Auto Cloud

5/23/2019

Digitalisering & Visualisering av Steinknuseranlegg

Bacheloroppgave 2019

Muhammet Pamuk

Homan Mousavi

Lilly Nguyen

Sunniva Melkild

OsloMet – Storbyuniversitet

Pilestredet P35, 0166 Oslo

ELTS3900

OSLOMET

SIEMENS

Ingenuity for life

Forord

Denne rapporten er skrevet på grunnlag av bacheloroppgaven våren 2019 for studieretningen ingeniørfag – Elektronikk og informasjonsteknologi. Vi er fire studenter ved OsloMet som gjennom denne oppgaven har vist at vi kan løse en ingeniørfaglig problemstilling gjennom våre faglige kunnskaper, teknologiske ferdigheter og vår nysgjerrighet. Vi fikk en oppgave av Siemens AS som hadde fokus på temaene Cloud Technology, Cyber Security og Asset Optimization Service.

Vi har arbeidet med oppgaven hele semesteret, og vi har lagt mange timer bak oss både når det gjelder skriving og i forhold til ulike praktiske oppgaver. Motivasjonen har alltid vært høy, vi har lært veldig mye nytt og fått gode erfaringer som automasjonsingeniører.

For å kunne gjennomføre denne oppgaven har vi vært avhengige av en rekke ressurspersoner. Vi ønsker å gi en stor takk til Kåre Ettestad som var vår veileder og kontaktperson fra Siemens gjennom hele prosjektet. Andre hjelpsomme ressurser i Siemens har vært Service Sale Specialist Kristian Andreas Kannelønning som bidro med sin kunnskap vedrørende Cyber Security. Automasjonsingeniør Marita Tangedal har vært hjelpsom i forhold til utfordringer knyttet til PLS-anlegget og AOS-rapporten. Serviceingeniør Tom Vegard Jacobsen har hjulpet til med oppsett av MindSphere. Ved OsloMet vil vi rette en stor takk til assisterende professor Knut Harald Nygaard for gode råd og veiledning av denne oppgaven. Vi følte oss alltid velkomne til å ta en prat på hans kontor.

Vi ønsker til slutt å takke hjelpsomme familiemedlemmer for korrekturlesing og innspill. Vi ønsker også å takke alle andre som har bidratt til dette prosjektet direkte og indirekte. Takk og god lesing!

Prosjektbeskrivelse

Prosjektet som er delegert av Siemens handler om å videreutvikle et steinknuseranlegg som er utviklet av forrige årets bachelorgruppe. Oppgaven er delt i tre ulike temaer; Cyber Security, Cloud Technology og AOS (Asset Optimization Service). I tillegg til disse tre temaene er det noe hardware endringer som Siemens har ønsket fra oss, blant annet idriftsettelse av drive via internett (G120 Wifi Smart Access).

Cloud Technology: Det skal velges ut kritiske og viktige datapunkter, også kalt KPI, fra modellen. Disse datapunktene skal sendes til Siemens sitt Cloud Technology programvare; MindSphere. I MindSphere skal disse datapunktene bli analysert og visualisert gjennom å utvikle et dashbord ved hjelp av Simatic Performance Insight.

Cyber Security: Denne delen har både en teoretisk og en praktisk del. I denne delen av oppgaven skal modellen analyseres og det skal utvikles en konkret prosedyre for hvordan modellen kan møte de krav som er stilt i IEC62443-serien – det vil si en konkret prosedyre som definerer implementering av sikre industriautomatiserings- og kontrollsystemer. Deretter skal disse sikkerhetselementene bli implementert i systemet.

Asset Optimization Service: Til sist skal det utvikles en AOS-rapport. I denne delen av oppgaven skal det lages en rapport av Siemens sine komponenter i modellen for å analysere og dokumentere leveringsrisikoen og livssyklusen til komponentene.

Hardware: Det ønskes også å teste ut bruk av G120 Wifi Smart Access som er et web-basert modul og ingeniørverktøy for styring av motorer via drives. Siemens ønsker å få en framstilling på hvordan dette fungerer i praksis.

Sammendrag

Implementering av skytjenester i industrien er en ny teknologi som er under utvikling. Mange bedrifter har fortsatt ikke tatt denne teknologien i bruk. Det er derfor stort potensiale innenfor skyteknologi. Siemens skytjeneste, MindSphere, er et nytt program, der vår bachelorgruppe antageligvis er den første til å ta i bruk programmet i Siemens Norge. De viktigste resultatene vi har oppnådd gjennom arbeidet med MindSphere er muligheten til en kontinuerlig datastrøm og overvåking av spesifikt utvalgte KPI-er i anlegget. Denne dataen kan man få tilgang til fra PC, mobil eller nettbrett. Uansett hvor man er kan brukeren altså sjekke tilstanden til anlegget og agere dersom feil eller nedetid oppstår. Simatic Performance Insight gjør det også mulig å implementere alarmer slik at brukeren kan få et varsel dersom noe er galt i anlegget.

Med den økende utviklingen innenfor bruk av skytjenester følger det også med en økt sikkerhetsrisiko. Sjansene for dataangrep blir større, og konsekvensene kan være enorme. Angrepet på IT-systemet i Hydro i 2019 er nok et eksempel på konsekvensen av et innbrudd, der estimerte kostnader er på 450 millioner kroner. [29]

Vi har jobbet med å implementere Cyber Security i henhold til IEC62443 på anlegget for å redusere risikoen for innbrudd. Her har vi fokusert på den fysiske sikkerheten rundt anlegget. Det har blitt gjennomført en risikoanalyse, og blant sikkerhetstiltakene er det bestemt at RJ45 plugger skal implementeres i anlegget for å gjøre det vanskeligere for uvedkommende å få tilgang. I tillegg krever standarden at kontrollrommet kun er tilgjengelig med korttilgang. Vi har derfor implementert RFID-kortleser. Man trenger med andre ord et unikt fysisk nøkkelkort for å kunne logge seg inn på HMI-en. Alle innlogginger logges slik at anleggseier til enhver tid har full oversikt over de som er og har logget seg inn på styringssystemet i kontrollrommet. Kontrollrommet er inngjerdet og har i tillegg kameraovervåking. Disse tiltakene skal sikre innbrudd i anlegget.

For å få en oversikt over tilgjengeligheten til kritiske komponenter i anlegget, har vi utført en AOS-analyse av anlegget. AOS genereres ved bruk av et internt program i Siemens. Dette er et nytt program som enda ikke er tatt særlig i bruk i Siemens. Fordelen med AOS er at programmet forhindrer unødvendig nedetid i tilfelle man trenger å erstatte en eller flere

komponenter i anlegget. AOS sørger for at disse kritiske komponentene er på lager hos kunden. Dermed unngår kunden unødvendig nedetid og påfølgende økonomiske tap.

Innholdsfortegnelse

1 Figuroversikt

2 Tabelloversikt

3 Akronymer og forkortelser

AOS	Asset Optimization Services
SPI	Simatic Performence Insight
CS	Cyber Security
KPI	Key Performance Indicator «Viktige nøkkeltall»
IEC	International Electrotechnical Consule
MLFB	Machine-Readable Product Designation
Cyber Security	Sikkerhet i anlegget (IEC62443 standard)
Cloud Technology	Skytjenester – datalagring i MindSphere
MindSphere	Siemens sitt skyplattform
Asset Optimization Service	Metode for analysering av Siemens komponenter i anlegget
I/O	Inngang og utgang (Input/Output)
QA	Quality Assurance – Kvalitetssikringssystem
G120	Frekvensomformer
IEC62443-serien	En standard som definerer implementering av sikre industriautomatiserings- og kontrollsystemer.
IoT	Internet Of Things
G120 Smart WiFi Access	Tilgang til frekvensomformer via WiFi
RFID	Radiofrekvensidentifikasjon
NS5814	Standard for risiko
Asset Manager	Applikasjon i MindSphere for å konfigurere KPI

FM	Fleet Manager – visualiseringsapplikasjon
Visual Flow Creator	Applikasjon i MindSphere for programmering i NodeRed
IP-adresse	Unik identifikator
Subnet	Oppdeling av IP-adresse
TIA Portal	Siemens Software for programmering av PLS
ID	Identifikasjon
WinCC Runtime	Siemens Software for HMI
UID	Unik identifikasjon

4 Innledning og motivasjon

I denne rapporten vil vi presentere vår bacheloroppgave om digitalisering. Oppgaven ble tildelt av industriavdelingen i Siemens AS. Siemens har utfordret oss med tema som er både innovativt for dem og deres kunder. Denne utfordringen baserer seg på tre temaer; Cloud Technology (MindSphere), Cyber Security og AOS.

Redusering av nedetid, øke produksjon og bruk av eiendeler mer effektivt, er nøkkelfaktorer for at et firma skal vokse [1]. MindSphere er løsningen for å oppnå disse nøkkelfaktorene. Vår oppgave og problemstilling er derfor hvordan denne teknologien kan implementeres og selges til Siemens sine kunder. Dette ønskes realisert ved bruk av en helt ny applikasjon i MindSphere; Simatic Performence Insight.

Cyber Security er noe de fleste bedrifter per dags dato ikke har fokus på. Dette har sin bakgrunn i både økonomiske forhold og fordi de fleste bedrifter mener at det ikke er nødvendig. I juni 2017 ble Ukraina angrepet av et datavirus som hadde innvirkning på flere business-firmaer med tilknytning til Ukraina. Firmaer som Reckitt Benckiser, TNT og Maersk ble påvirket av viruset og dette kostet dem over 1.2 milliarder dollar [2]. Siemens ønsker derfor en forenklet og metodisk fremstilling av hvordan et anlegg kan beskyttes mot angrep fra utenforstående - det vil si i henhold til IEC62443.

Det er et kjent problem at nedetid kan forårsake tap av inntekt. Nedetid kan oppstå av flere grunner, men en av årsakene er nettopp det at elektriske komponenter ikke vil fungere til evig tid, de vil måtte bli erstattet. Dette kan ha en stor innvirkning på inntekt dersom kritiske komponenter slutter å fungere. Siemens ønsker at leveringsrisikoen og livssyklusen på deres produkter i modellen blir analysert og dokumentert, dette ønskes realisert ved bruk av AOS.

Med utgangspunkt i dette har vi valgt å fokusere på følgende problemstillinger:

- Hvordan kan en forenklet og metodisk fremstilling av et anlegg beskytte mot angrep fra utenforstående, både fysisk og over nettet? Det vil si i henhold til IEC62443.
- Hvordan kan man unngå driftsstans og unødvendig dødtid dersom det oppstår problemer med kritiske komponenter?

- Hvordan kan teknologien rundt MindSphere brukes for å sikre at anlegget til kunden er kontinuerlig overvåket og i drift? Hva er styrker og svakheter ved bruk av MindSphere?

Vi har valgt en arbeidsprosess der vi tilnærmer oss oppgaven fra kundens ståsted, og videre frem til leverandørens leveranse. Vi har da valgt å utføre en risikoanalyse av anlegget i forhold til CS sett fra kundes ståsted og registrert MLFB-nummer over installerte Siemens komponenter. Vi har designet ønsket dashbord med tilhørende KPI. Dette blir beskrevet mer detaljert i dokumentet kravspesifikasjon [04.001 – Kundens kravspesifikasjon].

Rapporten beskriver vår prosess vedrørende utfordringene Siemens har gitt oss. Vår arbeidsprosess vil bli beskrevet mer detaljert i eget hovedkapittel i rapporten. Deretter vil vi gi en utdypende forklaring på valgte problemstillinger.

