Universitetet i Sørøst-Norge

www.usn.no

TS3000 1 Bachelor 24V

Utvikling av industriell miniatyrmodell for simulering av cyberangrep

IA6-24-4

Fakultet for teknologi, naturvitenskap og maritime fag
Campus Porsgrunn

Universitetet i Sørøst-Norge

www.usn.no

Emne: TS3000 1 Bachelor 24V

Tittel: Utvikling av industriell miniatyrmodell for simulering av cyberangrep

Denne rapporten utgjør en del av vurderingsgrunnlaget i emnet.

Prosjektgruppe: IA6-24-4 **Tilgjengelighet:** Åpen

Gruppedeltakere:

William Selmer
Abdikadir Aden
Sjur Aanesen
Anders Pedersen Skogli
Mohamed Ismail

Veileder: Hans-Petter Halvorsen

Prosjektpartner: **Mnemonic**

Godkjent for arkivering: _____

Universitetet i Sørøst-Norge

www.usn.no

Sammendrag:

Trusselen for cyberangrep i industrielle anlegg er økende, og etterspørselen for sikkerhetsløsninger er stor. Mulighetene for testing og utvikling av løsninger på operasjonelle anlegg er forholdsvis dårlige. IT-selskapet Mnemonic ønsker derfor et realistisk testmiljø for demonstrasjon av cyberangrep, opplæring, og testing av sikkerhetsløsninger.

Prosjektet går ut på å kartlegge kjente angrep, med sårbarheter og konsekvenser, og å redegjøre for sikringstiltak og standarder. Hovedmålet med prosjektet er å bygge en realistisk miniatyrmodell som benytter seg av utstyr som er utbredt i industrielle anlegg. Til slutt skal det utføres en nettverksanalyse av anlegget, og gjøres et forsøk på et cyberangrep.

For løsning av oppgaven utføres det en litteraturstudie med formål om å kartlegge kjente cyberangrep, og forstå oppbygningen av aktuelle anlegg. Det utføres en analyse av sårbarheter og konsekvenser ved angrepene. Det gjennomføres konseptutvikling for potensielle løsninger av industrielle anlegg. Løsningen som blir valgt designes og implementeres. Til slutt blir hele anlegget testet og evaluert.

Ved prosjektets slutt har fire kjente hendelser, og aktuelle sikkerhetsstandarder blitt undersøkt. Fire forskjellige konsepter for miniatyrmodeller har blitt skissert og vurdert, og en løsning har blitt valgt. Anlegget som har blitt valgt er et kombinert elkraftanlegg, som baserer seg på solkraft og vannkraft. Det aktuelle anlegget har blitt bygd, koblet opp og programmert. Det har til slutt blitt gjennomført nettverksanalyse og et enkelt cyberangrep.

Forord

Denne rapporten er et resultat av arbeidet rundt utvikling av miniatyrmodell for simulering av cyberangrep. Prosjektoppgaven er gitt og finansiert av Mnemonic, et norsk IT-sikkerhetsselskap. Rapporten er skrevet for lesere som har interesse innen cybersikkerhet og automatisering, både for de med og uten teknisk bakgrunn.

Studentgruppen består av fire studenter fra informatikk og automatisering, og en student fra elkraft. Løsningen er utført på USN, campus Porsgrunn som en bacheloroppgave innen elektroingeniørfag.

Gruppen ønsker å gi en spesiell takk til Hans-Petter Halvorsen, Fredrik Hansen og Eirik Fallrø for veiledning og støtte gjennom prosjektet.

Porsgrunn, 21.05.2024

Nomenklaturliste

AC	«Alternating current», på norsk vekselstrøm.
DC	«Direct current», på norsk likestrøm.
DDoS	DDoS står for "Distributed Denial of Service" på engelsk, og på norsk betyr det "Distribuert tjenestenektangrep". Dette er en type cyberangrep der en målrettet nettside eller nettverk blir overbelastet med en stor mengde forespørsler, som gjør at det blir utilgjengelig for ekte brukere.
Dos	DoS (Denial of Service), og på Norsk "tjenestenektangrep". Forskjell fra et DDoS-angrep, hvor angrepet distribueres fra flere kilder, utføres et DoS-angrep fra en enkelt kilde. Målet med et DoS-angrep er også å forstyrre eller forhindre normal drift av en nettside eller tjeneste.
ICS	«Industrial control system», på norsk «Industrielle styresystemer» er systemer som styrer og overvåker prosesser i industrielle anlegg, inkludert PLS, SCADA (overvåking og datainnsamling) og andre komponenter for effektiv produksjon.
IEC 60870-5-101	IEC101 er en standard for overvåking, kontroll og tilhørende kommunikasjon for fjernstyring, fjernbeskyttelse og tilhørende telekommunikasjon for elektriske kraftsystemer
IEC 60870-5-104	IEC 104 er en standard for telekontrollutstyr og systemer med kodet seriell dataoverføring i TCP/IP-baserte nettverk for overvåking og styring av geografisk spredte prosesser.
IEC 61850	er en internasjonal standard som definerer kommunikasjonsprotokoller for intelligente elektroniske enheter ved elektriske transformatorstasjoner.
NC	«Normally closed» beskriver brytere som i normaltilstand er lukket. Så når en NC bryter blir aktivert vil den åpne seg istedenfor å lukke seg som er mer vanlig for brytere.
OPC Data Access	er en gruppe standarder som gir spesifikasjoner for å kommunisere sanntidsdata fra datainnsamlingsenheter som PLC-er og HMI-er
OT	Operasjonell teknologi: Teknologien brukt i industrien for å styre og overvåke fysiske prosesser, i motsetning til IT (informasjonsteknologi) som fokuserer på datanettverk og informasjonssystemer.
PLS	Programmerbar logisk styring: En enhet som brukes til å kontrollere industrielle prosesser ved å programmere logiske instruksjoner for å styre maskiner og utstyr.

PSU	Power Supply Unit: er en strømforsyning som tar in AC for å konvertere det til DC for å forsyne komponenter med strøm.
SIS	Sikkerhetsinstrumenterte systemer: Systemer designet for å beskytte anlegg og personell ved å detektere farlige situasjoner og iverksette sikkerhetsfunksjoner for å hindre uønskede hendelser
(ISO) 27001	ISO 27001 er en internasjonal standard for informasjonssikkerhet som fastsetter krav til et informasjonssikkerhetsstyringssystem (ISMS).
(ISA)/IEC 62443	ISA/IEC 62443 er en serie med internasjonale standarder utviklet for å håndtere cybersikkerhetsutfordringer spesifikt knyttet til industrielle automatiseringssystemer (IAS) og kontrollsystemer (ICS).
NERC	NERC står for "North American Electric Reliability Corporation». NERC utvikler og håndhever standarder for drift og planlegging av elektrisitetsforsyningssystemet, samt for beskyttelse av kritisk infrastruktur mot cybertrusler
NIST Sikkerhetsrammeverk	NIST Sikkerhetsrammeverk refererer til det cybersikkerhetsrammeverket utviklet av National Institute of Standards and Technology (NIST) i USA.

Innholdsfortegnelse

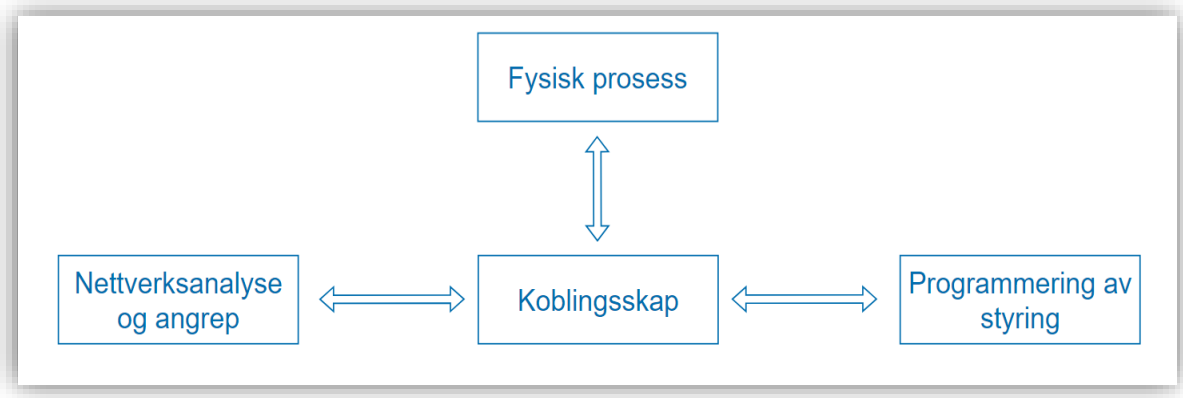
1 Innledning

Denne rapporten handler om utviklingen av en konseptmodell for å simulere cyberangrep på industrielle kontrollsystemer, et prosjekt som utføres for det norske IT-sikkerhetsselskapet Mnemonic. Formålet med prosjektet er å utvikle en miniatyrmodell av en fabrikklinje eller prosessanlegg for å teste og utvikle nye sikkerhetsprodukter, samt trene interne IT-eksperter på industrielle kontrollsystemer (OT-systemer). Målet med rapporten er å beskrive hele utviklingsprosessen av modellen, fra ide til testing.

Rapporten starter med en bakgrunn som gir en oversikt over de forskjellige delene av prosjektet, som en litteraturstudie, sårbarhetsanalyse og utviklingen av ulike konseptmodeller for industrielle testmiljøer. Etter vurdering av ulike modeller, som vannkraftverk, avfallssorteringsanlegg, solcelleanlegg og kombinerte kraftverk, bestemmes det å fokusere på en modell som simulerer både vann- og solkraft. Designet av modellen inkluderer detaljerte tegninger, koblingsskjemaer og en liste over komponenter med kostnadsestimering, for å holde prosjektet innenfor budsjettet. Modellen skal bygges på en flyttbar plattform med låsbare hjul for å møte Mnemonics behov.

Den ferdige modellen testes grundig for å sikre at den fungerer som den skal. Testingen inkluderer simulering av cyberangrep for å vurdere modellens evne til å demonstrere konsekvensene av angrep og teste ulike sikkerhetstiltak. Verktøy som Wireshark, Nmap, Proneta og Grassmarlin brukes til nettverksanalyse og testing av angrep på modellen. Resultatene fra testingen brukes til å vurdere modellens robusthet og evne til å håndtere cybertrusler uten ekstra beskyttelsestiltak.

Rapporten gir en helhetlig og lett forståelig presentasjon av arbeidet, med innsikt i både bredden og dybden av problemstillingen, og avslutter med anbefalinger for fremtidige studier eller praktiske tiltak. Figur 1-1 viser hvordan systemet i prosjektet ser ut.

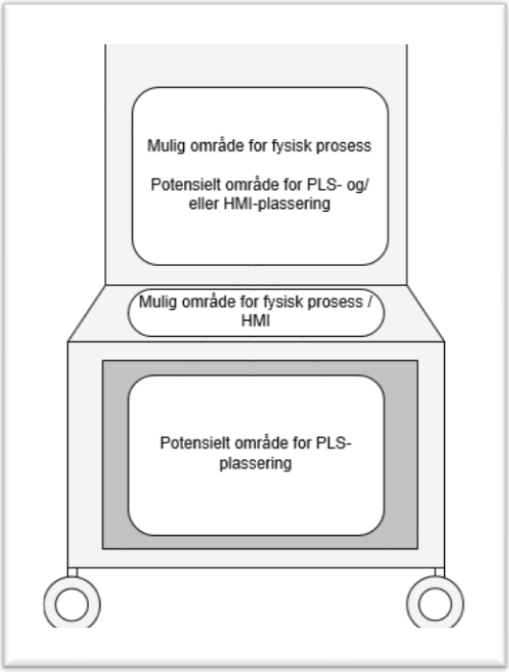


Figur 1-1: Systemoversikt for oppgaven.

1.1 Bakgrunn

Bakgrunnen for rapporten dreier seg om et prosjekt initiert av det norske IT-sikkerhetsselskapet Mnemonic, som har som mål å utvikle et testmiljø for cybersikkerhetsprodukter på industrielle installasjoner. Per i dag finnes det få muligheter for å teste slike sikkerhetsprodukter på industrielle anlegg, og Mnemonic ser derfor et behov for en løsning som kan møte denne utfordringen.

Prosjektet fokuserer på å undersøke ulike typer angrep, konsekvenser og sårbarheter i operasjonelle teknologiske systemer (OT-systemer) for å få en bedre forståelse av OT-sikkerhet. Målet er å utvikle en realistisk miniatyrmodell av et OT-system som kan brukes som et allsidig verktøy for testing, opplæring og demonstrasjon av cybersikkerhetsprodukter i industrielle kontrollmiljøer. Det innebærer også en analyse av nettverkstrafikken for å forstå oppbygningen av industriell nettverkstrafikk og for å utføre testangrep på systemet for å demonstrere konsekvensene. Ved å gjennomføre dette prosjektet, vil Mnemonic kunne tilby en plattform for bedre å forstå og sikre industrielle kontrollsystemer mot cyberangrep. Figur 1-2: Illustrerer skisse for en flyttbar miniatyrmodell som simulerer en industriell prosess.



Figur 1-2: Skisse for en flyttbar miniatyrmodell som simulerer en industriell prosess [1].

1.2 Målsettinger og fremdrift

Prosjektet har som hovedmål å utvikle en realistisk og funksjonell miniatyrmodell av et operasjonelt teknologisystem (OT-system) som kan brukes til testing, opplæring og demonstrasjon av cybersikkerhetsprodukter i industrielle kontrollmiljøer.

For å oppnå hovedmålet er prosjektet delt opp i mindre delmål som igjen er delt inn i oppgaver. Disse oppgavene er definert i fremdriftsplanen som kan finnes i vedlegg 2a. Fremdriftsplanen gir oversikt over alle oppgavene som må utføres, samtidig som den fordeler ansvar og setter planlagt dato for utførelse opp mot faktisk dato for utførelse av oppgaven. De viktigste oppgavene er kort oppsummert i punktene under.

- Undersøke cyberangrep på OT-systemer og identifisere sårbarheter, konsekvenser og aktuelle sikringstiltak
- Utvikle en miniatyrmodell for demonstrering, testing og opplæring.
- Gjennomføre nettverksanalyse og testangrep på miniatyrmodellen.

1.3 Metoder

Dette delkapittelet beskriver metodene som skal brukes for å utvikle konseptmodellen for simulering av cyberangrep. Metodene baserer seg på undersøkelser av litteratur, analyse av kjente cyberangrep på OT-systemer, og konseptutvikling. På grunnlag av metodene skal det utvikles forslag til konsepter som legger til rette for videre utvikling av modellen.

1.3.1 Litteraturstudie

For å forstå de ulike aspektene av cyberangrep på industrielle kontrollsystemer (ICS), skal det utføres litteraturgjennomgang for å danne grunnlag for senere arbeid. Dette inkluderer akademiske artikler, og dokumentasjon fra tidligere kjente cyberangrep som BlackEnergy, Stuxnet, Triton, og Industroyer. Litteraturstudien hjelper også med å identifisere sårbarheter, konsekvenser av angrep, og eksisterende sikkerhetstiltak. I tillegg, skal litteratur som spesifikt handler om vannkraft og solkraft vurderes, for å bedre forstå disse systemene og deres potensielle sårbarheter.

1.3.2 Konseptutvikling

I denne delen av rapporten bli det utviklet flere konseptuelle modeller for et industrielt testmiljø. Modeller for forskjellige typer kraftverk, som vannkraftverk, sorteringsanlegg, solcelleanlegg og kombinert kraftverk, vil bli vurdert. Hver modell vil bli analysert med hensyn til deler som kan være utsatt for cyberangrep, samt deres fordeler, ulemper, og kostnader. Ut fra dette skal den mest hensiktsmessige modellen velges. Målet er å lande på en kombinert kraftverksmodell som kan simulere både vannkraft og solkraft.

1.3.3 Design og implementering

Detaljerte designskisser og koblingsskjemaer utarbeides for den kombinerte kraftverksmodellen. En komponentliste med kostnadsestimering utvikles for å sikre at prosjektet holder seg innenfor budsjettet.

Modellen konstrueres på en flyttbar plattform med låsbare hjul, som beskrevet i kravene fra Mnemonic. Byggingen inkluderer installasjon av PLS/HMI-systemer, solcellepaneler, vanntanker, pumper, og andre nødvendige komponenter.

1.3.4 Testing og evaluering

Etter ferdigstillelse, testes modellen for å sikre at den fungerer som forventet. Dette inkluderer funksjonstester av solcelle- og vannkraftsystemene, samt verifisering av PLS-programmeringen.

Simulerte cyberangrep gjennomføres for å evaluere modellens evne til å demonstrere konsekvensene av slike angrep. Angrepsverktøy som Wireshark, Nmap, Proneta og Grassmarlin brukes til nettverksanalyse og testing av angrep på modellen.

1.4 Avgrensinger

Mnemonic har gitt en liste over krav eller spesifikasjoner som stilles til modellen med tanke på kvalitet og praktikalitet. Kravene danner rammer for hvordan den ferdigstilte modellen skal se ut, og hvordan den skal fungere. I tillegg til kravene som er satt av oppdragsgiver, er det bestemt at modellen skal benytte komponenter som både er utbredt i industrien, og som gruppen har erfaring med fra tidligere emner. Kravene som er satt av oppdragsgiver er listet opp under.

- Krav 1: Modellen skal stå på låsbare hjul og være designet for å være flyttbar.
- Krav 2: Modellen skal være transporterbar.
- Krav 3: Modellen skal bruke relevant type PLS/HMI som er utbredt i industrien.
- Krav 4: Modellen skal på en enkel måte vise status på OT-prosessene for personell uten særlig kunnskap om OT.
- Krav 5: Modellen bør la monteringssted for PLS være synlig
- Krav 6: Modellen skal designes for å være skalerbar, for eksempel ved å ha plass til å iverksette ytterligere PLS og/eller nettverksutstyr.
- Krav 7: Hvis prosessen i modellen inneholder væske, så skal modellen kunne fange opp væsken i en beholder ved lekkasje.
- Krav 8: Modellen skal bygges sterkt og tåle misbruk av kontrollsystem,
- Krav 9: Modellen skal støtte både manuell drift gjennom HMI og automatisk drift av prosessen.
- Krav 10: Det er gitt et budsjett på omtrent 100 000kr av Mnemonic som kan brukes til deler og komponenter.

1.5 Leserveileding

Målet med leseveilederen er å gi leseren en grundig og sammenhengende innsikt i utviklingen av en konseptmodell for simulering av cyberangrep på industrielle kontrollsystemer (ICS). Hver del av rapporten bygger på den foregående for å lede leseren gjennom prosjektets mål, metoder, funn og konklusjoner.
Prosjektet utvikler en testmodell for cybersikkerhet i industrielle kontrollsystemer (ICS) for Mnemonic, som trenger en slik modell for å demonstrere og teste sikkerhetsprodukter.

Kjente cyberangrep på ICS, som BlackEnergy, Stuxnet, Triton og Industroyer, blir beskrevet og analysert for sårbarheter og konsekvenser. Sikringstiltak og relevante sikkerhetsstandarder blir også diskutert.

Ulike konseptmodeller for testmiljøet, inkludert vannkraftverk, sorteringsanlegg, solcelleanlegg og kombinert kraftverk, blir utviklet. Fordeler, ulemper og kostnader for hver modell blir analysert. Begrunnelse for valg av kombinert kraftverksmodell.

Beskrivelse av systemoversikt, komponentliste og kostnadsestimering for det kombinerte kraftverket. Design og tilpassing av solceller og vanntanker, samt integrasjon av sol- og vannkraft i modellen.

Implementering av designskisser, koblingsskjemaer og komponentbeskrivelser. Testing av systemet for funksjonalitet og sikkerhet.

Nettverksanalyser utført med verktøy som Wireshark, Nmap, Proneta og Grass Marlin. Simulerte cyberangrep for å evaluere modellens sikkerhet.

Kritisk vurdering av prosjektets funn og resultater. Anbefalinger for fremtidige forbedringer av sol- og vannkraftsystemene, nettverksanalysen og sikkerhetstiltak.

Oppsummering av prosjektets suksesser og utfordringer. Diskusjon av overordnede konklusjoner og implikasjoner for fremtidig arbeid. Innholdet i rapporten er kort oppsummert i punktene under.

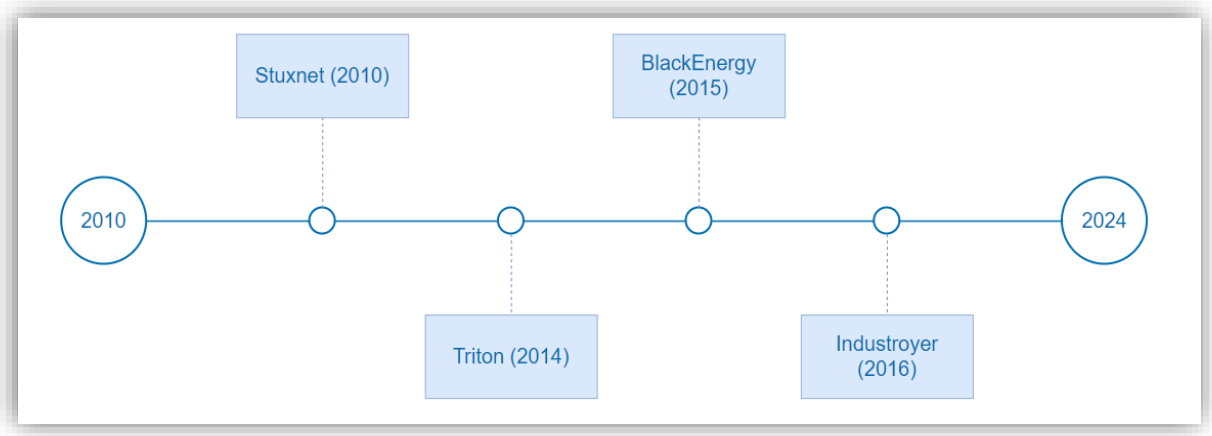
- Kjente angrep, konsekvenser og sårbarheter
- Konseptutvikling for miniatyrmodell
- Planlegging og tilpassing for modell av kombinert kraftverk
- Realisering av kombinert kraftverk
- Nettverksanalyse og angrep

2 Cyberangrep, konsekvenser og sårbarheter

Dette kapittelet tar for seg de ulike angrepene som har rammet operasjonelle teknologisystemer (OT-systemer), samt konsekvensene når disse angrepene lykkes og hvorfor systemene er sårbare. De angrepene som vil bli utforsket nærmere i kommende delkapitler er oppsummert i punktene under.

- Stuxnet
- Triton
- BlackEnergy
- Industroyer

OT-systemer spiller en avgjørende rolle i funksjonen til samfunnets infrastruktur, inkludert strømforsyning, vannforsyning, transport og fabrikker. Imidlertid blir disse systemene stadig mer aktuelle mål for nettbaserte angrep. Dette utgjør et betydelig problem, da slike angrep kan få alvorlige konsekvenser for samfunnet og nasjonal sikkerhet. For å bedre forstå og kunne håndtere truslene mot OT-systemene må det undersøkes kjente angrepsmetoder, konsekvensene av vellykkede angrep og de sårbarhetene som finnes i systemene. Figur 2-1 presenterer en tidslinje som illustrerer historiske angrep på OT-systemer. Denne tidslinjen gir et visuelt innblikk i når disse angrepene fant sted.



Figur 2-1: Tidslinje for angrep på OT-systemer.

2.1 Stuxnet (2010)

Stuxnet, en avansert og vedvarende trussel, spredte seg gjennom 14 industrielle nettsider i Iran, men var spesifikt rettet mot et produksjonsanlegg i Natanz, Iran, med mål om å forstyrre landets kjernefysiske program.

Angrepet var utrolig sofistikert og ble den første kjente skadevaren som var designet for å angripe industrielle kontrollsystemer. Stuxnet utnyttet fire tidligere ukjente sårbarheter i Windows operative system og rettet seg spesifikt mot Siemens S7 PLC-er. Ved å utnytte disse maskinene kunne Stuxnet sikre at det bare infiserte systemer som var relevante for sitt angrep, noe som bidro til å begrense spredningen og redusere risikoen for å bli oppdaget. Videre fokusert Stuxnet spesifikt på PLS-logikk som styrte frekvensomformere.

Frekvensomformere er enheter som kontrollerer hastigheten på elektriske motorer og er avgjørende for prosesser som urananrikning. Ved å manipulere denne logikken kunne Stuxnet forstyrre og skade de industrielle prosessene som var knyttet til urananrikning, som var hovedmålet for angrepet[2].

Stuxnet var designet for å kommunisere med kommando- og kontrollservere, som er eksterne datamaskiner eller servere som angriperne bruker til å sende instruksjoner til den infiserte maskinen og hente informasjon tilbake. For å skjule aktivitetene sine og hindre oppdagelse, krypterte Stuxnet meldingene som ble sendt til og fra disse serverne [3]. Når det gjelder spredningsmetoder, var Stuxnet selektiv i hvordan det spredte seg. Det infiserte bare maskiner som kjørte Siemens S7 programvare, et verktøy som brukes til å programmere og konfigurere industrielle kontrollsystemer [2].

2.1.1 Konsekvenser

Stuxnet forårsaket alvorlig skade på rundt 1000 sentrifuger som var avgjørende for uranberikelsesprosessen ved Natanz-anlegget. Denne skaden førte til en betydelig reduksjon på anleggets evne til å berike uran, noe som hadde direkte innvirkning på Irans produksjonskapasitet for både sivile og eventuell militære formål. Oppdagelsen av Stuxnet vekket bekymring angående sikkerheten til Irans datamaskinsystemer. For å håndtere angrepets konsekvenser og styrke systemenes sikkerhet måtte Iran investere betydelige ressurser i sikkerhetseksperter [4].

2.1.2 Sårbarheter

Stuxnet utnyttet flere sikkerhetshull for å angripe Natanz-fasiliteten. Blant disse var fire zero-day sårbarheter i Microsoft Windows. Zero-day sårbarheter refererer til sikkerhetshull i programvare som er ukjente for utviklerne. Siden utviklerne ikke er klar over disse sårbarhetene, har de ikke hatt mulighet til å lage og distribuere oppdateringer eller reparasjoner for å fikse dem. Navnet "zero-day" kommer fra det faktum at utviklerne har "null dager" til å løse problemet etter at det blir oppdaget av angripere. Disse sårbarhetene var ukjente for Microsoft på det tidspunktet, noe som betydde at det ikke fantes tilgjengelige oppdateringer eller reparasjoner. Dette gjorde dem spesielt utsatt for angrep og ga Stuxnet en betydelig fordel i å infiltrere og spre seg i systemer som brukte Windows.

Stuxnet utnyttet også en sårbarhet i Windows' behandling av snarveier. Ved å infisere en USB-stasjon med en skadelig snarvei fil kunne Stuxnet spre seg til andre datamaskiner når

USB-stasjonen ble koblet til. Når brukeren åpnet USB-stasjonen, forsøkte Windows automatisk å vise ikonet for filen, og dermed startet kjøringen av Stuxnet-koden uten brukerens samtykke eller interaksjon.

En annen sårbarhet som Stuxnet utnyttet var i Windows' printerstøtte. Ved å manipulere utskriftsforespørsler til delt skriver, kunne Stuxnet legge til sin ondsinnede kode i disse forespørslene. Dette gjorde at Stuxnet kunne infisere andre datamaskiner som mottok utskriftsforespørslene fra den delte skriveren, noe som gjorde spredningen av viruset effektiv og vanskelig å oppdage.

I tillegg var det spesifikke sikkerhetshull i Siemens-systemene som fabrikken brukte. Disse inkluderte bruk av svake passord, manglende verifisering av brukeridentiteter og overdreven tilgang til viktige deler av systemets funksjonalitet. Alt dette tillot Stuxnet å komme seg inn og endre fabrikkens kontrollsystemer uten å bli lagt merke til [5].

2.2 Triton (2014)

Triton er en avansert form for industriell skadevare designet spesifikt for å angripe sikkerhetsinstrumenterte systemer (SIS) i industrielle kontrollsystemer. Sikkerhetsinstrumenterte systemer er designet for å beskytte mennesker, industrielle anlegg og de omkringliggende samfunnene ved å kontrollere eller stenge ned industrielle anlegg i tilfelle farlige forhold. Disse SIS-systemene er i essens et sikkerhetstiltak mot industrielle ulykker. Selv om Triton-angrepet ikke direkte forårsaket skade, er det fortsatt bekymringsverdig. Dette skyldes at skadevare var rettet mot sikkerhetssystemer som er designet for å beskytte liv [6]. Denne skadelige programvaren angriper Schneider Electrics sikkerhetsinstrumenterte system.

2.2.1 Konsekvenser

Triton-angrepet, som var rettet mot SIS-kontrollsystemer ved saudiarabiske oljeraffinerier, kunne ha hatt katastrofale konsekvenser hvis det hadde lykkes fullstendig. Ved vellykket gjennomføring kunne angrepet ha ført til utslipp av giftige gasser som hydrogensulfid, og i verste fall forårsaket eksplosjoner [6]. Den mulige ødeleggelsen ville ha vært omfattende, og konsekvensene for både mennesker og miljø ville vært alvorlige. Den økonomiske skaden ville ha vært betydelig, og det ville tatt tid å gjenopprette normal drift. Selv om angrepet ikke oppnådde sine ønskede mål, klarte det å midlertidig stenge ned driften ved minst ett anlegg. Dette førte til produksjonsavbrudd, tap av inntekt og mulige langsiktige økonomiske konsekvenser for selskapet og regionen som helhet.

2.2.2 Sårbarheter

Triton fikk tilgang til nettverket til den petrokjemiske bedriften fra 2014, muligens gjennom en dårlig konfigurert digital brannmur som er sikkerhetsenhet eller programvare som overvåker og kontrollerer innkommende og utgående nettverkstrafikk basert på forhåndsbestemte sikkerhetsregler, som ikke klarte å hindre uautorisert tilgang [6].

Etter å ha fått tilgang til anleggets nettverk, infiltrerte angriperne en ingeniørarbeidsstasjon ved enten å utnytte en sårbarhet i Windows-koden eller ved å fange opp en ansatts påloggingsinformasjon. Angriperne oppdaget også en "zero-day"-sårbarhet, noe som betyr at det var et sikkerhetshull i programvaren som var ukjent for produsenten. Hackere utnyttet denne sårbarheten til å angripe systemer før noen løsning eller oppdatering ble utgitt av programvareprodusenten i fastvare til Triconex-modellen eller Schneider Elektriske sikkerhetsinstrument system (SIS), som gjorde det mulig for dem å injisere kode i sikkerhetssystemenes minne for å sikre tilgang til kontrollerne når som helst. Angriperne brukte ulike taktikker for å unngå deteksjon, inkludert etterligning av legitime administratoraktiviteter.

2.3 BlackEnergy KillDisk (2015)

BlackEnergy-skadevare er en avansert programvare som brukes i cyberangrep. Den har flere funksjoner, inkludert å utføre massive DDoS-angrep for å krasje nettsider, ødelegge data på infiserte datamaskiner, stjele sensitiv og personlig informasjon, og opprette bakdørtilgang for angripere til å kontrollere systemene eksternt. Denne skadevare har blitt brukt i angrep mot ulike mål, inkludert kritisk infrastruktur og regjeringsorganisasjoner, og utgjør en alvorlig trussel mot datasikkerheten.

Det mest kjente tilfellet av skadevare som ble brukt til å angripe kraftforsyningsinfrastrukturer i Ukraina skjedde i desember 2015. En gruppe hackere, som mistenktes for å være statlige aktører, brukte en skadevare kalt "BlackEnergy" i kombinasjon med en annen skadelig programvare kalt "KillDisk" for å angripe kraftforsyningsselskaper.

BlackEnergy-skadevare ble brukt til å få tilgang til nettverket, mens KillDisk ble brukt til å slette systemfiler og lamme datamaskiner, noe som gjorde det vanskelig å gjenopprette normal drift. Hendelsen førte til økt bekymring for cybertrusler mot kritisk infrastruktur og har siden blitt brukt som et eksempel på potensielt farlige konsekvenser av cyberangrep mot energisystemer [7].

2.3.1 Konsekvenser

Den 23. desember 2015 ble det ukrainske strømnettet kraftig angrepet i det første kjente cyberangrepet mot et strømnett. Angrepet førte til strømavbrudd for nesten 230 000 forbrukere, som varte i flere timer. Skadene på nettet tok flere måneder å reparere fullstendig [7]. Angrepet var svært sofistikert og involverte bruk av BlackEnergy- og KillDisk-skadevare, fjernstyring av industrielle kontrollsystemer, og deaktivering av systemer som uavbrutt strømforsyning og modemer. Disse angrepene førte også til forstyrrelser i kommunikasjonen med forbrukerne, da et DoS-angrep ble rettet mot kundesentrene og hindret dem i å gi oppdatert informasjon. Det ble ansett som det første dokumenterte tilfellet der et cyberangrep direkte påvirket kritisk infrastruktur og forårsaket fysisk skade.

2.3.2 Sårbarheter

BlackEnergy-skadevare er farlig fordi den utnytter svakheter i datamaskiner og nettverk. Svakheter i programvare, dårlig sikkerhetspraksis blant brukere, og mangel på oppdateringer gjør det enkelt for BlackEnergy å angripe og forårsake skade. Denne skadevare kan spre seg raskt gjennom nettverk og infisere flere systemer, og dens skadelige handlinger kan føre til datatap, nedetid og personvernbrudd.

Beskyttelse mot BlackEnergy er avgjørende for å sikre datasystemene. Dette inkluderer å oppdatere programvare jevnlig, være forsiktig med mistenkelige e-poster og lenker, og sikre nettverket ordentlig. Ved å ta disse forholdsreglene, kan organisasjoner og enkeltpersoner redusere risikoen for å bli offer for BlackEnergy-skadevare og dens skadelige virkninger [7].

2.4 Industroyer (2016)

Industroyer er en sofistikert type skadevare designet for å forstyrre industrielle kontrollsystemer, spesifikt de som brukes i elektriske stasjoner. Den ble kjent etter å ha utløst et omfattende strømbrudd i Kiev, Ukraina, i desember 2016. Dette programmet er det fjerde kjente eksempelet på ondsinnet programvare rettet mot industrielle kontrollsystemer, etter Stuxnet, BlackEnergy 2 og Havex [8].

2.4.1 Konsekvensene

Manipuleringen av elektriske stasjoner og kontrollsystemer resulterte i omfattende strømbrudd for tusenvis av hjem i deler av Kyiv, Ukraina, i omtrent en time den 17. desember 2016. Angrepet inkluderte også manipulering av brytere i en elektrisk transformatorstasjon, noe som hindret operatørene i å gjenopprette normal drift. Disse hendelsene førte til betydelige økonomiske tap, forstyrrelser i strømforsyningen og i ekstreme tilfeller trusler mot liv og sikkerhet [9].

Strømbruddet hadde store konsekvenser for samfunnet og økonomien i Kiev. Det påvirket folks evne til å jobbe, kommunisere og utføre daglige aktiviteter. Bedrifter, transportnettverk og offentlige tjenester ble også alvorlig påvirket. Angrepet har ført til alvorlig skade på maskinvarekomponenter i nettverkskontroll- og telekontrollsystemer [8].

2.4.2 Sårbarheter

Industroyer utnytter spesifikke protokoller og sårbarheter som finnes i disse systemene, for eksempel IEC 60870-5-101 Protokollen kan være sårbar for man-in-the-middle-angrep, hvor en uautorisert tredjepart kan avlytte eller manipulere kommunikasjonen mellom master(server)- og slavenheter(klient). I tillegg kan manglende autentisering tillate angripere å få uautorisert tilgang til systemet.

