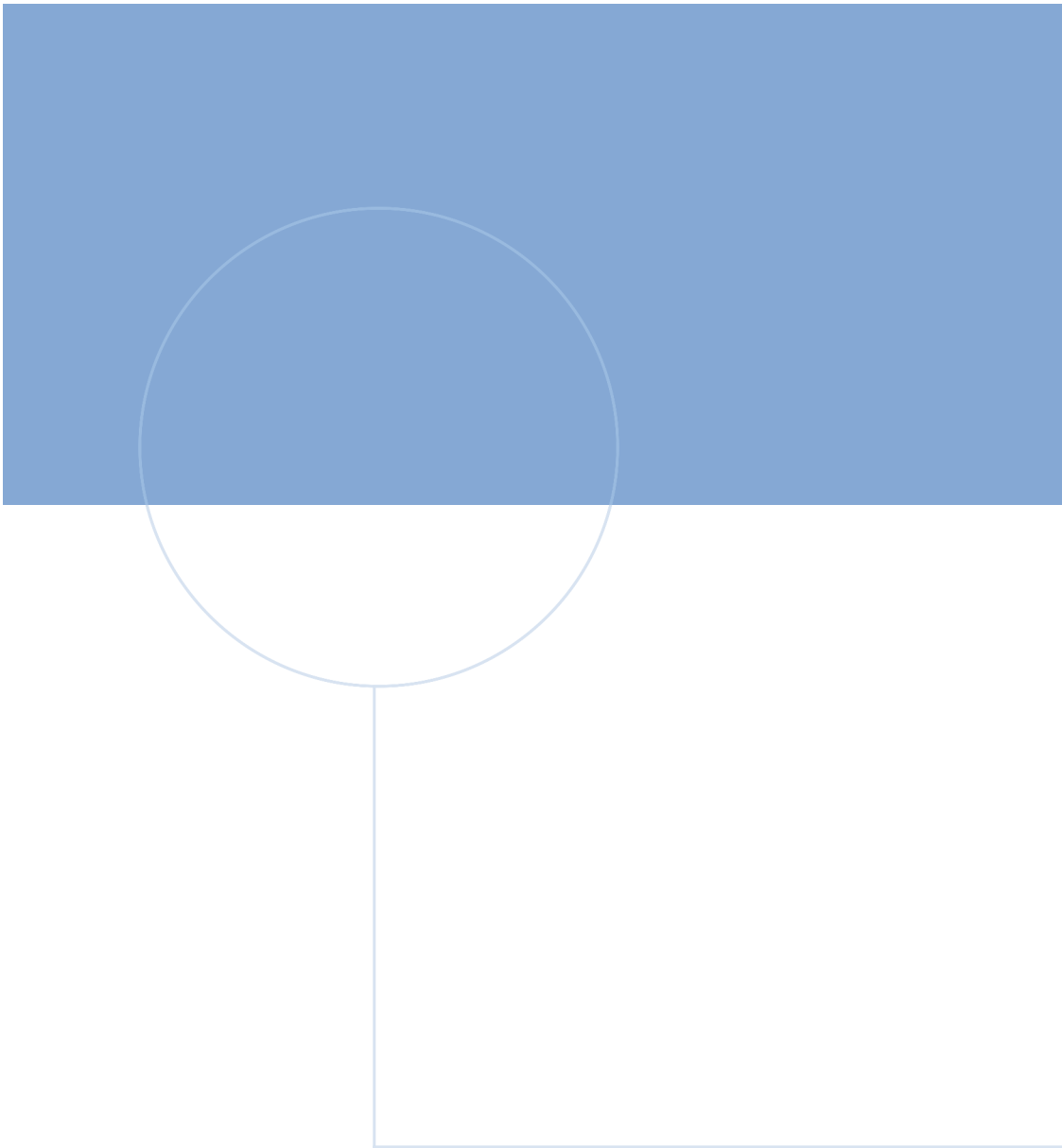
[95] Courtney Schneider. *DMZ: THE INDUSTRIAL CONTEXT*. 3OCT 2019. URL: https://waterfall-security.com/dmz-the-industrial-context/.

[96] Verdinor. *Offentlige anskaffelser - hva er en rammeavtale?* 20.04.2021. URL: https://www.verdinor.no/nyheter/hva-er-en-rammeavtale/.

[97] Visaya. *A guide to the PROFINET network communication protocol*. 25.01.2018. URL: https://visaya.solutions/en/video/video-profinet-communication.

[98] Wikipedia. *HART-protokoll*. 4.10.2013. URL: https://nn.wikipedia.org/wiki/HART-protokoll.

[99] wikipedia. *Francis turbine*. 5. mars 2021. URL: https://en.wikipedia.org/wiki/Francis_turbine.



NTNU

Norwegian University of
Science and Technology