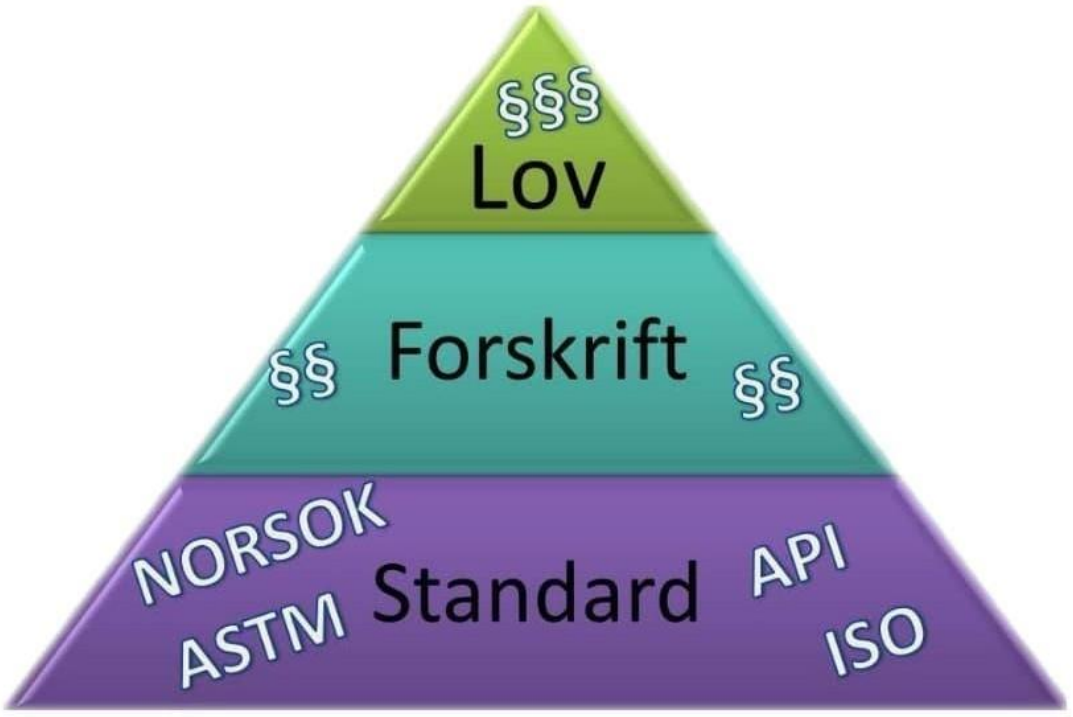
For oversiktens skyld, begrunner vi de ulike avgrensningene som er gjort for hvert enkelt tema nedenfor:

- **MindSphere:** Avgrensningene vi har gjort i forhold til MindSphere er å ha maksimum femten KPI. Dette fordi vi både har et forenklet anlegg og for at vi lett kunne ha tatt for oss altfor mye arbeid.
- **Cyber Security:** Vi har valgt å avgrense oppgaven til å gjelde den fysiske sikkerheten rundt anlegget, ettersom programmet vi bruker for overføring av data er kryptert og regnes som sikkert.
- **Asset Optimization Service:** Avgrensningene vi har under AOS er at vi ikke har mange Siemens utstyr i anlegget og dermed ikke får generert en stor rapport. I tillegg har vi ikke fått tilgang til programmet som brukes for å generere AOS rapport og dermed har vi bare første utgave av AOS-rapporten. Vi har heller ikke noe lager hvor vi har reserve komponenter, dette vil derfor ikke være med i rapporten.

5 Arbeidsprosessen

Som nevnt i innledningen, har vi valgt en arbeidsprosess der vi tilnærmer oss oppgaven fra kundens ståsted, og videre frem til leverandørens leveranse. Siden vi har tre ulike temaer, startet vi med å se på hvert tema for seg selv. For CS ble standarder og normer studert. Dette ble gjort for å få en oversikt over de gjeldende normer slik at anlegget vi jobber med ble sikret innenfor regelverket; IEC62443. Videre fokuserte vi på MindSphere, men siden det er helt nytt, fantes det ikke noen dokumenter å støtte seg på. Derfor valgte vi å studere de dokumentene som ble gitt av Siemens AS, og de dokumentene som er på nettsiden deres i temaet MindSphere. I tillegg presenterte Siemens AS de ulike temaene for oss under et bedriftsbesøk. Underkapitlene i dette kapittelet skal synliggjøre det vi har gjort for å fullføre prosjektet for Siemens AS.

5.1 Rammevilkår og regler



Figur 1 – Oversikt over rammevilkår og regler [3]

For å løse de teknologiske utfordringene, ble det opprettet standarder hvor målet var å redusere gjennomføringstiden og kostnadene for prosjektering og idriftsettelse [3]. Internasjonale elektrotekniske standarder (IEC) er opprettet med målsetting om å definere standarder som kan brukes innenfor elektrotekniske prosjekter. Det finnes også andre standarder som NORSOK, ISO osv.

IEC62443-serien er standarden som er brukt i dette prosjektet i tilknytning til CS. Denne serien inneholder standarder og tekniske rapporter som definerer prosedyrer for implementering av sikre industriautomatiserings- og kontrollsystemer [4].

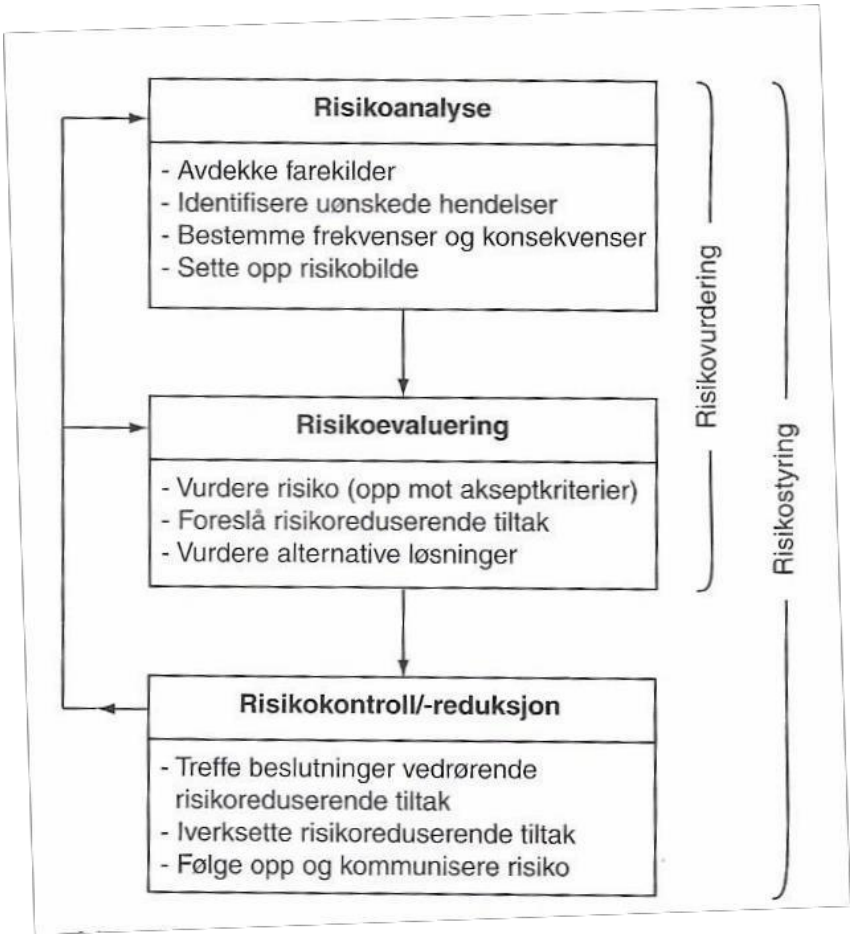
IEC62443-serien har flere underkategorier, blant disse finner vi IEC62443-3-3 og IEC62443-2-1. Disse har forskjellige fokus, og definisjonen er følgende:

- IEC62443-2-1: Denne standarden fokuserer på hvordan man kan implementere et nettverkssikret system, og hvilken metode som brukes for å sikre det fysiske systemet og nettverket.
- IEC62443-3-3: Denne standarden brukes for å evaluere hvilket sikkerhetssystem og sikkerhetsnivå som ligger til grunn for anlegget.

Definisjonen på disse er hentet fra håndbok for Cyber Security. Se håndbok for referanser til kilder.

5.2 Risikovurdering av anlegget

I NS5814 standarden gis risiko følgende forklaring: «Uttrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse.» [5]



Figur 2 – Oversikt over utførelse av risikoanalyse. [5]

5.2.1 Risikoanalyse

Det første vi gjorde for å utarbeide en risikoanalyse var å designe kontrollrommet hvor anlegget ble styrt i fra. Det ble også utarbeidet en prosedyre på hvordan man utfører en sikkerhetsanalyse og hvorledes man finner tiltak mot eventuelle sikkerhetsbrudd. Design av kontrollrommet og prosedyren finnes under vedleggene med navn [04.002 – Design av kontrollrom] og [06.000 – Cyber Security IEC62443]. Dette ble gjort for å kunne evaluere mulige farekilder rundt tilgangen til kontrollrommet, samt at det ble lettere å følge en konkret prosedyre med fastsatte grenser for å analysere sikkerheten rundt anlegget. Sammen med

tegningen av kontrollrommet og prosedyren for å utføre CS, la dette grunnlaget for å identifisere de farer som kan utgjøre en risiko for steinknuseranlegget. (Kilde som ble brukt for risikoanalyse: [18])

Da vi skulle identifisere de farer som kan utgjøre en risiko for anlegget, valgte vi å se på det fra flere perspektiver. Det vil si at vi valgte å se på både den fysiske tilgangen til kontrollrommet og de menneskelige og organisatoriske faktorene. Farekildene ble avdekket og uønskede hendelser ble identifisert, samt at konsekvensene og sannsynligheten for de ulike uønskede hendelsene ble fastsatt. Dette gav oss et grunnlag for å evaluere og vurdere en detaljert risikoevaluering og risikoreduksjon av steinknuseranlegget.

5.2.2 Risikovurdering

Etter å ha avdekket alle farekilder og uønskede hendelser ble det utført en risikovurdering. Ved å identifisere uønskede hendelser, bestemme frekvenser og konsekvenser fikk vi et grunnlag for å utarbeide risikomatrisen. Dette gjøres ved å tallfeste risikoen ut ifra de frekvenser og konsekvenser som er bestemt. Vi vil redegjøre nærmere for dette i hovedkapittelet for CS - der vil vi ta for oss risikovurderingen på detaljnivå. (Kilde som ble brukt for risikovurdering: [19])

5.2.3 Risikoreduksjon

Når man utfører risikovurdering, identifiserer man uønskede hendelser som har høy risiko. Disse risikoene kan reduseres ved å implementere beskyttelsestiltak. Vi analyserte først de eksisterende beskyttelsestiltakene, og ut ifra risikovurderingen vurderte vi å utvide beskyttelsestiltakene for å kunne redusere de farekildene som ble identifisert i risikovurderingen. De ulike tiltakene vi har implementert i systemet blir beskrevet nærmere i hovedkapittelet om CS. (Kilde som ble brukt for risikoreduksjon: [20])

5.3 Instrumenter og MLFB-registrering

For å få en oversikt over Siemens utstyr som er brukt i anlegget, måtte vi registrere MLFB-numrene til alt av Siemens sitt utstyr. Dette utføres enten av kunde eller leverandør.

Vi kartla all utstyret fra Siemens som er brukt i anlegget og registrerte tilhørende MLFB nummer på utstyret i et dokument. Dette dokumentet finnes under vedlegg med navn [04.007 – Utstyrsliste modell].

Deretter ble MLFB numrene registrert i et Excel-ark, og et internt program hos Siemens genererte en rapport om leveringsrisikoen og livssyklusen til Siemens utstyret ute i anlegget. Denne rapporten finnes under vedlegg med navn [04.003 – AOS].

5.4 KPI

I boken Key Performance Indicators defineres KPI på følgende måte – vår oversettelse: "Kritiske suksessfaktorer (KPI) representerer et sett med tiltak som fokuserer på de aspektene av organisatorisk ytelse som er mest kritiske for den nåværende og fremtidige suksessen til organisasjonen" [6].

For å kunne lage dashbord og visualisere anlegget, måtte vi finne ut hvilke kritiske datapunkter (KPI) som kunden ønsket å visualisere. Vi utarbeidet derfor et dokument som illustrerer kundens behov og ønsker. KPI'ene ble valgt ved at vi satte oss i kundens ståsted og analyserte de behov og ønsker en anleggseier kan ha. Dokumentet for KPI er integrert i vedlegget [04.000 – Kundens kravspesifikasjon].

5.5 Kundens kravspesifikasjon

Kravspesifikasjon er en viktig faktor når en bestilling blir sendt til leverandøren. I kravspesifikasjonen spesifiserer man hva man som kunde ønsker av leverandør. Dokumentet bør inneholde all informasjon om hva oppdragsgiver ønsker å anskaffe, hvordan ønsket produkt skal se ut og hvilke funksjoner produktet skal oppfylle. Et slikt dokument har vi utarbeidet [04.000 – Kundens kravspesifikasjon].

I dokumentet vi utarbeidet finner man generell informasjon om anlegget, arbeidet som skal utføres og ansvarsområder.

5.6 Leverandørens designspesifikasjon

Leverandørens designspesifikasjon er svaret leverandøren gir til kundens kravspesifikasjon. Dette dokumentet blir utarbeidet av leverandøren, i vårt tilfelle er dette AutoCloud. Dokumentet skal inneholde hva kunden ønsker, risikovurdering, samt hvilke andre krav kunden har til anleggets funksjonalitet.

Dette dokumentet finnes under vedlegget med navn [04.001 – Leverandørens designspesifikasjon]. Dokumentet skal inneholde mulige løsninger for de krav som er satt og

hvordan vi som leverandør har tolket kundens bestilling. Dette gjøres for å unngå misforståelser og konflikter.

Dokumentet vi har utarbeidet inneholder omfanget av prosjektet, en kort beskrivelse av løsning, og en beskrivelse av det ansvaret som leverandøren innehar. Siden vi i hovedkapitlene har laget en detaljert løsning på de krav som er satt av kunden, valgte vi å skrive en kort versjon av designspesifikasjonen slik at innholdet i rapporten ikke blir gjentatt.