Protokollen IEC 60870-5-104 er utsatt for sikkerhetssårbarheter. Hvis implementeringen av protokollen ikke er korrekt utført, kan det føre til buffer overflow. Buffer overflow oppstår når et program prøver å lagre mer data i en buffer enn det den har kapasitet til å håndtere. Dette gir angripere muligheten til å injisere ondsinnet programkode på enheten, noe som utgjør en sikkerhetstrussel.

IEC 61850 kan være sårbart for feilhåndtering av input, noe som kan føre til systemkrasj og gi angripere kontroll over enheten. En svakhet i autentisering kan tillate uautorisert tilgang til systemet.

OPC DA sårbarhet er at kommunikasjonen mellom klient og server kan være sårbar for avlytting eller manipulering hvis den ikke er tilstrekkelig sikret med kryptering eller autentisering. I tillegg har Industroyer også verktøy for portskanning og DoS-angrep mot Siemens SIPROTEC-enheter [10].

2.5 Sikringstiltak for OT-systemer

Sikringstiltak for OT-systemer er avgjørende for å beskytte industrielle prosesser og kritisk infrastruktur. OT-systemer brukes til å overvåke og kontrollere industrielle operasjoner. Disse systemene må være beskyttet mot trusler som kan skade deres tilgjengelighet og integritet. For å oppnå dette, følger organisasjoner ulike sikkerhetsstandarder og rammeverk som gir retningslinjer og beste praksis. De mest aktuelle sikkerhetsstandardene inkluderer ISO 27001, ISA/IEC 62443, NERC CIP og NIST Cybersecurity Framework. Dette kapittelet beskriver og sammenligner disse standardene [11].

2.5.1 Sikkerhetsstandarder ISO 27001

ISO 27001 gir en plan for å beskytte og sikre informasjonssystemer. Denne standarden, laget av International Organization for Standardization (ISO), hjelper organisasjoner med å beskytte sensitive data mot mulige trusler. Hovedpunktene i standarden inkluderer risikovurdering, der organisasjonen finner mulige trusler og svakheter, og setter inn tiltak for å redusere risikoen. Å bruke sterke sikkerhetstiltak som tilgangskontroll og kryptering er viktig for å beskytte informasjonen. Kontinuerlig overvåking og gjennomgang av sikkerhetssystemet sikrer at det fungerer godt og er oppdatert. Beredskapsplaner for sikkerhetshendelser gir veiledning om hvordan man skal reagere på og håndtere sikkerhetsbrudd. Fordelen med ISO 27001 er at den kan brukes i mange forskjellige bransjer og fokuserer på generell informasjonssikkerhet [11].

2.5.2 ISA/IEC 62443 - Standarder for automasjon- og kontrollsystemer

ISA/IEC 62443 er en serie standarder spesifikt utviklet for industrielle automasjon- og kontrollsystemer. Disse standardene gir omfattende retningslinjer inkludert tilgangskontroll for å forhindre uautorisert tilgang. Nettverkssikkerhet er en annen viktig komponent, med tiltak som nettverkssegmentering og bruk av brannmurer for å beskytte Industrielle-nettverk mot eksterne trusler. Programvaresikkerhet innebærer regelmessig patching og oppdatering av programvare for å fikse kjente sårbarheter. Beredskapsplaner og prosedyrer for hendelseshåndtering er avgjørende for å håndtere og gjenopprette etter sikkerhetshendelser. Regelmessige sikkerhetsvurderinger og revisjoner identifiserer mulige sårbarheter og iverksetter nødvendige tiltak. Fordelen med ISA/IEC 62443 er at den er spesielt utformet for industrien og gir omfattende retningslinjer for sikring av kritisk infrastruktur [11].

2.5.3 NIST – Rammeverk for cybersikkerhet

NIST er en veiledning for å forbedre cybersikkerhet. Den er basert på fem hovedområder: Identifisere og kartlegge alle fysiske eiendeler, gjennom å forstå organisasjons unike miljø kan man bedre lage sikkerhetstiltak. Oppdage sikkerhetshendelser gjennom kontinuerlige overvåking, respondere med riktig sikkerhets tiltak og tilslutt gjenopprette normal drift etter sikkerhet hendelse .[11].

2.5.4 NERC CIP – Standarder for elektrisitetsnettverket

NERC CIP standarder er rettet mot sikkerheten til elektrisitetsnettverket. standarder er utformet for å sikre påliteligheten og sikkerheten til strømnettet. Disse standardene dekker flere områder, inkludert tilgangskontroller for å hindre uautorisert tilgang, cybersikkerhet for å

lage nettverkssegmentering og jevnlige program oppdateringer. I tillegg beskytte eiendeler fysisk for å begrense tilgang til sensitive områder, til noen som ikke skal ha slik tilgang. Til slutt hendelseshåndtering når det oppstår og jevnlige sikkerhetsvurderinger [11].

2.5.4 Sammenligning av standarder

Når man sammenligner disse standardene, er det tydelig at ISO 27001 og NIST CSF er brede og kan brukes i mange industrier. mens ISA/IEC 62443 og NERC CIP er spesifikke for henholdsvis industriell automasjon og energisektoren.

ISA/IEC 62443 og NERC CIP gir mer detaljerte retningslinjer for sektorspesifikke behov henholdsvis innen automatisering og elektrisitet, mens ISO 27001 og NIST CSF gir mer generelle rammeverk. NIST CSF er svært fleksibel og tilpasningsdyktig, noe som gjør den egnet for organisasjoner med varierende sikkerhetsbehov og modenhet. Disse standardene tilbyr et rammeverk for risikostyring, implementering av sikkerhetskontroller, kontinuerlig overvåking og beredskapsplanlegging, noe som bidrar til å opprettholde integriteten og tilgjengeligheten til OT-systemer i ulike sektorer [11].

3 Konseptutvikling for miniatyrmodell

Dette kapittelet vil undersøke fire mulige løsninger for miniatyrmodeller av industrielle anlegg som kan brukes for testing, demonstrering og opplæring innen cybersikkerhet på OT-systemer. Disse inkluderer miniatyrmodeller av et vannkraftverk, et sorteringsanlegg, et roterende solcelleanlegg og et kombinert kraftverk. Løsningene vil beskrives ved hjelp av skisser, utstyrslister, og fordeler og ulemper ved den aktuelle løsningen fra et cybersikkerhetsperspektiv. De fire løsningene inkluderer også en del felles komponenter som blir tatt opp i delkapittelet under. Innholdet for hele kapittelet er kort oppsummert i punktene under.

- Felles komponenter for potensielle løsninger
- Miniatyrmodell av vannkraftverk
- Miniatyrmodell av sorteringsanlegg
- Miniatyrmodell av roterende solcelleanlegg
- Miniatyrmodell av kombinert kraftverk
- Oppsummering av potensielle løsninger

3.1 Felles komponenter for potensielle løsninger

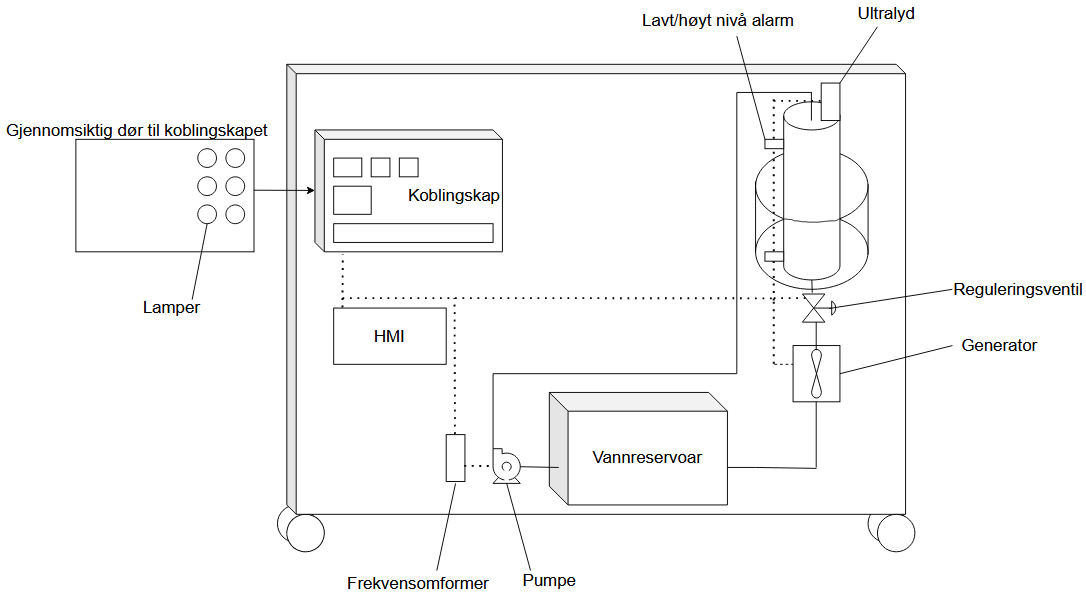
Alle fire løsningsforslagene vil ta utgangspunkt i de samme komponentene for styring og human machine interface (HMI). Dette inkluderer en programmerbar logisk styring (PLS) med lisens, switch, koblingsskap, strømforsyning (PSU), skaplamper, DIN-skinner og rekkeklemmer. Det kan også være aktuelt med tilleggsmoduler i noen av løsningene, og dette vil beskrives under den aktuelle løsningen. Tabell 3-1: Oversikt over felles komponenter med estimert pris (NOK). under gir en oversikt over felles komponenter som er med i koblingsskapet, inkludert HMI, monteringsvegg og lisens.

Tabell 3-1: Oversikt over felles komponenter med estimert pris (NOK).

Komponentliste for felles komponenter			
Komponent	**Beskrivelse**	**Antall**	**Estimert pris (NOK)**
HMI	Touchskjerm for styring og visning av data.	1	10000
Switch	Sammenkobling mellom PLS og HMI.	1	8500
PLS	PLS for styring av prosess.	1	4000
Strømforsyning	Strømforsyning til alle komponenter.	1	3000
Lisens	Lisens for PLS og HMI.	1	5000
Monteringsvegg	Monteringsvegg for montering av komponenter.	1	10000
Koblingsskap	Koblingsskap for komponenter til styring.	1	3000
Diverse	Rekkeklemmer, kabelkanaler og skaplamper.	-	2000
Total	-	-	**45500kr**

3.2 Miniatyrmodell av vannkraftverk

Den første potensielle løsningen er en miniatyrmodell av et vannkraftverk som kan brukes for simulering av cyberangrep. Figur 3-1 viser et mulig oppsett for anlegget. I figuren representer heltrukne linjer rør, og dottete linjer ledninger. Virkemåten til anlegget starter med at vannet blir ført opp fra vannreservoaret til vannmagasinet via en pumpe som blir styrt av en frekvensomformer. I vannmagasinet blir vannivået målt av en ultralyd, i tillegg til to nivåvakter som virker som en høy og en lav alarm. For å styre mengden vann som renner til generatoren brukes det en reguleringsventil. Vannet som renner gjennom generatoren, ender da opp tilbake i vannreservoaret.



Figur 3-1: Skisse for miniatyrmodell av vannkraftverk.

3.2.1 Styring av modellen

For å styre anlegget vil det bli brukt en PLS i sammenheng med en HMI-skjerm. PLS-en vil kunne styre vannivået i magasinet via frekvensomformeren og hvor mye som vann som renner gjennom generatoren via reguleringsventilen. PLS-en vil ta inn alle signalene fra de forskjellige sensorene slik at den kan styres automatisk via en PID-løsning (proporsjonal integrasjon derivasjon), eller kan styres manuelt ved hjelp av HMI-skjermen. Fra HMI-skjermen kan informasjon fra sensorer og strømproduksjon overvåkes. Det vil også være lamper på utsiden av koblingsskapet som vil informere om forskjellige statuser som høyt/lavt nivå, om anlegget er i drift og om generatoren produserer strøm.

3.2.2 Komponentoversikt for modellen

Komponentoversikten er laget som en generell liste over komponenter som må til for å bygge vannkraftmodellen. Tabell 3-2 under viser den generelle oversikten, med beskrivelse av komponentene, antall komponenter og estimert pris.

Tabell 3-2: Komponentliste for vannkraftmodellen med beskrivelse, antall og estimert pris (NOK).

Komponentliste for vannkraftmodell			
Komponent	**Beskrivelse**	**Antall**	**Estimert pris (NOK)**
Pumpe	Pumpe som fører vann fra reservoar til magasin.	1	3000
Frekvensomformer	Frekvensomformer til styring av pumpa.	1	4000
Ultralyd nivåmåler	Nivåmåler for vannstand i magasinet.	1	4000
Reguleringsventil	Ventil som styrer vannstrøm til generator.	1	3000
Nivåvakt	Nivåvakt for feilsikring av vannstanden.	2	2000
Generator	Turbin som produserer lesbar spenning.	1	2000
Diverse	Vanntanker og fester.	-	4000
Felles komponenter	Komponenter til koblingsskap (se tabell 3-1).	-	45500
Total			**67500kr**

3.2.3 Utsatte deler og konsekvenser ved cyberangrep

Ved eventuelt cyberangrep er det først og fremst pumpa og reguleringsventilen som er utsatt. Konsekvenser inkluderer full stopp av prosessen, som kan oppnås ved å stoppe pumpen. Det er også mulighet for oversvømmelse i vannmagasinet dersom ventilen stenges helt, og pumpen fortsetter å kjøre. Konsekvensen av dette er både oversvømmelse av vann, og tap av potensiell strømproduksjon.

3.2.4 Fordeler ved modellen

En fordel er at det vil være flere måter å se når et angrep har blitt utført, både fysisk på prosessen og visuelt via HMI og statuslamper. Dette gjør løsning aktuell for testing, demonstrasjon og opplæring av cybersikkerhet. Anlegget vil også få brukt mye utstyr som brukes i industrien, noe som gjør det til en mer realistisk modell for simulering av et reelt vannkraftverk. Det blir også en del plass som settes til fremtidig videreutvikling, slik at modellen kan oppdateres og holdes i bruk over en lengere periode. Flere av de viktigste fordelene er kort oppsummert i punktene under.

- Løsningen simulerer en realistisk prosess som er relevant, spesielt i Norge.
- Komponentene holder industristandard.
- Modellen gir rom for videre utvikling og utvidelse.
- Demonstrerer tydelige konsekvenser ved cyberangrep.

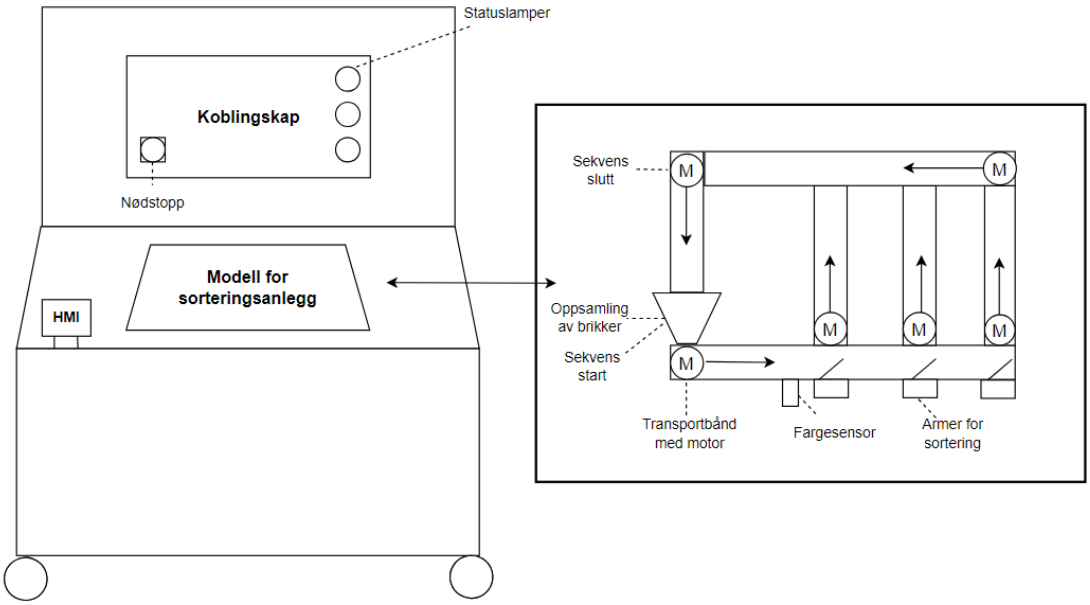
3.2.5 Ulemper ved modellen

En av de større utfordringene blir å designe en bevegelig modell av en vannprosess uten å ha noe mulighet for søl. Dette kan føre til komplikasjoner i bygge- og planleggingsprosessen. Spesielt under byggingsperioden vil det kreve en god utføring av at rør og komponenter blir montert riktig slik at det ikke blir noe lekkasje i fremtiden. Siden det er et mindre anlegg i forhold til industrien kan det være vanskelig å finne deler som passer til en miniatyr modell. Det er også ønskelig å ha så mange industrielle komponenter som mulig dette gjør at prosjektet kommer til å bli dyrere. Flere av de viktigste ulempene er kort oppsummert i punktene under.

- Fare for lekkasje og vannsøl, spesielt etter lengre tid.
- Det kan være vanskelig å finne komponenter som passer modellen.
- Krever kompetanse innenfor rør og tetting.
- Tilpassede deler kan gjøre modellen kostbar.

3.3 Miniatyrmodell av sorteringsanlegg

Det andre løsningsforslaget baserer seg på et anlegg for sortering. Anlegget vil benytte ett instrument for dosering som legger brikker på et transportbånd. En fargesensor er installert for å skille mellom ulike fargene på brikkene, og armer skyver brikkene videre til riktig transportbånd. Brikkene ender opp i en beholder for oppsamling (instrument for dosering) som gjør det mulig for systemet å kjøre i loop. Modellen vil settes på en flyttbar benk for enkel transportering. Figur 3-2 under illustrerer hvordan anlegget kan se ut.



Figur 3-2: Skisse for miniatyrmodell av sorteringsanlegg. Modellen er plassert på en flyttbar benk med koblingsskap.

3.3.1 Styring av modellen

For styring av anlegget vil det benyttes en PLS som monteres i koblingsskapet. Denne vil koordinere operasjonene i anlegget, og ved hjelp av sensorene, sørge for at brikkene blir sortert riktig. Det er også satt opp en HMI hvor det er mulig å styre anlegget manuelt, sette anlegget i automatisk drift, og se alarmer og oversikt over sensorer. Det vil også installeres en switch i koblingsskapet som sørger for kommunikasjon mellom alle komponentene i anlegget, inkludert ekstern PC.

3.3.2 Komponentoversikt for modellen

Komponentoversikten er laget som en generell liste over komponenter som må til for å bygge sorteringsanlegget. Tabell 3-3 under viser den generelle oversikten, med beskrivelse av komponentene, antall komponenter og estimert pris.

Tabell 3-3: Komponentoversikt for modell av sorteringsanlegg inkludert estimert pris (NOK).

Komponentoversikt for modell av sorteringsanlegg			
Komponent	**Beskrivelse**	**Antall**	**Estimert pris (NOK)**
Fargesensor	Fargesensor som skiller brikker basert på ulike farger.	1	4000
Transportbånd	Transportbånd for frakt av brikker.	6	6000
DC-motorer	Motorer til transportbånd.	6	2500
Lineær aktuator	Armer for sortering av brikker.	3	4500
Felles komponenter	Felles komponenter i koblingsskap. (se Tabell 3-1)	-	45500
Total			**62500kr**

3.3.3 Utsatte deler og konsekvenser ved cyberangrep

Ved eventuelle angrep er det flere deler av anlegget som er utsatt. Angrep på PLS-en kan gi konsekvenser som tap av kontroll over prosessen, noe som fører til avbrudd kontinuitet og overvåkning. Angrep kan også rettes direkte mot styringen og føre til konsekvenser som, feil hastighet på transportbånd, feil sortering, blokkering med sorteringsarmer, eller full stopp.

3.3.4 Fordeler ved modellen

Det er flere fordeler knyttet til modellen for sorteringsanlegget som bygger løsbarhet og hvor aktuell løsningen er i forhold til angrep på reelle anlegg. Modellen for sorteringsanlegget er en åpen løsning som kan representere flere ulike prosesser, som sortering av varer, produkter, avfall og mye mer. Flere av de viktigste fordelene er kort oppsummert i punktene under.

- Prosessen er enkel å forstå.
- Tydelige demonstrering av konsekvenser ved cyberangrep.
- Modulbasert (prosessen kan forenkles og utvides etter ønske).
- Representerer en rekke realistiske prosesser.

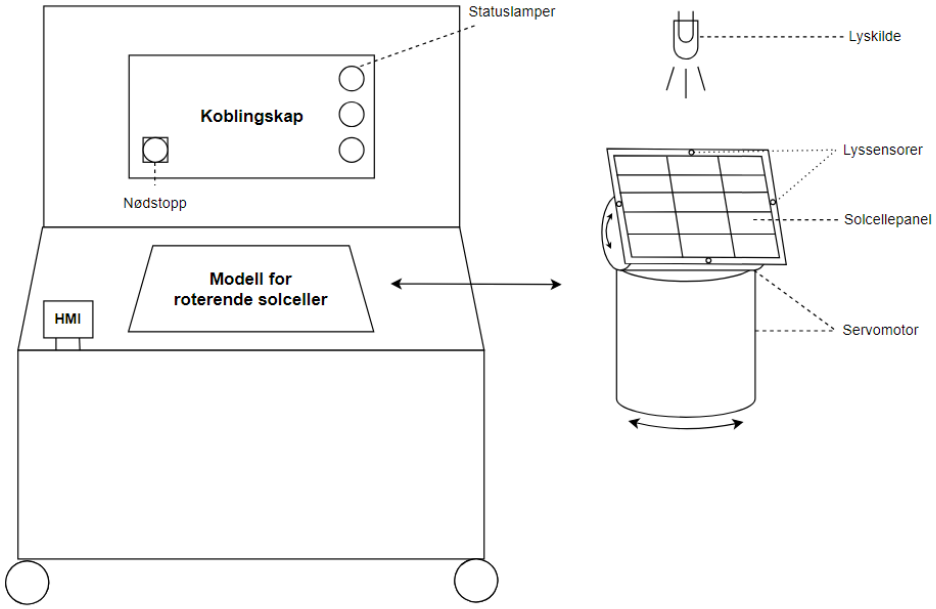
3.3.5 Ulemper ved modellen

Det er også ulemper ved modellen for sorteringsanlegget, spesielt når det kommer til løsbarhet og praktikalitet. Det er blant annet en utfordring at brikker setter seg fast mellom transportbånd, i sorteringsarmer eller i samlepunktet gjennom prosessen, som hindrer kontinuiteten til prosessen. Flere av de viktigste ulempene er kort oppsummert i punktene under.

- Kostbart og vanskelig å finne riktige komponenter i miniatyrstørrelse.
- Fare for at brikkene setter seg fast eller faller av under transportering.

3.4 Miniatyrmodell for roterende solcelleanlegg

Den tredje potensielle løsningen er en miniatyrmodell av et roterende solcelleanlegg. Fire lyssensorer brukes til å måle orienteringen til panelet i forhold til sola, eller i dette tilfellet en alternativ lyskilde. En servomotor brukes til å justere rotasjon på panelet i forhold til himmelretning/kompassorientering. Posisjonen til denne motoren justeres på bakgrunn av verdiene som leses ut av lyssensorene på venstre og høyre side av panelet. En annen servomotor brukes til å tilte panelet vannrett til loddrett. Posisjonen til denne motoren justeres etter verdiene lest av fra lyssensorene på toppen og bunnen av panelet. Systemet fungerer optimalt når panelet peker direkte mot lyskilden. Figur 3-3 illustrerer systemskisse av solcelle som roterer med lyskilde.



Figur 3-3:Systemskisse solcellepanelløsning. Viser en solcelle som roteres mot lyskilde, plassert på en flyttbar benk.

3.4.1 Styring av modellen

Anlegget skal styres med en PLS og det er flere måter å programmere denne på. Orientering kan enten styres manuelt, forhåndsprogrammeres ved hjelp av timer, eller reguleres automatisk ved hjelp av lyssensorene. Fra HMI-en skal det kunne stilles inn manuell eller automatisk styring av servomotorene.

3.4.2 Komponentoversikt for modellen

Komponentoversikten er laget som en generell liste over komponenter som må til for å bygge det kombinerte kraftverket. Tabell 3-4 under viser den generelle oversikten, med beskrivelse av komponentene, antall komponenter og estimert pris.

Tabell 3-4: Komponentoversikt for solkraftverk med beskrivelse, antall og estimert pris (NOK).

Komponentoversikt for roterende solcelleanlegg			
Komponent	**Beskrivelse**	**Antall**	**Estimert pris (NOK)**
Lyssensor	Lyssensor for deteksjon av lys.	10	120
Servomotor	Motor som roterer panel ut ifra lysets vinkel.	2	2500
Solcellepanel	Solcellepanel for produksjon av spenning.	1	1000
Lyskilde	Lyskilde for solcellepanelet.	1	500
LED	LED for illustrert produksjon.	1	300
Felles komponenter	Felles komponenter i koblingsskap (se Tabell 3-1).	-	45500
Total			**49920kr**

3.4.3 Utsatte deler og konsekvenser ved cyberangrep

Solcelleanlegget har flere sårbarheter og angrepsvinkler. Et angrep på PLS-en kan føre til tap av kontroll over styringen av solcellenes rotasjon og føre til energitap. Her er det også mulighet for at angriperen styrer rotasjonen av servomotorene i motsatt retning av lyskilden. En angriper kan også forsøke å koble ut lyssensorene, noe som kan ødelegge for automatisk regulering av posisjon, eller i verste fall skade på systemet. Et annet alternativ kan være å rotere enhetene såpass mange ganger om seg selv at det kan føre skade på koblingen av komponenter, eller solcellepanelene.

3.4.4 Fordeler ved modellen

Det er flere fordeler knyttet til solkraftmodellen som bygger løsbarhet og hvor aktuell løsningen er i forhold til angrep på reelle anlegg. Solcelleteknologi blir stadig viktigere for bærekraftig energiproduksjon, noe som fører til økt etterspørsel for sikkerhetsprodukter. Dette gjør modellen aktuell i forhold til reelle anlegg og gir et realistisk bilde når det kommer til cybersikkerhet. Flere av de viktigste fordelene er kort oppsummert i punktene under.

- Modellen kan utvides eller forenkles etter ønske.
- Modellen representerer et realistisk og aktuelt anlegg.
- Det er flere vinkler og konsekvenser ved cyberangrep.

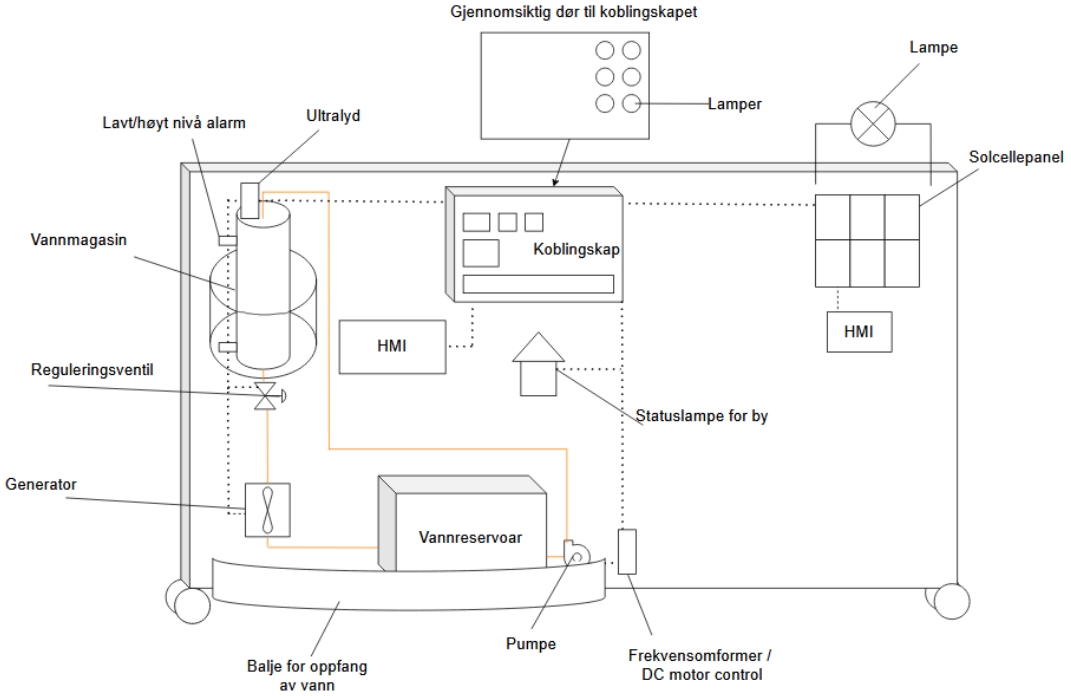
3.4.5 Ulemper ved modellen

Det er flere ulemper knyttet til modellen for roterende solcelleanlegg som baserer seg på kompleksitet, og lite visuelle konsekvenser ved angrep. Programmeringen av servomotorene som styrer posisjonen til solcellene kan vise seg å være komplekst og by på utfordringer. I tillegg er fysiske konsekvenser ved angrep på modellen lite visuelle. Flere av de viktigste ulempene er kort oppsummert i punktene under.

- Det kan vise seg å være komplekst å programmere servomotorene.
- Konsekvenser av angrep er ikke så visuelle og egner seg derfor ikke like godt for demonstrering av cyberangrep.

3.5 Miniatyrmodell for kombinert kraftverk

Det fjerde og siste løsningsforslaget er basert på en kombinasjon av løsningsforslag for vannkraftsmodellen og solcellemodellen. Figur 3-4 viser en skisse for oppsettet av det kombinerte kraftverket. Her er det et koblingsskap som er plassert sentralt på en flyttbar vegg. Koblingsskapet inneholder en nettverk-switch, to PLS-er for styring av anleggene, tilleggsmoduler for PLS-er og en strømforsyning. Utenpå skapet er det montert lamper som indikerer driftsstatus og en nødstopp. I tillegg settes det en HMI under koblingsskapet som gir oversikt over vannkraftverket. Til høyre for koblingsskapet er et solcellepanel plassert med en lampe som simulerer sola og en HMI for drift av anlegget. Til venstre for koblingsskapet ligger vannkraftanlegget med to tanker, en pumpe, en generator, en ultralyd nivåmåler og en ventil. I tillegg er det lagt til baljer for oppsamling ved eventuell lekkasje. Under koblingsskapet er det montert lamper som simulerer strømmen i en by eller husstand, produsert av kraftverkene.



Figur 3-4:Skisse av miniatyrmodellen for kombinert kraftverk.

3.5.1 Styring for modellen

Modellen av det kombinerte kraftverket vil styres ved hjelp av to PLS-er. En PLS vil styre vannkraftverket som inkluderer styring av pumpe, reguleringsventil og sende informasjonen til en HMI. Styringen for pumpen vil basere seg på input fra ultralyd nivåmåler og nivåvakter for å holde vannivået innenfor satte grenser. Reguleringsventilen kontrollerer vannstrømmen fra magasintanken, gjennom generatoren og vil styres basert på generatorens strømproduksjon, med settpunkt som kan stilles inn på HMI-en. Den andre PLS-en vil styre solkraftverket og sende informasjon til den andre HMI-en som viser strømproduksjon for solcellepanelet.

Lampen over solcellepanelet skal styres ved hjelp av settpunkt for strømproduksjon. I tillegg skal pumpa, reguleringsventilen og lamper kunne styres manuelt fra HMI-ene.

3.5.2 Komponentoversikt for modellen

Komponentoversikten er laget som en generell liste over komponenter som må til for å bygge det kombinerte kraftverket. Tabell 3-5 under viser den generelle oversikten, med beskrivelse av komponentene, antall komponenter og estimert pris.

Tabell 3-5: Oversikt for komponenter med beskrivelse, antall og estimert pris (NOK).

Komponentoversikt for kombinert kraftverk			
Komponent	**Beskrivelse**	**Antall**	**Estimert pris (NOK)**
Analog I/O	Tilleggsmodul med analoge inn- og ut-ganger	1	4000
Solcellepanel	Solcellepanel for produksjon av spenning.	1	500
Lyskilde	Lyskilde for solcellepanelet.	1	500
LED-lys	LED for illustrert produksjon.	1	300
Pumpe	Pumpe som fører vann fra reservoar til magasin.	1	3000
Frekvensomformer	Frekvensomformer til styring av pumpa.	1	4000
Ultralyd nivåmåler	Nivåmåler for vannstand i magasinet.	1	4000
Reguleringsventil	Ventil som styrer vannstrøm til generator.	1	3000
Generator	Turbin som produserer lesbar spenning.	1	2000
Nivåvakt	Nivåvakt for feilsikring av vannstanden.	2	2000
Felles komponenter	Felles komponenter til koblingsskap (se Tabell 3-1)	-	45500
Total			**68800kr**

3.5.3 Utsatte deler og konsekvenser ved cyberangrep

Ved angrep er det først og fremst pumpa og ventilen som er mest utsatt for ekstern påvirkning. Et angrep på disse delene vil få konsekvenser for selve prosessen, og vises tydelig ved minket strømproduksjon og oversvømmelse. Hver enkelt PLS, og HMI, vil også være aktuelle deler for angrep, og konsekvenser kan være tap av kontroll og overvåking av prosessen eller full stopp.

3.5.4 Fordeler ved modellen

Det er flere fordeler ved det kombinerte kraftverket som bygger løsbarhet og hvor aktuell løsningen er i forhold til angrep på reelle anlegg. Det kombinerte kraftverket vil benytte komponenter som er utbredt i industrien, noe som gjør modellen godt egnet for testing, demonstrering og opplæring innen cybersikkerhet i OT-systemer. Det vil være flere måter å enkelt oppdage når et angrep har skjedd, både fysisk i prosessen og visuelt via HMI og statuslamper. Flere av de viktigste fordelene er oppsummert i punktene under.

- Det kommer tydelig frem når cyberangrep er utført på anlegget.
- Det er mange angrepsvinkler og konsekvenser som gjør modellen godt egnet for testing, demonstrering og opplæring innen cyberangrep på OT-systemer.
- Modellen for det kombinerte kraftverket representerer reelle anlegg, både i virkemåte, og i sårbarheter og konsekvenser.
- Modellen legger til rette for tilpassinger og utvidelser.

3.5.5 Ulemper ved modellen

Det er flere ulemper knyttet til det kombinerte kraftverket som baseres på løsbarhet og kompleksitet til anlegget. Det kan være utfordrende og kostbart å finne riktige komponenter som både fungerer sammen, og har riktig størrelse for modellen. Flere av de viktigste ulempene er oppsummert i punktene under.

- Anlegget baserer seg i stor grad på analoge signaler, som kan være krevende å jobbe med ovenfor digitale signaler.
- Anlegget har en risiko for lekkasje og vannsøl, og krever kompetanse innen rør.
- Pumpen skal ikke kjøres tørr, så bruk av anlegget krever forståelse.
- Det kan vise seg utfordrende og kostbart å finne miniatyrkomponenter som fungerer sammen, og samtidig passer i modellen.

3.6 Oppsummering av løsningsforslagene

Modellen for vannkraftverket simuleres ved hjelp av pumpe, reguleringsventil og en generator for strømproduksjon. Anlegget styres med PLS og HMI for automatisk eller manuell drift. Fordeler inkluderer realistisk simulering, mens ulemper omfatter kompleks bygging og potensielle lekkasjeproblemer.