5.7 Kvalitetskontroll

Kvalitetssikringsprosessen (QA) deles i følgende tre stadier:

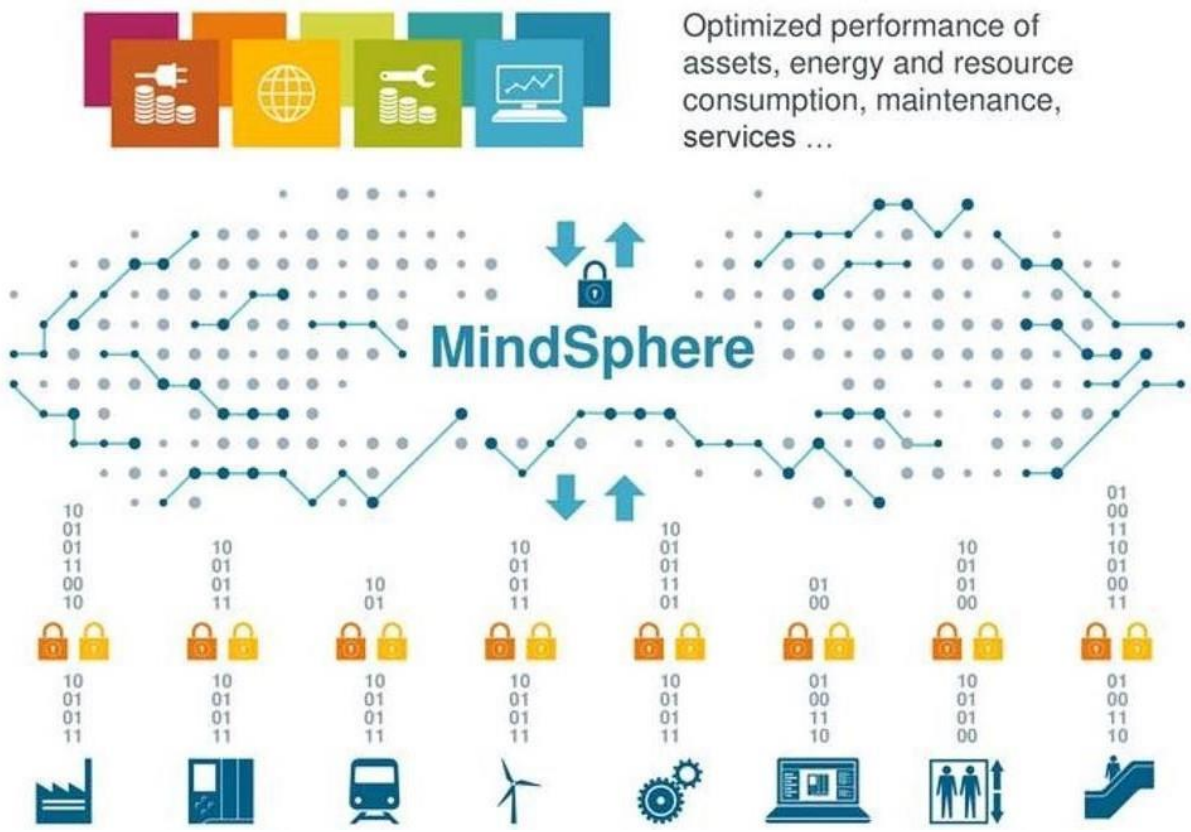
- Kvalitetsplanlegging
- Kvalitetsstyring
- Kvalitetsforbedring

Kvalitetsplanlegging: Kvalitetsplanlegging er det man gjør før man eventuelt starter med et prosjekt. Dette gjøres for å unngå avvik. Man planlegger aktiviteten og beskriver hvordan alt skal utføres i et og samme dokument [04.001 – Leverandørens designspesifikasjon] [7].
Kvalitetsstyring: Kvalitetsstyring er det man gjør under og etter produksjonen for å sjekke at kvaliteten er oppnådd. Ved eventuelle avvik kan man korrigere/reparere [7]. Dette blir gjort ved enten å skrive rapport eller enkle sjekklister. Vi har derfor utarbeidet en enkel sjekkliste [04.004 – QA-sjekkliste] for å kvalitetssikre arbeidet vi har gjort.
Kvalitetsforbedring: Etter prosjektet ser man tilbake på hva som har blitt gjort og avvikene som har forekommet, slik at man kan foreta forbedringer ved neste prosjekt. Avvikene blir dokumentert i en avviksrapport og det tas videre stilling til om avvikene kan korrigeres [7]. Vi har utarbeidet et dokument der vi kan registrere avvik som har oppstått under prosjektet. Dokumentet finnes under vedlegg med navn [04.005 – Avviksrapport].

6 MindSphere

6.1 Generelt om MindSphere

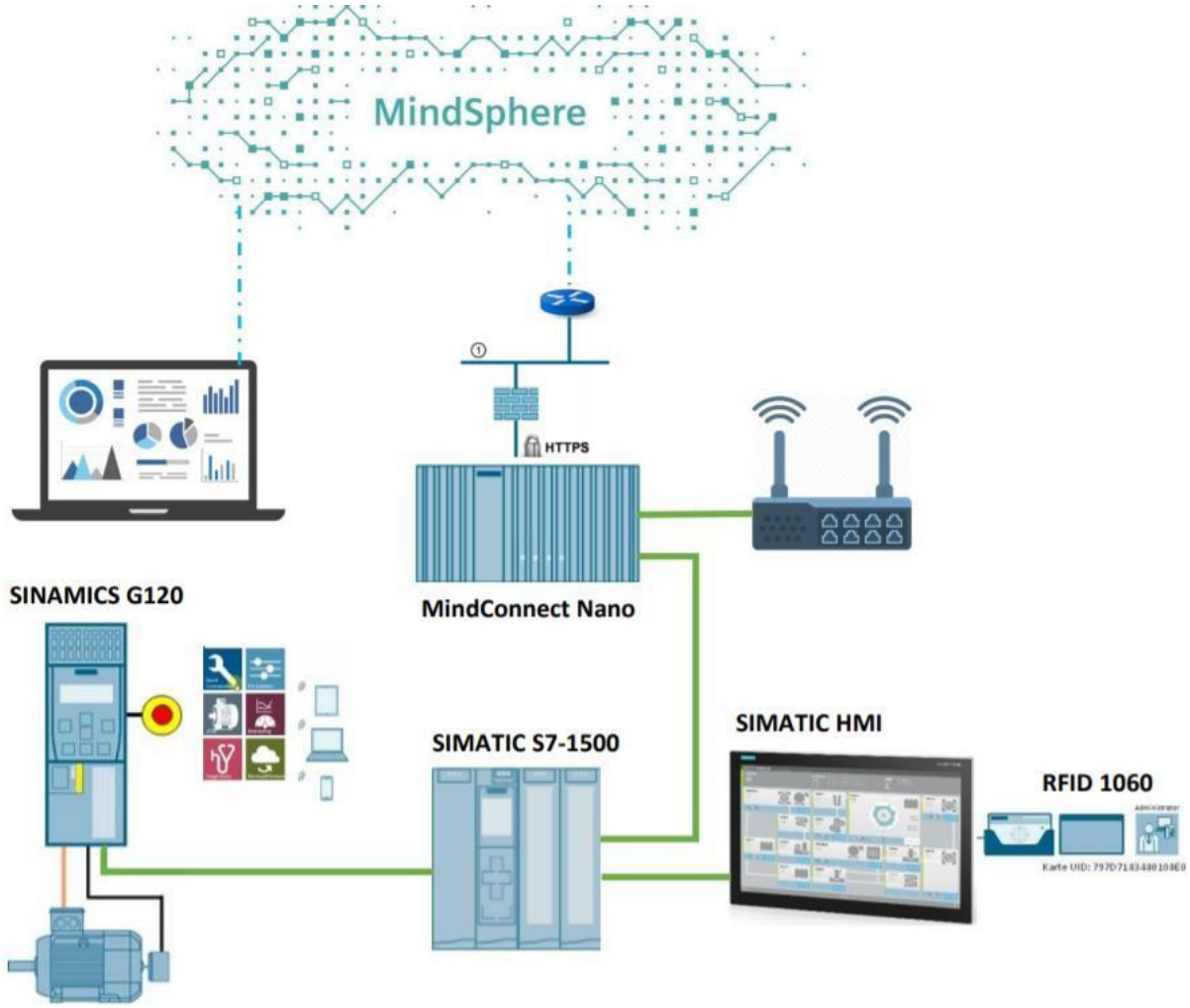
MindSphere er en skyplattform som er et åpent operativsystem som forbinder produkter, systemer og maskiner, slik at det kan utnyttes av data som skapes av Internet Of Things (IoT) gjennom en avansert analyse. MindSphere er Siemens rammeverk for industrielle skytjenester som gjør det mulig å koble til enheter og eiendeler fra en sikkert lagret operasjonsdata som er overført fra industrielle eiendeler til MindSphere. I utgangspunktet er dette en IOT-plattform hvor stor mengde av data kommer fra millioner av enheter som ventiler og sensorer, og MindSphere sørger for at dataene blir tilgjengelige og kan benyttes på PCer, mobiler og nettbrett. Dataene prosesseres, og konverteres til forståelig informasjon som hjelper industrien til å oppnå bedre resultater ved hjelp av digitalisering- og visualiseringsverktøy. MindSphere bidrar også til å sikre sikkerhet og pålitelighet gjennom forutgående vedlikehold.



Figur 3: Figuren viser hvordan data sendes opp til skyplattformen og appene man kan bruke i MindSphere. [9]

6.2 Hardware - Topologi

Vi har utarbeidet et topologiskjema som viser koblingen mellom ruter, MindConnect Nano og kontrollsystemet.



Figur 4: Topologiskisse av koblingen mellom PLS-anlegget og MindSphere ved bruk av MindConnect-Nano.

6.2.1 MindConnect Nano

MindConnect Nano-boksen er en boks som håndterer en jevn strøm av data som den overfører til MindSphere-plattformen. Denne boksen er bindeleddet mellom MindSphere og anlegget.

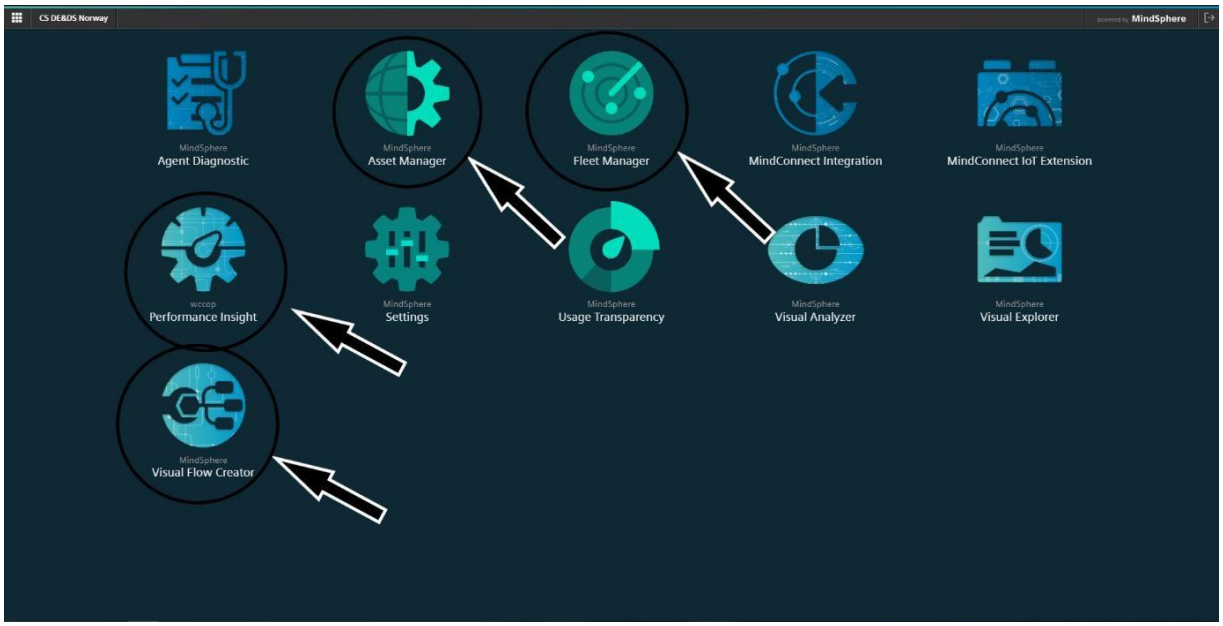
Figur 5: Figuren viser MindConnect Nano boksen fra forskjellige vinkler [15]

Boksen blir koblet til en ruter ved hjelp av en Ethernet-kabel og en Ethernet-kabel til PLS-systemet. Denne blir konfigurert i MindSphere-plattformen, og en filtype blir installert ved hjelp av en minnebrikke (USB) som formateres før bruk slik at annen data ikke blir installert i MindConnect Nano-boksen. Konfigurasjonen blir beskrevet mer detaljert i de neste kapitlene.

6.3 MindSphere-plattformen

For å kunne sende data opp til skyplattformen må det konfigureres slik at MindConnect Nano-boksen gjenkjenner PLS-systemet som sender disse dataene. Dette gjøres i MindSphere plattformen som nevnt tidligere.

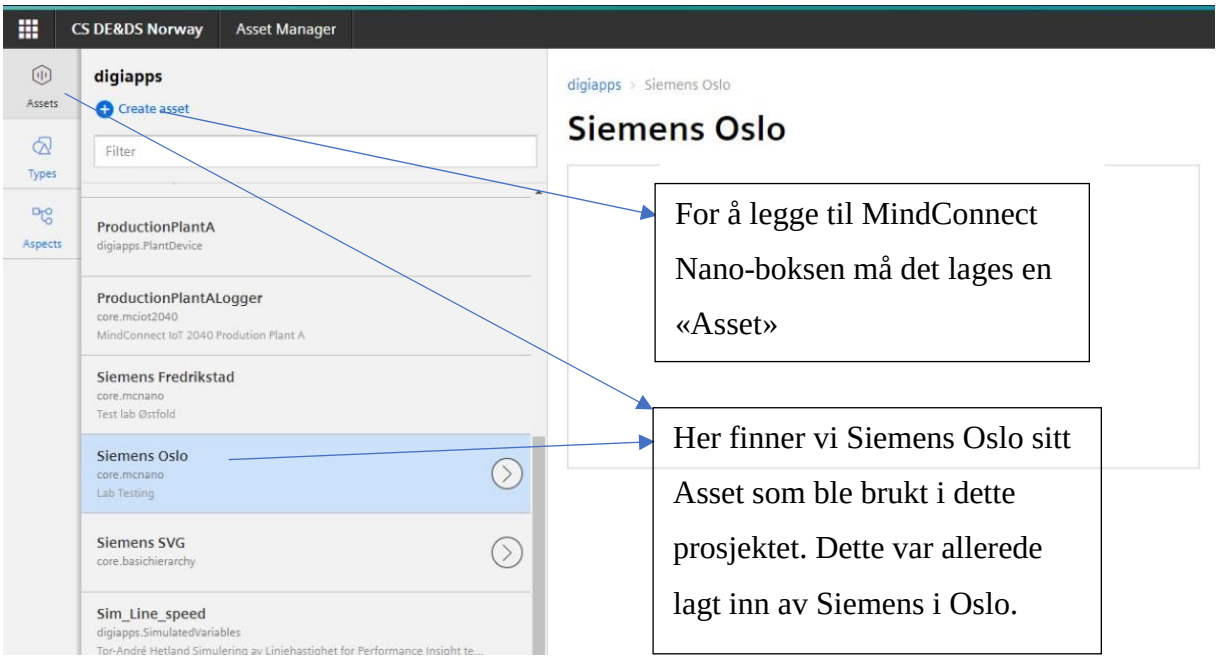
MindSphere-plattformen har et enkelt brukergrensesnitt. Det er flere applikasjoner som har ulike funksjoner. Vi valgte å bruke fire av disse. Disse er «Asset Manager», «Fleet Manager», «Performance Insight» og «Visual Flow Creator».



Figur 6: Figuren viser de ulike applikasjonene som er blitt brukt under prosjektet i MindSphere.

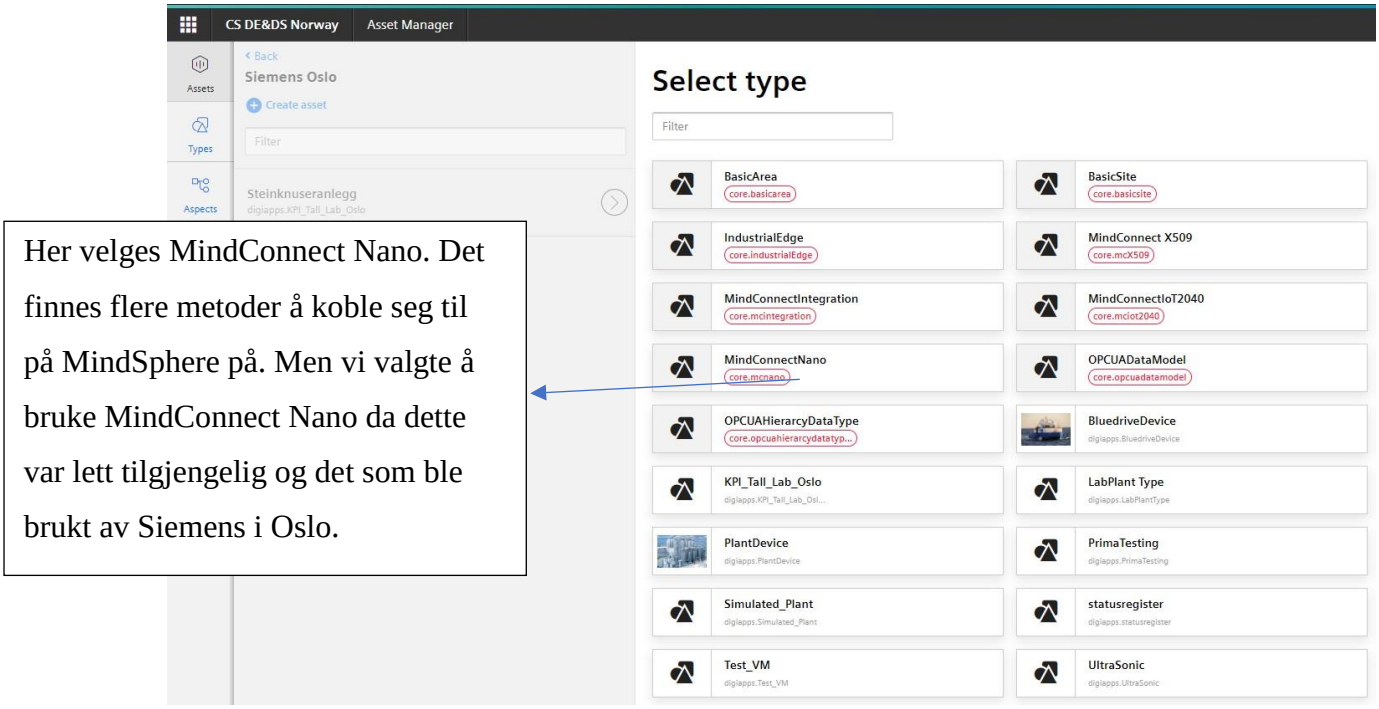
6.3.1 Asset Manager

I Asset Manager modellerer du strukturen i en industriprosess ved bruk av «Assets», «Types» og «Aspects». Men først skal vi se nærmere på konfigureringen av MindConnect Nano-boksen.



Figur 7: Figuren viser hvordan man lager en «Asset»

For å konfigurere MindConnect Nano-boksen må vi først legge til Nano-boksen i vår «Asset» som vist på figur 8.



Her velges MindConnect Nano. Det finnes flere metoder å koble seg til på MindSphere på. Men vi valgte å bruke MindConnect Nano da dette var lett tilgjengelig og det som ble brukt av Siemens i Oslo.

Figur 8: Figuren viser hva man skal velge for å koble seg til MindConnect Nano-boksen.

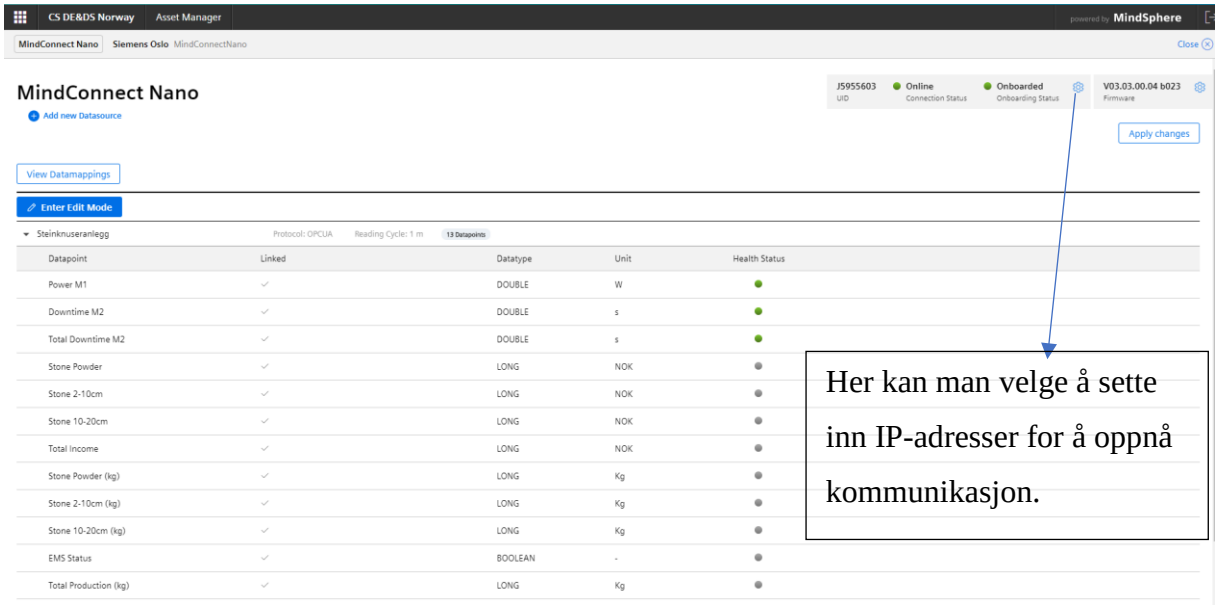
Når MindConnect Nano-boksen er lagt til vil man kunne se det i «Assets» under Siemens Oslo som vist på figur 9.

Her kan man se at MindConnect Nano-boksen er lagt inn og klar til å konfigureres.

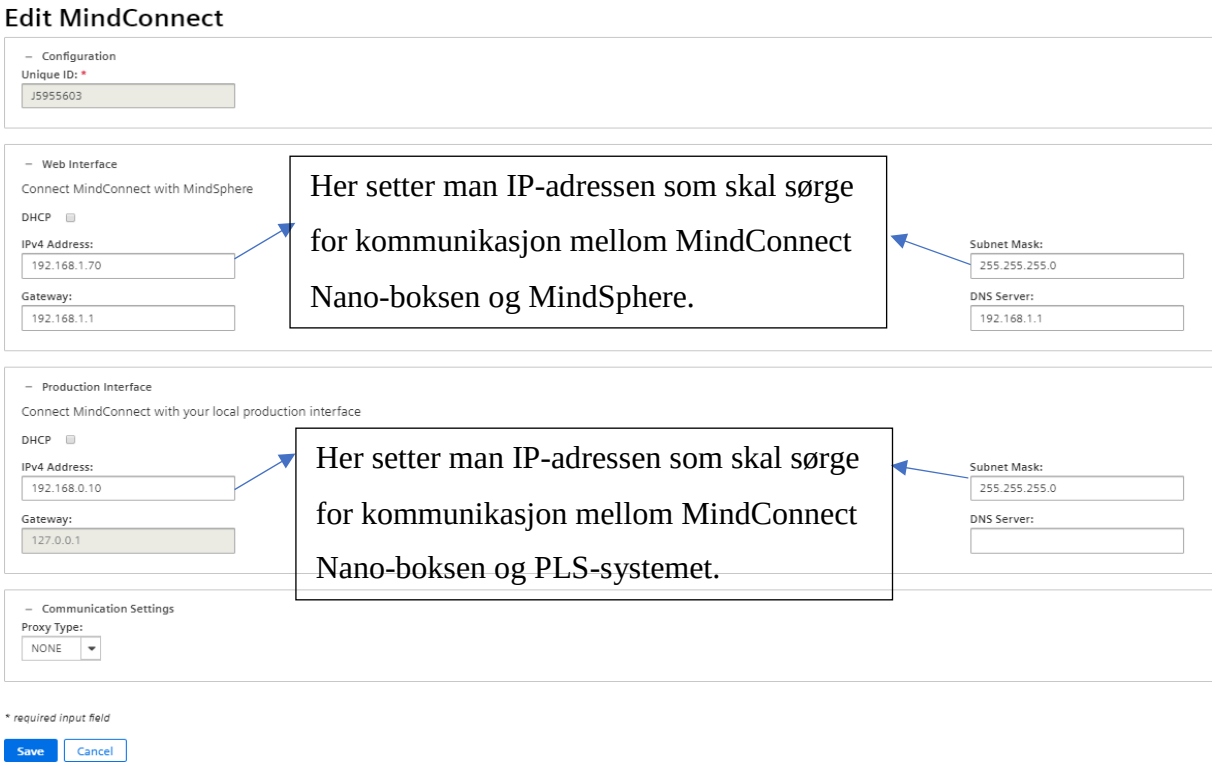
Figur 9: MindConnect Nano boksen er lagt inn i systemet og kan nå konfigureres

6.3.1.1 Konfigurering av MindConnect Nano-boks

Ved å trykke på «MindConnect Nano» på figur 9 vil man kunne legge til datakilde og kunne se UID-nummer, tilkoblingsstatus, firmware-versjon og «Onboarding Status» som viser om man er koblet til korrekt IP-adresse slik at MindSphere har kommunikasjon med MindConnect Nano-boksen. Ved å trykke på tannhjulet som vist på figur 10 kan man sette inn IP-adresser.



Figur 10: Figuren viser siden som åpnes når man trykker på MindConnect Nano, her kan man sette IP-adresse, legge til datapunkter fra PLS-systemet og oppdatere «firmware».



Figur 11: Figuren viser hvor man setter inn IP-adressene for å få kommunikasjon med MindConnect Nano-boksen.