Modellen for sorteringsanlegget sorterer brikker ved hjelp av fargesensor og transportbånd og lineære aktuatorer. PLS-styring og HMI benyttes for manuell og automatisk drift av modellen. Fordeler inkluderer enklere implementering og mindre søl. Ulemper kan være behov for stor plass og begrenset transportmulighet.

Modellen for roterende solceller justerer solcellepaneler etter lyskilden ved hjelp av servomotorer og lyssensorer. Programmerbar styring og simulert sollys. Fordeler inkluderer bærekraftig energiproduksjon og mens ulemper inkluderer avhengighet av analoge signaler.

Kombinert Kraftverk Miniatyrmodell kombinerer vann- og solkraftverk i en modell med PLS-styring og HMI. Fordeler inkluderer realistisk simulering og bredt kompetansebehov, men ulemper inkluderer kompleksitet i implementering.

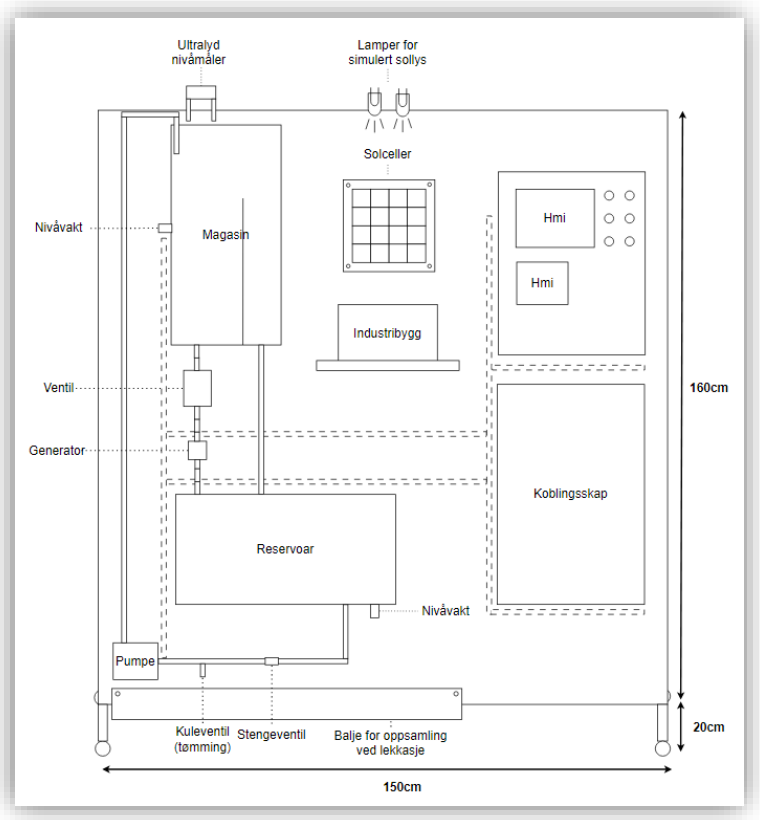
4 Planlegging og tilpassing for modell av kombinert kraftverk

Dette kapittelet vil ta for seg planlegging, tilpassing og alle forberedelser som er gjort i forbindelse med det kombinerte kraftverket i forkant av montering. Dette kommer frem ved hjelp av skisser, bilder og beskrivelser for virkemåte og planlagt utførelse av arbeid. Målet med kapittelet er å gi en oversikt over alt arbeid som er lagt inn i forkant av montasje. Innholdet i kapittelet er oppsummert i punktene under.

- Systemoversikt og virkemåte
- Komponentoversikt og kostnadsestimering
- Dimensjonering og tilpassing
- Oppsett og konfigurasjon av nettverk

4.1 Systemoversikt og virkemåte

Figur 4-1 viser en dimensjonert skisse for monteringsveggen. Dimensjonene er basert på informasjon tilknyttet komponentene og er hentet fra datablader, produktsider og egenlagde dimensjonerte skisser. Systemskissen er designet for å gi oversikt over plassering av komponenter og utnyttelse av plass, før komponentene blir montert. Modellen består av et forenklet vannkraftverk og solkraftverk. Virkemåten til modellen vil vurderes opp mot reelle kraftverk i underkapitlene.



Figur 4-1: Dimensjonert skisse av monteringsvegg og komponenter.

4.1.1 Komponentoversikt

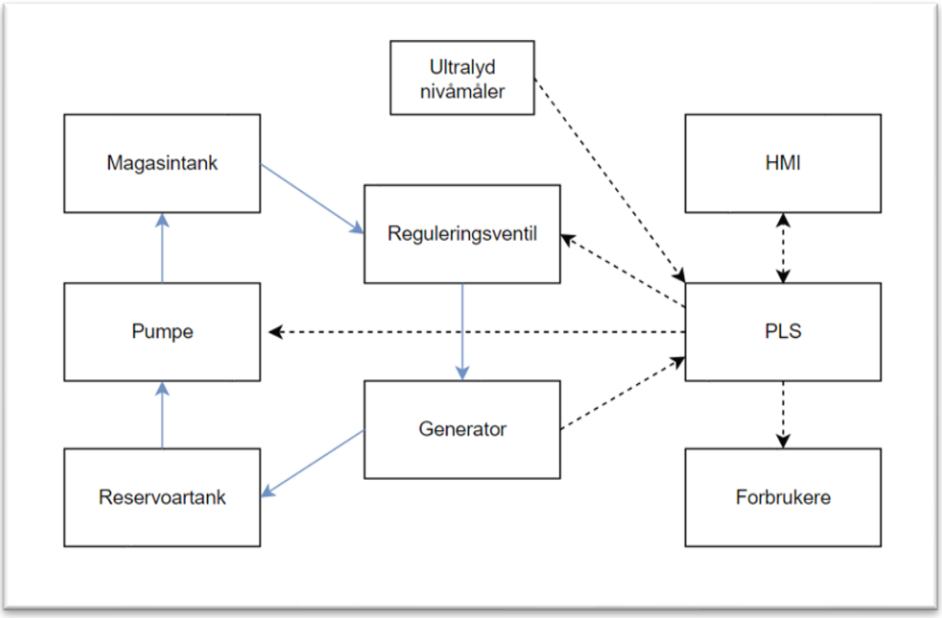
Tabell 4-1 er en komponentliste gir en oversikt over de viktigste komponentene som må til for å bygge det kombinerte kraftverket. Lista gir en oversikt over aktuelle komponenter og krav som stilles for at komponentene skal fungere sammen. Det er også inkludert en estimert pris basert på hva komponentene omtrentlig kommer til å koste. Dette gir et grunnlag for hva den totale kostnaden blir i forhold til prosjektets budsjett. viser estimert totalpris på 92600kr.

Tabell 4-1: Komponentliste for kombinert kraftverk med krav til komponenter og estimert pris.

Komponentoversikt med krav for kombinert kraftverk				
Komponent	**Krav 1**	**Krav 2**	**Antall**	**Pris (NOK)**
Vannpumpe	6-20 Liter/Min	Kontinuerlig drift.	1	2000
Reguleringsventil	1-10V, 1/2 til 3/4"		1	3000
Generator	1/2 til 3/4"	Lang levetid, miniatyrturbin.	1	500
Vanntanker	20+ Liter	Gjennomsiktig og robust.	2	14000
Slanger/rør og fester	4m, 1/2" til 3/4"	Slangenipler messing.	-	1500
Kuleventil	1/2"		2	200
Ultralyd	4-20mA	4-20mA<10cm blindsone.	1	2000
Nivåvakter	Må kunne festes i tanken.		2	3000
Vannkraftverk				**26200**
Solceller	Målbar produsert spenning		1	500
Feste solceller	Ikke-ledende materiale		1	500
Lamper	24V	Gir effekt på solceller	2	400
Solkraftverk				**1400**
PLS	24V		2	8000
I/O-tilleggsmodul	Analoge inn- og utganger.		2	11000
Switch	6+ innganger.	Industriell, span-port.	1	8500
Strømforsyning	24V	Kraftig nok for alle komponenter.	1	4000
HMI Stor	Kobling med PLS	Touchskjerm.	1	10000
HMI Liten	Kobling med PLS	Touchskjerm.	1	6000
Koblingsskap	Gjennomsiktig deksel.	Bakplate i skapet.	1	4000
Kontaktor	tåler 230V, 24V spole		4	2000
Kabler og diverse	Cat6 ethernet, RK.		-	1500
Koblingsskap				**55000**
Monteringsvegg	Låsbare hjul.	Får plass gjennom dører.		**10000**
Totalpris	< 100 000kr			**92600kr**

4.1.2 Planlagt virkemåte for vannkraftmodellen

Vannkraftanlegget fungerer ved å pumpe vann fra reservoaret til magasinet. En reguleringsventil regulerer mengden vann som slippes gjennom en generator for strømproduksjon, før det returneres til reservoaret. Anlegget skal enten kunne styres manuelt via HMI, eller settes til automatisk drift. Ved automatisk drift benyttes verdier fra ultralyd nivåmåler for å styre pumpen, basert på vannstanden i magasintanken. Figur 4-2 viser systemoversikt for vannkraftmodellen, med stiplede piler som representerer elektriske signaler, og blå piler som representerer vannstrømmen.



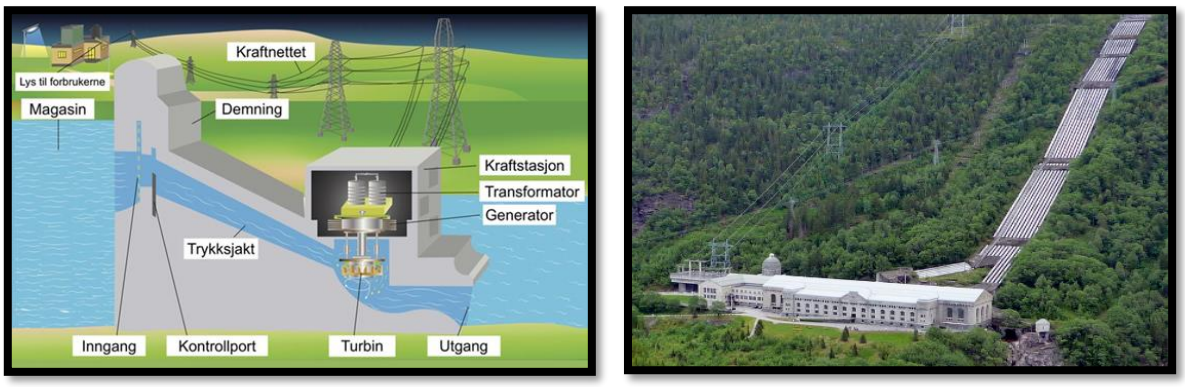
Figur 4-2: Systemskisse for vannkraftmodellen. Stiplede piler representerer elektriske signaler, og blå piler som representerer vannstrømmen.

4.1.3 Forskjellen mellom modellen og reelt kraftverk

Et vannkraftverk utnytter vannets potensielle energi fra fjell og nedbør ved å demme det opp i magasiner. Når vannet slippes ned gjennom rør til et kraftverk med turbiner, skaper det roterende bevegelse som driver generatorer og produserer strøm. En regulator justerer vannmengden for å kontrollere turbinens hastighet. Generatoren omdanner denne bevegelsesenergien til elektrisitet. En transformator øker spenningen før strømmen sendes ut på strømnettet. Et kontrollsystem alle prosessene og overvåker dem med sensorer. Operatører kan styre alt fra et kontrollrom, selv om anlegget også kan operere uten bemanning via en driftssentral.

Forskjellen mellom et reelt vannkraftverk og miniatyrmodellen ligger i skalaen og kompleksiteten. Mens et reelt vannkraftverk håndterer enorme vannmengder og genererer store mengder elektrisitet, er modellen designet for å demonstrere prinsippene i mindre skala og med fokus på læring og demonstrering. Modellen bruker mindre komponenter og vannmengder, men følger samme grunnleggende virkemåte for å illustrere prosessene i en fullskala

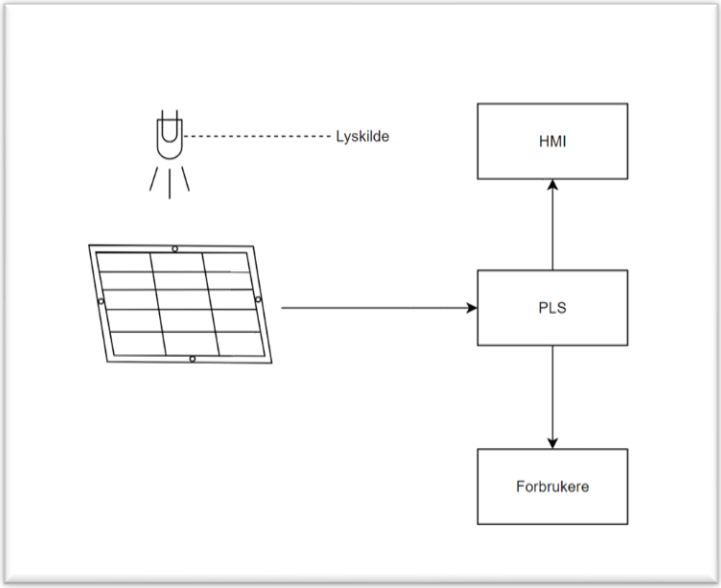
vannkraftverk [12]. Figur 4-3 viser en systemoversikt av et reelt vannkraftverk til venstre, og hvordan et vannkraftverk kan se ut til høyre.



Figur 4-3: virkemåten av et reelt vannkraft [13], [14].

4.1.4 Planlagt virkemåte for solkraftmodellen

Solkraftanlegget fungerer ved at lampene lyser direkte inn på solcellepanelet for å simulere sollys. Solcellepanelet produserer strøm som både indikeres med lys i byen og på HMI-en. HMI-en kan brukes for å slå lampen av og på, vise relevant data, alarmer og status for anlegget. For å sikre at nok strøm blir produsert til byen til enhver tid, vil anleggene kommunisere og skru seg av eller på ved overproduksjon eller mangel på strøm. Figur 4-4 viser systemskissen for den planlagte virkemåten for solkraftmodellen.

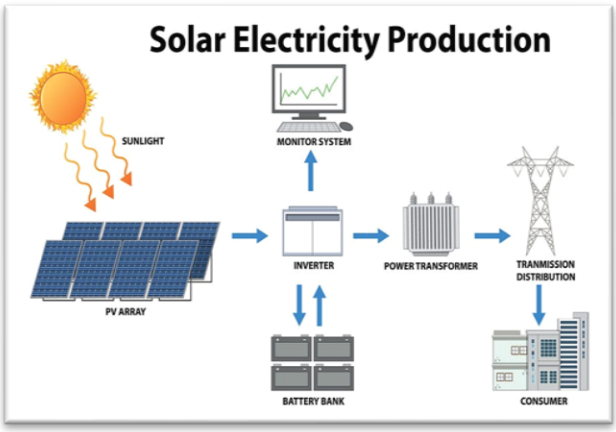


Figur 4-4: Systemskisse for solkraftmodellen.

4.1.5 Forskjellen mellom modellen og reelt kraftverk

Solenergi omdannes til elektrisitet ved hjelp av solcellepaneler. Når sollys treffer solcellene, laget av halvledermaterialer som silisium, absorberes fotoner som frigjør elektroner. Elektriske felt i solcellene skaper en strøm av disse elektronene, genererende likestrøm (DC).

Denne likestrømmen konverteres til vekselstrøm (AC) ved hjelp av en inverter for å kunne brukes av vanlige apparater eller sendes til strømnettet. For å lagre elektrisitet til senere bruk, kan den lagres i en batteribank som også lagrer likestrøm. Den lagrede strømmen kan konverteres tilbake til vekselstrøm ved behov. Den genererte og eventuelt lagrede elektrisiteten kan sendes til et kraftnett eller brukes lokalt i bygninger og apparater [15]. Figur 4-5 viser illustrasjon av reelt solkraftverk og solpanel.



Figur 4-5: Virkemåten av reelt solkraftverk satt opp mot solkraftverket i modellen.

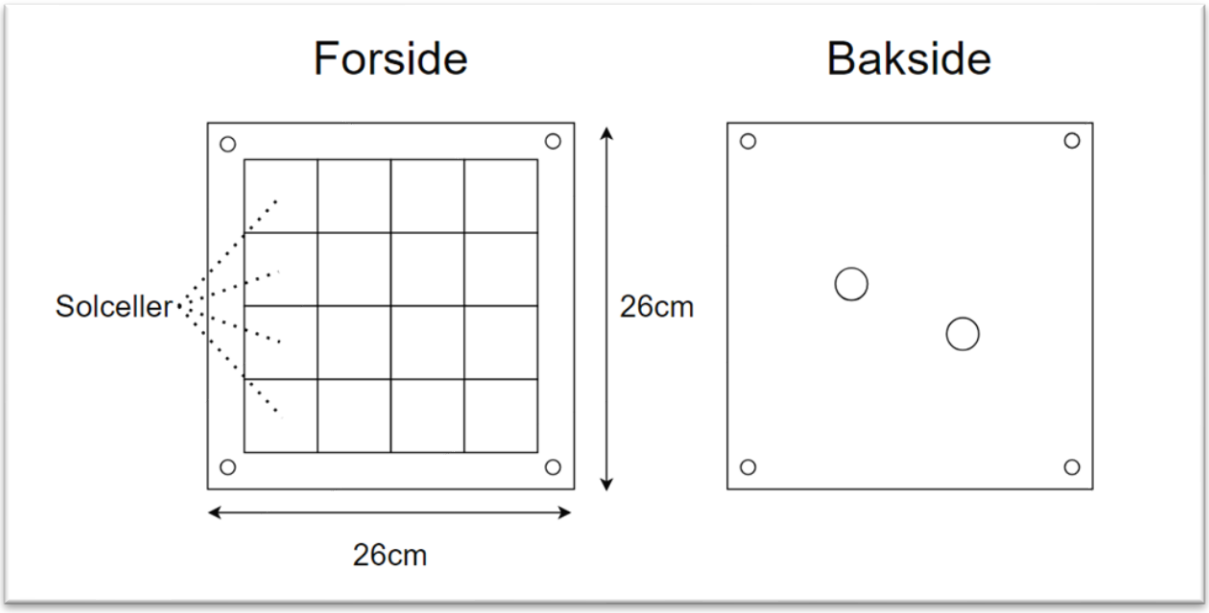
Forskjellen mellom et ekte solkraftverk og modellen er skalaen og kompleksiteten. Det ekte anlegget bruker sollys og lager strøm til mange husholdninger eller industrier, mens modellen bruker en lampe og lager strøm i en liten skala for å vise hvordan prinsippene fungerer. Modellen er designet for å være pedagogisk og enklere å håndtere.

4.2 Dimensjonering og tilpassing

Det er flere ulike deler av modellen som må tilpasses for å passe sammen med andre komponenter i forhold til plass og plassering. Dette delkapittelet vil ta for seg tilpassingene og planleggingen som er gjort tilknyttet vanntanker, solceller, koblingsskap, og område for illustrert strømproduksjon.

4.2.1 Tilpassing av solceller

Solcellepanelet må festes, og som løsning på dette er det tenkt at panelet skal festes på en bakplate som boltes i veggen. Figur 4-6 viser hvordan forsiden av platen har solcellepanelet festet på seg. med bolter i hvert hjørne, og baksiden viser åpning for kabler. Med denne løsningen vil det være enkelt å feste panelet, og det gir rom for justering av vinkel på platen ved hjelp av boltene.

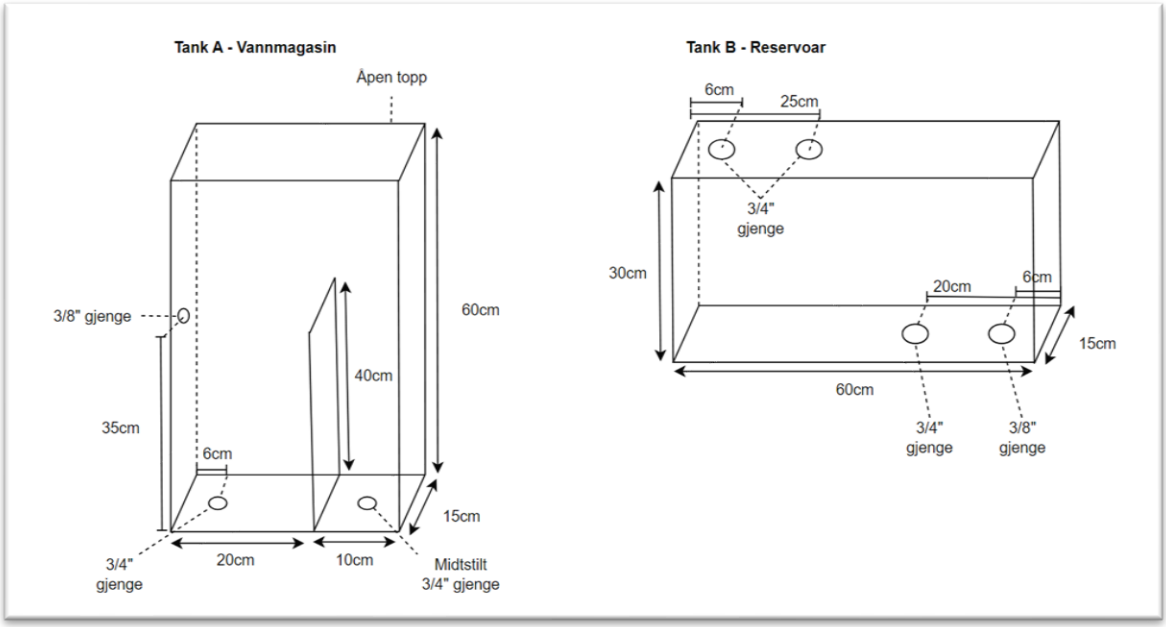


Figur 4-6: Solceller plassert på en plate med åpninger for kabler.

4.2.2 Design og bestilling av vanntanker

Vanntankene er noen av de mer utsatte delene ved modellen, og det er viktig at de er designet og bygget skikkelig. Det er derfor utarbeidet skisser for tankene med dimensjoner, plassering og størrelse på gjenger, som vist i Figur 4-7 under. Materialet på tankene skal ønskelig være gjennomsiktig, samtidig som det skal tåle transport i varebil, og det ble derfor valgt plexiglass. Begge tankene er designet med en lik og smal dybde for å redusere horisontal belastning på veggen. Tankene er også designet ut ifra volum slik at pumpen aldri går tørr og vannmagasinet (tank A) aldri oversvømmes. Volumet til hver tank er 27L, men som vist i Figur 4-7 er det i tank A montert en skillevegg hvor vannet som renner over veggen tilbakeføres direkte til Tank B. Vannmagasinet vil derfor kunne holde maksimalt 12L.
Gjengene i bunn av tank A og toppen av tank B er plassert slik at slanger eller rør kan trekkes

vertikalt mellom tankene. Gjengenes størrelse er 3/4" der hvor rør eller slanger skal settes inn, og 3/8" for innfesting av nivåvakter.



Figur 4-7: Skisser av vanntanker med dimensjoner og plassering av gjenger.

4.2.3 Vannsikkerhet - oppsamlingskar under vannsystemet

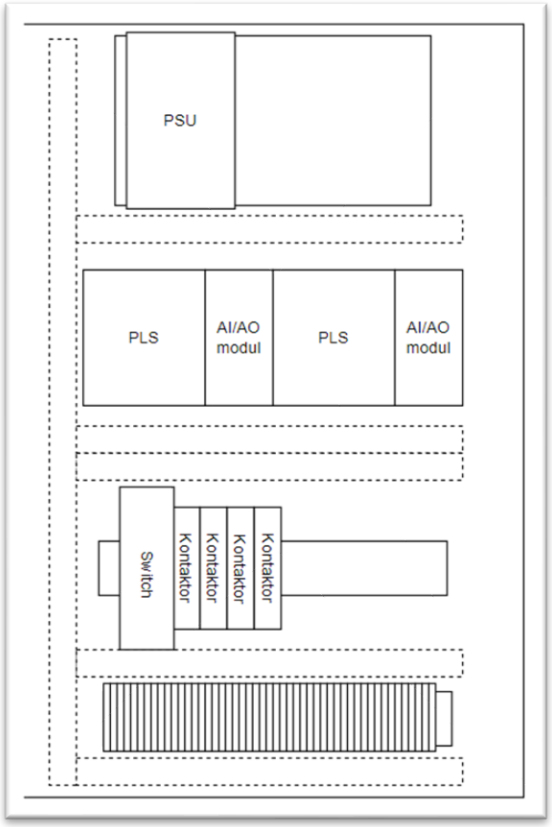
I tillegg til vanntankene er det et ønske om en tank eller oppsamlingskar som kan holde den totale vannmengden i systemet dersom det skulle forekomme lekkasjer. Dette betyr at oppsamlingskaret bør være langt nok og bredt nok til å dekke hele vannsystemet. Siden Reservoartanken er 60cm lang og 15cm bred, og vannsystemet strekker seg omtrent 20cm utover lengden, vil det være hensiktsmessig å ha et oppsamlingskar som er mellom 80-100cm langt og 18-25cm bredt. I tillegg vil den totale vannmengden i tankene ligge mellom 14-18 liter, så et oppsamlingskar med volum på 20 liter vil være passende.

4.2.4 Design av miniatyrby for illustrert strømproduksjon

Miniatyrbyens hensikt er å illustrere når kraftverket produserer nok strøm i forhold til et valgt settpunkt. Tanken er at det skal monteres en benk hvor det skal festes en miniatyrby med lyspærer som viser når solcellene og generatoren produserer strøm.

4.2.5 Dimensjonering og tilpassing av koblingsskap

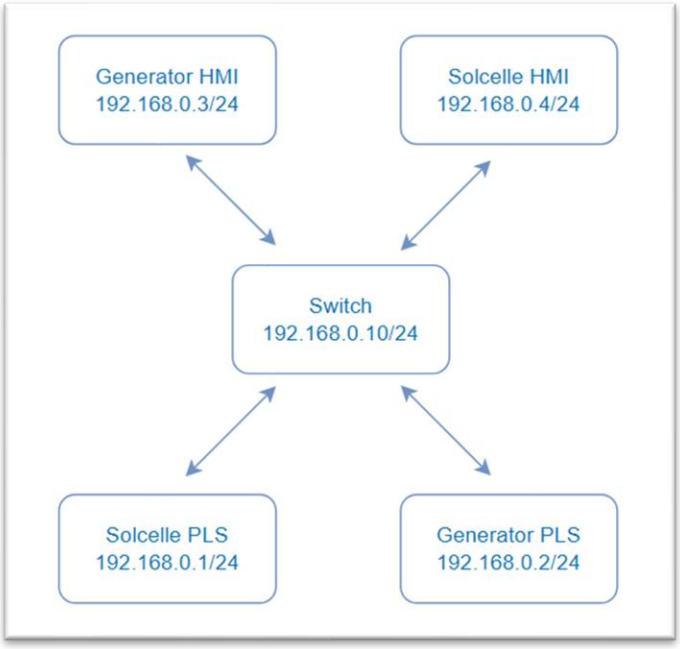
Koblingsskapet skal ha plass til alle komponentene og plassen må derfor utnyttes godt. Figur 4-8 viser hvordan komponentene i skapet skal plasseres på DIN-skinner og hvor kabelkanaler (stiplede rektangler) skal legges for å håndtere kabler etter kobling. Det må også drilles hull på undersiden av koblingsskapet for kabelgjennomføringer. Dette sikrer at skapet blir tett for både vann og andre fremmede objekter.



Figur 4-8: Skisse av innhold koblingsskap.

4.3 Oppsett og konfigurasjon av nettverk

HMI-er og PLS-er kobles til en industriell nettverk-switch. Denne må konfigureres før den kan tas i bruk, og standard administrator brukernavn og passord må byttes ut. Disse blir satt til brukernavn; «admin», og passord; «Porsgrunn_2024». Videre blir access-port nr. 8 konfigurert til å håndtere span trafikk, eller «port-mirroring» som det blir kalt i konfigurasjonsportalen. Resten av portene forblir åpne. Figur 4-9 viser en oversikt over nettverket med hvilke enheter som er tilkoblet, og tilhørende IP-adresser og subnettmaske.



Figur 4-9: Oversikt over enheter tilkoblet nettverket med tilhørende IP-adresser og subnettmaske.

5 Realisering av kombinert kraftverk

Dette kapittelet vil ta for seg gjennomføringen av det kombinerte kraftverket, med beskrivelser og bilder knyttet til byggeprosessen og de valgte komponentene. De viktigste komponentene vil også beskrives med generell virkemåte og hvilken rolle de spiller for anlegget. Kapittelet vil også inneholde programkode for PLS-er og HMI-er som er utviklet i TIA-portal. Innholdet i kapittelet er oppsummert i punktene under.

- Systemoversikt for miniatyrmodellen
- Spesifikk komponentoversikt for det kombinerte kraftverket
- Oppsett av solkraftmodellen
- Oppsett av vannkraftmodellen
- Oppsett for illustrert strømproduksjon
- Styringsfilosofi

5.1 Systemoversikt

Figur 5-1 er et bilde av modellen av det kombinerte kraftverket satt opp på monteringsveggen. På veggen er det festet en modell av et vannkraftverk, en modell av et solkraftverk, koblingsskap og et industribygg som illustrerer kraftproduksjon. Modellen for solkraftverket og vannkraftverket kan sees på som to separate systemer som jobber mot samme mål om å nå settpunktet for strømproduksjon i industrihallen.

Figur 5-1: Bilde av den fysiske modellen.

5.2 Spesifikk komponentoversikt for miniatyrmodellen

Den komplette komponentoversikten som blir brukt i modellen vises i Tabell 5-1. Tabellen gir en kort beskrivelse av komponentene, produsenten, antall og prisen. Det som blir inkludert i tabellen er de viktigste komponentene for å drive anlegget. Småting og festematerieller blir ikke spesifisert, men kan finnes i den komplette komponentoversikten som ligger i vedlegg 3. Ut ifra tabellen kan man se at totalprisen for anlegget kommer på 117 453kr.

Tabell 5-1: Komponentoversikt for endelig system

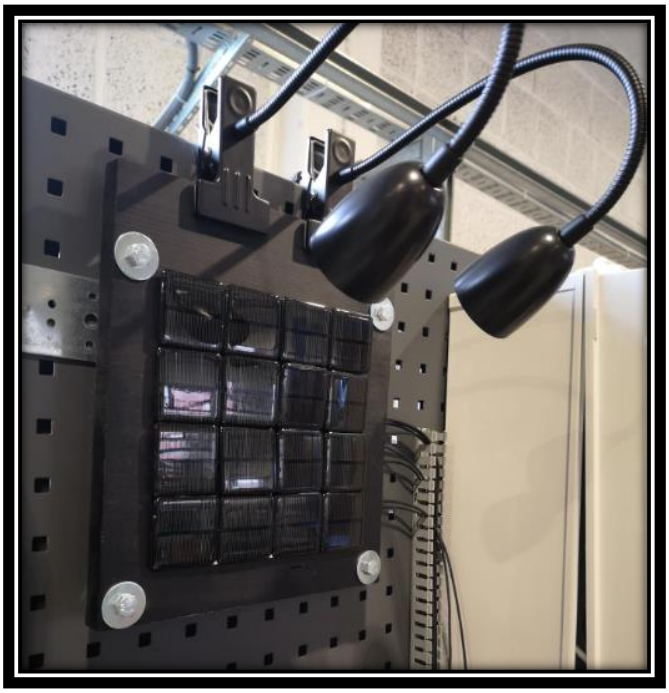
Komplett komponentoversikt for modellen av kombinert kraftverk					
Komponent	**Beskrivelse**	**Produsent**	**Antall**	**Enhetspris**	**Totalpris (NOK)**
HMI KTP700	24V, 7"	Siemens	1	10031	10031
HMI KTP400	24V, 4"	Siemens	1	5381	5381
Switch	24V, 8 porter	Siemens	1	8324	8324
PLS	24V, 1212C DC/DC/DC	Siemens	2	3890	7780
Analog modul	24V, 4Ai, 2AQ	Siemens	2	5465	10930
Strømforsyning	24V, 10A	Siemens	1	3939	3939
Kabinett	Koblingsskap	Fibox	1	2051	2051
Koblingsskap	Gjennomsiktig dør	Fibox	1	2974	2974
Kontaktor	24V, 25A 2NO	Siemens	4	354,31	1417,24
Lisens TIA-portal		Siemens	1	4077	4077
Koblingsskap total					**56904,24**
Småting koblingsskap					**5054,11**
Pumpe	14L/min	Xylem Flojet	1	3684	3684
Generator	10V	Wonofa	3	120	360
Ultralydsensor	4-20mA	Pepperl+Fuchs	1	3487	3487
Frekvensomformer	240V	Schneider Electric	1	3157	3157
Reguleringsventil	2-10V	Belimo	1	3509	3509
Nivåvakt	NC, 24V	Carlo Gavazzi	2	717	1434
Vanntanker	Begge er 27 liter	Plexon	2	-	17750
Vannkraftverk					**33381**
Vannsystem småting					**4546,96**
Solceller	16stk, 2V per	SUNYIMA	2	160	320
Lamper	12V	Northlight	2	149,9	299,8
Solkraftverk					**619,8**
Solkraft småting					**358,7**
Verktøystavle			1	9095	**9095**
Skruer og festemateriale					**2996,02**
Diverse					**4703**
Totalpris					**117453kr**

5.3 Oppsett og komponentbeskrivelse av solkraftmodellen

Solkraftanlegget bruker en lampe til å simulere sollys på solcellepanelet, som genererer strøm. Strømproduksjonen indikeres på en HMI, som lar brukeren kontrollere lampen, vise data og overvåke anleggets status. Anleggene kommuniserer for å sikre tilstrekkelig strøm-produksjon til byen, og kan skru seg av eller på ved behov.

5.3.1 Design av solceller

Solcellene er limt på en plate og seriekoblet slik at strømmen går gjennom alle cellene. Platen har to hull på baksiden for kabelgjennomgang, for å hindre at kablene er lett tilgjengelig og står i veien. Det er også to justerbare lamper festet på platen som lyser på solcellepanelet for å simulere sollys. Lampene er koblet til hver sine skjøteledninger, som igjen er koblet til hver sin kontaktor. Kontaktorne styres med PLS og kan skrus av og på via HMI. Lampene kan dermed styres direkte fra HMI, og lysnivået kan reguleres ved å skru av og på, en og en lampe. Solcellepanelet produserer strøm, som både indikeres med lys i industrihallen og på HMI-en. Figur 5-2 er et bilde av det solcellene satt opp på monteringsveggen.



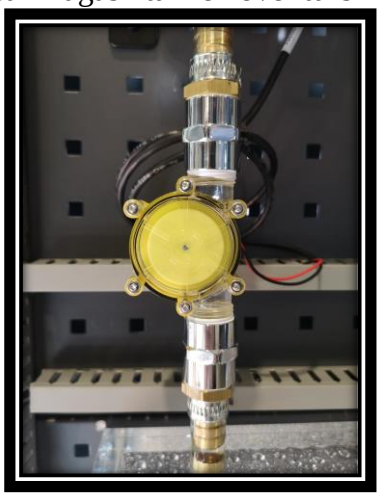
Figur 5-2: Design av solcellene.

5.4 Oppsett og komponentbeskrivelse av vannkraftmodellen

Vannkraftmodellen bruker en generator for å produsere strøm. For å oppnå ønsket produksjon blir det brukt en rekke komponenter som jobber sammen for å drifte anlegget. Delkapittelet under tar for seg funksjonen og virkemåten til de viktigste komponentene som blir brukt i vannkraftmodellen.

5.4.1 Generator – oppsett og virkemåte

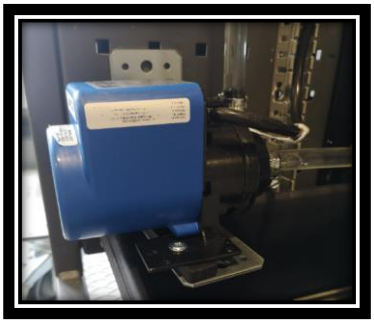
For vannkraftdelen av anlegget er det generatoren som står for produksjonen av strøm. Generatoren er en gjennomsiktig miniatyrversjon av en vannturbin. Vannturbinen gjør om mekanisk energi til elektrisk energi ved at vannet strømmer gjennom en turbin som spinner en aksel koblet til en generator. Den mekaniske energien i dette anlegget vil være fra trykket som blir skapt av nivået av vannet i magasintanken. Siden generatoren er montert under vanntanken vill det trykket skape en strømning som vil få turbinen til å spinne. Den energien som blir generert vil da bli sendt videre inn til PLS-en for å kunne måles. Figur 5-3 viser generatoren montert under magasin tanken. Trykket som virker på generatoren (turbinene) er direkte proporsjonalt med høyden av vannet i magasintanken over turbinen [16].



Figur 5-3: Vannturbin/generator i vannkraftverket.

5.4.2 Pumpe – oppsett og virkemåte

For å kunne forflytte vann mellom tankene blir det brukt en pumpe. I dette anlegget blir det brukt en sentrifugal pumpe, som vist i Figur 5-4. Hoveddelen til sentrifugale pumper er en roterende impeller som sitter inne i pumpehuset. Når pumpen går vil impelleren rotere i en høy hastighet så når vannet går inn i pumpehuset vil det bli akselerert kraftig og bli sendt videre. I anlegget vil pumpen flytte vannet fra en reservoartank opp til et vannmagasin for å kunne bruke vannet til å drive generatoren. Pumpen som blir brukt i anlegget er ikke selvfyllende så den må stå under vannstanden siden den ikke har muligheten til å trekke vann som er lavere en pumpen [17], [18].



Figur 5-4: Sentrifugalpumpe for pumping av vann fra reservoar- til magasintank.

5.4.3 Ultralyd nivåmåler – oppsett og virkemåte

Funksjonen til ultralyden er å måle vannstanden i vannmagasinet. Ultralyden fungerer ved å sende et lydsignal ut fra sensoren som vill treffe objektet som blir målt og reflekterer tilbake til sensoren. Sensoren vil da ta tiden fra lydsignalet blir sendt ut til det kommer tilbake for å finne ut hvor langt unna objektet er å gi et utgangssignal på 4-20mA. Ultralyden blir stilt inn ved å koble opp og installere den over tanken i posisjonen den skal være under drift. Etter det må tanken tømmes slik at det blir mulig å sette den lavere verdien for ultralyden via knappene på sensoren. På lik måte blir tanken fylt opp og den høyere verdien blir satt. Så når tanken er tom for vann vil utgangssignalet være 4mA og ved full tank vil signalet være på 20mA. Dette signalet blir sendt inn til PLS-en slik at det blir en kontinuerlig overvåkning av vannstanden i vannmagasinet som kan brukes til å styre resten av anlegget. Formel 1 viser beregning for avstand mellom ultralydmåleren og overflaten.

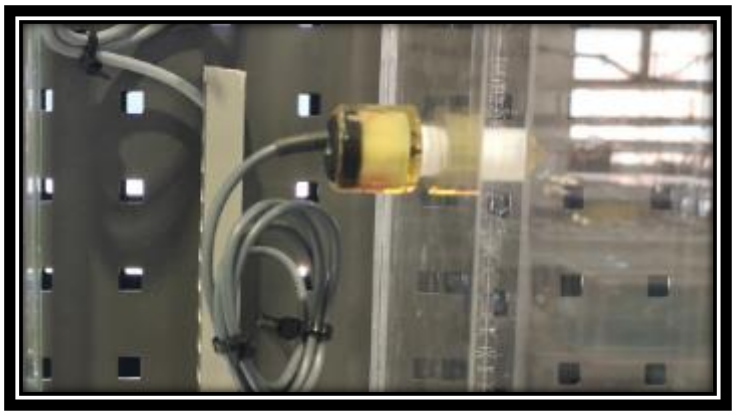
$$s = \frac{c * T_{tof}}{2} \tag{1}$$

Her er avstanden mellom måleren, ned til overflaten og opp, beregnet ved å multiplisere lydens hastighet i luft c med tiden som lyden bruker fra sender, ned til overflaten og opp til mottaker T_{tof} (Time of flight). Deretter deles dette på 2 for å finne avstanden i en strekning. Figur 5-5 viser ultralyd montert over magasintanken [19], [20], [21].

Figur 5-5: Ultralyd nivåmåler plassert over vannmagasinet.

5.4.4 Nivåvakt – oppsett og virkemåte

Hver tank i anlegget har en nivåvakt. Figur 5-6 viser plassering for nivåvakt i vannmagasinet. Funksjonen til nivåvakten i vannmagasinet er å varsle om høyt nivå i vannmagasinet. Nivåvakten i reservoartanken har som funksjon å varsle når tanken ikke har nok vann til å drifte anlegget slik det ikke kan startes uten å ha nok vann. Nivåvaktene er en optisk sensor som bruker infrarødt lys til å detektere vann. Det infrarøde lyset sprer seg ut fra prismet på tuppen av sensoren som blir fanget opp av en mottaker også installert i nivåvakten. Når det bare er luft rundt nivåvakten blir nesten alt av det infrarøde lyset reflektert tilbake til mottakeren, men når vannet går over sensoren vil nesten ingenting bli reflektert tilbake til mottakeren. Ut ifra det vill nivåvakten kunne se når vannet dekker for sensoren. Nivåvakten består også av en NC-bryter koblet direkte inn til PLS-en som blir aktivert når nivåvakten detekterer vann. Grunnen til at det blir brukt NC-brytere er for å øke sikkerheten til anlegget. Hvis det skulle skje en feil ved nivåvakten vil signalet til PLS-en forsvinne på grunn av at nivåvakten bruker NC bryteren. Dette gjør det umulig å drifte anlegget med for lite vann, selv om det skulle skje en feil ved nivåvakten i reservoartanken [22], [23].



Figur 5-6: Nivåvakt med gjenge som er skrudd inn i vanntanken.

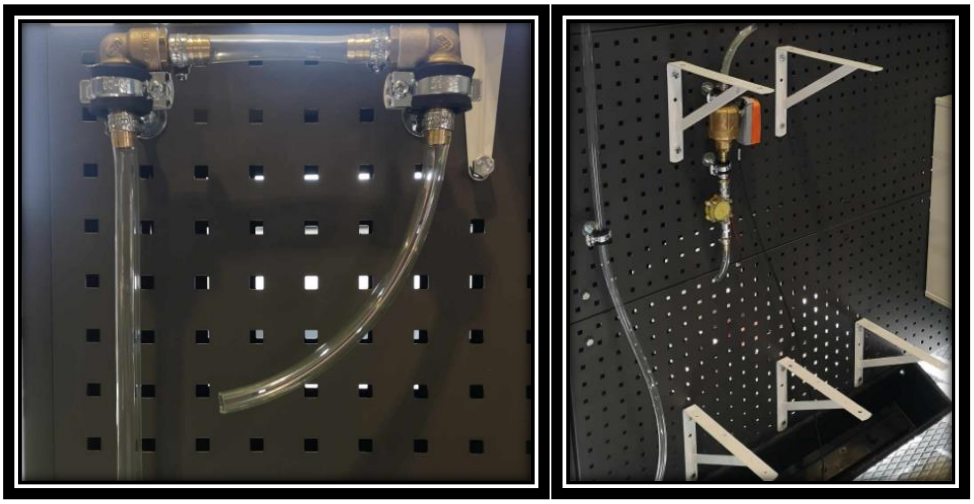
5.4.5 Reguleringsventil – oppsett og virkemåte

For å kunne styre mengden vann som renner fra vannmagasinet til generatoren blir det brukt en reguleringsventil. Figur 5-7 viser et bilde av reguleringsventilen med aktuatoren festet. Det er en kuleventil som blir styrt av en elektrisk aktuator. Den elektriske aktuatoren blir styrt av et signal på 2-10V som kommer fra PLS-en hvor 2V utgjør en lukket ventil og 10V utgjør en helt åpen ventil. Dette gjør det mulig å kontrollere mengden vann som renner til generatoren via PLS-en ved å åpne eller lukke ventilen ut ifra informasjonen som PLS-en har. Reguleringsventilens åpning blir konstant oppdatert gjennom PID-regulering som skjer i PLS-en.

Figur 5-7: Bilde av reguleringsventil og aktuator festet med rørklemmer.

5.4.6 Fester i vannsystemet

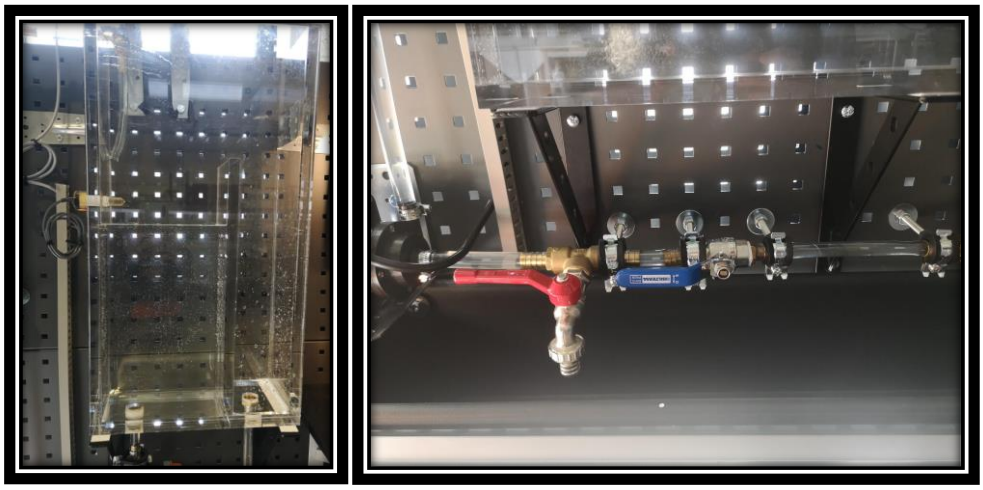
For festing av slanger, overganger, styreventil, generator og kuleventiler skal det brukes rør-klammer med boltgjenger, noe som gjør det enkelt å bolte klammene rett i veggen og stramme etter behov. For feste og tetting av gjenger brukes det gjengeteip på slangeniplene før de skrus inn. Til venstre i Figur 5-8 vises festing av fester for slanger og overganger, og til venstre høyre vises festing av vinkelbraketter for støtting av vanntanker. Når det kommer til festing av vanntankene skal det brukes vinkelbraketter som boltes i veggen. Tankene står oppå brakettene og det limes i tillegg braketter på sidene av tankene og boltes til veggen. vi-ser hvordan brakettene tenkes å festes i veggen for støtte av vanntankene.



Figur 5-8: Til venstre festing av rørklammer og slangeoppsett, og til høyre festing av vinkelbraketter til støtting av vanntanker.

5.4.7 Tømming, fylling og stenging av vann

Påfylling av vann i reservoartanken kan enkelt gjøres gjennom toppen av vannmagasinet. Siden vannmagasinet kan romme 12L væske før det renner over til reservoaret, er det satt en minste påfyllgrense på 15L vann. Dette er både for å ha nok vann til å demonstrere konsekvenser av cyberangrep, og for at pumpa aldri skal kunne kjøre tørr. Det er også satt en maksgrense på 18L vann i systemet, slik at oppsamlingskaret skal kunne fange alt vannet ved eventuell lekkasje. Figur 5-9 viser magasintanken som kan brukes for påfyll av vann til venstre, og kuleventiler for stenging og tømming av vann til høyre. For å stenge av vannsystemet mellom reservoartanken og pumpen kan den blå spaken rettes oppover. Dette er en feilsikring dersom noe skulle skje med pumpen, eller slangen som er festet på pumpen. Det er også montert en kuleventil med rød spak som kan brukes for tømming av reservoartanken. For tømming kan den røde spaken vendes ut fra veggen.



Figur 5-9: Magasintank for påfyll av vann til venstre, og kuleventiler for stenging og tømming av vann til høyre.

5.5 Illustrasjon av strømproduksjon – oppsett og virkemåte

For å illustrere strømproduksjonen til kraftverkene er det bygget en miniatyrmodell av en industrihall med dimensjonene 28x14,2x10cm. Industrihallen er plassert på en plate som hviler på vinkelbraketter. Inni industrihallen er det montert en lampe som skrur seg av og på basert på produsert strøm ut ifra settpunkt på HMI-en. Lampen styres av en PLS gjennom en kontaktor. Figur 5-10 viser oppsettet og utseende av industrihallen.

Figur 5-10: Industrihall fra Togbutikken.no.

5.6 IO-liste

IO-liste er en samlet liste som har alle innganger, utganger og indre minne på PLS-en. Listen gir et komplett overblikk av alt informasjon og alle mulige handlinger som PLS-en har tilgang til. Tabell 5-2 viser IO listen til generatoren og Tabell 5-3 viser IO listen til solcelle PLS-en. Tabellene inneholder navn på taggen, adressen, data type og en kort beskrivelse av signalet taggen bruker.

Tabell 5-2: Oversikt over alle innganger og utganger til generator PLS med type signal.

I/O-liste for generator PLS				
Navn	**Data type**	**Adresse**	**Enhet**	**Signaltype**
LevelGuardLow	Bool	%I0.0	PLS	24V inngang
LevelGuardHigh	Bool	%I0.1	PLS	24V inngang
GeneratorRaw	Int	%IW64	PLS	Analogt 0-10V inngang
UltrasonicRaw	Int	%IW96	PLS	Analogt 4-20mA inngang
PumpSwitch	Bool	%Q0.0	PLS	24V utgang
LampMain	Bool	%Q0.1	PLS	24V utgang
LampG2	Bool	%Q0.2	PLS	24V utgang
LampR2	Bool	%Q0.3	PLS	24V utgang
LampG1	Bool	%Q0.4	PLS	24V utgang
LampR1	Bool	%Q0.5	PLS	24V utgang
Valve	Int	%QW96	PLS	Analogt 2-10V utgang
StartPumpLevel	Real	%MD0	PLS	Real verdi (minne)
ValveSetPoint	Int	%MW4	PLS	Int verdi (minne)
ValveManualSwitch	Bool	%M6.0	PLS	Av/på BOOL verdi (minne)
HoldingContact	Bool	%M6.1	PLS	Av/på BOOL verdi (minne)
PumpManualSwitch	Bool	%M6.2	PLS	Av/på BOOL verdi (minne)
PumpOnOff	Bool	%M6.3	PLS	Av/på BOOL verdi (minne)
Override	Bool	%M6.4	PLS	Av/på BOOL verdi (minne)
AutomaticControl	Bool	%M6.5	PLS	Av/på BOOL verdi (minne)
Generatorscaled	Real	%MD10	PLS	Real verdi (minne)
StopPumpLevel	Real	%MD14	PLS	Real verdi (minne)
Setpoint	Int	%MW20	PLS	Vekslende av/på BOOL verdi (minne)
TotalProduction	Real	%MD22	PLS	Real verdi (minne)
AlwaysTRUE	Bool	%M29.2	PLS	Alltid på verdi (minne)
Clock_2Hz	Bool	%M30.3	PLS	Vekslende av/på BOOL verdi (minne)
UltrasonicScaled	Real	%MD32	PLS	Real verdi (minne)
SetPointRange	Real	%MD36	PLS	Real verdi (minne)
GeneratorEqualized	Real	%MD42	PLS	Real verdi (minne)
AlwaysFALSE	Bool	%M29.3	PLS	Alltid av verdi (minne)

Tabell 5-3: Oversikt over alle innganger og utganger til solcelle PLS med type signal.

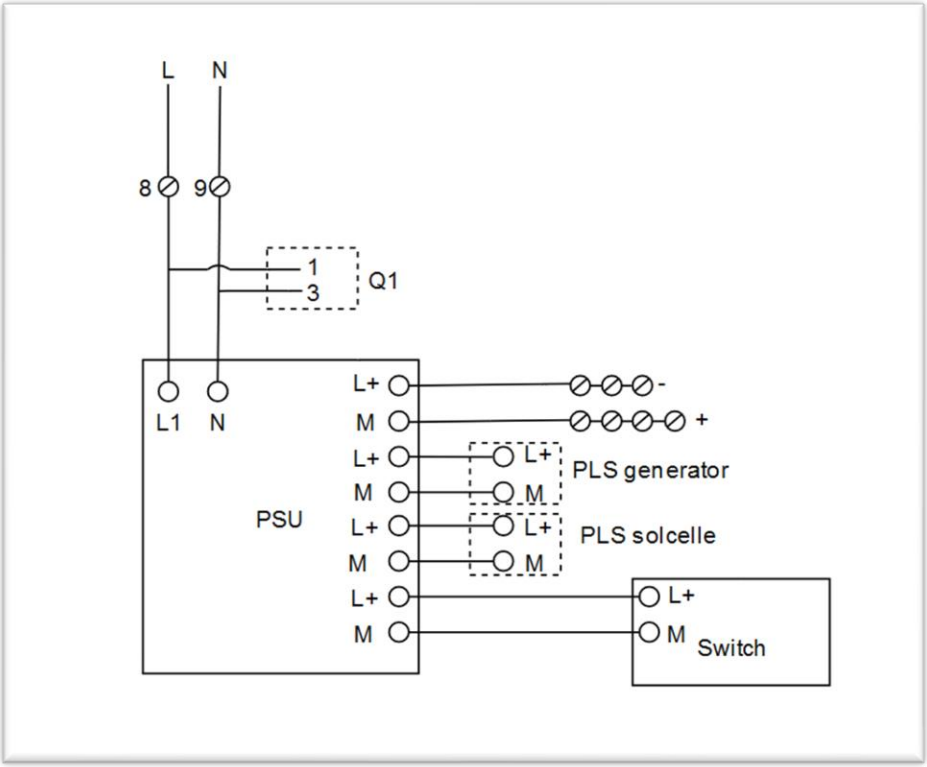
I/O-liste for solcelle PLS				
Navn	**Data type**	**Adresse**	**Enhet**	**Signaltype**
SolarRaw1	Int	%IW96	PLS	Analogt 0-10V inngang
SolarScaled1	Real	%MD25	PLS	Real verdi (minne)
SolarScaled2	Real	%MD26	PLS	Real verdi (minne)
SolarRaw2	Int	%IW98	PLS	Analogt 0-10V inngang
SolarScaled3	Real	%MD27	PLS	Real verdi (minne)
SolarRaw3	Int	%IW100	PLS	Analogt 0-10V inngang
LampSolar1	Bool	%Q0.0	PLS	24V utgang
LampSolar2	Bool	%Q0.1	PLS	24V utgang
LampR3	Bool	%Q0.3	PLS	24V utgang
LampG3	Bool	%Q0.4	PLS	24V utgang
Manualswitch	Bool	%M5.0	PLS	Av/på BOOL verdi (minne)
ManualLamp1	Bool	%M5.1	PLS	Av/på BOOL verdi (minne)
ManualLamp2	Bool	%M5.2	PLS	Av/på BOOL verdi (minne)
SolarScaledCombined	Real	%MD15	PLS	Real verdi (minne)
SolarEqualized	Real	%MD0	PLS	Real verdi (minne)
Lamp1Holding	Bool	%M4.0	PLS	Av/på BOOL verdi (minne)
Lamp2Holding	Bool	%M4.1	PLS	Av/på BOOL verdi (minne)
SolarCalibratedValue	Real	%MD6	PLS	Real verdi (minne)
Lamp1Limit	Real	%MD10	PLS	Real verdi (minne)
Lamp2Limit	Real	%MD20	PLS	Real verdi (minne)

5.7 Koblingsskjemaer

Koblingsskjema for anlegget er delt opp i fem forskjellige deler. Dette er gjort for at det skal være lett å finne fram til det man ønsker og for å unngå unødvendig rot. Koblingsskjemaene er delt inn i strømforsyning pluss switch, generator PLS, solcelle PLS, pumpe pluss lamper og HMI-skjermer.

5.7.1 Koblingsskjema for strømforsyning og switch

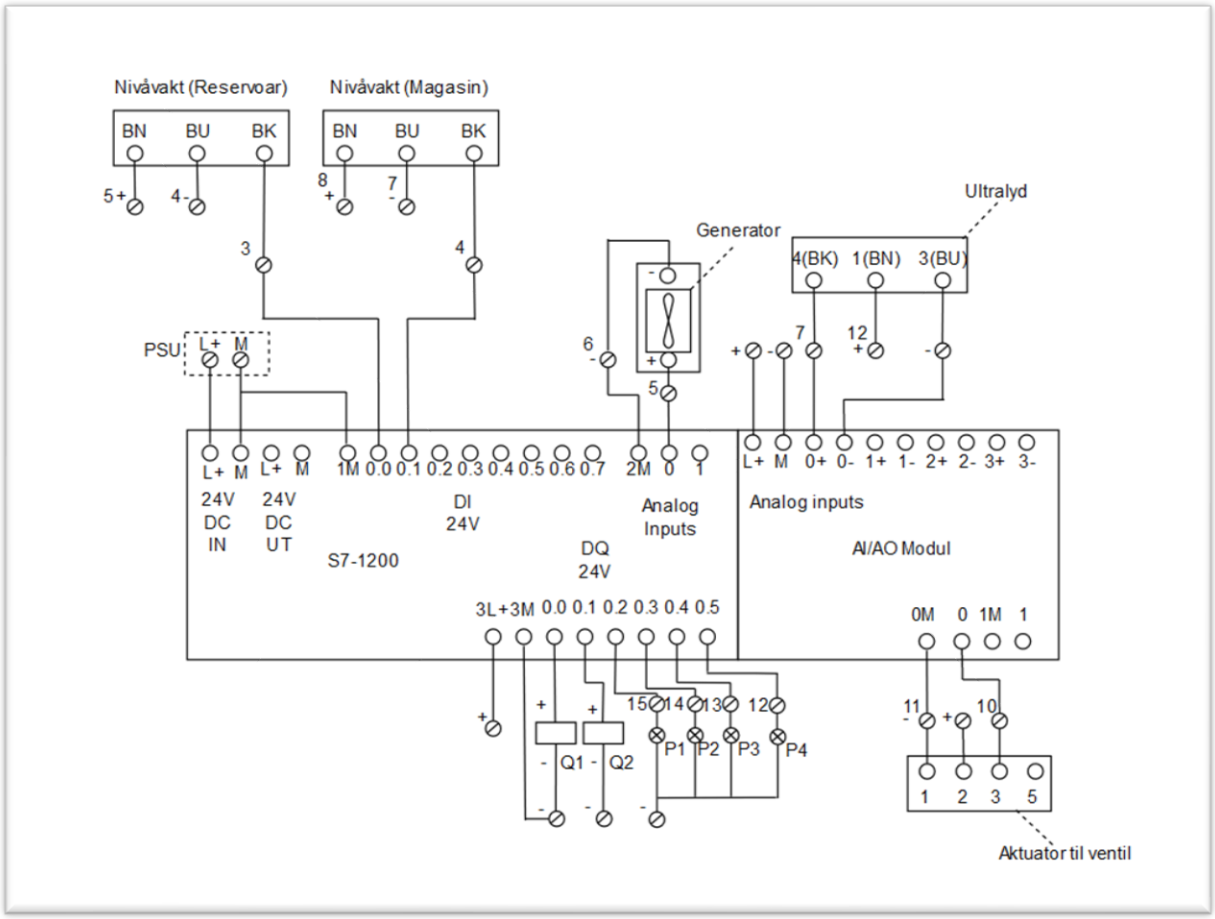
Figur 5-11 viser koblingsskjema for PSU og switchen. PSU-en er strømforsyningen i anlegget den tar in 230V AC fra stikkontakten vist som L og N på koblingsskjema for å gjøre det om til 24V DC. Mesteparten av anlegget bruker 24V DC inkludert switchen som blir forsynt direkte fra strømforsyningen. Hvis noen av koblingene mellom komponentene er langt vekk fra hverandre på tegningene blir det brukt rektangler med dottete linjer for å vise hvor koblingen går. Dette er for å forhindre rot og holde alt oversiktlig.



Figur 5-11: Koblingsskjema for strømforsyning og switch.

5.7.2 Koblingsskjema for PLS-kontroll av vannkraft

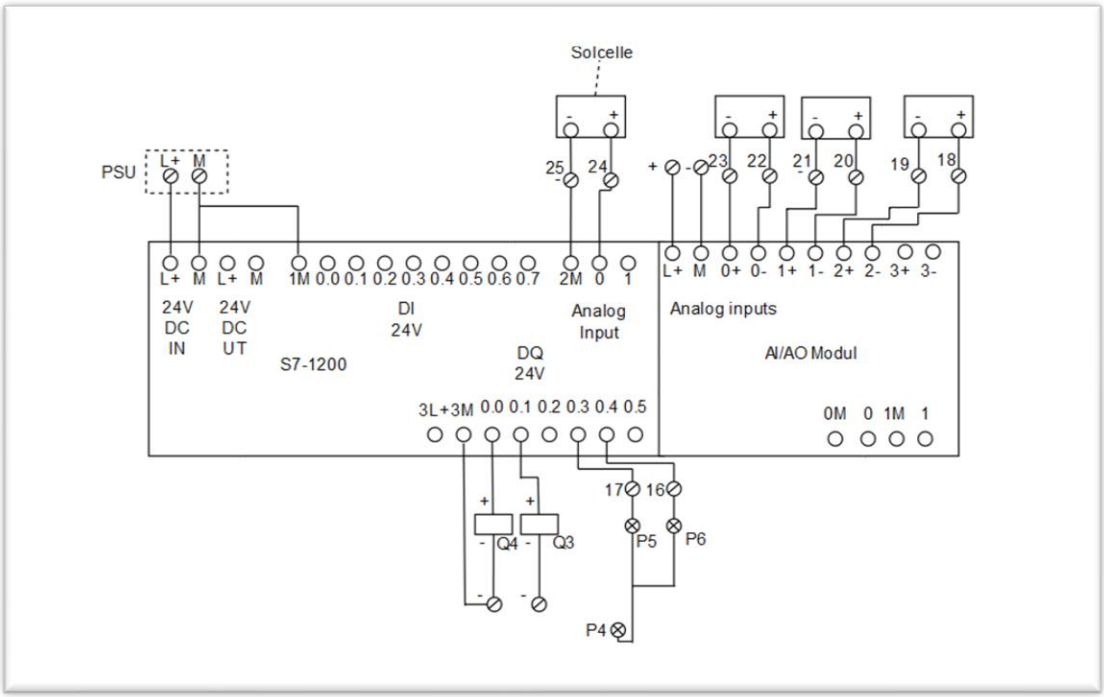
Koblingsskjemaet for generator PLS-en og den tilknyttete analog modulen er vist i Figur 5-12. Alle koblinger i Figur 5-12 er 24V DC. På inngangssiden viser tegningen koblingen på nivåvaktene som er de digitale inngangene. Generatoren og ultralyden blir tatt in som de analoge inngangene. For de digitale utgangene er det to spoler som styrer kontaktorer de er merket med Q og fire lys som er merket med P. Det er også et analogt utgangssignal som går til aktuatoren som styrer ventilen.



Figur 5-12: Koblingsskjema for generator PLS

5.7.3 Koblingsskjema for PLS-kontroll av solkraft

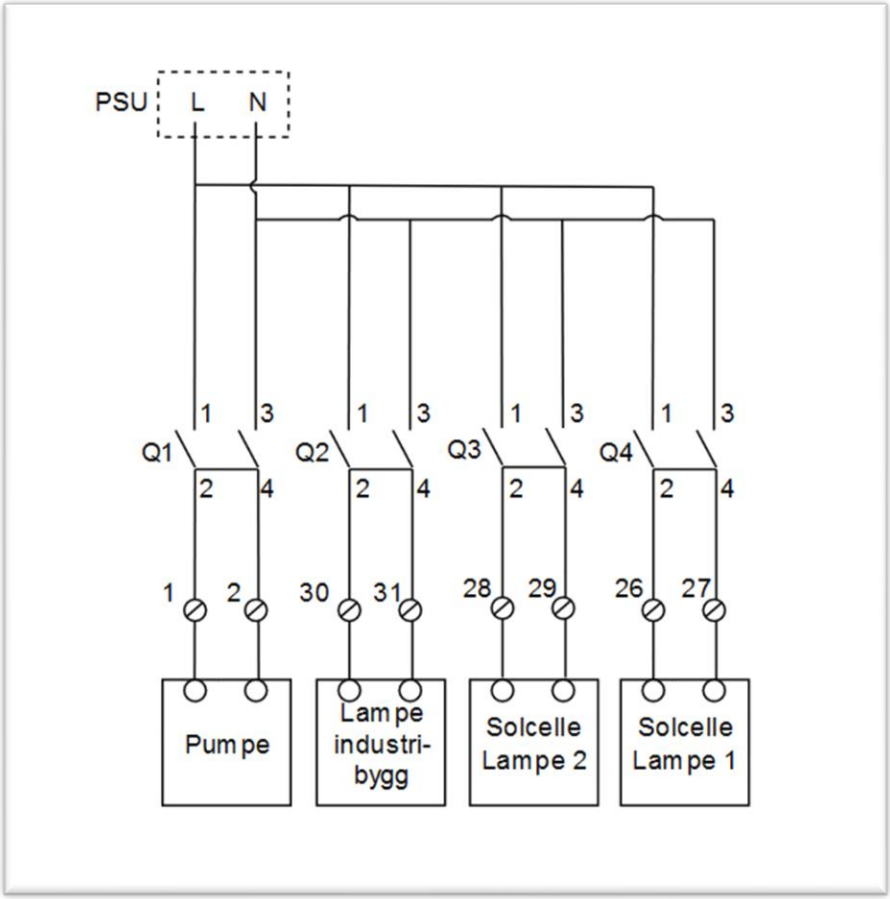
Den andre PLS-en for solcelle anlegget og tilknyttet analog modul har koblingsskjema i Figur 5-13 .Likt med generator PLS-en er alle koblinger i Figur 5-13, 24V DC. Solcelle PLS-en har ingen digitale innganger, men har alle solcellene som analoge innganger. På utgangsiden er det fire digitale og ingen analoge utganger. De digitale utgangene går til to kontaktor spoler og to lys.



Figur 5-13: Koblingsskjema for solcelle PLS

5.7.4 Koblingsskjema for pumpe og lamper

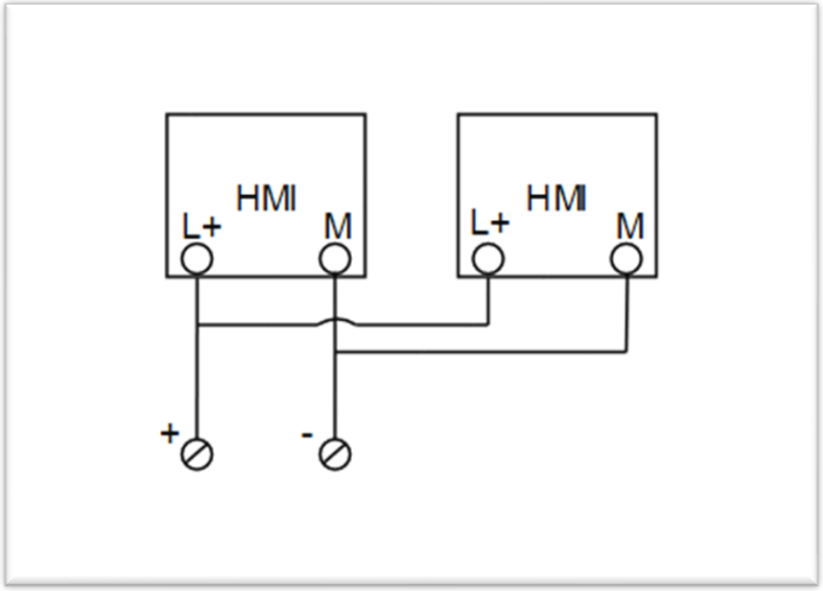
Figur 5-14 viser koblingsskjema for pumpen og lampene som blir brukt til styring av anleggene. Alle koblinger i figur 5-14 er 230V AC. Kontaktorbrytersettene lukker seg når spolen blir aktivert fra utgangen på PLS-en. Q1 og Q2 blir styrt av generator PLS-en. Q3 og Q4 blir styrt av solcelle PLS-en.



Figur 5-14:Koblingsskjema for pumpe og lamper

5.7.5 Koblingsskjema for HMI-skjermer

Koblingsskjema for HMI-skjermene er i Figur 5-15. HMI-skjermene er 24V DC og kobles sammen med hverandre for å unngå ekstra ledninger.



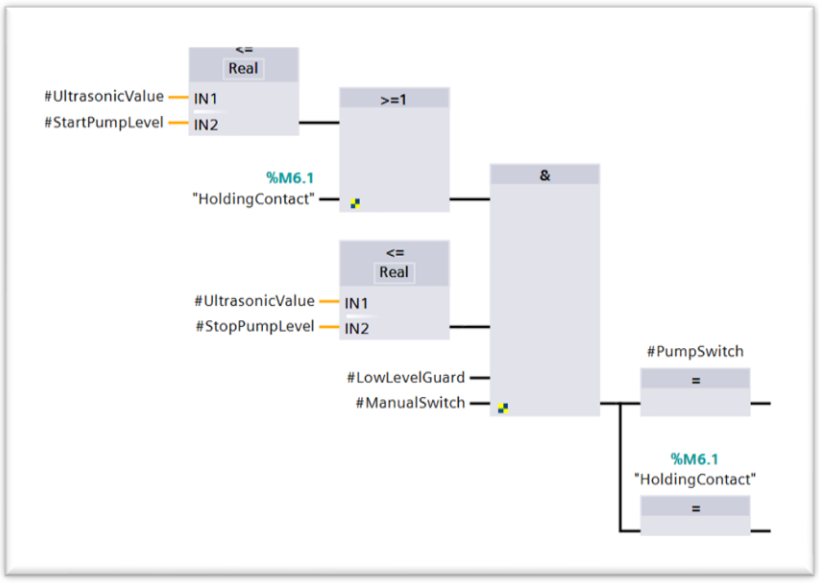
Figur 5-15: Koblingsskjema for HMI-skjermer

5.8 Styringsfilosofi

For å styre anlegget er det brukt to PLS-er og to HMI-skjermer koblet sammen av en switch. Alt av programmeringen for både PLS og HMI er gjort i Siemens TIA-portal. Dette delkapittelet vill forklare de viktigste styrefunksjonene til anlegget og gi en oversikt over HMI-skjermene. Hele programmet for generator PLS ligger i vedlegg 4a og hele programmet for solcelle PLS ligger i vedlegg 4b.