Som vist på figur 11 så er IP-adresser allerede satt for å få kommunikasjon. Vi startet med å teste ulike IP-adresser og fikk ingen kommunikasjon grunnet feil IP-adresse. Grunnet ingen god beskrivelse på hvordan man gjør dette prøvde vi oss frem. Vi fant ut at IP-adressen som brukes for å koble MindConnect med MindSphere måtte være i samme subnet – det vil si samme IP-adresse, men ulikt nettverkssegment [10]. Vi koblet derfor ruteren opp og fant IP-adressen og regnet oss frem til en av de IP-adressene som er i samme subnet som MindConnect Nano-boksen. Dette gjorde vi ved å koble oss til ruteren med en Ethernet-kabel og pinge ruteren med «Command prompt» (Kommandolinje) for å finne ruterens IP-adresse og subnet-maske. IP-adressen vi fant var 192.168.1.54 med subnet-maske 255.255.255.0 – det vil si at vi kunne velge en IP-adresse fra 192.168.1.1 til og med 192.168.1.254 ekskludert 192.168.1.54. [11]

Vi brukte samme prosedyre når vi skulle sette IP-adresse for PLS-systemet og MindConnect Nano-boksen. PLS-systemet har IP-adresse 192.168.0.1 med subnet-maske 255.255.255.0. Vi valgte derfor å bruke 192.168.0.10 for å være i samme subnet som PLS-systemet.

Dersom konfigurasjonen er gjort på en korrekt måte skal «Onboard Status» lyse grønt – det vil si at tilkoblingen med MindConnect Nano-boksen er suksessfull.

6.4 KPI

KPI er som sagt i kapittel 4; "Kritiske suksessfaktorer (KPI) representerer et sett med tiltak som fokuserer på de aspektene av organisatorisk ytelse som er mest kritiske for den nåværende og fremtidige suksessen til organisasjonen" [6].

KPI'ene vi valgte er vist på tabell;

KPI	Detaljer
Økonomi	
Totale inntekter	Totale inntekt, dvs. totale inntektene fra steinproduksjon
Inntekt 1	Stein 10-20 cm
Inntekt 2	Stein 2-10 cm
Inntekt 3	Steinpulver
Produksjon	
Totale produksjon (kg)	Totale produksjon, dvs. total produksjon av stein
Produksjon – stein 10-20 cm (kg)	Stein 10-20 cm (kg)
Produksjon – stein 2-10 cm (kg)	Stein 2-10 cm (kg)
Produksjon – steinpulver (kg)	Steinpulver (kg)
Status	
Motor temperatur	Temperatur av motor hentes fra frekvensomformer
Nødstopp status	Status på nødstopp
Nedetid	Nedetid for hver gang driften stoppes. Skal være mulig å resette nedetid når maskinen er i drift igjen.
Totale nedetid	Totale nedetid, skal ikke være mulig å resette. Ønskes at det starter å telle så fort maskinen stopper.
Været i Oslo	Ønsker å visualisere været i Oslo.

Energi bruk	Ønsker å vite energibruk, hentes fra frekvensomformer
Totale energi bruk	Totale energibruk

Tabell 1: Viser de KPI som er valgt

Vi delte KPI'ene i tre kategorier; Økonomi, produksjon og status. Dette fordi det blir mer oversiktlig å ha tre ulike dashbord. Disse KPI'ene var ikke programmert av forrige års studenter, så vi måtte programmere det selv i TIA-Portal for å kunne visualisere disse på applikasjonen SPI.

Vi har derfor laget flytskjema for hver kategori som tar for seg logikken bak programmering av disse KPI'ene. Disse finner dere under vedlegg med navn:

- [05.006 – Flytskjema økonomi]
- [05.007 – Flytskjema produksjon]
- [05.008 – Flytskjema status]

Grunnen til at vi valgte å lage flytskjema istedenfor å vise programmeringen er fordi det er ganske enkelt å programmere disse KPI'ene og derfor vil flytskjema gjøre det mer oversiktlig for leserne.

Vi mener at det viktigste for en anleggseier er å vite om han tjener penger, hvor mye han produserer og ikke minst statusen på systemet. Dette gir anleggseier muligheten til å kunne dra til reiser fritt uten å måtte tenke på om det kommer til å skje noen nødstilfeller med anlegget. Disse vil han kunne se gjennom MindSphere.

Anleggseier vil til enhver tid få vite hvor mye penger han tjener på hvert av sine produkt og totale inntekten han har tjent. Han kan sjekke hvor mye han har tjent før i tiden og sammenligne verdiene. Han vil også få kunne seg hvor mye han produserer av hvert produkt og se totale produksjon, dette kan analyseres og det kan ses på om det er mulig å redusere kostnadene.

Anleggseier vil til enhver tid få status på systemet. Dersom produksjonen stopper, eller noe annet nødstilfelle skjer vil han få status på dette i MindSphere. Han vil få lokale nedetid for hver gang maskinen stopper, som kan resettes og vil også få se totale nedetid av systemet

gjennom en tidsperiode han velger selv. Energibruk og totale energibruk vil bli vist på MindSphere, dette kan analyseres og se om kostnadene kan reduseres. I tillegg vil anleggseier til enhver tid se været i Oslo. Dersom det blir for varmt eller kaldt kan han utføre tiltak for å beskytte sine komponenter.

Vi mener derfor at de KPI'ene vi har valgt vil komme anleggseier til gode.

6.4.1 Frekvensomformer

To av KPI'ene har vi hentet fra frekvensomformeren som styrer motoren. Disse er:

- Motor temperatur
- Energibruk

Vi har aldri vært borti frekvensomformere før og dermed ble det brukt veldig mye tid på å finne løsning på hvordan vi skulle programmere det slik at vi kunne hente ut data fra frekvensomformer for å kunne visualisere det på SPI.

Vi utarbeidet derfor et dokument med fremgangsmåten på hva vi har prøvd og løsningen vi til slutt fant, vi valgte å skrive metoden på eget dokument for ordens skyld. Denne finner dere under vedlegg med navn: [05.009 – Frekvensomformer]

6.5 Simatic Performance Insight

Med SPI kan du nå dine mål ved å spore de viktige ytelsesindikatorene til maskinene. Med ulike visualiseringsalternativer vises maskinforholdene i henhold til brukerens behov.

SPI er ett helt ny applikasjon som ble produsert av Siemens i Tyskland. Den ble lansert i januar i år. Vi er de første som har brukt denne applikasjonen i Norge. I motsetning til «Fleet Manager» som var standard visualiseringsverktøy i MindSphere før SPI, er den mer brukervennlig og ser grafisk bedre ut.

Vi valgte å bruke SPI istedenfor «Fleet Manager» fordi vi ville teste ut noe nytt og fordi Siemens også ønsket å vite brukergrensesnittet for SPI.

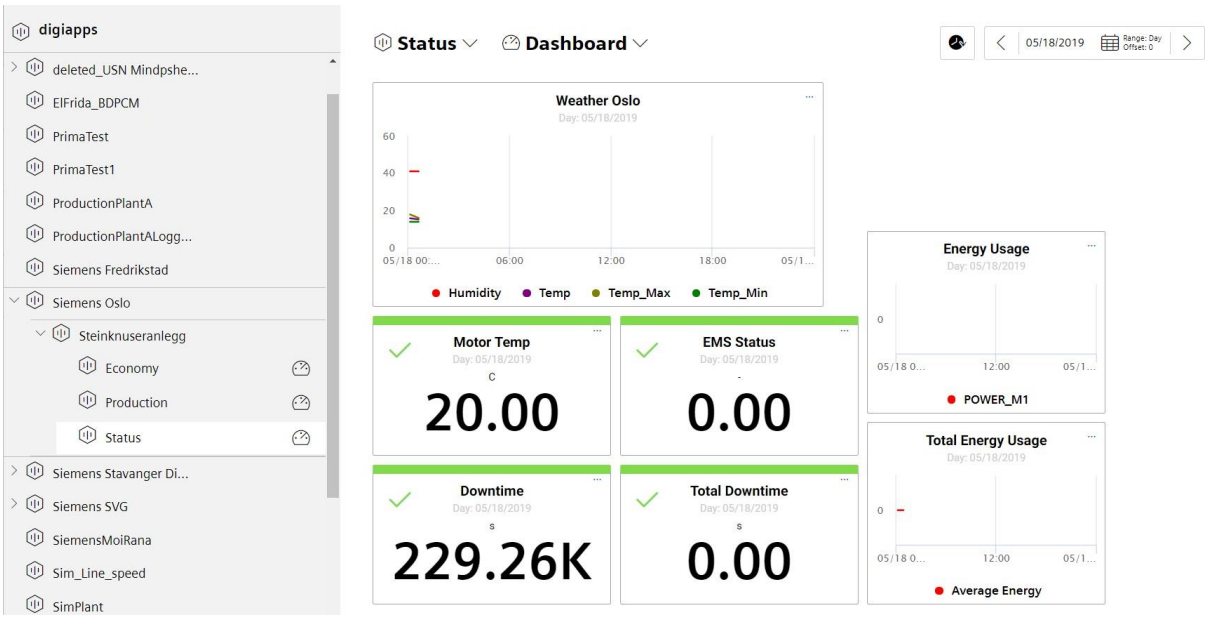
6.5.1 Fremgangsmåte

Vi har utarbeidet et dokument på fremgangsmåten for å både sende data fra PLS-systemet til MindSphere og for å kunne visualisere disse i SPI. Grunnen til at vi valgte å sette det som vedlegg er fordi det blir fort mange sider grunnet bruk av mange figurer.

Dokumentet beskriver en detaljert metode for å finne ID til datapunkter, sende disse til MindSphere og visualisere disse i SPI. I tillegg gir den en beskrivelse på hvordan man kan hente data fra andre kilder enn PLS-systemet. Dette dokumentet finner dere under vedlegg med navn: [05.010 – Simatic Performance Insight]

6.5.2 Resultater

Ved å følge fremgangsmåten beskrevet i vedlegget ovenfor fikk vi laget tre ulike dashbord. I dashbordene visualiserte vi de KPI'ene som vi hadde valgt, disse ble visualisert i SPI.



Figur 12: Viser status dashbordet som er laget for å vise status på steinknuseranlegget

I status dashbordet har vi lagt til temperaturen av motor, nedetid, totale nedetid, nødstopp status, været i Oslo, energibruk og totale energibruk. Nødstopp status blir rød dersom den blir aktivert.

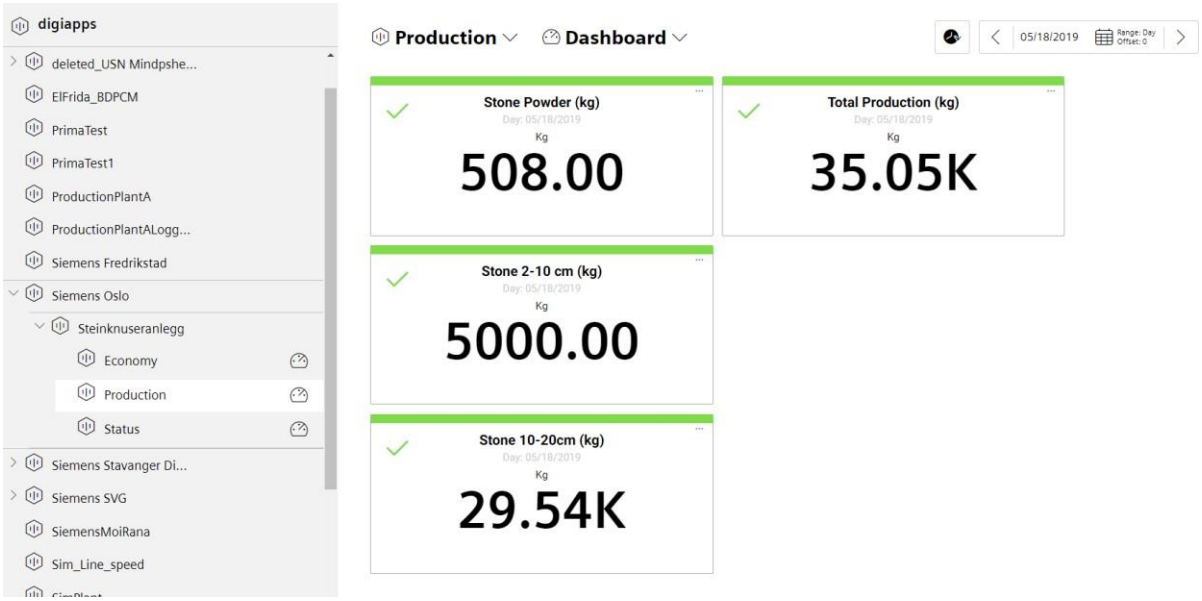
Vi satt inn grenser på motor temperaturen, dersom den er varmere enn 35 grader og mindre enn 10 grader vil det bli utstedt en advarsel. Hvis den går over 50 grader eller under 1 grader vil det bli utstedt en alarm. Dette er tall vi bestemte oss for ved å se på motorens datablad som dere finner under vedlegg [06.030 - Motor].

Nedetid er den lokale nedetiden – det vil si for hver gang anlegget stopper vil den begynne å telle. Den stopper når anlegget er oppe og går igjen. Anleggseier vil få muligheten til å skrive

ned tiden på hvor lenge maskinen stoppet og resette dette via HMI. Totale nedetid derimot vil holde denne verdien og fortsette å telle neste gang det blir stopp i anlegget.