5.8.1 Styring av pumpe

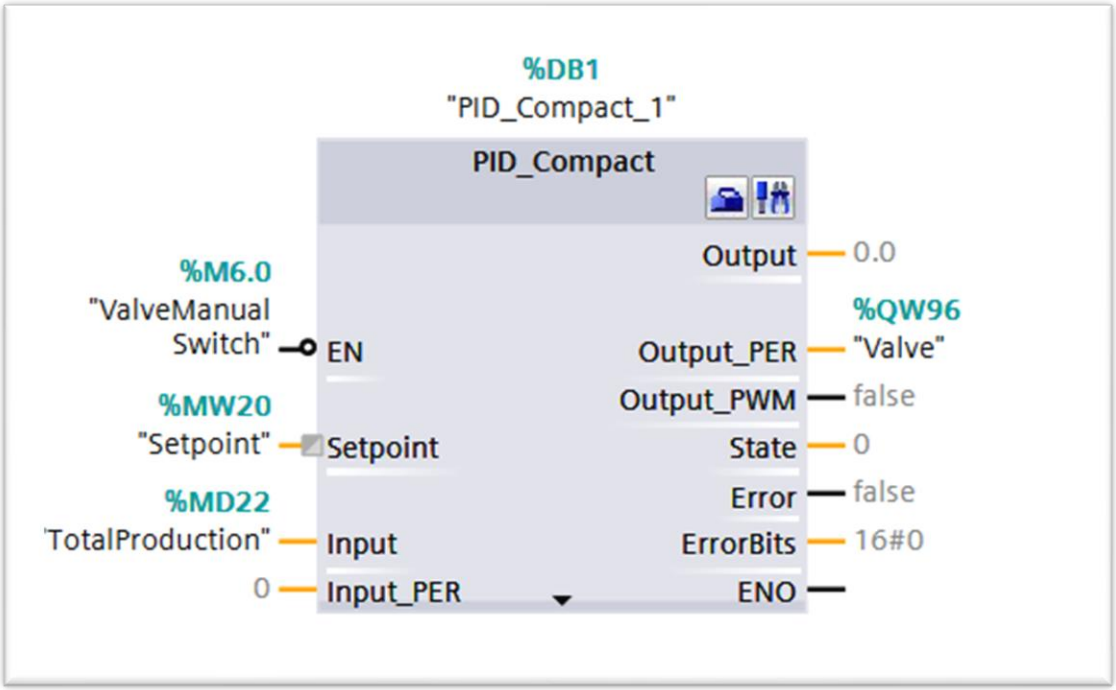
Anlegget har to forskjellige måter å styre pumpen på, manuell og automatisk. I manuell modus kan man enkelt via knappene på HMI-skjermen skru av og på pumpen. Når anlegget er satt i automatisk modus vil ultralyden bli brukt for å styre pumpen. Logikken til funksjonen for automatisk styring kan bli sett under i Figur 5-16.Funksjonen tar inn tre parametere #startPumpLevel, #stopPumpLevel #ultasonicValue. Virkemåten blir da at man setter et område for å starte og stoppe pumpen som blir sammenlignet med verdien til ultralyden for å se om pumpen skal driftes eller ikke. Verdiene for start og stopp av pumpe kan settes fra 0-100% hvor 0% er når vannmagasinet er tomt og 100% er når vannmagasinet er fult. For et eksempel hvis start av pumpe er satt på 70% og stopp av pumpe er satt til 80% vil pumpen driftes når ultralyden viser at vannstanden er under 70%. Den vil fortsette å fylle helt til den treffer 80% hvor pumpen da vil stoppe og vannet vil renne ut mellom generatoren som får vannstanden til å synke igjen. Når vannstanden detter ned til under 70% igjen vil pumpen driftes på nytt. Det er også programmert forriglinger slik at pumpen ikke kan være i manuell og automatisk modus samtidig. Pumpen vil også ikke kunne driftes når nivåvakten i reservoar tanken viser at det er ikke er nok vann til å drifte anlegget.



Figur 5-16: Funksjon for automatisk styring av pumpe

5.8.2 Styring av reguleringsventil

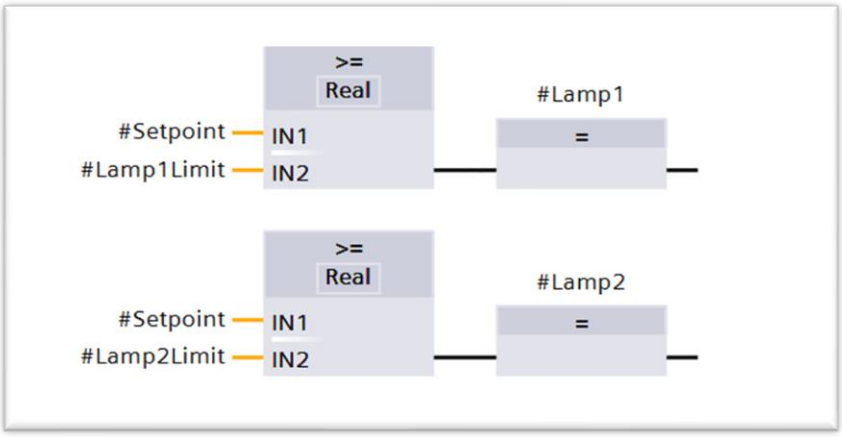
Reguleringsventilen kan bli automatisk styrt via en PID kontroller som er innebygd i PLS-en. PID algoritmens hovedfunksjon er å få prosessverdien til å bli så nære som mulig til settpunktet. PID kontrolleren satt opp i TIA-portalen kan bli sett i Figur 5-17. PID kontrolleren tar inn to inngangsverdier settpunktet og den totale produksjonen. Settpunktet er da den ønskelige produksjon av spenningen som blir satt av operatør på HMI-skjerm. Den totale produksjonen blir da prosessverdien som er spenningen generert av solcellene og generatoren slått sammen. De to inngangsverdiene blir da sendt inn til PID algoritmen for å få et utgangssignal som går direkte til reguleringsventilen. For å finne parameterne for kontrolleren ble det brukt den automatiske tuneren i TIA Portalen. PID kontroller kjører og blir oppdatert kontinuerlig så lenge ikke reguleringsventil er satt i manuell modus. For å sette reguleringsventilen i manuell modus finnes det en bryter på HMI-skjermen ved siden av bryteren er det et felt operatør kan fylle ut for å sette åpningsprosenten til reguleringsventilen mellom 0-100%.



Figur 5-17: Oppsett for PID-kontroller

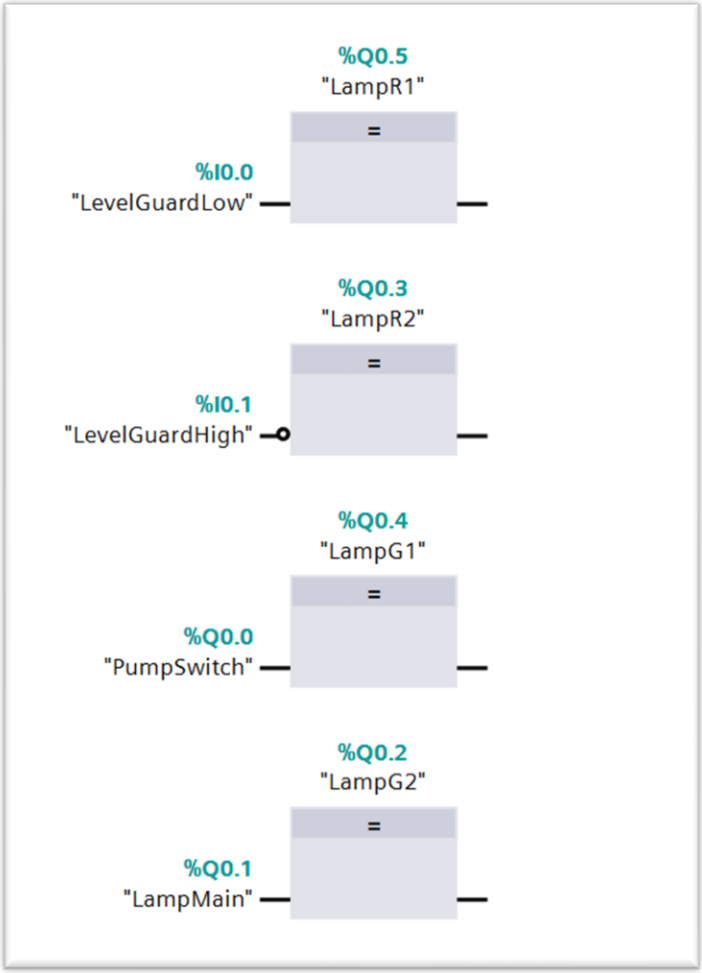
5.8.3 Styring av lamper

Lampene for solcelleanlegget har en manuell og automatisk styring. For den manuelle styringen kan operatør via HMI-skjerm sette den i manuell modus via en bryter. Når den er satt i manuell modus vil det være to av/på brytere for de to lampene. Lampene er under automatisk styring når bryteren til manuell styring er av. Under automatisk styring vil lampene skru seg selv på når settpunktet treffer ulike nivå. Funksjonen for dette vises Figur 5-18 standard verdiene for funksjonen er #Lamp1Limit satt til 10 og #Lamp2Limit satt til 25. Funksjonen fungerer da slik at når settpunkt blir satt til 10 eller høyre vil lampe 1 lyse og da når settpunkt blir satt til 25 eller høyere vil lampe 2 lyse.



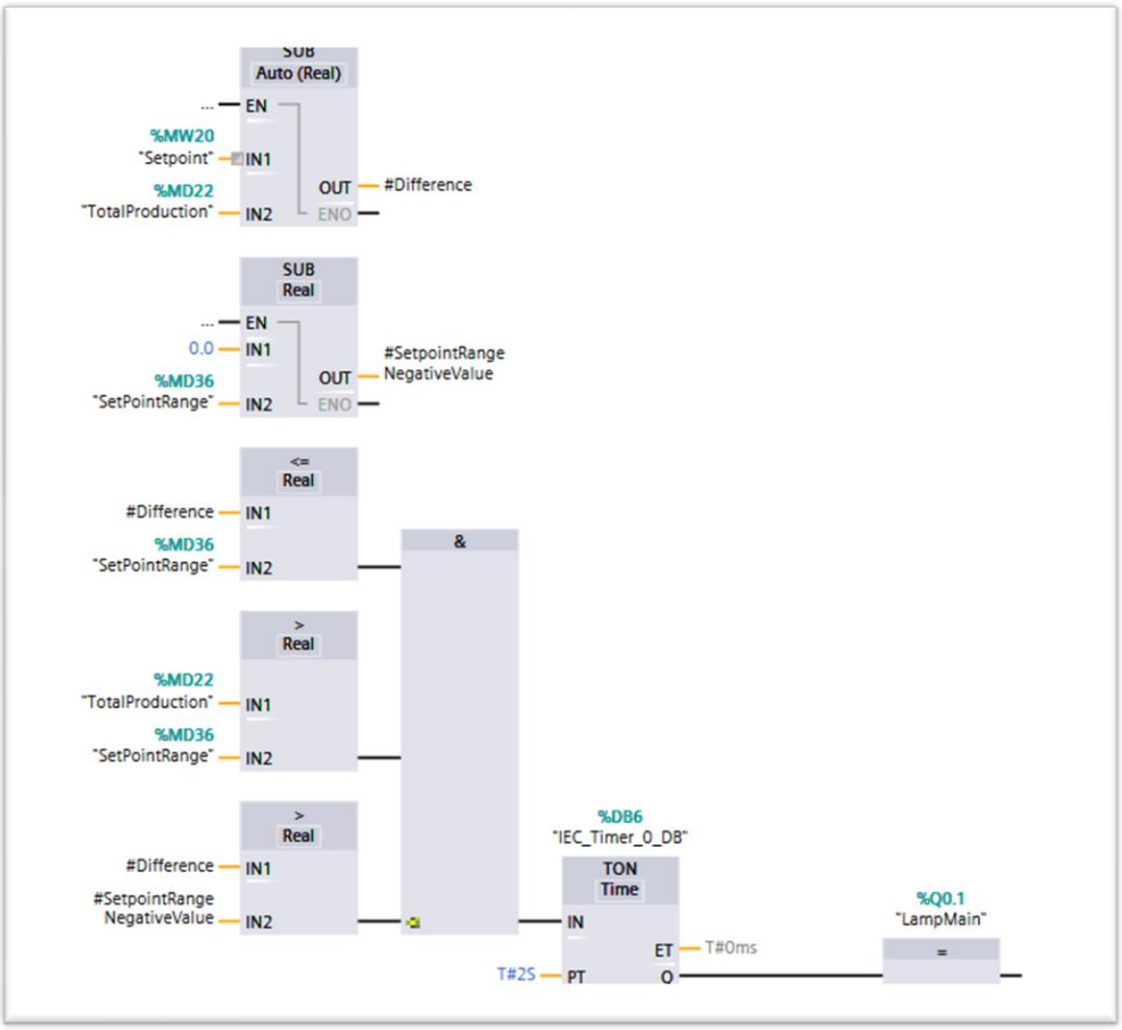
Figur 5-18: Automatisk styring av solcelle lamper

Det er også tre grønne og tre røde lamper på det ene koblingsskapet. Programmeringen til de forskjellige lampene kan bli sett i *Figur 5-19*. For de grønne lampene er den øverste grønne lampen en statuslampe for pumpen som lyser når pumpen er i drift. Den midterste grønne lampen vil lyse når hovedlyset til industribygget lyser. Den nederste grønne lampen lyser når lampene til solcellene er satt i automatisk modus. For de røde lampene vil den øverste røde lampen lyse når nivåvakten til reservoar tanken viser lavt nivå. Den midterste røde lampen vil lyse når nivåvakten i vannmagasinet viser høyt nivå. Den nederste røde lampen vil lyse når manuell styring av lampene til solcellene er på.



Figur 5-19: Programmering av lamper på koblingsskap

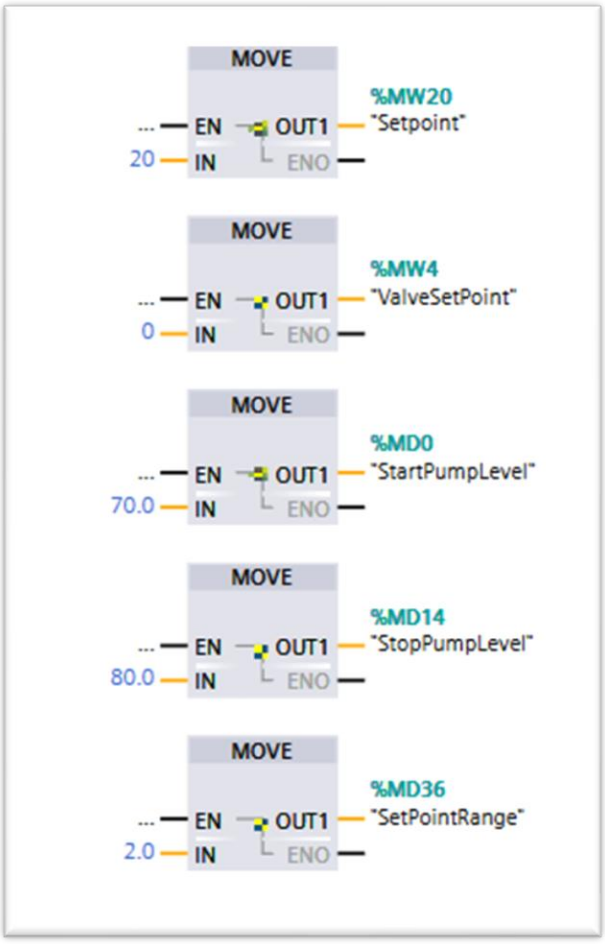
Lampen i industribygget er ment for å vise når man har oppnådd ønsket produksjon. Den blir skrudd på når den faktiske produksjon som er produksjon til solcellene og generatoren slått sammen blir tilnærmet likt ønsket produksjon som er settpunktet. Det er lagt inn en margin som har en standardverdi på to volt. Denne marginen betyr at den totale produksjon kan ligge i område på to volt under eller over settpunkt for å få lampen til lyse. Det blir også lagt inn en timer slik at den totale produksjonen må ligge i området i to sekunder før lampen skrur seg på. Dette er for å forhindre at lampen skrur seg av og på flere ganger når den nærmer seg sett-punkt. Programmeringen for lampen i industribygget vise i Figur 5-20.



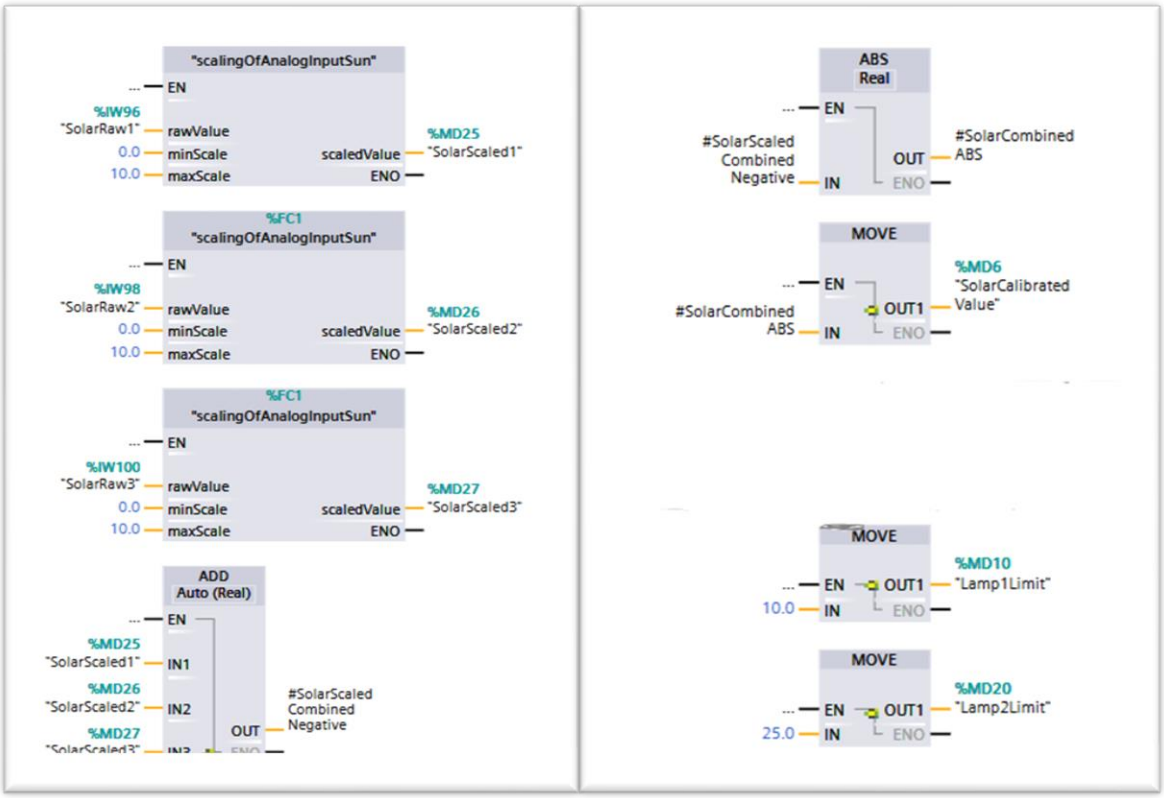
Figur 5-20: Programmering for lampe i industribygg

5.8.4 Oppstart syklus og utjevning av verdier

Hver gang en PLS starter vil det bli kjørt en oppstart syklus. Oppstartsyklusen for generator PLS-en kan bli sett i Figur 5-21 og oppstartsyklusen for solcelle PLS-en kan bli sett i Figur 5-22. På oppstart vil det bli satt en rekke standardverdier for generator PLS-en. For solcelle PLS-en blir det også satt noen standard verdier, men det blir også tatt en måling av solcelle panelene. Den målingen blir tatt uten at noen av lampene er på før anlegget starter. Den verdien som blir målt blir brukt som en kalibreringsverdi slik at solcellene kan vise null volt når lampene for solcelle anlegget er av. Dette fører til at solcellene vil bare produsere via lampene som er satt opp og ikke av lysforurensing fra rommet. Alle verdiene som blir satt på oppstart kan endres via konfigurasjons skjermen på PLS-ene.



Figur 5-21: Oppstart syklus for generator PLS

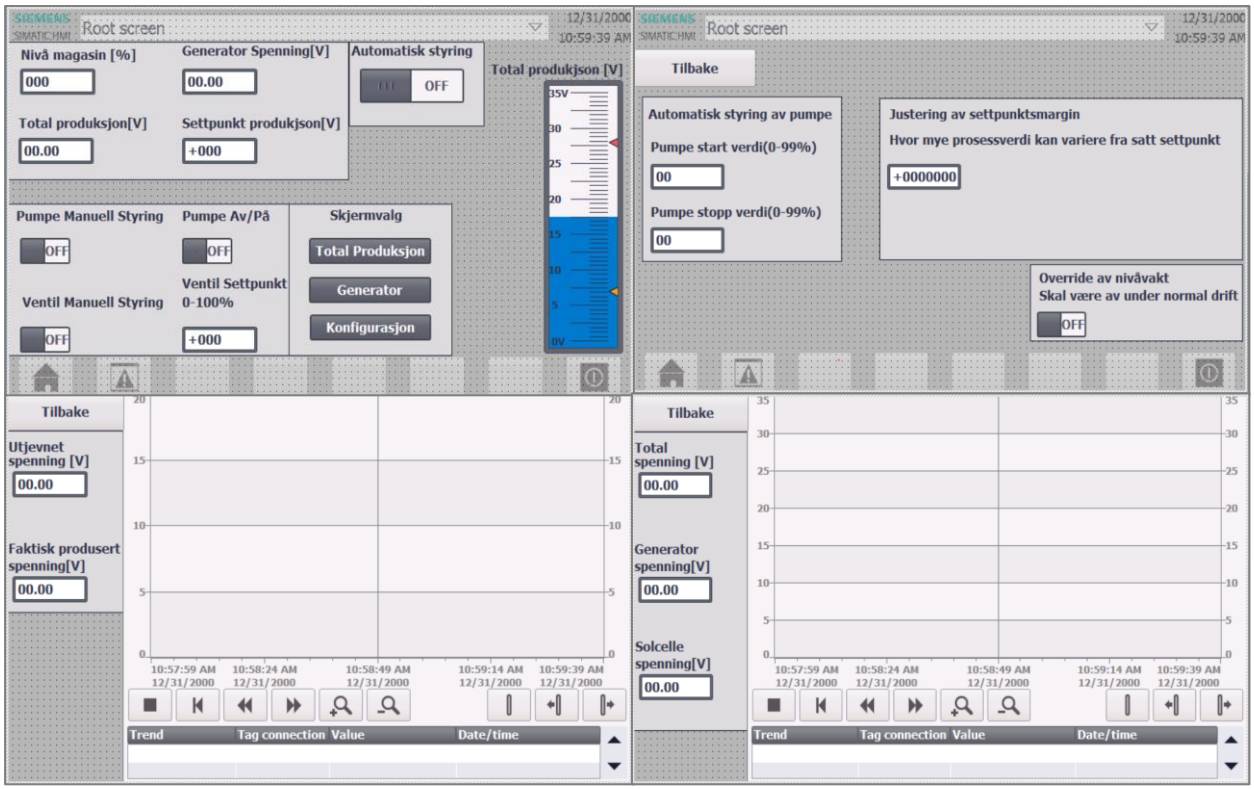


Figur 5-22: Oppstart syklus for solcelle PLS

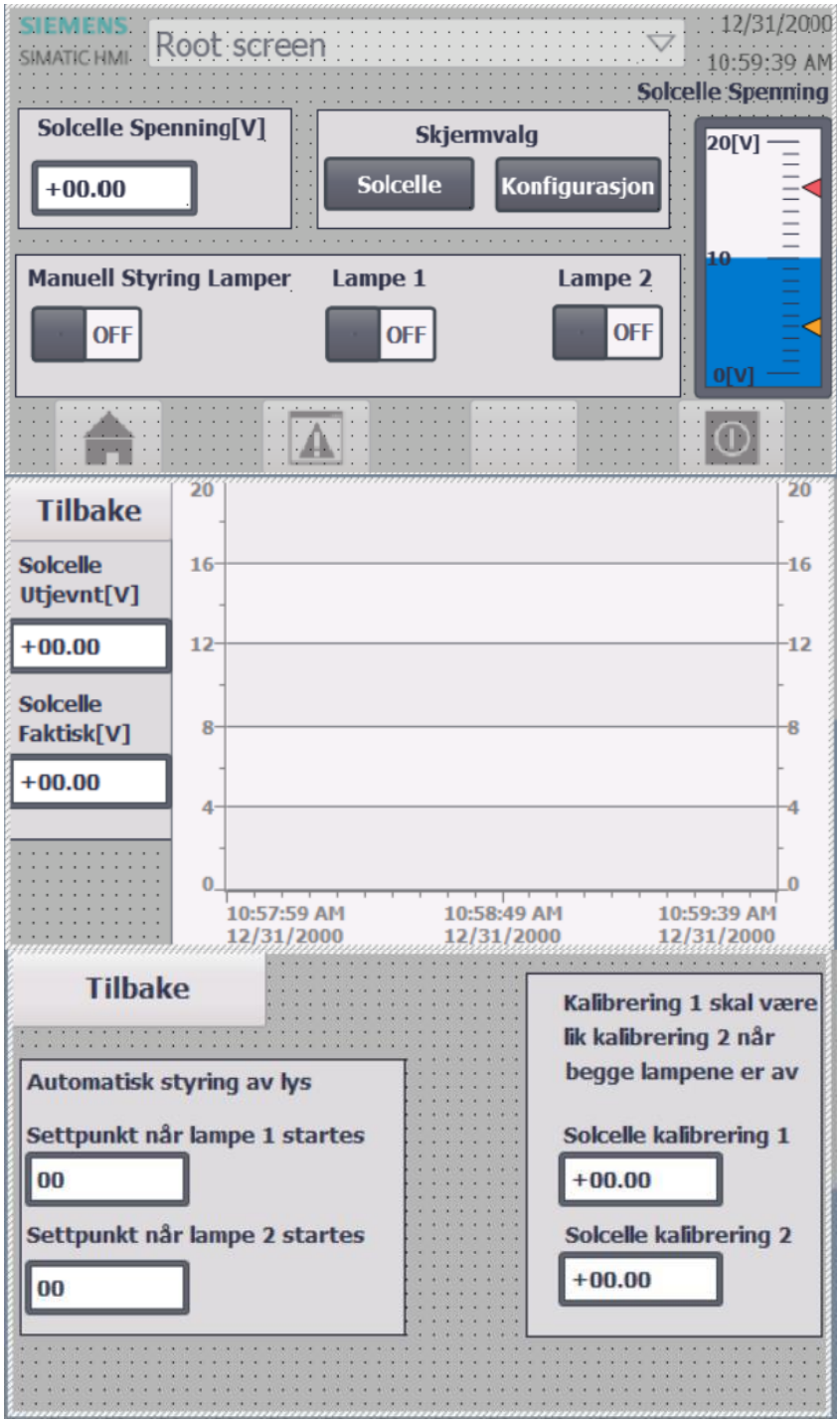
Det blir også utført en utjevning på tallene fra generatoren og solcellene. Dette blir gjort for å sørge for at både solcellene og generatoren produserer omtrent like mye. Det hjelper med styringen av anlegget og sørger for at tallene ikke blir altfor små.

5.8.5 Brukergrensesnitt i HMI-er

I Figur 5-23 er det en oversikt over HMI-skjermene til generator PLS-en og i Figur 5-24 er det en oversikt over HMI-skjermene til solcelle PLS-en. Begge skjermene har en hoved-skjerm. Hovedskjermene gir generell informasjon om anlegget og gir muligheten til å styre anlegget manuelt eller sette det i automatisk modus. Settpunkt blir også satt på hovedskjer-men og det er mulig å navigere til alle de andre skjermene fra hovedskjermen. Det er satt opp tre forskjellige grafer som viser spenning produsert fra den totale produksjonen, generatoren og solcellene. Hver HMI-skjerm har en egen konfigurasjon side hvor forskjellige parameterne for anlegget kan endres.



Figur 5-23: HMI-skjermer for generator PLS



Figur 5-24: HMI-skjermer for solcelle PLS.

6 Nettverksanalyse og angrep

Dette kapittelet tar for seg nettverksanalyse med påfølgende angrep på riggen. Analyse av OT-nettet gjøres både underveis og etter at riggen er ferdig programmert, og i forkant angrepet for å hente inn informasjon. Deretter gjennomføres forsøk på et cyberangrep. Etter angrepet er utført blir analyseverktøyene tatt i bruk igjen for å demonstrere konsekvensene av angrepet. Innholdet i kapittelet er kort oppsummert i punktene under.

- Nettverksanalyse gjennom switch
- Cyberangrep på modellen
- Nettverksanalyse i etterkant av cyberangrep

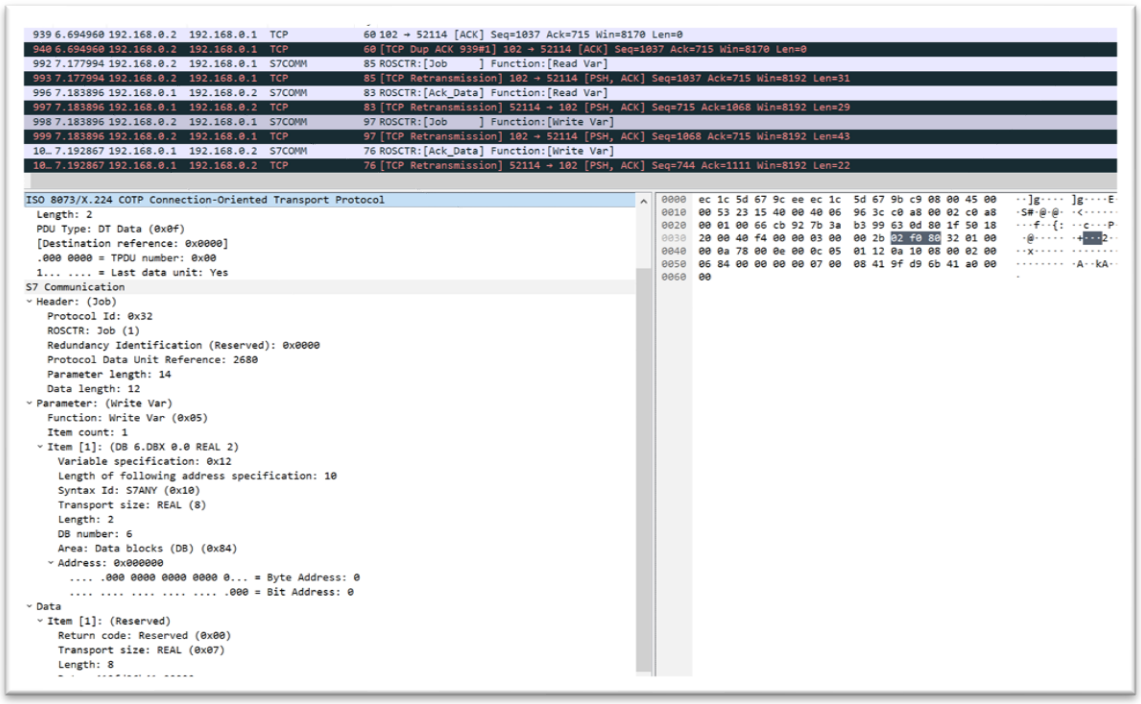
6.1 Nettverksanalyse gjennom switch

For å kunne gjennomføre et angrep på riggen, må det først utføres en nettverksanalyse. Det brukes en rekke verktøy som blant annet Wireshark, Nmap, Proneta og Grassmarlin, med formålet om å hente ut informasjon som IP-adresser, porter som er i bruk, kommunikasjonsprotokoller, leverandører på enheter, osv.

6.1.1 Wireshark

Wireshark er et grafisk verktøy som brukes for å analysere nettverkstrafikk. For å utføre analyse med Wireshark, kreves det at en datamaskin er tilkoblet til en span-port på nettverket, i dette tilfellet port 8. Dette gir mulighet til å overvåke all nettverkstrafikk som passerer gjennom switchen. All trafikk som blir fanget opp ved hjelp av Wireshark kan lagres i en pcap-fil og analyseres videre på et senere tidspunkt. Andre alternativer til Wireshark inkluderer windump eller tcpdump, avhengig av operativsystemet som brukes.

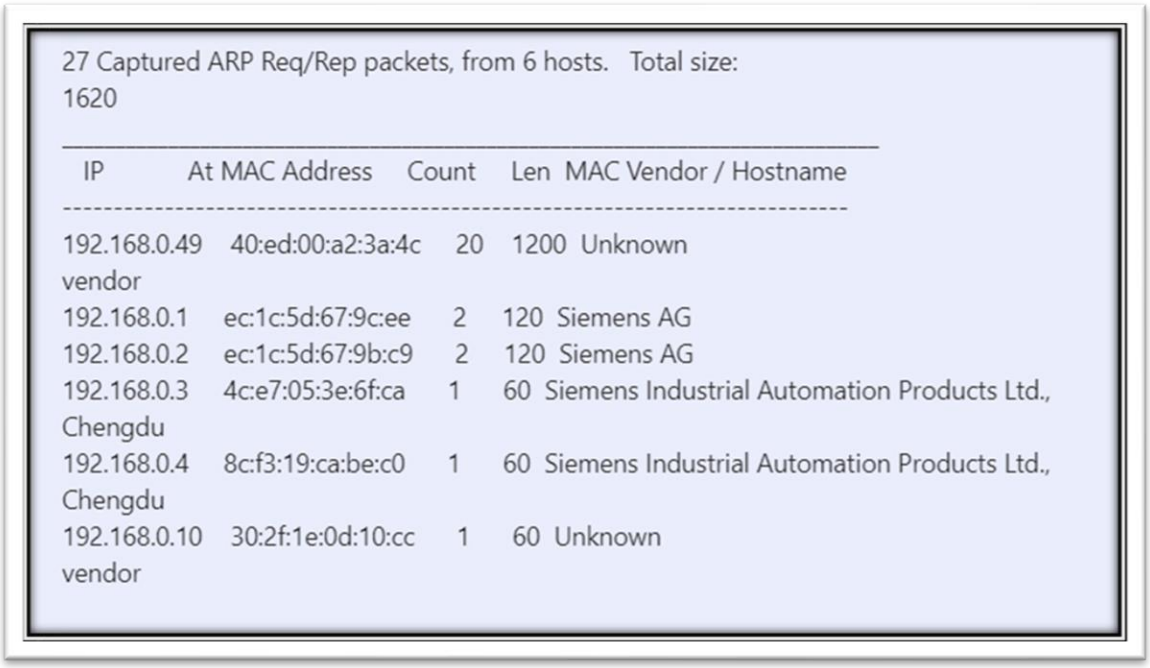
Formålet med Wireshark er å observere nettverkstrafikken under normale forhold, for å få innsikt i hvilke IP-adresser som kommuniserer med hverandre, hvilke porter som er i bruk, hvilke protokoller som benyttes, samt MAC-adressene til enhetene på nettverket. Figur 6-1 viser en oversikt over trafikken mellom to PLS-er.



Figur 6-1: Oversikt over kommunikasjon mellom to PLS-er fra Wireshark

6.1.2 Netdiscover for kartlegging av tilkoblede enheter

Netdiscover er et verktøy som kommer inkludert med Kali Linux. Netdiscover blir brukt til å kartlegge enheter tilkoblet nettverket. Figur 6-2 viser resultatet fra Netdiscover med kommandoen: sudo netdiscover -r 192.168.0.0/24. Enheter 1-4 er allerede kjent fra Wireshark, men det hintes til at enhet 1 og 2, er en type Siemens produkt, og at enhet 3 og 4 er to andre produkter. Enhet 49 er maskinen som utfører skanningen, og enhet 10 blir først kjent ved bruk av Netdiscover. Etter kjøring av Netdiscover kan åpne porter på samtlige enheter sjekkes ved hjelp av Nmap.



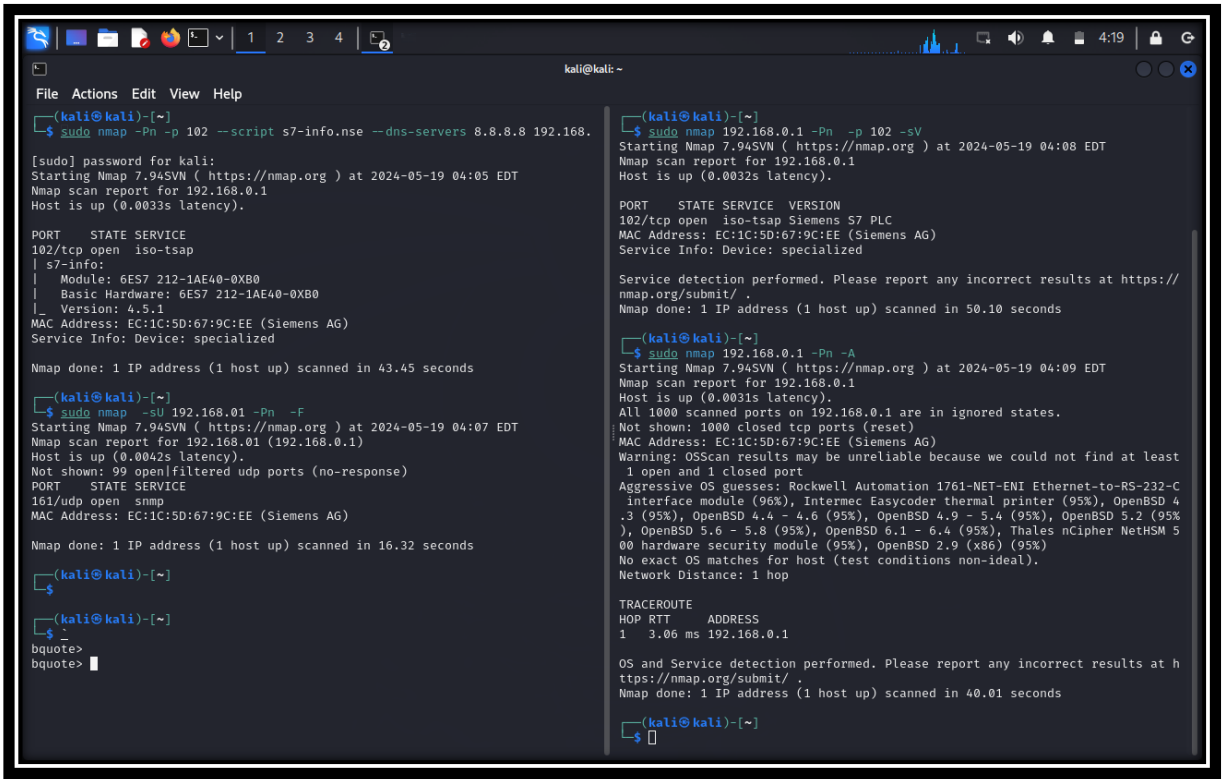
Figur 6-2: Skjermutklipp fra Netdiscover der aktive enheter på nettet listes opp.

6.1.3 Nmap for kartlegging av åpne porter

Nmap er et åpen-kildekode verktøy tilgjengelig som en kommandolinjeapplikasjon (CLI). Verktøyet er fleksibelt og inneholder et bredt spekter av funksjonalitet. Det er viktig å merke seg at Nmap er et aktivt verktøy, som betyr at det genererer sin egen nettverkstrafikk. Dette kan potensielt skape problemer i reelle OT-systemer, avhengig av ressursbruken til skanningen [24]. Det er derfor nødvendig å vise forsiktighet ved bruk av Nmap på OT-systemer.

Nmap brukes til å kartlegge åpne porter tilknyttet IP-adressene på nettverket. Aktuelle IP-adresser er; 192.168.0.1-10, og disse er kjent fra Wireshark. Porter som er i aktiv bruk vises også i Wireshark, Nmap skanningen vil i dette tilfelle liste opp øvrige porter som er åpne og aktive, men ikke nødvendigvis er i bruk. Ved å skanne de første 1024 portene, for alle IP-adressene som er i bruk, gir dette informasjon om eventuelle kommunikasjonsprotokoller som kan brukes til å kommunisere med enhetene [25], [26].

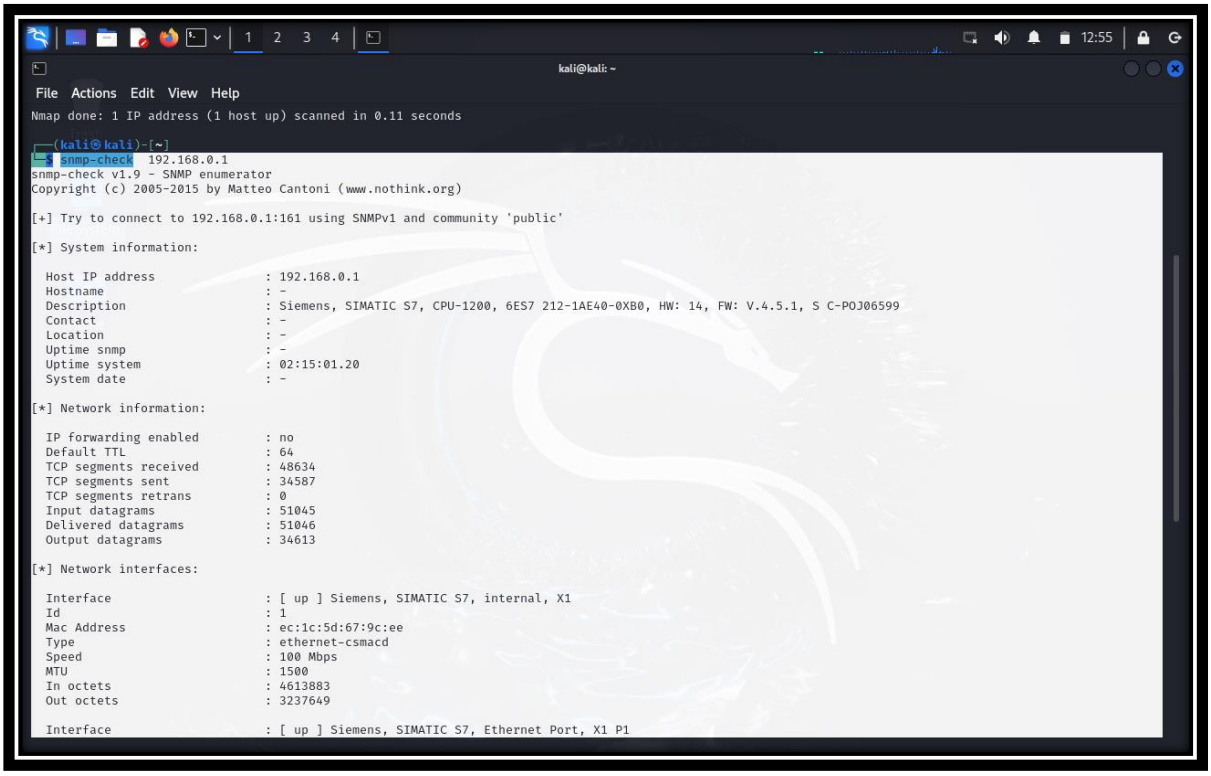
Kjøring av Nmap med: nmap -v -sV -p0-1023 192.168.0.1-4, gir informasjon om de første 1024 portene for enheter 1-4 på nettverket. Figur 6-3 viser et skjermbilde fra Nmap.



Figur 6-3: *Skjermbilde av Nmap fra Kali Linux, som tydelig viser hvilke porter som er åpne på målmaskinene.*

6.1.4 Snmp-check for henting av detaljert informasjon om PLS og switch

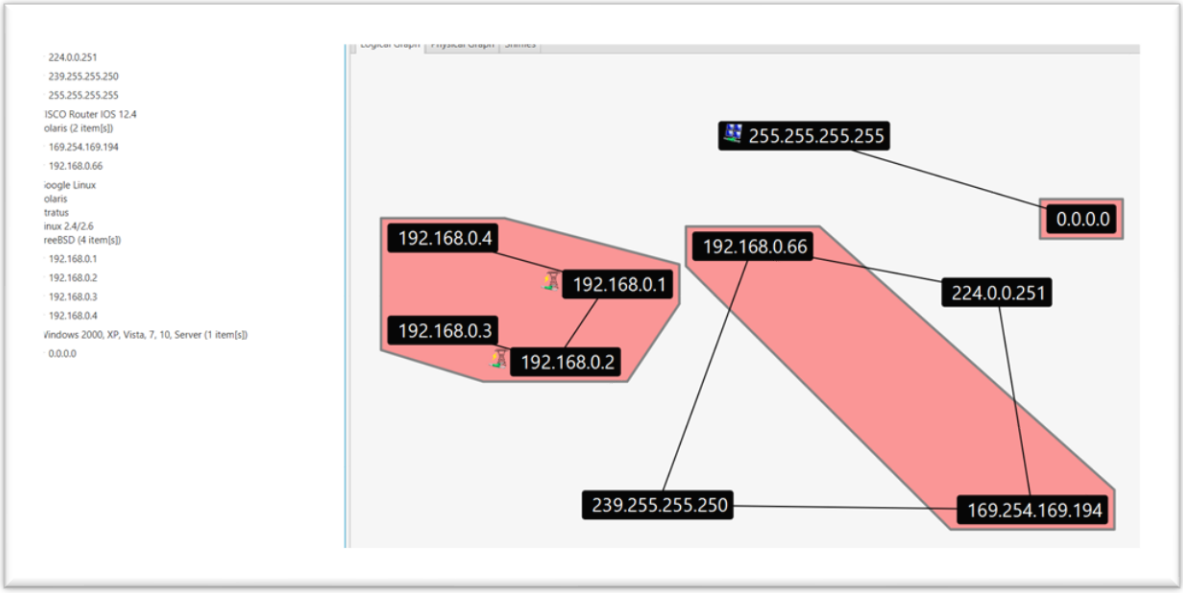
Snmp-check er et verktøy som er inkludert med Kali Linux. Snmp-check sjekker port 161 på enheten som blir sendt inn og gir detaljert informasjon om enheten dersom porten er åpen. Formålet med snmp-check er å hente ut detaljert informasjon om enhetene. Figur 6-4 viser en kjøring av snmp-check på enhet 1 på nettverket. Her kommer det fram at enheten er en Siemens S7-1200 PLS, med modellnummer og fastvare utgave.



Figur 6-4: *Skjermbilde fra snmp-check-kommandoen uført med 192.168.0.1 som parameter.*

6.1.5 Grassmarlin for visualisering av nettverket

Grassmarlin er en åpen-kildekode programvare utviklet av National Security Agency (NSA) i USA [27]. Grassmarlin brukes til å visualisere enhetene som er tilkoblet nettverket, og forholdet mellom enheter. Verktøyet er spesielt nyttig ved analyse på nettverk med flere enheter, og eventuell segmentering. Grassmarlin gir også et estimat på hvilke operativ system som er i bruk hos de aktuelle enhetene, uten at denne er spesielt nøyaktig. I Figur 6-5 vises en visualisering av nettverket.

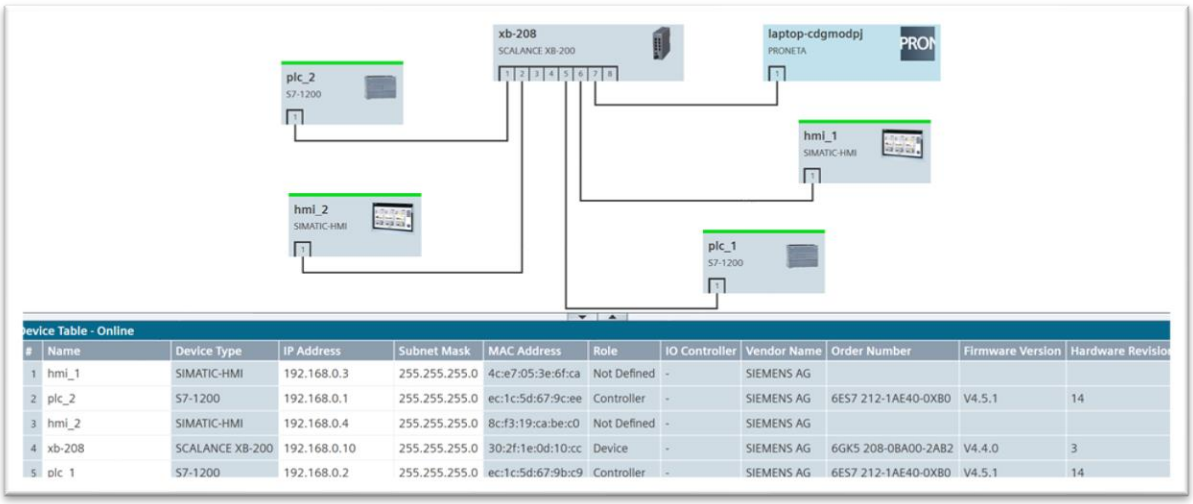


Figur 6-5: Visualisering av nettverket fra Grassmarlin.

6.1.6 Proneta for helhetlig oversikt

Proneta er et analyseverktøy som er utviklet av Siemens, spesifikt for Siemens OT-systemer. En grunnleggende utgave av Proneta kan lastes ned gratis fra Siemens nettsider, mot at en oppretter en bruker. Proneta fungerer kun på Windows-maskiner, og gir kun informasjon om Siemens produkter. Det er derfor et verktøy som er spesielt nyttig i denne sammenheng, men som ikke nødvendigvis vil være aktuelt ved analyse av OT-systemer som baserer seg på andre leverandører.

Proneta fungerer ved at en pc kobles opp på en access port, og velger riktig nettverkskort i programmet. Deretter vises en grafisk oversikt over komponentene på nettverket, og en tabell-loversikt med data over enhetene på nettverket. I Figur 6-6 vises et skjermbilde fra Proneta, med faktiske IP og MAC adresser som blir benyttet i modellen.



Figur 6-6: Skjermbilde fra Proneta.

6.1.7 Oppsummering av nettverksanalyse

Her oppsummeres resultater av nettverksanalysen. Fra Wireshark kommer det fram at IP-adresser 192.168.0.1-4 er i bruk. Port 102 brukes gjennomgående for TCP, COTP og S7COMM protokoller. MAC-adresser til samtlige enheter har blitt funnet. MAC-adressene viser at enhetene på OT-nettverket er produsert av Siemens. Fastvare utgaven på PLS-ene er også blitt kjent, dette er informasjon som kan ha påvirkning på hvilke sårbarheter som eksisterer på enhetene.

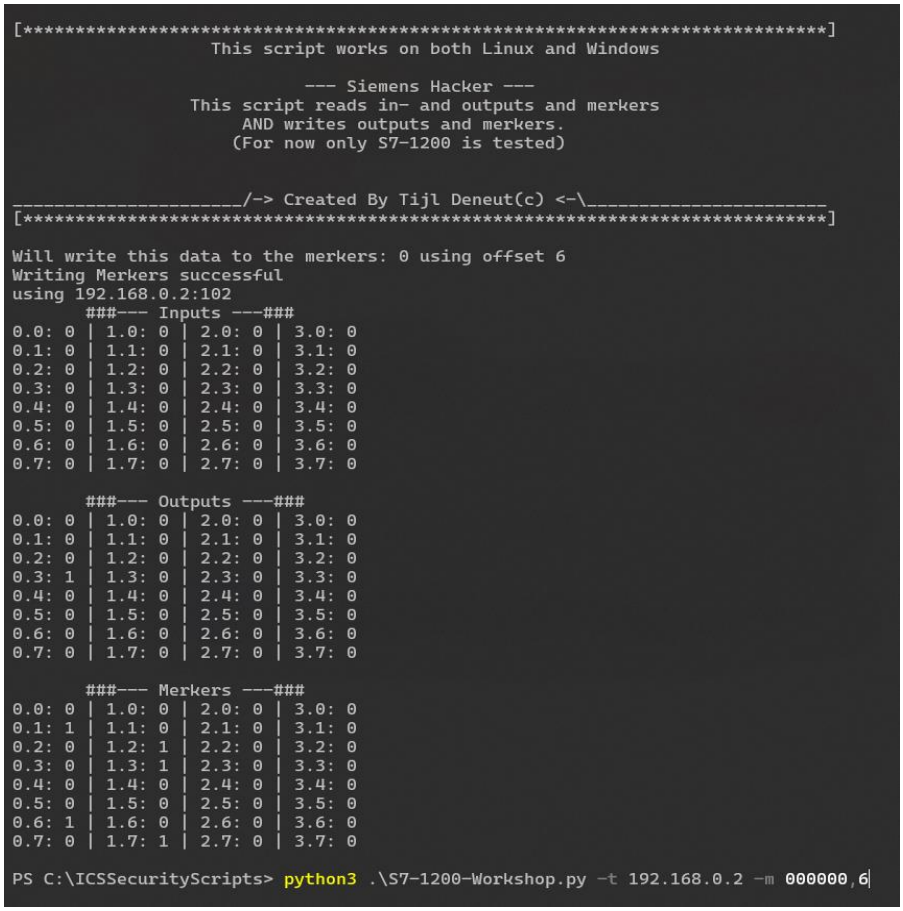
6.2 Angrep på modellen

For gjennomføringen av angrep benyttes en samling med Python-skript kalt ICSSecurity-Scripts [28]. Fra denne samlingen brukes SiemensScan.py, og S7-1200-Workshop.py. SiemensScan.py er det mest omfattende skriptet og fungerer som en interaktiv konsollapplikasjon. S7-1200-Workshop.py er et noe enklere skript, som kan ta inn argumenter fra kommandolinjen.

Status på digitale innganger, digitale utganger og minneblokker eller «merkers», kan leses ut ved kjøring av skriptene. Samtlige digitale utganger kan settes ved bruk skriptene, men disse vil bli overskrevet ved neste CPU-syklus i tilfeller hvor PLS-en styrer utgangene logisk. Alle utgangene på begge PLS-ene styres logisk, derfor er ikke dette spesielt effektivt.

Skriptene kan også endre på variabler i minne. PLS-en som styrer generatoren kan påvirkes ved å endre på variabler 0-3 på adresse 6. Dette gir kontroll over pumpa, og ventilen settes til settpunktet som er ført opp i HMI-en. PLS-en som styrer solcellene, kan påvirkes ved å endre på variabler 0-2 på adresse 5. Bryterne som kontrollerer hvorvidt PLS-ene styres manuelt eller automatisk ligger på disse adressene. Etter at PLS-ene har blitt satt over til manuell kontroll, kan enkelte utganger settes direkte.

Figur 6-7 viser kjøring av S7-1200-Workshop.py, der variabler i minne adresse 6 settes til 0. IP-adresse er satt til 192.168.0.2.



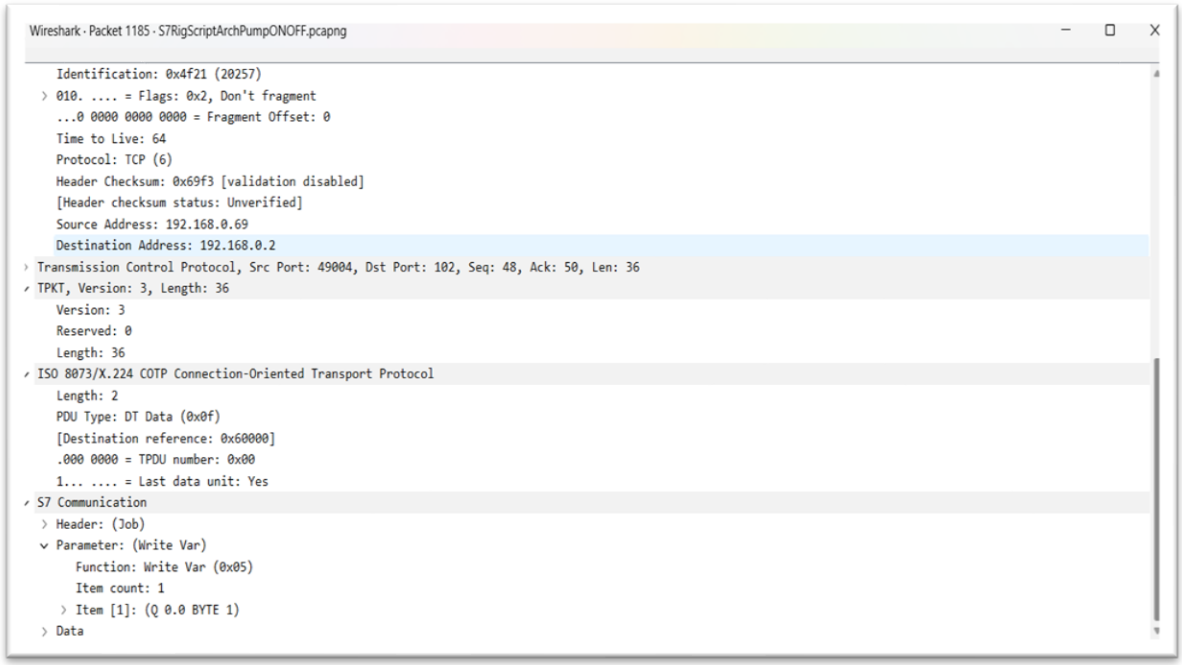
Figur 6-7: Skjermbilde fra kjøring av S7-1200-Workshop.py

SiemensScan.py har noe ytterligere funksjonalitet, utover S7-1200-Workshop.py. Dette inkluderer muligheten til å få LED lysene på PLS-er og switchen til å blinke kontinuerlig, og skjermen på HMI-er kan også blinkes ved bruk av samme funksjon.

Skriptet skal også ha mulighet til å sette start/stop modus på PLS-ene, dette fungerer ikke for øyeblikket. I tillegg skal det ha muligheten til å endre IP-adressene til enheter, og navn på enhetene. Denne funksjonen har ikke blitt testet ut ennå.

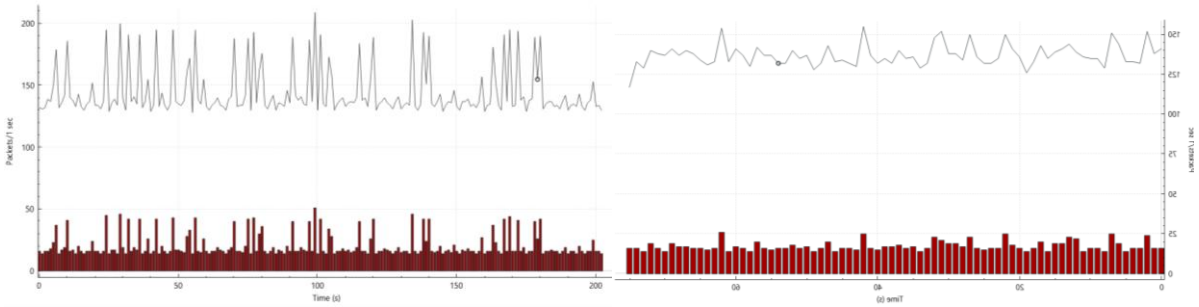
6.3 Nettverksanalyse i etterkant av angrep

I etterkant av angrepet kan Wireshark benyttes igjen for å analysere nettverkstrafikken mellom angrepsmaskinen og aktuelle enheter. I Figur 6-8 vises pakken som sendes fra angrepsmaskin for å starte pumpa på PLS-en som styrer generatoren.



Figur 6-8: Denne pakken viser bruk av S7COMM-protokoll for kommunikasjon fra angrepsmaskin til PLS.

Under gjennomføring av angrepet øker nettverkstrafikken betraktelig. I Figur 6-9 under, vises en graf over nettverkstrafikken under angrep til venstre, sammenliknet med normal trafikk til høyre. Sort strek representerer totalt antall pakker per sekund, og tcp feilpakker representeres av røde stolper.



Figur 6-9: Plott fra nettverkstrafikk

6.4 Forutsetninger for gjennomføring av angrep

Sikringstiltak på anlegget har innvirkning på om angrepet fungerer eller ikke. Etter ønske fra oppdragsgiver iverksettes det ikke sikringstiltak på riggen. Noen av disse settes opp automatisk av TIA portal, og må derfor skrus av manuelt. For å kunne få uautorisert tilgang til datablokker på s7-1200 PLS-er må «Optimized block access» skrus av. «Access level» må settes til «full access» på begge PLS-er. «Permit access with PUT/GET communication from remote partner» må også settes opp.

For å faktisk sikre anlegget, må tiltakene som er listet opp over reverseres. Det vil også være hensiktsmessig i en reell setting å stenge ubrukte fysiske porter på switchen.

7 Diskusjon

I dette kapittelet diskuteres resultatene og erfaringene fra prosjektet, med fokus på løsningens relevans i forhold til problemstillingen. Kapittelet vil også ta for seg miniatyrmodellen av det kombinerte kraftverket og sammenligne relevansen i forhold til reelle anlegg. Utfordringer og uforutsette hendelser underveis vil også diskuteres, og det vil settes lys på hva som fungerte bra og hva som ikke fungerte etter planen. Innholdet i kapittelet er kort oppsummert i punktene under.

- Diskusjon for undersøkelse av cyberangrep, konsekvenser og sårbarheter
- Diskusjon av potensielle løsninger
- Diskusjon av vannkraftmodellen
- Diskusjon av solkraftmodellen
- Diskusjon av styresystem og HMI
- Diskusjon av nettverksanalyse og angrep

7.1 Diskusjon for undersøkelse av cyberangrep, konsekvenser og sårbarheter

Hensikten ved undersøkelsen var å danne en oversikt og et grunnlag for å kunne utvikle en miniatyrmodell av et industrielt anlegg som kan brukes til testing, demonstrering og opplæring av cybersikkerhet i OT-systemer. Det ble funnet at cyberangrep på SCADA-systemer har blitt gjennomført over lang tid, siden styresystemer først ble tatt i bruk. Først i 2010, har angrep og skadevare blitt direkte rettet mot sårbarheter i OT-systemer. Det viser seg også at cyberangrep mot OT-systemer er en økende trussel, ettersom automatiserte kontrollsystemer blir mer og mer utbredt. Undersøkelsen begrenset seg til fire kjente hendelser, som var av betydelig relevans for utvikling av miniatyrmodellen. Resultatet av undersøkelsen er en faktor for valg av løsning for modellen, og valg av komponentene som er tatt i bruk i modellen. I alle fire hendelsene er det enten elkraftanlegg, eller anlegg som bearbeider naturressurser som har vært målene for angrep.

7.2 Diskusjon av potensielle løsninger

Det ble i utgangspunktet utviklet tre potensielle løsninger til miniatyrmodeller av industrielle anlegg som kan brukes for testing og demonstrering av cyberangrep. De tre løsningsforslagene baserer seg på miniatyrmodeller for vannkraftverk, sorteringsanlegg og roterende solcelleanlegg. Alle tre løsningene hadde sine fordeler og ulemper basert på løsbarhet, kostnader og relevans til problemstillingen. Etter tilbakemelding fra oppdragsgiver ble det utviklet et fjerde løsningsforslag som baserte seg på en kombinasjon av vannkraftverket og solkraftverket.

Hensikten ved å utvikle flere løsningsforslag var å både få en bredere kunnskap og oversikt over hvilke prosesser som kan være utsatte for cyberangrep; og for å kunne vurdere hvilken løsning som passet best til å fylle kravene og problemstillingen fra oppdragsgiver.

7.2.1 Diskusjon for valg av løsning

Den endelige løsningen som ble valgt var miniatyrmodellen for kombinasjonen av vann- og solkraftverket. Denne løsningen inkluderte to prosesser som kunne skilles fra hverandre, og samtidig ha et felles aspekt om å møte strømproduksjonens settpunkt. Det kombinerte kraftverket hadde også flere sårbarheter og angrepsvinkler enn de tidligere løsningsforslagene, som gjorde modellen bedre egnet for å brukes til demonstrasjon av cyberangrep og testing av sikkerhetsprodukter. Siden det kombinerte kraftverket slo sammen to tidligere løsningsforslag var det også ulemper knyttet til kostnad og kompleksitet i programmering av PLS-ene.

7.3 Diskusjon av vannkraftmodellen

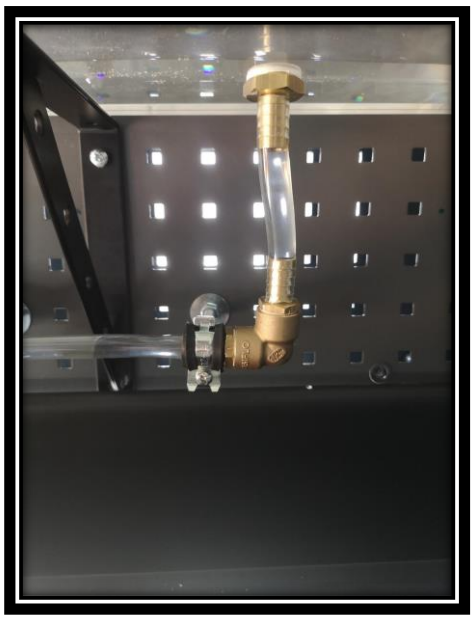
Dette delkapittelet vil diskutere ulike aspekter ved design og implementering av vannkraftmodellen. Det skal sees nærmere på utfordringer knyttet til designet av vanntankene, festing og oppsett av komponenter, og generatoren og reguleringsventilen. I tillegg skal det gjennomgås utfordringer knyttet til ultralydsensorens plassering og pumpens funksjon.

7.3.1 Design av vanntanker

Magasintanken er designet med åpen topp, som fører til en risiko for vannsprut. På venstre side av magasintanken, hvor vannet renner inn, er risikoen annullert ved å legge en lengre slange for å redusere fallhøyden til vannet. På høyre siden av magasintanken er det derimot et problem. Dersom magasintanken fylles og vannet renner over, vil alle åpninger ned til reservoartanken tettes. Dette fører til at reservoartanken fylles med vann, men ikke har noe åpning for å slippe ut luft, som igjen fører til at vannet spruter opp fra avløpet i magasintanken. For å løse dette ble det laget et lokk som dekker høyre siden av magasintanken.

7.3.2 Fester og støtte

Slangene i vannsystemet er koblet inn i slangenipler, som er festet ved hjelp av rørklammer boltet fast i monteringsveggen. Under design og dimensjonering av vanntankene og gjengene i tanken, ble det ikke tatt hensyn hvor støttene under tanken kunne boltes. Dette fører til at slangen mellom reservoartanken og stengeventilen er bøyd. I tillegg skal det merkes at plasseringen av gjengene i vanntankene er midstilt i tankenes dybde. Dette setter gjengenes plassering 7,5cm ut fra veggen, og dette er lengre enn boltene rekker ut. Det er derfor enkelte steder i modellen hvor slangene bøyer seg inn mot veggen. Figur 7-1 viser hvordan slangen bøyes inn mot veggen og til siden. Likevel har ikke bøyingen av slangen noe funksjonell konsekvens for vannsystemet, men det går utover utseende. Det ble forsøkt å feste rørklammene på andre steder langs slangen, men dette løste ikke problemet.



Figur 7-1: Bilde av slange som er bøyd innover mot veggen og mot høyre.

Et annet problem oppstod gjennom monteringsperioden når komponenter ble boltet i monteringsveggen. Siden monteringsveggen er bygget av stålplater på baksiden og forsiden av veggen, bøydes platene mot hverandre når boltene ble strammet. Dette førte til at enkelte fester ble løse. Som løsning ble alle bolter strammet med hendene i stedet for med skiftenøkkel, for å minimere bøyingen av platene, og sørge for at alle bolter ble strammet likt.

7.3.3 Generator og reguleringsventil

Et problem med generatoren som blir brukt i modellen er at den er for liten i forhold til slangene og vannstrømmen. Dette gir reguleringsventilen litt mindre kontroll over vannstrømmen siden generatoren begrenser strømningen rett etter reguleringsventilen. Selv om kontrollen over vannstrømmen er begrenset er den fortsatt god nok til å kunne styre anlegget som det var ønsket. Et annet problem er at trykket som modellen skaper i vannmagasinet ikke var nok til å få generatoren til maks produksjon. Løsningen for dette var å skalere verdien i PLS-programmet. Dette ble gjort for å utjevne verdien med solcellene slik at begge produksjonsenhetene produserte tilnærmet likt. Denne løsningen gir en bedre kontroll over anlegget og gjør det mer oversiktlig for de som betjener anlegget.

7.3.4 Ultralyd og pumpe

På grunn av mangel på plass over magasintanken er ultralyden installert over monteringsveggen. Det var problemer under kalibreringen med at ultralydens signal reflekterer av veggene til tanken som ga målinger. Dette ble fikset ved å konfigurere signalet fra ultralyden til å dekke et mindre område. Pumpen som ble valgt gjorde designprosessen litt vanskeligere, da det i etterkant viste seg at den ikke var selvforsynende. Dette betydde at pumpen trengte et fall mellom reservoartanken og ned til inntaket til pumpen. For å løse dette ble reservoartanken festet høyere på veggen enn planlagt, som førte til mindre vertikal plass på veggen, og mindre fall fra magasintanken og gjennom generatoren.

7.4 Diskusjon av solkraftmodellen

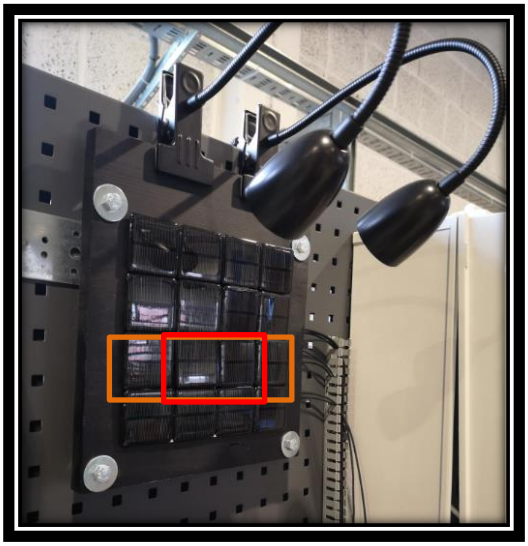
Dette delkapittelet vil diskutere utfordringer knyttet til solcellemodellens oppsett, lysforstyrrelser i solcellepanelet og tilpassing av lyskilden. Løsningene for utfordringene vil også komme fram i underkapitlene.

7.4.1 Oppsett av solceller

Solkraftmodellen består av en tilpasset treplate som ble spraymalt i matt sort farge. Platen er boltet fast i monteringsveggen, og individuelle solceller er koblet og loddet sammen til fire rader.

Solcellene ble bestilt som individuelle celler og måtte kobles og loddes sammen for å lede strøm i serie. Dette var en utfordrende oppgave da cellene og loddepunktene er relativt skjøre, med fare for at loddepunktene kunne falle av. Dette var tilfellet i to punkter på den tredje raden i solcellepanelet, som førte til at raden ikke leder strøm. Det ble forsøkt å rette opp i feilen ved å demontere raden som var påvirket, men dette førte kun til mer skade på solcellene. Raden ble derfor festet på igjen for utseendes skyld.

I Figur 7-2 markerer den oransje boksen den raden som er berørt av feilen, og rød boks markerer cellene med ødelagte koblingspunkter. Som løsning på feilen er det kun de tre ledende radene som er koblet til PLS-en. Dette fører til en mindre strømproduksjon, men siden solcellenes produksjon er skalert i PLS-en, har ikke dette noe å si for funksjonen til panelet.



Figur 7-2: Feil i solceller som fører til ikke-ledende koblinger. Oransje boks markerer raden som er berørt av feilen, og rød boks markerer cellene med ødelagte koblingspunkter.