Energibruk viser energibruket av motoren i sanntid. Vi laget egen KPI i SPI som beregner totalenergi.

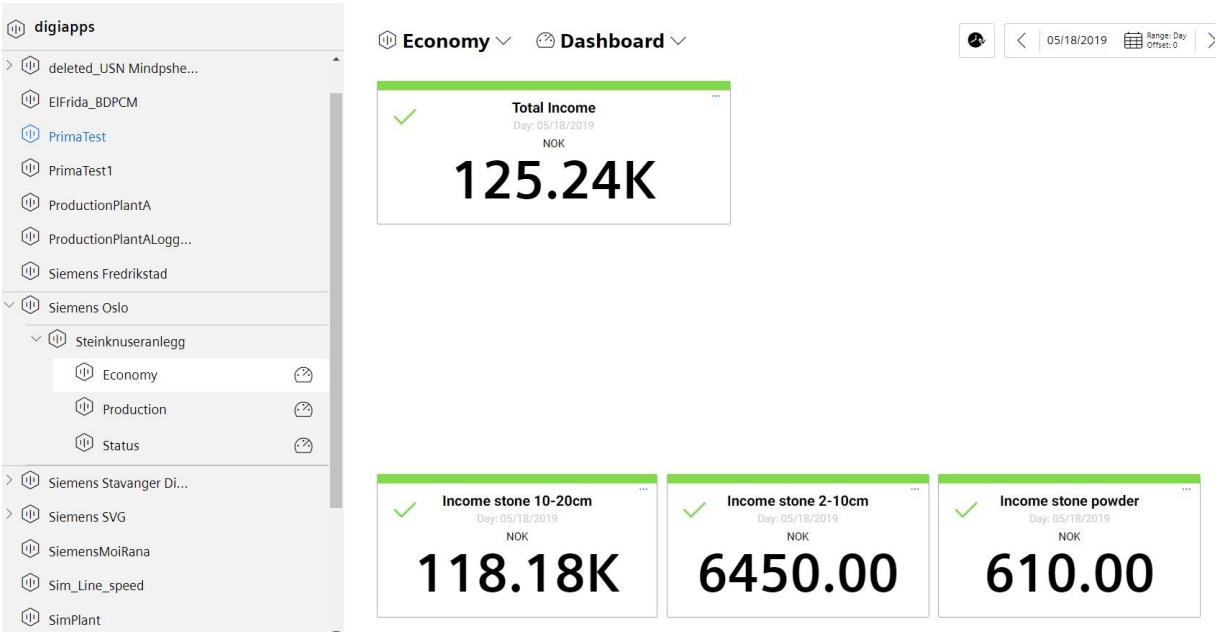
Til sist visualiserte vi været i Oslo med grenser for advarsler og alarm for å gi anleggseier mer oversikt over været. Dette kan anleggseier bruke for å sikre komponentene i anlegget.



Figur 13: Viser produksjons dashbord som er laget for å vise produksjonen i steinknuseranlegget

Vi visualiserte produksjonen av steinpulver, stein som er 2-10cm og stein som er 10-20cm. Dette er tre ulike produkter som blir produserte i steinknuseranlegget.

Antall kilogram som blir produsert for hvert produkt blir registrert via PLS-systemet og vi beregnet da totale produksjonen av alle disse tre produktene.



Figur 14: Viser økonomi dashbordet som er laget for å vise økonomien av steinknuseranlegget

Vi brukte standard pris som vi mente er hensiktsmessig ved salg av steiner. Prisen for stein pulver satt vi til å bli 1.2 kr per kilogram, for stein 2-10 cm satt vi prisen 1.29 kr per kilogram og for stein 10-20 cm satt vi prisen 4 kr per kilogram. Deretter summerte vi alle tre inntektene og fikk totalinntekten. Disse er viktig nøkkeltall som anleggseiere er meget interesserte i å vite.

7 Cyber Security

Siemens ønsket en prosedyre på hvordan man utfører en sikkerhetsanalyse. Vi utarbeidet en slik håndbok [06.000 – Cyber Security IEC62443 Håndbok]. Vi tok utgangspunkt i denne prosedyren når vi sikkerhetsanalyserte anlegget vårt.

7.1 Prosedyre

Prosedyren for sikkerhetsanalysering av anlegget består av tre faser:

- **Fase 1:** For å få oversikt over nåværende sikkerhet i anlegget og eventuelle nødvendige sikkerhetstiltak, gjennomføres det en risikoanalyse av anlegget. Dette blir gjennomført ved å analysere og vurdere dokumentasjonen gitt av kunden. Dokumentasjonen som ble analysert for dette anlegget er som følger:
  - Design av kontrollrom [06.002 – Design av kontrollrom]
- **Fase 2:** Etter at uønskede hendelser og farekilder blir identifisert, blir det utført et dybdeintervju med anleggseier. Under intervjuet blir risikoanalyse og eksisterende beskyttelsesmekanismer gjennomgått. Deretter blir anlegget besøkt for å foreta grundige undersøkelser. Det blir utarbeidet en risikomatrise slik at vi får oversikt over høye risikoer.
- **Fase 3:** Etter at risikomatrisen er utarbeidet og høye risikoer er identifisert, anbefales det sikkerhetstiltak for å kunne redusere risikoen og konsekvensen av disse hendelsene. Kunden blir også informert om hvilket sikkerhetsnivå anlegget ligger på ut ifra IEC62443-standarden.
  (Kilde: [21])

7.2 Fase 1: Innsamling av informasjon

I henhold til håndbok for Cyber Security består første steg av å samle inn informasjon om anlegget. Dette gjøres for å avdekke sikkerhetstrusler og utarbeide et utkast for sikkerhetstiltak. For å gjennomføre dette foretas det en risikoanalyse. Første steg av risikoanalysen er å finne mulige årsaker til angrep på anlegget. Det stilles 200 spørsmål til kunden fra standarden for IEC. Dette gjøres for å finne mulige årsaker til angrep. Disse spørsmålene er konfidensielle, og vi ble derfor nødt til å begrense antall spørsmål fra 200 til fire:

- Hva kan forårsake reduksjon eller tap av produksjon på et eller flere steder?
- Hvordan kan det forårsake skader eller dødsulykker i nærområdet?
- Hvordan kan produkter eller utstyr saboteres?
- Hva kan forårsake tap av sensitiv eller konfidensiell informasjon?

(Kilde: [22] og [23])

7.1.1 Identifisering av farekilder

ID:	Uønskede hendelser
Risiko 1	Reduksjon eller tap av produksjon i et eller flere områder
Risiko 2	Skader eller dødsulykker i nærområde
Risiko 3	Ødeleggelse av utstyr eller produkter

Tabell 2: Tabellen viser uønskede hendelser

7.1.2 Klassifisering av sannsynlighet og konsekvens

Risiko er målt ut fra sannsynligheten for og konsekvensen av en hendelse [5]. Formelen for risiko er følgende:

$$Risiko = Sannsynlighet * Konsekvens$$

[5]

For å beregne risiko er det nødvendig å definere og klassifisere sannsynligheter og konsekvenser. Det er denne informasjonen vi tar utgangspunkt i for å beregne risikonivåer. Sannsynligheten med skala lav-til høy er illustrert i figur 1. Ulike konsekvenser med skala fra lav-til høy er illustrert i figur 2. (Kilde: [24])

Sannsynlighetsskala	
Skala	Beskrivelse
Høy (A)	En trussel eller sårbarhet vil forekomme i de neste årene
Medium (B)	En trussel eller sårbarhet vil forekomme i løpet av de neste 10 årene
Lav (C)	En trussel eller sårbarhet har ikke forekommet tidligere eller anses som usannsynlig

Tabell 3: Sannsynlighetskala beskriver hvilken frekvens trusselen eller sårbarheten ligger på, og hvilken spesifikk frekvens som skal til for å oppnå hvert nivå.(Kilde: [25])

Konsekvens Del 1					
Risikokategorier					
	Produksjon		Informasjonssikkerhet		
Kategori	**Produksjonsbrudd på et område på anlegget**	**Produksjonsbrudd på flere områder på anlegget**	**Kostnad i NOK**	**Lovlig**	**Offentlig tillit**
Høy	Lengre enn 7 dager	1 dag eller mer	>5 000 000	Straffbar hendelse	Tap av bedriftens merkenavn
Medium	Mellom 6-2 dager	1 time eller mer	>500 000		Tap av kundens tillitt
Lav	1 dag eller mindre	Mindre enn 1 time	< 500 000	Ingen	Ingen

Konsekvens Del 2						
Risikokategorier						
	Industridriftsikkerhet		Miljøsikkerhet			Nasjonal innvirkning
Kategori			**Kostnad i NOK**	**Lovlig**	**Offentlig tillit**	**Infrastruktur og service**
Høy	Lengre enn 7 dager	1 dag eller mer	>5 000 000	Straffbar hendelse	Tap av merkenavn på bedriften	Påvirker flere virksomhet sektorer eller forstyrrer samfunnstjenester
Medium	Mellom 6-2 dager	1 time eller mer	>500 000	Bøter/ samfunns tjeneste	Tap av kundens tillitt	Potensial for å påvirke næringslivet utover det enkelte selskap
Lav	1 dag eller mindre	Mindre enn 1 time	<500 000	Ingen	Ingen	Litt eller ingen innvirkning på næringslivet utover det enkelte selskap

Tabell 4: Konsekvenstabell beskriver hvilket nivå konsekvensen ligger på, og kravene som oppfyller disse nivåene. Grunnet for stor matrise har vi valgt å dele den opp i to tabeller. (Kilde: [26])

7.3 Fase 2: Gjennomgang av eksisterende beskyttelsestiltak

Etter grundige undersøkelser i anlegget og dybdeintervju med anleggseier, har vi kartlagt eksisterende beskyttelsestiltak og vurdert hvilken nye beskyttelsestiltak som burde implementeres for å redusere risiko. Se figur 4 og 5 for detaljer.

7.2.1 Risikonivå

Risikonivå er en benevnelse vi har brukt for å angi hvilket nivå hver risiko ligger på.

	nivå	konsekvens kategori martrise		
sannsynlighet		A	B	C
	høy	høy-risk	høy-risk	medium-risk
	medium	høy-risk	medium-risk	lav-risk
	lav	medium-risk	lav-risk	usannsynlig-risk
nivå 1	**nivå 2**	**nivå 3**	**nivå 4**	
usannsynlig (lav +C)	lav	medium	høy	

Tabell 5: Risikonivå angir hvilket risikonivå hendelsen har, gitt konsekvensene og sannsynligheten (Kilde: [27])

7.2.2 Risikomatrise

Neste steg av risikoanalysen er å sette alle risikomomenter inn i en risikomatrise. Figur 4 viser de mulige årsakene. Resultatet for sannsynligheten og konsekvens føres inn i matrisen. Ved hjelp av risikonivå, se figur 3, bestemmes det hvilket risikonivå hendelsen har.

Risikomatrise						
Mulig uønsket hendelse/fare	**Mulig årsak**	**Eksisterende beskyttelsestiltak**	**Sannsynlighet**	**Konsekvens**	**Risikonivå**	**Nivå**
Reduksjon eller tap av produksjon i et eller flere områder	Cyberangrep av uvedkommende eller ansatte. Slår av maskinene på et eller flere steder	Kryptert programvare	C	Medium	Lav-risk	Nivå 2

	Ansatte stopper anlegget for å gjøre hærverk	Overvåknings-kamera og begrenset tilgang til kontrollrom	C	Høy	Medium-risk	Nivå 3
	Ansatte kan stjele produktet eller deler	Kameraovervå king	C	Høy	Medium-risk	Nivå 3
	Ansatte infiserer systemet med virus	Windows Defender Security	C	Høy	Medium-risk	Nivå 3
Skade eller dødsulykker i nærområdet	Uvedkommende får fysisk tilgang til anlegget	Dørene er låst for uved-kommende	B	Medium	Medium-risk	Nivå 2
Ødeleggelse av utstyr eller produkter	Cyberangrep ved å øke hastigheten av maskin	Sikkerhets-gjerde, overvåknings-kamera	C	Høy	Medium-risk	Nivå 2
	Stjele deler av maskinen	Kameraover-våking	B	Medium	Medium-risk	Nivå 2
	Ansatte sprer ut sensitiv informasjon	Taushetser-klæring og personell-opplæring	C	Høy	Medium-risk	Nivå 3

Tabell 6: Risikomatrise gir oversikt over mulige inntrufne årsaker, sannsynligheten og konsekvensen for at dette inntreffer. (Kilde: [28])

Risikomatrisen er altså en oppsummering av analysen i henhold til håndboken. Den viser mulige årsaker til angrep og eksisterende sikkerhetstiltak som kunden har implementert før analysen. Til høyre ser man hvilket nivå sannsynlighet og konsekvens ligger på. Man ser også

hvilket risikonivå hver årsak ligger på. Dette er viktig informasjon for å kunne kartlegge hvilke hendelser som har høy risiko og som dermed trenger ekstra sikkerhetsfokus.

Alle hendelser bør ligge på et lavt risikonivå. Det vil si at dersom vi har hendelser som ligger på nivå 3 eller 4, er det viktig å implementere sikkerhetstiltak for å redusere risikoen for at disse hendelsene inntreffer. Hvis en hendelse derimot er på nivå 1 eller 2, er det ikke et krav med sikkerhetstiltak, men det anbefales likevel å implementere sikkerhetstiltak.

7.4 Fase 3: Anbefaling av sikkerhetstiltak – risikoreduserende tiltak

Som leverandør anbefaler vi sikkerhetstiltak som kan redusere risikoen av uønskede hendelsene. Disse anbefalingene finner dere i figur 5 under «Anbefalt beskyttelsestiltak».

Risikoreduserende tiltak			
Mulig uønsket hendelse/fare	**Mulig årsak**	**Eksisterende beskyttelsestiltak**	**Anbefalt beskyttelsestiltak**
Reduksjon eller tap av produksjon i et eller flere områder	Cyberangrep av uvedkommende eller ansatte. Maskinene blir avslått på et eller flere steder	Kryptert programvare	Antivirus, høyt sikkerhetsnettverk og brannmur
	Ansatte stopper anlegget for å gjøre hærverk	Overvåkningskamera og begrenset tilgang til kontrollrom	Kortleser med pinkode som logger ID. Plugger i PLS-systemet for å hindre at uvedkommende kobler seg til
	Ansatte kan stjele produktet eller deler	Kameraovervåking	Kortleser med pinkode som logger ID.
	Ansatte infiserer virus i systemet	Windows Defender Security	Windows Defender Security.

Skade eller dødsulykker i nærområdet	Uvedkommende får fysisk tilgang til anlegget	Dørene er låst for uvedkommende	Korttilgang til HMI-systemet. Korttilgang med PIN-kode inn til kontrollrom.
Ødeleggelse av utstyr eller produkter	Cyberangrep ved å øke hastigheten av maskin	Sikkerhetsgjerdet, overvåkningskamera	Nøkkellås på USB, overvåking og nøkkelkort
	Stjele deler av maskinen	Kameraovervåking	Ingen tiltak
	Ansatte sprer ut sensitiv informasjon	Taushetserklæring og personell opplæring	Begrenset tilgang til informasjon, kun anleggseier har administratorrettigheter

Tabell 7: Risikoreduserende tiltak viser både eksisterende tiltak og anbefalt beskyttelsestiltak.

Ut ifra analysen ble det bestemt at anlegget bør ligge på sikkerhetsnivå 2 i forhold til IEC62443 standarden. På sikkerhetsnivå 2 er det et minimums krav at den fysiske tilgangen til bygget begrenses ved bruk av korttilgang. I tillegg kreves det brukernavn og passord for innlogging til HMI og PC. Vi bestemte oss for å implementere disse tiltakene for å oppnå de krav som stilles for sikkerhetsnivå 2.

7.5 Implementering av sikkerhetstiltak

Vi implementerte korttilgang ved bruk av RFID-teknologi. Vi installerte det på HMI slik at uautoriserte brukere ikke skulle få tilgang til kontrollsystemet. I tillegg installerte vi plugger i PLS-systemet slik at uvedkommende ikke har mulighet til å koble seg til nettverket.

7.5.1 Installasjon av RFID – SIMATIC RF1060R

Siemens tilbyr produkter og løsninger med industrielle sikkerhetsfunksjoner som sikrer sikker drift av anlegg, systemer, maskiner og nettverk. Det finnes fire forskjellige kategorier:

- SIMATIC RF200
- SIMATIC RF300
- SIMATIC RF600
- SIMATIC RF1000

Figur 15: Viser en RFID kortleser av typen RF1060R [16]

Gruppen valgte å bruke et produkt fra RF1000-kateteret. SIMATIC RF1060R er en leser for tilkobling til en Windows-basert datamaskin eller en HMI. Tilkoblingen er via et USB-grensesnitt, og den håndteres av WinCC Runtime. Det er mulig å koble RF1060 til en datamaskin eller direkte til en Simatic HMI.

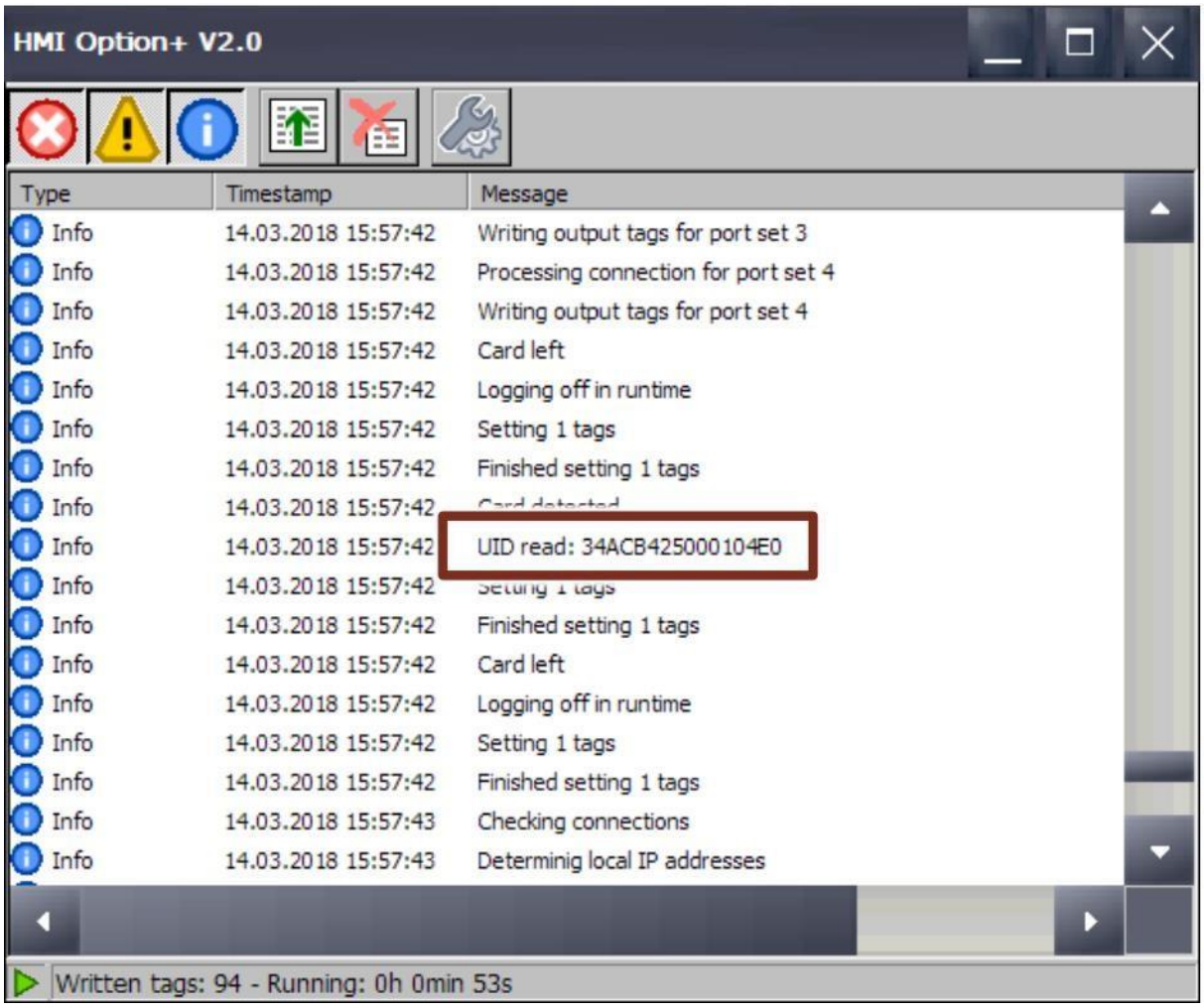
SIMATIC RF1060R-leseren gir mulighet til å bruke identifikasjonskort også når man bruker andre maskiner enn HMI. Dette gjør det mulig å implementere nøye graderte tilgangskonsepter, eller brukerspesifikke instruksjoner - alt sammen med ett kort.

Kilde [12] ble brukt for å skrive generelt om RFID kortleseren.

7.5.1.1 Simatic HMI Option+

Simatic HMI Option+ er et nytt program som fungerer som bindeleddet mellom operativsystemet og Runtime av HMI-panelet. I de fleste HMI vil man ikke ha mulighet til å styre operativsystemet, da det som oftest er fullskjerm med tilhørende styringsskjerm for anlegget. HMI Option+ gir denne muligheten ved å tilkalle det via en tag fra styringsskjermen. Dette gjør det mulig å vise systeminformasjon, brukeridentifikasjoner, og videre ha muligheten til å bruke avanserte funksjoner for maskinovervåking.

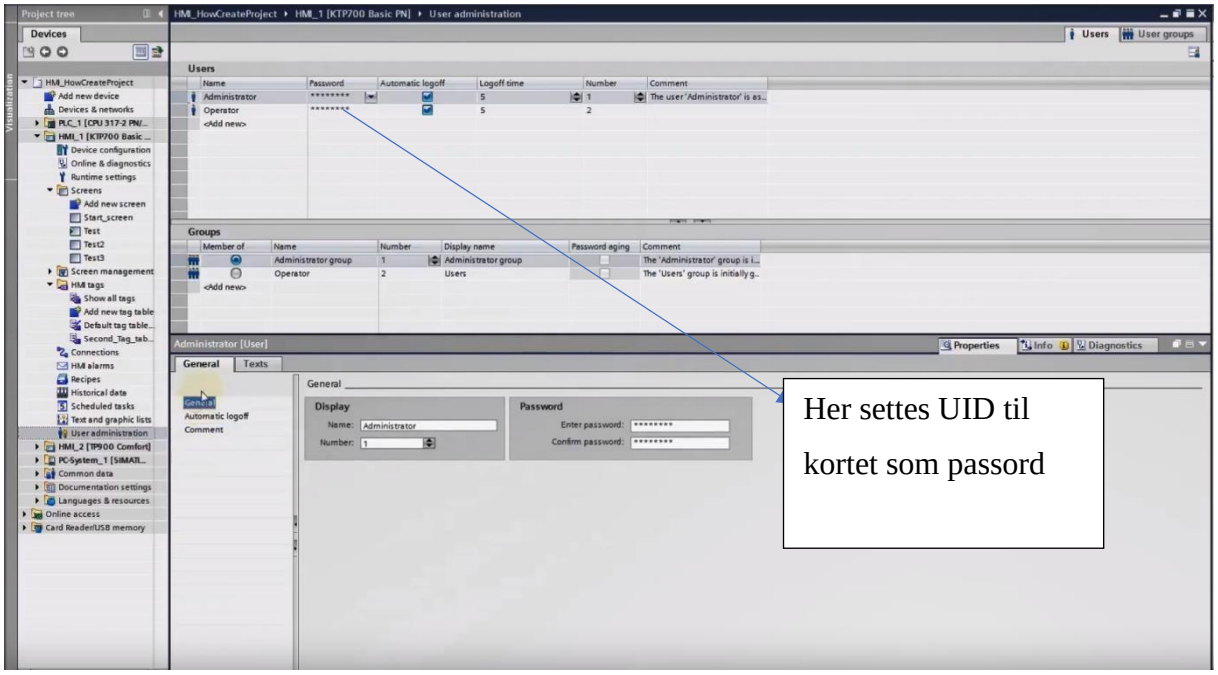
En av tjenestene i Simatic HMI Option+ er PM-Logon Basic, som brukes for brukeridentifikasjon via RF1060R-leseren.



Figur 16: Viser at programmet HMI Option+ gir oss UID til kortet som ble brukt på RFID kortleseren.

PM-Logon Basic Runtime forbinder seg med RFID-leseren og leser kortets UID så snart det er nært nok. Klokkeslett og dato blir også registrert, slik at man kan se hvem som har logget

seg inn.



Figur 17: Viser hvor man setter kortets UID som passord for å gi bruker tilgang til HMI.

Kortets registrerte UID leses fra HMI Option+ og dette blir registrert i passord på «User Administration» i TIA Portal, se figur 10. Hvert kort har sitt unike UID-passord – det vil si at hver bruker har sitt unike kort som kan brukes for å logge seg inn i HMI.

```
Sub PMLOGON_UID_Changed()

' Card not available
If SmartTags("PMLOGON_UID") = "-1" Then
    Logoff
    SmartTags("Status") = 0

' Card available
Else
    Logon "PMLOGON_UID", "UserName"
    SmartTags("Status") = 1
    GetUserName "CurrentUser"

' User does not exist
    Dim zeichenkette
    Dim laenge
    zeichenkette = SmartTags("CurrentUser")
    laenge = Len(zeichenkette)

    If laenge < 1 Then
        SmartTags("Status") = 2
    End If
End If

End Sub
```

Figur 18: Denne figuren viser skriptet som ble brukt for å gjenkjenne kortet når det skannes på RF1060R-leseren.