7.4.2 Lysforstyrrelser fra rombelysning i solcellepanelet

Størrelsen og kvaliteten til solcellene fører til at spenningsproduksjonen oppnår høye verdier, selv i normalt belyste rom. Som konsekvens av dette, har ikke lampene den planlagte virkningen på cellenes spenningsproduksjon, med mindre lyset i omgivelsene er lavt. En enkel

løsning for dette er å skjerme cellene for lys, og kun la lampene virke på panelet. Dette ble testet ved å holde en plate over cellene for å blokkere omgivelseslys. Uten skjerming produserte panelet mellom 15-17V i normal rombelysning, og med platen ble produksjonen dempet til mellom 2-5V. Ved å skru på lampene hoppet verdien igjen opp til 15-17V produsert spenning.

Løsningen som ble valgt var å dempe verdien til solcellene i PLS-en. Det blir gjort ved å ta en måling når PLS-en starter av alle solcellene når lampene er av. Den målingen viser da hva som blir produsert av belysningen i rommet. PLS-en kan da ta denne verdien å subtrahere den fra det som blir målt. Dette setter da verdien til solcelle panelet til null når lampene for solcellene er av og sørger for at solcellene bare produserer når lampene er på. Denne løsningen fungerer imidlertid ikke dersom rombelysningen er sterkere enn lampene. Likevel fungerer denne løsningen godt i kombinasjon med andre løsninger.

7.4.3 Tilpassing av lyskilde

Det ble kjøpt inn to 230V klemmelamper, som viste seg å ha 12V adaptere i støpselet. Dette var ikke forventet at lampene kom med adaptere, og siden den opprinnelige planen var å kutte av støpselet og styre lampene med 230V gjennom kontaktorne, måtte det jobbes med en alternativ løsning. Første tanken for å løse problemet var å kutte av støpselet og bruke PSU som strømkilde, men siden PSU er 24V og lampene tar 12V, var ikke dette en mulighet.

Det ble vurdert å montere en dobbel stikkontakt på baksiden av veggen som var koblet til to kontaktorer, men utfordringen her ble å finne ut hvordan dette kunne monteres i veggen. Et annet problem var å finne en dobbel stikkontakt, hvor hvert stikk kunne styres separat. Det ble derfor vurdert et enklere og rimeligere alternativ.

Løsningen ble til slutt å kjøpe to skjøteledninger med en utgang hver. Disse ble kuttet og kobla inn i hver sine kontaktorer, slik at adapterne kunne kobles i hver sin skjøteledning. Lampene kunne dermed styres med PLS via kontaktorne. Skjøteledningene ble trukket gjennom monteringsveggen før de ble kobla i kontaktorne.

7.5 Tilpassing og oppsett av koblingsskap

Koblingsskapene som ble bestilt var uten hull for kabelgjennomføringer og fester; så dette måtte bores i etterkant. Mengden kabelgjennomføringer ble bestemt for å ha nok plass til alle kablene som skulle brukes og i tillegg ha en del ekstra for å sørge for at utvidelser var mulig. Når det kommer til det indre oppsettet av koblingsskapet med PLS-ene ble det vurdert oversikt og trekking av kabler. Siden koblingsskapet er gjennomsiktig var det viktig å tenke på oversikten og utseende var bra slik at det var mulig å se komponentene drive anlegget. Kabelkanalene ble plassert slik at det trengtes å trekke så lite kabel som mulig. Det andre koblingsskapet som ikke var gjennomsiktig, ble brukt til å montere HMI-skjermene og status lampene. Det ble gjort for å gjøre det enkelt å montere alt på et sted istedenfor å ha separate fester for alt sammen. Dette gjorde det mye lettere og ryddigere når alt måtte kobles sammen.

7.6 Diskusjon av styresystemet og HMI

Det største problemet med å designe et styresystem er å få alle de forskjellige komponentene til å fungere og kommunisere sammen på en god måte. Måten dette ble løst på var å starte med å teste komponentene en og en ved å koble det inn på PLS-en uten at komponentene var montert på modellen. På denne måten kan alle komponentene bli testet og stilt inn uten å bli påvirket av problemer fra de andre komponentene. Når alt er testet kan det da monters på modellen med alle de andre komponentene. For grensesnittet til HMI-en var det viktig å sørge for at det var oversiktlig med nok informasjon og styringsmuligheter. Det var to forskjellige størrelser på HMI-ene generator HMI-en var større og solcelle HMI-en var mindre. Det ble derfor valgt å ha mesteparten av informasjonen og styringsmulighetene på generator HMI-en for å holde det ryddig. Så solcelle HMI-en ble designet med mindre styringsmuligheter og bare den informasjonen som var nødvending.

7.7 Diskusjon av nettverksanalyse og angrep

I løpet av nettverksanalysen på miniatyrmodellen ble det samlet inn informasjon ved hjelp av verktøyene Wireshark, Nmap, Proneta, Netdiscover og Grassmarlin. Analysen resulterte i detaljer knyttet til nettverkets struktur, inkludert IP-adresser, MAC-adresser, åpne porter og kommunikasjonsprotokoller. Samtidig ble det identifisert mer informasjon om angrepsmålet.

Ved bruk av spesialiserte verktøy som Python-skriptene SiemensScan.py og S7-1200-Workshop.py fra samlingen ICSSecurityScripts, ble det gjennomført et angrep på testriggen. Dette angrepet involverte manipulering av digitale utganger og minneblokker på PLS-enhetene, og hadde potensial til å få alvorlige konsekvenser for systemets kontroll. For eksempel kunne angriperen aktivere eller deaktivere pumpen, noe som kunne forstyrre systemets operasjoner, inkludert oversvømmelseskontroll og solcellenes lyskilde.

Under kjøringen av skriptene avdekket analysen av nettverkspakker med Wireshark en test av redundanssystemet, noe som antydet mulige forsøk på å prøve eller forstyrre redundansfunksjoner. Profinet MRP (Media Redundancy Protocol) ble observert. I tillegg ble mange retransmisjonspakker av TCP-protokollen merket som dårlig TCP, noe som har vært et problem på nettverket gjennomgående, men som også kan tyde på uautorisert aktivitet. Oppdagelsen av lesing og skriving til PLS-enheter gjennom S7-protokollen på Wireshark var en klar indikasjon på potensiell uautorisert tilgang.

Forsøkene på å bruke Metasploit for å fjernstyre CPU-modellen, inkludert å slå den av og på, mislyktes. I tillegg fungerte ikke en funksjon i SiemensScan-skriptet som var ment for å endre CPU-tilstanden etter hensikt. Disse erfaringene understreker den forbedrede sikkerheten til Siemens PLS-er. Selv med avanserte skript og rammeverk som Metasploit, var det ikke mulig å endre CPU-tilstanden på disse spesifikke punktene.

Selv om full tilgang ("Access level" satt til "full access") ble gitt på begge PLS-ene og tillatelse for tilgang med PUT/GET-kommunikasjon fra eksterne partnere ble aktivert, var det fortsatt vanskelig å endre CPU-tilstanden gjennom penetrasjonstesting. Dette indikerer at sikkerheten til PLS var solid mot forsøk på uautorisert tilgang.

8 Videre arbeid

Dette kapittelet vil ta for seg videre arbeid knyttet til miniatyrmodellen av det kombinerte kraftverket, med fokus på forbedringer av modellen, ferdigstilling av uoppnådde mål og eventuelle utvidelser av systemet. Det vil også bli beskrevet aktuelle løsninger knyttet til det videre arbeidet.

8.1 Videre arbeid for undersøkelse av cyberangrep, konsekvenser og sårbarheter

Videre arbeid tilknyttet undersøkelse av cyberangrep vil være å undersøke andre angrep som har blitt utført. Hendelsene kan også undersøkes i ytterligere detalj. Angrepene som er blitt tatt opp er komplekse, og utnytter flere titalls forskjellige sårbarheter. Enkelte av sårbarhetene som finnes i angrepene kan i teorien demonstreres ved hjelp av miniatyrmodellen.

8.2 Videre arbeid i solkraftverket

Loddepunktene til to av solcellene er knekt av og ødelagte, som fører til at en av radene i panelet ikke er koblet opp. En mulig løsning på problemet ville vært å bestille nye celler og vært mer nøye med både kobling og lodding. Her kan det også være en fordel å lime cellene på bakplata, med bedre planlegging for hvor kablene legges, for å få panelet flatt. En annen mulighet er å bestille et solcellepanel med tilhørende feste som kan boltes fast i monteringsveggen.

Et annet problem ved solcellene er lysforstyrrelser fra rombelysningen. Solcellene produserer en relativt høy spenning ved normalt belyste rom, som fører til at lampene ikke har en særlig stor effekt på produksjonen. En løsning for dette vil være å montere en plate som skjermer for rombelysningen og kun la lampene virke på panelet.

8.3 Videre arbeid i vannkraftverket

Dette delkapittelet vil ta for seg videre arbeid basert på løsninger for skjevheter i vannsystemet, videre arbeid ved magasintanken og manglende installering av frekvensomformer. Problemene vil bli kort oppsummert og deretter vil mulige løsninger forklares.

8.3.1 Skjevheter i vannsystemet

Slangene i vannsystemet er koblet inn i slangenipler, som er festet ved hjelp av rørklemmer boltet fast i monteringsveggen. Under design og dimensjonering av vanntankene og gjengene i tanken, ble det ikke tatt hensyn hvor brakettene som tanken hviler på kunne boltes. Dette fører til at slangen mellom reservoartanken og stengeventilen er bøyd. Her er det mulig å bore hull gjennom monteringsveggen, som kan brukes for å bolte rørklemmene med mer nøyaktighet for å rette ut slangen. En annen løsning er å benytte rørklammer som kan stilles i vinkel. Dette gir mer rom for justering av festet, men krever god installasjon.

Et annet problem er at gjengene i vanntankene stikker lengre ut av veggen enn boltene og rørklammene rekker. Dette har ført til at slangene blir trukket inn mot veggen mellom reservoar-

og magasintanken og under reservoartanken. En løsning på dette er å bruke helgjenga M8x12cm bolter for å gi mer rom for justering og rette opp slangene.

8.3.2 Manglende installering av frekvensomformer

Pumpen som ble valgt er en 230V en-fase motor, og frekvensomformeren som ble bestilt er bare kompatibel med tre-fase motorer. Som konsekvens av dette kunne ikke frekvensomformeren brukes for å regulere pumpens hastighet. Frekvensomformeren ble derfor ikke montert på modellen, men legges ved for videre utvidelse av systemet, eller ved et eventuelt bytte av pumpe.

8.4 Forbedringer i styresystem og HMI

Noe som kan jobbes videre med i anlegget er å utvide modellen med flere komponenter. Dette vil åpne opp for flere type angrep og øke kompleksiteten på anlegget som hjelper med å få det til å bli mer industrielt. PLS-programmet kan også endres for å gjøre systemet mer eller mindre sikkert som ønskelig ut ifra hva som testes. HMI-grensesnittet kan jobbes videre med ved å legge til flere styringsfunksjoner for å utvide styringsmulighetene til anlegget. Det kan også jobbes med å legge til flere innstillinger i konfigurasjons skjermen som også hjelper å bedre styring av modellen.

8.5 Forbedringer ved nettverksanalyse og cyberangrep

Målet er å utvikle miniatyrmodellen til å fungere som en realistisk treningsplattform for nettverksanalyse og penetrasjonstesting. Et sett med verktøy, inkludert Wireshark, Grassmarlin, Nmap, Proneta og SNMP, brukes for grundig overvåking og analyse av nettverkstrafikken. Ved å automatisere disse verktøyene kan kontinuerlig overvåkning av nettverket gjennomføres, og trusler og sårbarheter oppdages på et tidlig stadium. Videre, simulering av realistiske angrepsscenarioer for å lære og øve på identifisering, analyse og respons på faktiske trusler, inkludert penetrasjonstesting for å vurdere systemets sikkerhet og evaluere eventuelle sårbarheter.

For å forbedre cyberangrepet kan ICS-skriptene oppgraderes. For eksempel kan det legges til funksjonalitet som muliggjør lesing og skriving av settpunkter, for ventilåpning og vannivå. Bruk av skriptene kan også automatiseres ved hjelp av bash eller powershell. Da kan hele angrepssekvensen gjennomføres med ett tastetrykk, på begge PLS-ene. Angrepet kan for eksempel også gjennomføres gjentatte ganger ved spesifikke tidspunkter, uten at noen må sitte foran en maskin å gjøre dette manuelt.

Det er også muligheter for å oppdage og utnytte nye sårbarheter. «Man in the middle»-angrep kan gjennomføres ved å koble en maskin mellom en PLS og tilhørende HMI, og manipulere nettverkstrafikken som går gjennom. HMI-ene er sårbare for DoS-angrep, dette er noe som kan utvikles videre. Det kan også være muligheter for å få til et brute force I/O angrep.

Konklusjon

Ved prosjektets slutt har fire kjente hendelser, og aktuelle sikkerhetsstandarder blitt undersøkt. Det har blitt satt fokus på Stuxnet, Triton, Black Energy, og Industroyer. Vesentlige sårbarheter og konsekvenser for disse har blitt kartlagt og en rekke sikringsstandarder har også blitt forklart. Resultatene fra undersøkelsene har hatt innvirkning på resten av arbeidet, spesielt valg av miniatyrmodell, og valg av komponenter.

Fire forskjellige konsepter for miniatyrmodellen har blitt skissert og vurdert, og en løsning har blitt valgt. Løsningene som har blitt vurdert er et vannkraftanlegg, sorteringsanlegg, roterende solcelleanlegg, og til slutt et kombinert kraftverk, basert på solkraft og vannkraft. Anlegget som har blitt valgt er det kombinerte kraftverket.

Det aktuelle anlegget har blitt designet, og dimensjonert basert på komponenters spesifikasjoner og krav fra oppdragsgiver. Komponentlister har blitt utviklet, for oversikt og til hjelp for innkjøp. Komponenter har også blitt kjøpt inn og vanntanker har blitt spesialbestilt fra Plexon. Anlegget har blitt bygget, og tilpasninger har blitt gjort underveis. Anlegget har også blitt ferdig koblet opp og programmert. Uttesting og kvalitetskontroll har blitt gjort etter ferdigstilling av anlegget.

Det har til slutt blitt gjennomført nettverksanalyse av nettverket som anlegget baserer seg på. Fra nettverksanalysen har det blitt kartlagt informasjon som blant annet IP-adresser, nettverksporter og kommunikasjonsprotokoller som er i bruk i anlegget. Det har også blitt gjennomført et enkelt cyberangrep, basert på funnene fra nettverksanalysen.

Referanser

[1] Eirik Fallrø, «Oppgavebeskrivelse Bacheloroppgave». 3. november 2023.

[2] OTW, «SCADA Hacking: Anatomy of Cyber War, the Stuxnet Attack». 20. november 2018. [Online]. Tilgjengelig på: https://www.hackers-arise.com/post/2019/11/01/scada-hacking-anatomy-of-the-stuxnet-attack

[3] D. Kushner, «The Real Story of Stuxnet», IEEE Spectrum 53, No. 3, 48, 2013. [Online]. Tilgjengelig på: https://spectrum.ieee.org/the-real-story-of-stuxnet

[4] CSS ,ETH ZURICH, «Hotspot Analysis: Stuxnet», okt. 2017. [Online]. Tilgjengelig på: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf

[5] Josh Fruhlinger, «Stuxnet explained: The first known cyberweapon», 31. august 2022. [Online]. Tilgjengelig på: https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html#:~:text=In%20order%20to%20infect%20the,used%20in%20the%20Conficker%20attack.

[6] Martin Giles, «Triton is the world's most murderous malware, and it's spreading». 5. mars 2019. [Online]. Tilgjengelig på: https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

[7] «BlackEnergy APT Attacks in Ukraine», www.kaspersky.com. Åpnet: 6. mai 2024. [Online]. Tilgjengelig på: https://www.kaspersky.com/resource-center/threats/blackenergy

[8] Rhebo.com, «Industroyer». [Online]. Tilgjengelig på: https://rhebo.com/en/service/glossar/industroyer-25114/?fbclid=IwZXh0bgNhZW0CMTAAAR2AjFsQIdcHfVlarRVjuTQWoTgIrd2tKUjLS-Mv6XMBmEZaWPeBQgZj9uY_aem_Af_drWjoLRcVj2cX9vu4TuSEEDGCQLbzUVSvheDcU3oro2HQkVdIVpd4F2IIwZB-dgmQ2OPkQsz6wGFEuvYVGM7W

[9] André Lameiras, «Industroyer: A cyber-weapon that brought down a power grid». [Online]. Tilgjengelig på: https://www.welivesecurity.com/2022/06/13/industroyer-cyber-weapon-brought-down-power-grid/

[10] Anton Cherepanov, ESET, «Industroyer», jun. 2017. [Online]. Tilgjengelig på: https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf

[11] Ismail Tasdelen, «What are the ICS/OT security standards?» 12. desember 2022. [Online]. Tilgjengelig på: https://medium.com/databulls/what-are-the-ics-ot-security-standards-588675eef505

[12] H. Skansgård, K. Marcus, R. Strand, og S. Kold Huseby, «Fremtidige PLS-baserte kontrollanlegg i vannkraftverk», Bachelor thesis, NTNU, 2021. Åpnet: 7. mai 2024. [Online]. Tilgjengelig på: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2778311

[13] «Vannkraft – Slik produseres strøm i Norge», Strøm.no. Åpnet: 7. mai 2024. [Online]. Tilgjengelig på: https://xn--strm-ira.no/vannkraft

[14] «Vemork gamle kraftstasjon - Riksantikvaren». Åpnet: 20. mai 2024. [Online]. Tilgjengelig på: https://riksantikvaren.no/fredninger/vemork-gamle-kraftstasjon/

[15] I. B. Nore og K. Winther, «Optimizing Hybrid Hydro-Solar Power Systems Using Two-Stage Stochastic Programming», Master thesis, NTNU, 2023. Åpnet: 7. mai 2024. [Online]. Tilgjengelig på: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3111990

[16] «Hydroelectric Power: How it Works | U.S. Geological Survey». Åpnet: 15. mai 2024. [Online]. Tilgjengelig på: https://www.usgs.gov/special-topics/water-science-school/science/hydroelectric-power-how-it-works#overview

[17] «Centrifugal pump working principle - HAOSH Pump». Åpnet: . mai 2024. [Online]. Tilgjengelig på: https://www.haoshpump.com/centrifugal-pump-working-principle/

[18] «143912 | Xylem Flojet 230 V 1.4 bar Magnetic Coupling Centrifugal Water Pump, 14L/min | RS». Åpnet: 15. mai 2024. [Online]. Tilgjengelig på: https://no.rs-online.com/web/p/water-pumps/0266979

[19] «Beginner's guide to ultrasonic level transmitter». Åpnet: 15. mai 2024. [Online]. Tilgjengelig på: https://www.coulton.com/beginners_guide_to_ultrasonic_level_transmitters.html

[20] «Ultrasonic level measurement | Endress+Hauser». Åpnet: 15. mai 2024. [Online]. Tilgjengelig på: https://www.endress.com/en/field-instruments-overview/level-measurement/Ultrasonic-level-measurement

[21] Pepperl+Fuchs, «Ultrasonic sensor UB2000-F42-I-V15», Pepperl+Fuchs. Åpnet: . mai 2024. [Online]. Tilgjengelig på: https://www.pepperl-fuchs.com/norway/no/classid_186.htm

[22] «How Do Optical Level Sensors Work?», SMD Fluid Controls. Åpnet: . mai 2024. [Online]. Tilgjengelig på: https://www.fluidswitch.com/2022/02/16/how-do-optical-level-sensors-work/

[23] «VP01EP Optisk nivåfotocelle PNP NC», Carlo Gavazzi. Åpnet: . mai 2024. [Online]. Tilgjengelig på: https://www.gavazzi.no/produktutvelgelse/vp01ep-nivafotocelle/

[24] «Vulnerability Scanners: Passive Scanning vs. Active Scanning», RiskOptics. Åpnet: 21. mai 2024. [Online]. Tilgjengelig på: https://reciprocity.com/blog/vulnerability-scanners-passive-scanning-vs-active-scanning/

[25] «Common Ports Cheat Sheet: The Ultimate List». Åpnet: 19. mai 2024. [Online]. Tilgjengelig på: https://www.stationx.net/common-ports-cheat-sheet/

[26] SpeedGuide, «Port 102 (tcp/udp)», SpeedGuide. Åpnet: 19. mai 2024. [Online]. Tilgjengelig på: https://www.speedguide.net/port.php?port=102

[27] Jim Acord, «Situational awareness and ICS Using GRASS MARLIN», 4. november 2017. [Online]. Tilgjengelig på: https://www.infosecinstitute.com/resources/scada-ics-security/situational-awareness-ics-using-grass-marlin/#:~:text=Developed%20by%20the%20National%20Security,%2Fiadgov%2FGRASS%20MARLIN).

[28] T. Deneut, «tijldeneut/ICSSecurityScripts». 12. mai 2024. Åpnet: 18. mai 2024. [Online]. Tilgjengelig på: https://github.com/tijldeneut/ICSSecurityScripts

Vedlegg

Vedlegg 1 - Prosjektoppgave

Vedlegg 2a - Fremdriftsplan

Vedlegg 2b – Fremdriftsplan for rapport

Vedlegg 3 - Komplett komponentoversikt

Vedlegg 4a - PLS-program generator

Vedlegg 4b - PLS-program solcelle

Vedlegg 5 - Medforfattererklæring

Vedlegg 1: Oppgavebeskrivelse

mnemonic

TLP: Green

Oppgavebeskrivelse Bacheloroppgave
USN - Porsgrunn

Sted	**Oslo**
Dato	**03.11.2023**
Versjon	**1.0**
Forfatter	**E**irik Fallrø

Fysisk modell som viser konsekvens av cyberangrep

Firma: mnemonic

Kontaktperson: Eirik Fallrø, Sikkerhetskonsulent, Tlf.: 48180804, eirikf@mnemonic.no

Bakgrunn

mnemonic er et norsk IT-sikkerhetsselskap som har kunder i forskjellige bransjer. En del av kundene drifter operasjonell teknologi (OT) som stiller spesielle krav til cybersikkerhetsløsninger. Sikring av kontrollsystemene som brukes i OT blir stadig viktigere og mnemonic ønsker å bli bedre på dette området. Tilgang til et realistisk testmiljø er en utfordring for aktører som jobber mot OT-sikkerhet (cybersikkerhet i industrielle miljøer). Det er begrensede muligheter til å teste ut sikkerhetsprodukter ute hos kunder som har anlegg i drift da dette kan påvirke oppetid.

mnemonic ønsker derfor å få lagd en fysisk miniatyrmodell av en fabrikklinje, et prosessanlegg eller tilsvarende som skal brukes til å teste og utvikle nye sikkerhetsprodukter. Modellen skal brukes til opplæring mot interne ressurser med IT-bakgrunn som ønsker å bedre forstå industrielle kontrollsystemer. Modellen skal også brukes mot kunder som drifter OT-miljøer for å vise hvordan sikkerhetsprodukter fungerer i samhandling med et kontrollsystem. Fra et pedagogisk perspektiv er det ønskelig at modellen tydelig viser når kontrollsystemet og den fysiske prosessen fungerer som normalt og når modellen er blitt påvirket av et cyberangrep.

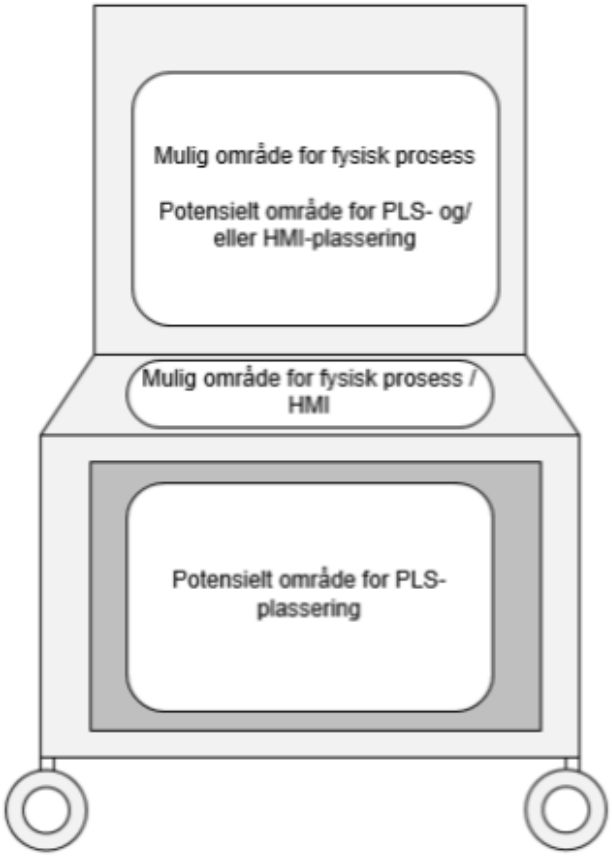
Deloppgaver

1. Undersøk litteratur og annen tilgjengelig informasjon for å lage en oversikt over de mest kjente angrepene, konsekvenser og sårbarheter for OT-systemer. Beskriv og sammenlign de mest aktuelle sikringstiltakene gjennom bruk av sikkerhetsstandarder og lignende.
2. Bygg en fysisk miniatyrmodell (av for eksempel.en fabrikklinje, et prosessanlegg eller tilsvarende) som viser konsekvensene av et vellykket cyberangrep. Bruk en typisk type PLS, HMI og switch som brukes i industrien for å gjøre modellen virkelighetsnær.
3. Gjør enkel analyse av nettverkstrafikk gjennom switch for å forstå oppbygningen av industriell nettverkstrafikk. Bruk denne kunnskapen til å beskrive og gjennomføre et cyberangrep på den fysiske modellen gjennom kontrollsystemet.

Målgruppe

Oppgaven kan passe både for studenter som er nysgjerrige på cybersikkerhet vel som studenter som ønsker en kreativ og praktisk oppgave rettet mot PLS-programmering. Vi er fleksible på omfang av oppgaven i forhold til bakgrunn hos studentene og gruppestørrelse. Vi er også åpne for å støtte med veiledning på cybersikkerhetsdelen av oppgaven. Vårt inntrykk er at kunnskap om cybersikkerhet i OT er etterspurt innenfor for drift-, prosjekt- og sikkerhetsroller i industrien.

Vedlegg: Skisse - Flyttbar modell



Vedlegg 2a: Fremdriftsplan

OPPGAVER OG MÅL	ANSVARLIG PERSON(ER)	PROGRESJON	PLANLAGT START	FAKTISK SLUTT
Møter med veileder og oppdragsgiver				
Første møte med Mnemonic og veileder		100 %	9.1.24	9.1.24
Møte med Mnemonic og veileder		100 %	22.1.24	22.1.24
Møte med Mnemonic og veileder		100 %	29.1.24	29.1.24
Møte med Mnemonic og veileder		100 %	5.2.24	5.2.24
Møte med Mnemonic og veileder		100 %	12.2.24	12.2.24
Møte med Mnemonic og veileder		100 %	19.2.24	19.2.24
Møte med Mnemonic og veileder		100 %	26.2.24	26.2.24
Besøk av oppdragsgiver fra Mnemonic		100 %	29.2.24	29.2.24
Møte med Mnemonic og veileder		100 %	18.3.24	18.3.24
Møte med Mnemonic og veileder		100 %	8.4.24	8.4.24
Møte med Mnemonic og veileder		100 %	6.5.24	6.5.24
Møte med Mnemonic og veileder		100 %	15.5.24	15.5.24

OPPGAVER OG MÅL	ANSVARLIG PERSON(ER)	PROGRESJON	PLANLAGT START	FAKTISK SLUTT
Deloppgave 1 – Cybersikkerhet, kjente angrep, sårbarheter og konsekvenser				
Selvstudium om cybersikkerhet	Alle	100 %	15.1.24	29.1.24
Lage en oversikt over de mest kjente cyberangrepene med konsekvenser og sårbarheter	Mohamed, Sjur, Abdikadir	100 %	15.1.24	29.1.24
Beskrive og sammenligne aktuelle sikringstiltak	Mohamed	100 %	15.1.24	29.1.24

OPPGAVER OG MÅL	ANSVARLIG PERSON(ER)	PROGRESJON	PLANLAGT START	FAKTISK SLUTT
Deloppgave 2 – Utvikling av fysisk modell				
Ideutvikling av mulige løsninger for fysisk modell				
Løsningsforslag 1: Vannkraftverk	Anders	100 %	15.1.24	21.1.24
Løsningsforslag 2: Avfallssortering	William/Mohamed	100 %	22.1.24	26.1.24
Løsningsforslag 3: Solkraftverk	Sjur/Abdikadir	100 %	22.1.24	28.1.24
Løsningsforslag 4: Kombinert kraftverk	Alle	100 %	29.1.24	4.2.24
Utvikling av valgt idee: Kombinert kraftverk				
Skisser av oppsett	William	100 %	5.2.24	12.2.24
Skisse for vanntanker	William	100 %	12.2.24	28.2.24
Skisse for koblingsskap + boring	Sjur/William	100 %	12.2.24	19.2.24
I/O-liste	Anders	100 %	19.2.24	26.2.24
Koblingsskjema	Anders	100 %	19.2.24	26.2.24
Ferdigstille komponentliste og ymse deler	Alle	100 %	5.2.24	19.2.24
Skisse for vannsystemet	William	100 %	12.2.24	28.2.24
Skisse for solcellene	Sjur/William	100 %	12.2.24	28.2.24
Utvikle by	Alle	100 %	12.2.24	28.2.24
Bestilling og innkjøp av komponenter				
Bestillings av hovedkomponenter (koblingsskap)	Eirik	100 %	19.2.24	22.2.24
Bestilling av monteringstavle	Eirik	100 %	19.2.24	22.2.24
Bestilling av vanntanker	Eirik	100 %	28.2.24	20.3.24
Innkjøp av smådeler	William/Mohamed	100 %	11.3.24	13.5.24
Festing og oppsett av modellen				
Festing av vannsystemet	William/Alle	100 %	18.3.24	10.4.24
Festing av støtter for vanntanker	William/Sjur/Abdikadir/Mohamed	100 %	24.3.24	10.4.24
Festing av koblingsskap	Abdikadir/Sjur/Anders/Mohamed	100 %	25.3.24	10.4.24
Festing av reguleringsventil og generator	William	100 %	25.3.24	10.4.24
Oppsett av HMI-er i koblingsskap	Alle	100 %	1.4.24	10.4.24
Oppsett av monteringsvegg	Sjur/Ander/Abdikadir/Mohamed	100 %	4.3.24	22.4.24
Festing av pumpe	William/Sjur	100 %	24.3.24	29.4.24
Festing av ultralyd nivåmåler	William	100 %	1.4.24	29.4.24
Kobling og programmering				
Kobling i koblingsskap	Anders	100 %	1.4.24	15.5.24
Kobling inn og ut av skapet	Anders	100 %	1.4.24	15.5.24
Programmering av PLS-er	Anders	100 %	8.4.24	15.5.24
Programmering av HMI-er	Anders	100 %	8.4.24	15.5.24
Testing av modellen				
Testing av komponenter	Anders/Alle	100 %	18.3.24	18.3.24
Testing av automatisk drift	Anders/Alle	100 %	22.4.24	29.4.24
Testing av manuell drift	Anders/Alle	100 %	22.4.24	29.4.24
Finpussing av modellen				
Oppsett av kabelkanaler	Anders/Sjur/William	100 %	29.4.24	8.5.24
Finpussing programmering	Anders	100 %	29.4.24	29.4.24
Finpussing oppsett og utseende av modellen	Alle	100 %	13.5.24	13.5.24

OPPGAVER OG MÅL	ANSVARLIG PERSON(ER)	PROGRESJON	PLANLAGT START	FAKTISK SLUTT
Deloppgave 3 – Nettverksanalyse og cyberangrep på fysisk modell				
Konfigurering av switch	Anders/Sjur	100 %	29.2.24	11.3.24
Cybersikkerhetskurs 301V og 401V	Sjur/Mohamed	100 %	3.3.24	26.3.24
Utføre nettverksanalyse	Sjur/Mohamed	100 %	8.4.24	15.4.24
Utføre cyberangrep på modellen	Sjur/Mohamed	100 %	15.4.24	15.5.24
Utføre nettverksanalyse etter angrep	Sjur/Mohamed	100 %	22.4.24	15.5.24

Vedlegg 2b: Fremdriftsplan for rapport

OPPGAVER OG MÅL	ANSVARLIG PERSON(ER)	PROGRESJON
Rapport	Alle	100 %
Forside	William	100 %
Forord	Alle	100 %
Sammendrag	Sjur	100 %
Kapittel 1: Innledning	Abdikadir/William	100 %
1.1 Bakgrunn	William	100 %
1.2 Målsettinger	Abdikadir	100 %
1.3 Metode	Abdikadir	100 %
1.4 Avgrensninger	William	100 %
1.5 Leserveiledning	Abdikadir	100 %
Kapittel 2: Cybersikkerhet, sårbarheter, konsekvenser og kjente angrep	Sjur/Mohamed	100 %
2.1 Stuxnet - Iran	Mohamed	100 %
2.1.1 Sårbarheter rundt stuxnet	Mohamed	100 %
2.1.2 Konsekvenser av stuxnet	Mohamed	100 %
2.2 Triton	Mohamed	100 %
2.2.1 Sårbarheter rundt Triton	Mohamed	100 %
2.2.2 Konsekvenser av Triton	Mohamed	100 %
2.3 Black Energy - Ukraina	Abdikadir	100 %
2.3.1 Sårbarheter rundt BlackEnergy	Abdikadir	100 %
2.3.2 Konsekvenser av BlackEnergy	Abdikadir	100 %
2.4 Industroyer	Mohamed	100 %
2.4.1 Sårbarheter rundt Industroyer	Mohamed	100 %
2.4.2 Konsekvenser av Industroyer	Mohamed	100 %
Sikringstiltak for OT-systemer	Mohamed	100 %
Kapittel 3: Potensielle løsninger	William	100 %
3.1 innledning	William	100 %
3.2 Vannkraftverk	Anders	100 %
3.3 Avfallsortering	William/Mohamed	100 %
3.4 Solkraftverk	Sjur/Abdikadir	100 %
3.5 Kombinert kraftverk	Alle	100 %
3.6 Oppsummering av løsningsforslag	Abdikadir	100 %

OPPGAVER OG MÅL	ANSVARLIG PERSON(ER)	PROGRESJON
Kapittel 4: Videreutvikling av kombinert kraftverk	William	100 %
4.1 Systemoversikt og virkemåte	William	100 %
4.1.1 Komponentoversikt og krav	William	100 %
4.1.2 Planlagt virkemåte for vannkraftmodellen	Abdikadir/William	100 %
4.1.3 Forskjellen mellom modellen og reelt kraftverk	Abdikadir/William	100 %
4.1.4 Planlagt virkemåte for solkraftmodellen	Abdikadir/William	100 %
4.1.5 Forskjellen mellom modellen og reelt kraftverk	Abdikadir/William	100 %
4.2 Dimensjonering og tilpassing	William	100 %
4.2.1 Tilpassing av solceller	William	100 %
4.2.2 Design og bestilling av vanntanker	William	100 %
4.2.3 Vannsikkerhet – oppsamlingskar under vannsystemet	William	100 %
4.2.4 Design av miniatyrby for illustrert strømproduksjon	Abdikadir/William	100 %
4.2.5 Dimensjonering og tilpassing av koblingsskap	William	100 %
4.3 Oppsett og konfigurasjon av nettverk	Sjur	100 %

OPPGAVER OG MÅL	ANSVARLIG PERSON(ER)	PROGRESJON
Kapittel 5: Realisering av kombinert kraftverk	Anders	100 %
5.1 Systemoversikt	William	100 %
5.2 Spesifikk komponentoversikt for miniatyrmodellen	William	100 %
5.3 Oppsett av solkraftmodellen	Abdikadir	100 %
5.3.1 Design av solceller	Abdikadir	100 %
5.4 Oppsett og komponentbeskrivelse av vannkraftmodellen	Anders	100 %
5.4.1 Generator – oppsett og virkemåte	Anders	100 %
5.4.2 Pumpe – oppsett og virkemåte	Anders	100 %
5.4.3 Ultralyd nivåmåler – oppsett og virkemåte	Anders	100 %
5.4.4 Nivåvakt – oppsett og virkemåte	Anders	100 %
5.4.5 Reguleringsventil – oppsett og virkemåte	Anders	100 %
5.4.6 Fester i vannsystemet	William	100 %
5.4.7 Tømming, fylling og stenging av vann	William	100 %
5.5 Illustrasjon av strømproduksjon – oppsett og virkemåte	Anders	100 %
5.6 IO-liste	Anders	100 %
5.7 Koblingsskjemaer	Anders	100 %
5.7.1 Koblingsskjema for strømforsyning og switch	Anders	100 %
5.7.2 Koblingsskjema for PLS-kontroll av vannkraft	Anders	100 %
5.7.3 Koblingsskjema for PLS-kontroll av solkraft	Anders	100 %
5.7.4 Koblingsskjema for pumpe og lamper	Anders	100 %
5.7.5 Koblingsskjema for HMI-skjermer	Anders	100 %
5.8 Styringsfilosofi	Anders	100 %
5.8.1 Styring av pumpe	Anders	100 %
5.8.2 Styring av reguleringsventil	Anders	100 %
5.8.3 Styring av lamper	Anders	100 %
5.8.4 Oppstart syklus og utjevning av verdier	Anders	100 %
5.8.5 Brukergrensesnitt i HMI-er	Anders	100 %

OPPGAVER OG MÅL	ANSVARLIG PERSON(ER)	PROGRESJON
Kapittel 6: Nettverksanalyse og angrep	Sjur/Mohamed	100 %
6.1 Nettverksanalyse gjennom switch	Sjur	100 %
6.1.1 Wireshark	Sjur	100 %
6.1.2 Netdiscoover for kartlegging av tilkoblede enheter	Mohamed/Sjur	100 %
6.1.3 Nmap	Mohamed/Sjur	100 %
6.1.4 Snmp-check for henting av detaljert informasjon om PLS og switch	Mohamed/Sjur	100 %
6.1.5 Grassmarlin for visualisering av nettverket	Mohamed	100 %
6.1.6 Proneta for helhetlig oversikt	Sjur	100 %
6.1.7 Oppsummering av nettverksanalyse	Mohamed/Sjur	100 %
6.2 Angrep på modellen	Mohamed/Sjur	100 %
6.3 Nettverksanalyse i etterkant av angrep	Mohamed/Sjur	100 %
6.4 Forutsetninger for gjennomføring av angrep	Sjur	100 %
Kapittel 7: Diskusjon	Sjur/William/Anders/Mohamed	100 %
7.1 Diskusjon for undersøkelse av cyberangrep, konsekvenser og sårbarheter	Sjur	100 %
7.2 Diskusjon av potensielle løsninger	William	100 %
7.3 Diskusjon av vannkraftmodellen	William	100 %
7.3.1 Design av vanntanker	William	100 %
7.3.2 Fester og støtte	William	100 %
7.3.3 Generator og reguleringsventil	Anders	100 %
7.3.4 Ultralyd og pumpe	Anders	100 %
7.4 Diskusjon av solkraftmodellen	William	100 %
7.4.1 Oppset av solceller	William	100 %
7.4.2 Lysforurensning i solcellepanelet	William	100 %
7.4.3 Tilpassing av lyskilde	William	100 %
7.5 Tilpassing og oppsett av koblingsskap	Anders	100 %
7.6 Diskusjon av styresystemet og HMI	Anders	100 %
7.7 Diskusjon av nettverksanalyse og angrep	Mohamed/Sjur	100 %

OPPGAVER OG MÅL	ANSVARLIG PERSON(ER)	PROGRESJON
Kapittel 8: Videre arbeid	Sjur/William/Anders/Mohamed	100 %
8.1 Videre arbeid for undersøkelse av cyberangrep, konsekvenser og sårbarheter	Sjur	100 %
8.2 Videre arbeid i solkraftverket	William	100 %
8.2.1 Oppsett av solceller	William	100 %
8.3 Videre arbeid i vannkraftverket	William	100 %
8.3.1 Skjevheter i vannkraftverket	William	100 %
8.3.2 Manglende installering av frekvensomformer	William	100 %
8.3.2 Magasintanken og vannsprut	William	100 %
8.4 Forbedringer i styresystem og HMI	Anders	100 %
8.4.1 Styresystem og HMI	Anders	100 %
8.5 Forbedringer ved nettverksanalyse og cyberangrep	Mohamed/Sjur	100 %
Konklusjon	Sjur	100 %
Konklusjon	Sjur	100 %

Vedlegg 3: Komplett komponentoversikt

Komponent	Dimensjoner	Beskrivelse	Produsent	Leverandør	Antall	Enhetspris	Rabatt	Totalpris
HMI KTP700	24V	-	Siemens	Proshop	1	10031	-	10031
HMI KTP400	24V	-	Siemens	Proshop	1	5381	-	5381
Switch	24V, 8 porter	-	Siemens	Proshop	1	8324	-	8324
PLS	24V, 1212C DC/DC/DC	-	Siemens	Proshop	2	3890	-	7780
Analog modul	24V, 4Ai, 2AQ	-	Siemens	Proshop	2	5465	-	10930
Strømforsyning	24V, 10A	-	Siemens	Proshop	1	3939	-	3939
Kabinett	-	Koblingsskap	Fibox	Elfadistrelec	1	2051	-	2051
Koblingsskap	-	Gjennomsiktig dør	Fibox	Elfadistrelec	1	2974	-	2974
Kontaktor	24V, 25A 2NO	-	Siemens	Elfadistrelec	4	354,31	-	1417,24
Lisens TIA	-	-	Siemens	Elfadistrelec	1	4077	-	4077
Koblingsskap total	-	-	-	-	-	-	-	**56904,24**
Verktøystavle			AJ-produkter	AJ-produkter	1	9095		**9095**
Nødstoppknapp	-	-	-	Elfadistrelec	1	253	-	253
Rekkeklemmer	-	-	-	Elfadistrelec	30	5,428	-	162,84
Jordingsklemmer	-	-	-	Elfadistrelec	3	63,3	-	189,9
Lasker	-	10-rad	-	Elfadistrelec	2	38,66	-	77,32
RK kabel	100m, 0.75mm	PVC	-	Elfadistrelec	1	354	-	354
Toll	-	Toll/tax	-	Elfadistrelec	-	-	-	412,3
Bakplate	-	-	-	Elfadistrelec	1	323	-	323
LED-lamper skap	-	Grønne	-	Elfadistrelec	3	170	-	510
Rekkeklemmer	-	-	-	Elfadistrelec	10	5,785	-	57,85
LED-lamper skap	-	Røde	-	Elfadistrelec	6	171	-	1026
DIN-skinner	-	-	-	Elfadistrelec	6	22,4	-	134,4
Kabelkanal	-	-	-	Elfadistrelec	5	119	-	595
Endehylser	0.75mm	100stk	-	Elektroimportøren	1	115	-	115
Teip	-	Elektrikerteip	-	Elektroimportøren	1	49	-	49
Rekkeklemme	-	-	-	Elektroimportøren	2	39	-	78
Jordklemme	-	-	-	Elektroimportøren	2	84	-	168
Ethernetkabel	-	Kat6	-	Elektroimportøren	1	119	-	119
Skjøteledning	5m	1-veis jorda	-	Elektroimportøren	2	89,25	-	178,5
Kabelnippel	M12	Med mutter, IP68	-	Elektroimportøren	3	19	-	57
Kabelnippel	M20	Med mutter, IP68	-	Elektroimportøren	2	19	-	38
Krympeslange	1m, 12/3mm	-	-	Elektroimportøren	1	156	-	156
Småting koblings-skap	-	-	-	-		-	-	**5054,11**

Komponent	Dimensjoner	Beskrivelse	Produsent	Leverandør	Antall	Enhetspris	Rabatt	Totalpris
Slangenippel	1/2 x 3/4"	Messing	-	Hydroscand	3	204	30 %	428,4
Slangenippel	1/2 x 3/4"	Messing	-	Hydroscand	4	204	50 %	408
Slangenippel	1/2 x 1/2"	Messing	-	Hydroscand	4	59,5	30 %	166,6
Slangenippel	1/2 x 1/2"	Messing	-	Hydroscand	6	59,5	50 %	178,5
T-kobling	1/2"	Messing	-	Hydroscand	1	176	30 %	123
90 grader kobling	1/2"	Messing	-	Hydroscand	1	130	30 %	91
90 grader kobling	1/2"	Messing	-	Hydroscand	2	130	50 %	130
Muffe	-	Messing	-	Hydroscand	1	89,5	30 %	62,65
MVA	-	-	-	Hydroscand	-	-	-	397,5
Slanger	5m 15mm	PVC	-	Biltema	1	94,9	-	94,9
Slanger	5m 12mm	PVC	-	Biltema	3	59,9	-	179,7
Slangeklemmer	13-16mm	2-pakning	-	Biltema	7	24,9	-	174,3
Gummipakning	3/4"	4-pakning	-	Biltema	3	36,9	-	110,7
Kuleventil	1/2"	Med spak	-	Biltema	1	119	-	119
Gjengeteip	12mm x 10m	PTFE	-	Biltema	1	14,9	-	14,9
Muffe	1/2"	-	-	Biltema	2	39,9	-	79,8
Rørklammer	26-28mm	-	Biltema	Biltema	3	46,9	-	140,7
Rørklammer	21-23mm	-	Biltema	Biltema	5	46,9	-	234,5
Rørklammer	15-19mm	-	Biltema	Biltema	1	44,9	-	44,9
Rørklammer	12-14mm	-	Biltema	Biltema	3	44,9	-	134,7
Kuleventil	1/2"	Stengeventil	Biltema	Biltema	1	99,9	-	99,9
Vanntanker	27L	Antatt 2000kr frakt	Plexon	Plexon	2	-	-	17750
Blomsterkasse	1m	20L	-	Hagelang	1	199	-	199
Pumpe	14L/min	-	Xylem Flojet	RS-online	1	3684	-	3684
Generator	10V	1/2"	Wonofa	Amazon	3	120	-	360
Ultralydsensor	4-20mA	-	Pepperl+Fuchs	Elfadistrelec	1	3487	-	3487
Frekvensomformer	240V	-	Schneider Electric	Elfadistrelec	1	3157	-	3157
Reguleringsventil	2-10V	1/2"	Belimo	Bilemo	1	3059	-	3059
Nivåvakt	NC	24V	Carlo Gavazzi	Elfadistrelec	2	717	-	1434
Kabel-ultralyd	2m	M12	Pepperl+Fuchs	Elfadistrelec	1	176	-	176
Toll	-	-	-	Elfadistrelec	-	-	-	758,31
Vannsystem total	-	-	-	-	-	-	-	**37477,96**

Komponent	Dimensjoner	Beskrivelse	Produsent	Leverandør	Antall	Enhetspris	Rabatt	Totalpris
Solceller	2V per celle	10stk	Xylem Flojet	Amazon	2	160	-	320
Dimmer	-	(Returnert)	Plejd	Elektroimportøren	1	599	-	0
Lyspære	E27	LED	-	Elektroimportøren	1	149	-	149
Spraymaling	400ml	Svart matt	-	Jula	1	79,9	-	79,9
Lampesokkel	E27	-	-	Jula	1	29,9	-	29,9
Lyspære	E27	LED	-	Jula	1	99	-	99,9
Lamper	12V	Med klemmer	-	Clas Ohlson	2	149,9	-	299,8
Solkraft	-	-	-	-	-	-	-	**978,5**
Dempingsbe-skyttelse	-	50stk	-	Biltema	1	32,9	-	32,9
Klebepute	-	Dobbeltsidig teip	-	Biltema	1	29,9	-	29,9
Mutter	M8	100stk	-	Biltema	1	69,9	-	69,9
Vinkelbrakett	-	-	-	Biltema	5	59,9	-	299,5
6-kt skrue/bolt	M8	50pk	-	Wurth	1	314	24 %	238,64
Skjermskive	8,5x30x1,5mm	100pk	-	Wurth	1	282	30 %	197,4
Moms	-	-	-	Wurth	-	-	-	109,01
Skrue	M6	10stk	-	Byggmax	1	59,95	-	59,95
Braketter	-	-	-	Byggmax	4	51,28	-	205,12
Superpoxy	-	-	-	Jula	1	129	-	129
Braketter	12.5x15cm	Hvit	-	Jula	10	14,9	99kr	50
Braketter	7,5x10cm	Hvit, (Returnert)	-	Jula	10	9,9	-	99
Braketter	180x230mm	Svart	-	Jula	8	69,9	-	349,5
Braketter	-	Siden av tanken	-	Jula	8	21,9	-	175,2
Hengeskinne	160cm	-	-	Jula	1	129	-	129
Treplate	90x30x1cm	Furu	-	Jula	1	129	-	129
Rundkrok	-	-	-	AJ-produkter	2	105	-	210
Trådkurv	-	-	-	AJ-produkter	1	150	-	150
Opphengskrok	-	-	-	AJ-produkter	1	93	-	93
Dobbelkrok	-	-	-	AJ-produkter	1	130	-	130
Fjærklemme	-	-	-	AJ-produkter	1	110	-	110
Skruer og festma-teriale	-	-	-	-	-	-	-	**2996,02**
USB	64GB	-	SanDisk	Komplett	2	148,5	-	297
Plastlokk	-	-	-	Biltema	1	29	-	29
Industribygg	-	-	-	Togbutikken	1	695	-	695
Plastlim	-	-	-	Togbutikken	1	75	-	75
Frakt	-	-	-	Togbutikken	-	125	-	125
RasberryPI	-	-	-	Proshop	2	899	-	1798
RasberryPI lader	-	-	-	Proshop	2	149	-	298
RasberryPI deksel	-	-	-	Proshop	2	99	-	198
SD - RasberryPI	-	-	-	Proshop	2	104	-	208
HDMI adapter	-	-	-	Proshop	2	99	-	198
Mus	-	-	-	Proshop	1	89	-	89
CAT6E	-	-	-	Proshop	2	69	-	138
CAT6E	-	-	-	Proshop	2	59	-	118
Skjøteledning	-	-	-	Proshop	2	59	-	118
CAT5E	-	-	-	Proshop	2	67	-	134
Tastatur	-	-	-	Proshop	1	185	-	185
Diverse	-	-	-	-	-	-	-	**4703**
Totalpris	Med forbehold om at enkelte priser kan være feil.							**117453kr**

Vedlegg 4a: Generator PLS

Totally Integrated Automation Portal

Project2eb / Generator PLS [CPU 1212C DC/DC/DC] / Program blocks

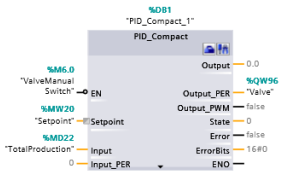
Cyclic interrupt [OB30]

Cyclic interrupt Properties							
General							
Name	Cyclic interrupt	**Number**	30	**Type**	OB	**Language**	FBD
Numbering	Automatic						
Information							
Title		**Author**		**Comment**		**Family**	
Version	0.1	**User-defined ID**					

Cyclic interrupt		
Name	**Data type**	**Default value**
Input		
Initial_Call	Bool	
Event_Count	Int	
Temp		
Constant		

Network 1:

PID-kontroller P=10 I=10 D=0



Totally Integrated Automation Portal		

Main [OB1]

Main Properties							
General							
Name	Main	**Number**	1	**Type**	OB	**Language**	FBD
Numbering	Automatic						
Information							
Title	"Main Program Sweep (Cycle)"	**Author**		**Comment**		**Family**	
Version	0.1	**User-defined ID**					

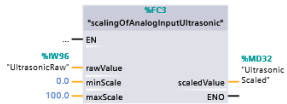
Name	Data type	Default value
Input		
Initial_Call	Bool	
Remanence	Bool	
Temp		
GeneratorEqualized	Real	
SetpointReal	Real	
Difference	Real	
SetpointRangeNegativeValue	Real	
Constant		

Network 1:

Manuell styring av ventil

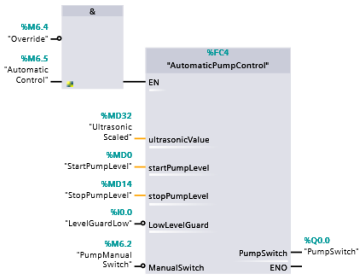
Network 2:

Skalerer input fra ultralyd nivåmåler om til 0-100% (vannstand)



Network 3:

Automatisk styring av pumpe. Foriglet når manuell kjøring er på og når det ikke er nok vann i reservoartank.



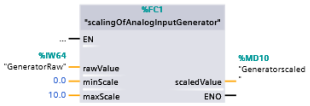
Network 4:

LampR1: Rød lampe høyt nivå vannmagasintank, LampR2: Rød lampe lavt nivå vannreservoartank, LampG1: Grønn lampe pumpe i drift, LampG2: Grønn lampe prosessverdi er innenfor settpunkt

Totally Integrated Automation Portal

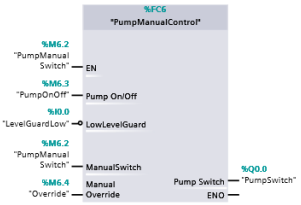
Network 5:

Skalerer input fra generatoren til 0-10V



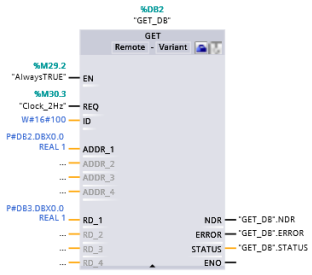
Network 6:

Manuell styring av pumpe. Forriglet når automatisk styring er på og når det lavt nivå i vannresorvartanken



Network 7:

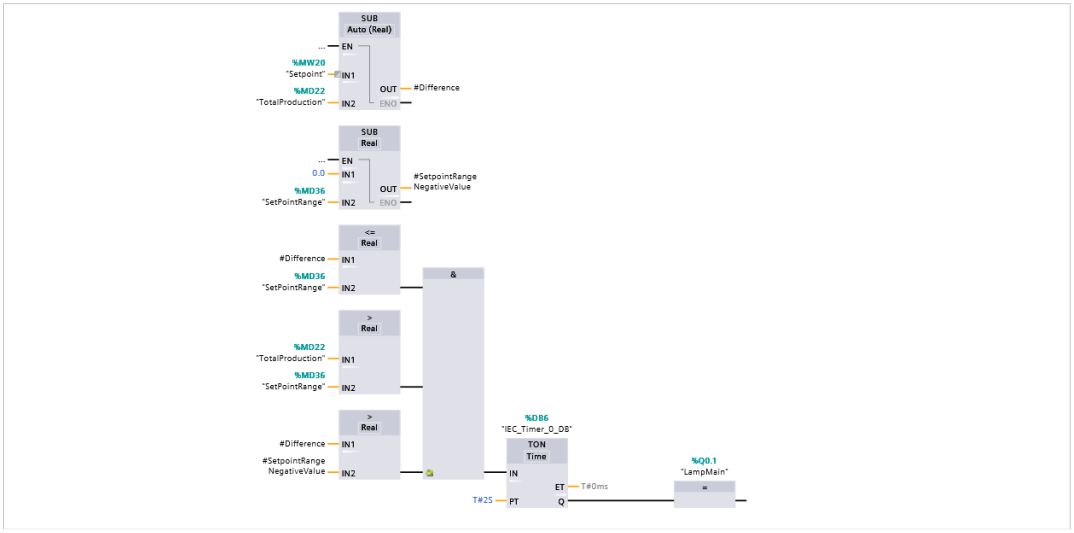
Henter verdi for solcellene fra den andre PLSen



Network 8:

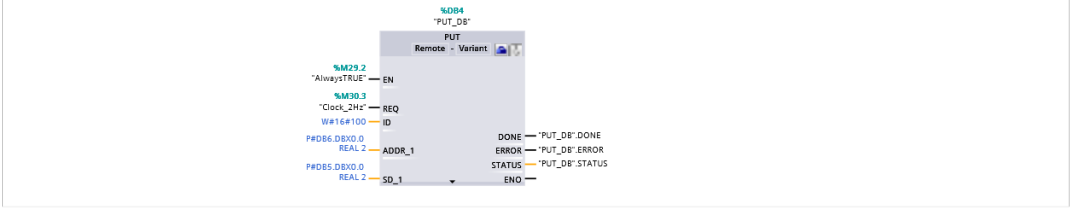
Styring av lampe i industribygg

Totally Integrated Automation Portal



Network 9:

Sender informasjon til den andre PLS, total produksjon og settpunkt blir sendt



Network 10:

Utjevner generator verdien

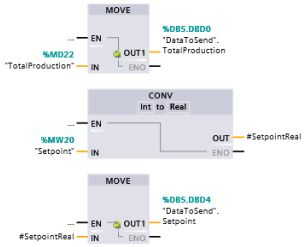
Network 11:

Regner ut spenning generert fra solceller og generator

Network 12:

Sender total produskjon og settpunkt til solcelle PLS

Totally Integrated Automation Portal		



Totally Integrated Automation Portal

Project2eb / Generator PLS [CPU 1212C DC/DC/DC] / Program blocks

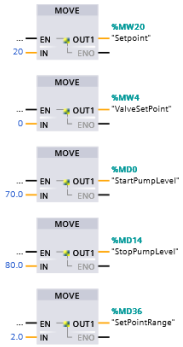
Startup [OB100]

Startup Properties							
General							
Name	Startup	**Number**	100	**Type**	OB	**Language**	FBD
Numbering	Automatic						
Information							
Title	"Complete Restart"	**Author**		**Comment**		**Family**	
Version	0.1	**User-defined ID**					

Startup		
Name	**Data type**	**Default value**
Input		
LostRetentive	Bool	
LostRTC	Bool	
Temp		
Constant		

Network 1:

Startup verdier blir satt



Totally Integrated Automation Portal

Project2eb / Generator PLS [CPU 1212C DC/DC/DC] / Program blocks

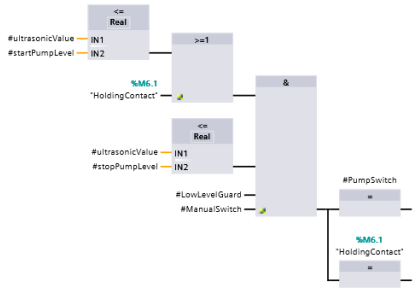
AutomaticPumpControl [FC4]

AutomaticPumpControl Properties							
General							
Name	AutomaticPumpControl	**Number**	4	**Type**	FC	**Language**	FBD
Numbering	Automatic						
Information							
Title		**Author**		**Comment**		**Family**	
Version	0.1	**User-defined ID**					

AutomaticPumpControl		
Name	**Data type**	**Default value**
Input		
ultrasonicValue	Real	
startPumpLevel	Real	
stopPumpLevel	Real	
LowLevelGuard	Bool	
ManualSwitch	Bool	
Output		
PumpSwitch	Bool	
InOut		
Temp		
Constant		
Return		
AutomaticPumpControl	Void	

Network 1:

Automatisk styring av pumpe



Totally Integrated Automation Portal

Project2eb / Generator PLS [CPU 1212C DC/DC/DC] / Program blocks

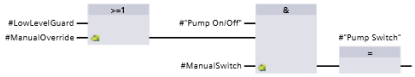
PumpManualControl [FC6]

PumpManualControl Properties							
General							
Name	PumpManualControl	**Number**	6	**Type**	FC	**Language**	FBD
Numbering	Automatic						
Information							
Title		**Author**		**Comment**		**Family**	
Version	0.1	**User-defined ID**					

PumpManualControl		
Name	**Data type**	**Default value**
Input		
Pump On/Off	Bool	
LowLevelGuard	Bool	
ManualSwitch	Bool	
ManualOverride	Bool	
Output		
Pump Switch	Bool	
InOut		
Temp		
Constant		
Return		
PumpManualControl	Void	

Network 1:

Manuell styring av pumpe



Totally Integrated Automation Portal		

Project2eb / Generator PLS [CPU 1212C DC/DC/DC] / Program blocks

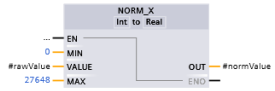
ScalingOfAnalogInputGenerator [FC1]

ScalingOfAnalogInputGenerator Properties							
General							
Name	ScalingOfAnalogInputGener-ator	**Number**	1	**Type**	FC	**Language**	FBD
Numbering	Automatic						
Information							
Title		**Author**		**Comment**		**Family**	
Version	0.1	**User-defined ID**					

scalingOfAnalogInputGenerator		
Name	**Data type**	**Default value**
Input		
rawValue	Int	
minScale	Real	
maxScale	Real	
Output		
scaledValue	Real	
InOut		
Temp		
normValue	Real	
Constant		
Return		
ScalingOfAnalogInputGenerator	Void	

Network 1:

Skalering av signal fra generator til 0-10V



Network 2:

Totally Integrated Automation Portal		

Project2eb / Generator PLS [CPU 1212C DC/DC/DC] / Program blocks

ScalingOfAnalogInputUltrasonic [FC3]

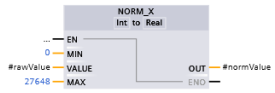
ScalingOfAnalogInputUltrasonic Properties							
General							
Name	ScalingOfAnalogInputUltra-sonic	**Number**	3	**Type**	FC	**Language**	FBD
Numbering	Automatic						
Information							
Title		**Author**		**Comment**		**Family**	
Version	0.1	**User-defined ID**					

scalingOfAnalogInputUltrasonic

Name	Data type	Default value
Input		
rawValue	Int	
minScale	Real	
maxScale	Real	
Output		
scaledValue	Real	
InOut		
Temp		
normValue	Real	
scaledValueToReverse	Real	
Constant		
Return		
ScalingOfAnalogInputUltrasonic	Void	

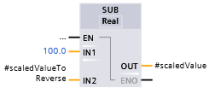
Network 1:

Skalering av input fra ultralyd til 0-100%



Network 2:

Network 3:



Totally Integrated Automation Portal		

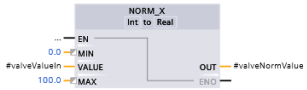
ScalingOfAnalogOutput(2-10V) [FC2]

ScalingOfAnalogOutput(2-10V) Properties							
General							
Name	ScalingOfAnalogOut-put(2-10V)	**Number**	2	**Type**	FC	**Language**	FBD
Numbering	Automatic						
Information							
Title		**Author**		**Comment**		**Family**	
Version	0.1	**User-defined ID**					

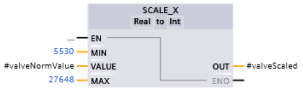
Name	Data type	Default value
Input		
valveValueIn	Int	
Output		
valveScaled	Int	
InOut		
Temp		
valveNormValue	Real	
Constant		
Return		
ScalingOfAnalogOutput(2-10V)	Void	

Network 1:

Skalering av output 2-10V



Network 2:



Vedlegg 4b: PLS Solcelle

Project2eb / Solcelle PLS [CPU 1212C DC/DC/DC] / Program blocks

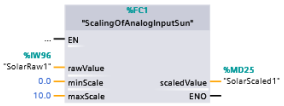
Main [OB1]

Main Properties							
General							
Name	Main	**Number**	1	**Type**	OB	**Language**	FBD
Numbering	Automatic						
Information							
Title	"Main Program Sweep (Cycle)"	**Author**		**Comment**		**Family**	
Version	0.1	**User-defined ID**					

Main		
Name	**Data type**	**Default value**
Input		
Initial_Call	Bool	
Remanence	Bool	
Temp		
SolarScaledCombinedNegative	Real	
SolarReset	Real	
SolarMultiplied	Real	
Constant		

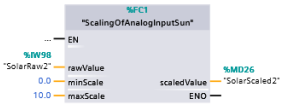
Network 1:

Skalering av solcelle input 1



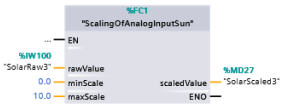
Network 2:

Skalering av solcelle input 2



Network 3:

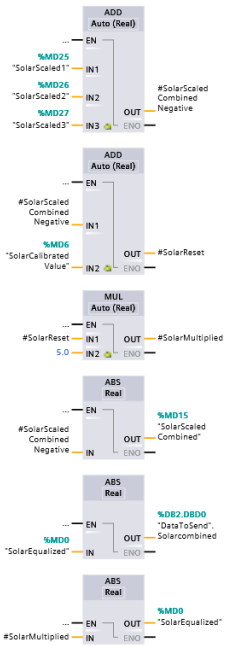
Skalering av solcelle input 3



Network 4:

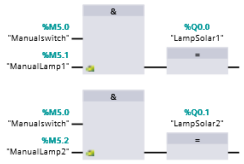
Samling og utjevning av verdier fra solcellene. Verdien blir også sendt til generator PLS

Totally Integrated Automation Portal		



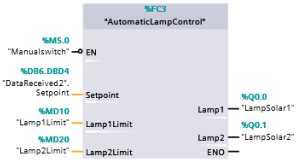
Network 5:

Manuell styring av solcelle lamper



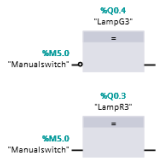
Network 6:

Automatisk styring av solcelle lamper



Network 7:

LampG3: Grønn lampe automatisk styring av solcelle lamper, LampR3: Rød lampe manuell styring av lys



Totally Integrated Automation Portal

Project2eb / Solcelle PLS [CPU 1212C DC/DC/DC] / Program blocks

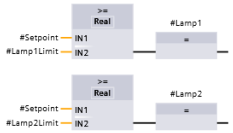
AutomaticLampControl [FC3]

AutomaticLampControl Properties							
General							
Name	AutomaticLampControl	**Number**	3	**Type**	FC	**Language**	FBD
Numbering	Automatic						
Information							
Title		**Author**		**Comment**		**Family**	
Version	0.1	**User-defined ID**					

AutomaticLampControl		
Name	**Data type**	**Default value**
Input		
Setpoint	Real	
Lamp1Limit	Real	
Lamp2Limit	Real	
Output		
Lamp1	Bool	
Lamp2	Bool	
InOut		
Temp		
Constant		
Return		
AutomaticLampControl	Void	

Network 1:

Automatisk styring av solcelle lamper



Totally Integrated Automation Portal		

Project2eb / Solcelle PLS [CPU 1212C DC/DC/DC] / Program blocks

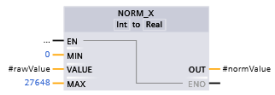
ScalingOfAnalogInputSun [FC1]

ScalingOfAnalogInputSun Properties							
General							
Name	ScalingOfAnalogInputSun	**Number**	1	**Type**	FC	**Language**	FBD
Numbering	Automatic						
Information							
Title		**Author**		**Comment**		**Family**	
Version	0.1	**User-defined ID**					

scalingOfAnalogInputSun		
Name	**Data type**	**Default value**
Input		
rawValue	Int	
minScale	Real	
maxScale	Real	
Output		
scaledValue	Real	
InOut		
Temp		
normValue	Real	
Constant		
Return		
ScalingOfAnalogInputSun	Void	

Network 1:

Skalering av input fra solceller til 0-10v



Network 2:

Totally Integrated Automation Portal

Project2eb / Solcelle PLS [CPU 1212C DC/DC/DC] / Program blocks

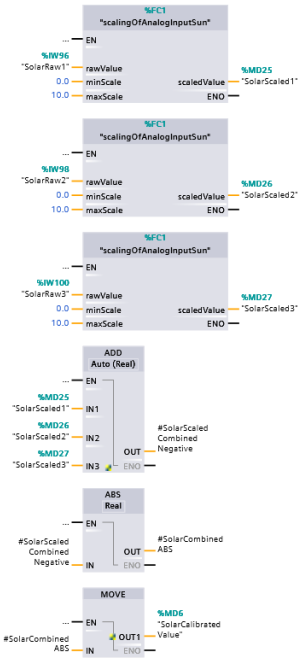
Startup [OB100]

Startup Properties							
General							
Name	Startup	**Number**	100	**Type**	OB	**Language**	FBD
Numbering	Automatic						
Information							
Title	"Complete Restart"	**Author**		**Comment**		**Family**	
Version	0.1	**User-defined ID**					

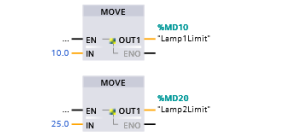
Startup		
Name	**Data type**	**Default value**
Input		
LostRetentive	Bool	
LostRTC	Bool	
Temp		
SolarCombinedABS	Real	
SolarScaledCombinedNegative	Real	
Constant		

Network 1:

Startup verdier blir satt og solceller blir kalibrert fra lysforurensing



Network 2:



Vedlegg 5 – Medforfattererklæring:

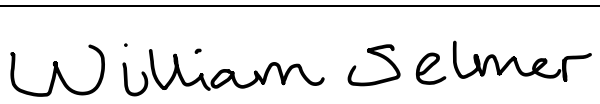
Medforfattererklæring - bacheloroppgave

Dette skjemaet skal fylles ut og signeres av alle studentene i prosjektgruppen. Ferdig utfylt og signert skjema skal ligge som et vedlegg i rapporten.

Tittel på oppgaven	Utvikling av konseptmodell for simulering av cyberangrep
Veileder fra USN	Hans-Petter Halvorsen

Beskriv hva hver student i prosjektgruppen har bidratt med i bacheloroppgaven. *Eksempelvis i forhold til problemformulering, litteratursøk, planlegging av forsøk/valg av metoder, datainnsamling/bygging av prototype, analyse/tolking av data/uttesting, skriving osv.* *Husk at alle studentene er ansvarlige for helheten av den innleverte oppgaven.*
Abdikadir Aden har bidratt med: - Skrive rapport. - Analyse av cyberangrep. - Festing av utstyr. - Finpussing av rapporten. - Beregne strømproduksjon til komponentene i modellen. - Designe deler av komponenter i modellen.
William Selmer har bidratt med: - Valg og innkjøp av mindre komponenter for modellen. - Komponentlister og kostnadsberegning. - Strukturering, layout, innhold og finpussing av rapport. - Dimensjonering, skissering, tilpassing og planlegging før og under montering. - Oppsett av vannsystemet og andre komponenter. - Møteleder og kommunikasjon med oppdragsgiver.
Anders Pedersen Skogli har bidratt med: - Valg av komponenter for modellen. - Ideutvikling av løsningsforslag. - Testing av komponenter for modellen. - Tegning av koblingsskjemaer og kobling av modellen. - Programmering av PLS og designing av styresystemet. - Programmering og design av HMI-grensesnitt.

- Skriving av rapport. - Møtereferent.
Mohamed Ismail har bidratt med: - Innkjøp av mindre komponenter sammen med William. - Skriving av rapport. - Gjennomføring av nettverksanalyse og cyberangrep. - Finpussing av rapporten. - Deltagelse under designdelen.
Sjur Aanesen har bidratt med: - Ideutvikling av løsningsforslag. - Valg av komponenter for modellen. - Tilpassing og skissering av koblingsskap og solcelleoppsett. - Bygging av modell. - Gjennomføring av nettverksanalyse og cyberangrep. - Skriving av rapport.

Dato	**Signatur**
20.05.2024	
20.05.2024	
20.05.2024	
20.05.2024	
20.05.2024