For at systemet skal gjenkjenne kortet når det skannes på RF1060R-leseren, må det brukes skript. Vi benyttet oss av VBScript i TIA Portal til å skrive en skript som sjekket om kortets UID ble lest eller ikke. Vi gav administrator muligheten til å legge til bruker og slette bruker via HMI, slik at kunden ikke skal trenge å tilkalle leverandør for å måtte endre på brukere. I tillegg satt vi et grensesnitt på den tiden en bruker kan være logget på systemet. Dersom operatør glemmer å logge seg av systemet, vil han automatisk logges av innen 60 minutter.

Kilde [13] inneholder instruksjoner på hvordan man gjør dette enda mer detaljert. Vi har fulgt denne instruksjonen.

7.5.2 Installasjon av plugger

For å kunne sikre inngangene og utgangene på PLS-systemet, valgte vi å bruke plugger som låser disse inngangene og utgangene slik at uvedkommende ikke klarer å koble seg til nettverket dersom de skulle klare å komme seg inn i operatørrommet.

Figur 19: Viser plugger som installeres i PLS-systemet [8]

7.6 Operatørrommet før og etter sikkerhetstiltak

Vi har designet operatørrommet på nytt for å vise de endringene som har blitt gjort etter at sikkerhetstiltakene er blitt implementert. Før- og etter-modell finnes under vedlegg med navn:

- [04.002 – Design av kontrollrom]
- [04.006 – KontrollromEtterTiltak]

8 Asset Optimization Service

AOS er en tjeneste utarbeidet av Siemens som analyserer leveringsrisikoen og livssyklusen på Siemens sitt utstyr i anlegget. [14] Dette gjøres for å få oversikt over tilgjengeligheten og leveringstiden på kritiske komponenter og reservedeler i anlegget. På denne måten kan man unngå uforutsette driftsstanser med unødvendig lang nedetid av produksjonen.

For å unngå driftsstans, vil man etter analysen få oversikt over hvilket utstyr som ikke lenger er tilgjengelig i originalversjon. Rapporten vil også gi informasjon om alternative deler til de utgåtte modellene. I tillegg vil rapporten også gi informasjon på status av Siemens sitt utstyr i eget lager. Dette vil sikre at man til enhver tid har mulighet til å bestille reservedeler som vil være tilgjengelig på lageret. Dette vil øke driftssikkerheten ved at eventuelle begrensende produksjonsfaktorer avdekkes.

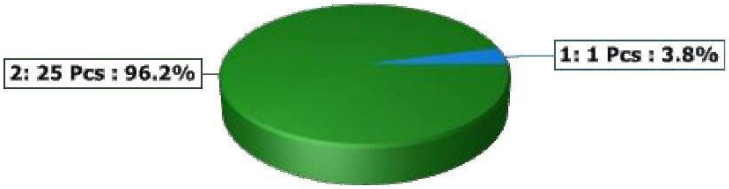
8.1 Utførelse av analyse

Første steg i analysen er å lage en oversikt over alt Siemens sitt utstyr i anlegget med tilhørende MLFB-nummer. De tilhørende MLFB-numrene finnes under vedlegg med navn [04.007 – Utstyrsliste Modell]. MLFB-numrene registreres i Excel [07.006 – CompressedMLFB] og kjøres i en intern programvare; Pridanett, og vi får et dokument med oversikt over komponentene i anlegget [04.003 – AOS]. Analysen gir detaljerte diagrammer over tilgjengelighet, erstatningskomponenter og leveringstid. Disse resultatene vil presenteres for kunden, og vi som leverandør vil gi en anbefaling av tjenester som kunden kan kjøpe for å sikre seg mot unødvendig nedetid i anlegget. Dette kan for eksempel være registrering av lager, forebyggende vedlikehold av anlegget eller teknisk inspeksjon av reservedeler på kundens lager.

8.2 Resultater av AOS-analysen

Identifiserte komponenter

Number of IBase items that have been read in		26		28
Of which, after consolidating identical article numbers:		Number of article numbers	As a per-centage	Quantity of items
2	Known article number	25	96.2%	27
1	Number of unknown article numbers	1	3.8%	1

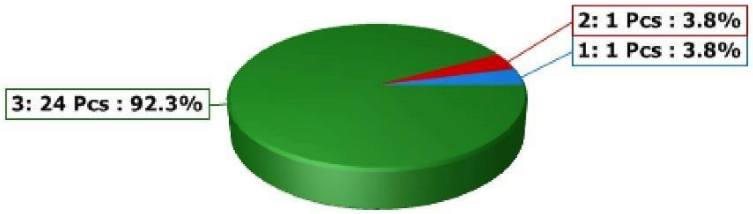


Figur 20: Viser hvor mange komponenter som er blitt registrert og hvor mange som er ukjent for systemet

Rapporten viser at det er en komponent i anlegget som systemet ikke klarer å gjenkjenne. MFLB-nummeret er altså ukjent for systemet. Dette kan ha flere årsaker; feil MFLB-nummer har blitt skrevet inn av eieren, det kan ha forekommet tastefeil ved registrering på Excel eller det kan hende at komponenten ikke er registrert i programmet. I vårt tilfelle ble det registrert feil MLFB-nummer av eier og den ene komponenten ble dermed ikke gjenkjent av programvaren.

Tilgjengelighet til originale komponenter

	Description	Number of article numbers	As a per-centage	Quantity of items	Asset Value
3	Items available as original item	24	92.3%	26	6,898 €
2	Items no longer available as original component; Items have already been discontinued, have been substituted or replacement types are available	1	3.8%	1	
1	Unknown article number	1	3.8%	1	
	Total	**26**		**28**	

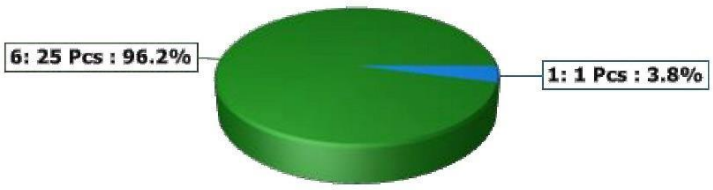


Figur 21: Viser hvor mange komponenter som er originale, og de komponenter som er tatt ut av produksjon

24 av komponentene er tilgjengelig i original versjon. En komponent er ute av produksjon. Den er imidlertid erstattet med et annet produkt eller andre tilgjengelige erstatningsprodukter. Det ukjente artikkelnummeret får man ikke analysert.

Anslått livssyklus

Level	Description	Number of article numbers	As a per-centage	Quantity of items	Asset Value
6	Availability horizon > 5 years	25	96.2%	27	7,778 €
5	Availability horizon 2 to 5 years	0	0.0%	0	
4	Availability horizon 1 to 2 years	0	0.0%	0	
3	Availability horizon < 1 year	0	0.0%	0	
2	Item has been discontinued and no successor has been defined; repair or replacement may be possible to a limited extent	0	0.0%	0	
1	Unknown article number	1	3.8%	1	
	Total	**26**		**28**	**7,778 €**



Figur 22: Viser anslåtte livssyklus for alle komponenter som er registrert

25 av komponentene vil være tilgjengelige i minst 5 år. Altså vil alle komponentene i anlegget utenom den ukjente komponenten være tilgjengelige i lang tid framover.

Leveringstid

Level	Group (delivery days)	Number of article numbers	As a per-centage	Quantity of items	Asset Value
7	Delivery time 1 until 4 days	11	42.3%	11	6,485 €
6	Delivery time 5 until 10 days	13	50.0%	15	1,293 €
5	Delivery time 11 until 30 days	1	3.8%	1	
4	Delivery time > 30 days	0	0.0%	0	
3	Delivery time on request	0	0.0%	0	
2	Items no longer available; Repair or replacement possible to a limited extent	0	0.0%	0	
1	Unknown article number	1	3.8%	1	
	Total	**26**		**28**	**7,778 €**

Figur 23: Viser leveringstiden for alle komponentene

11 av komponentene har leveringstid på mellom 1 og 4 dager. 13 av komponentene har leveringstid mellom 5 og 10 dager. En annen komponent har leveringstid på mellom 11 og 30 dager. Det er viktig å finne ut om komponentene med lang nedetid er kritiske komponenter ettersom dette kan føre til lang nedetid av anlegget.

Lagertilgjengelighet

Level	Description	Number of article numbers	As a per-centage	Quantity of items	Asset Value
6	The article number installed in the plant that is available in the warehouse	0	0.0%	0	
5	The article number installed in the plant that is not available in the warehouse	24	92.3%	26	6,898 €
4	The article number installed in the plant that is not available in the warehouse and will be discontinued within a year	0	0.0%	0	
3	The article number installed in the plant that is not available in the warehouse and repair or replacement is possible to a limited extent	1	3.8%	1	880 €
2	The unknown article number installed in the plant that is available in the warehouse	0	0.0%	0	
1	The unknown article number installed in the plant that is not available in the warehouse	1	3.8%	1	
	Total	**26**		**28**	**7,778 €**

Figur 24: Viser lagertilgjengeligheten av alle komponentene

Analysen viser at 24 av komponentene er ikke tilgjengelig i varehuset. Dette er fordi anlegget vårt ikke har noe lager og denne informasjonen vil derfor ikke være relevant for oss. Det er imidlertid et eksempel på hvordan programmet ville fungert i et anlegg for en kunde som har et lager.

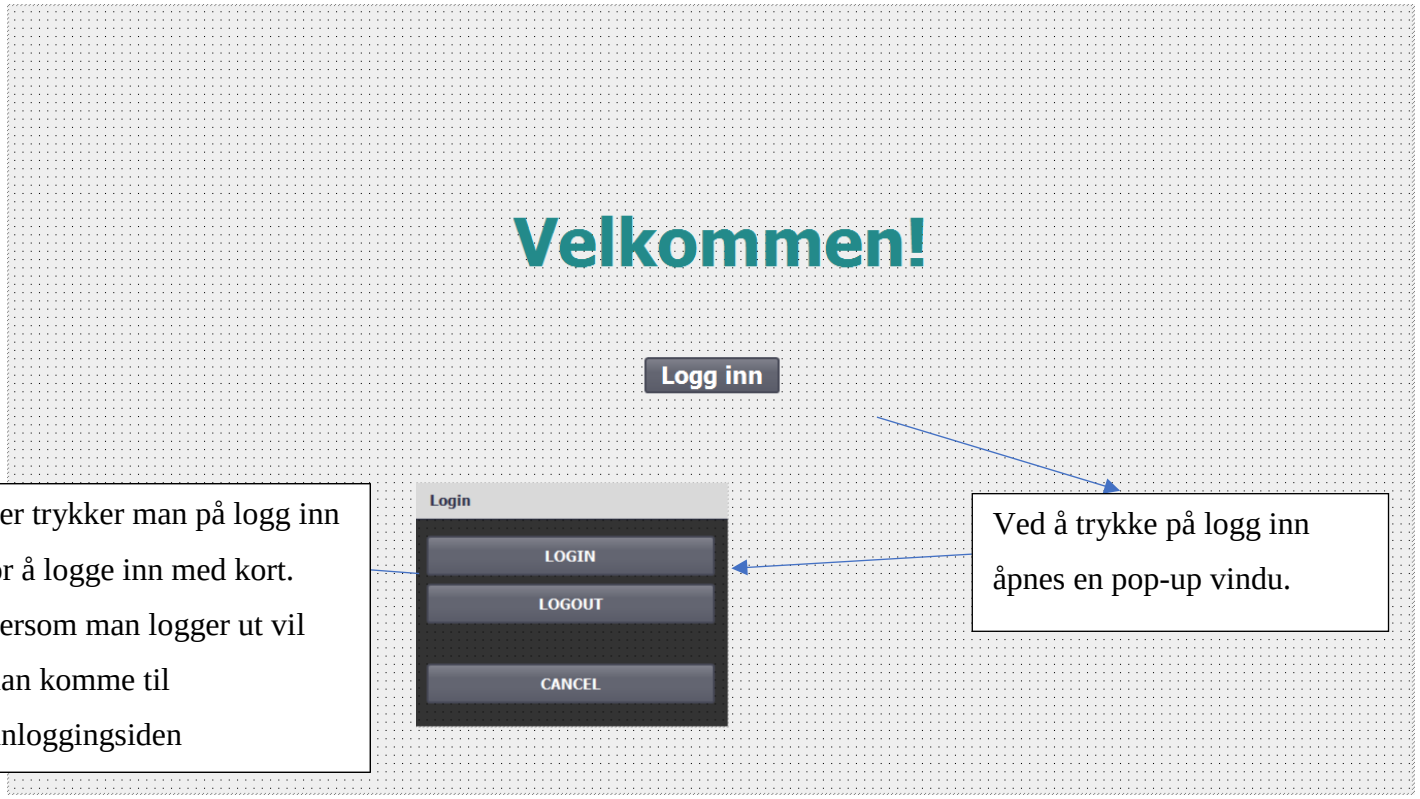
9 HMI

Det ble programmert et HMI fra forrigeårsstudenter for at maskinoperatører skal kunne ha muligheten til å styre maskinen manuelt. HMI som ble brukt på dette prosjektet er av typen «SIMATIC TP1500 Comfort Pro Touch-panel».

Forrige årets studenter har skrevet en brukermanual på hvordan deres HMI blir brukt, dette finner dere under vedlegg med navn [03.001 – HMI brukermanual]. Vi har oppgradert systemene deres og skal i dette kapittelet beskrive kort hva vi har endret.

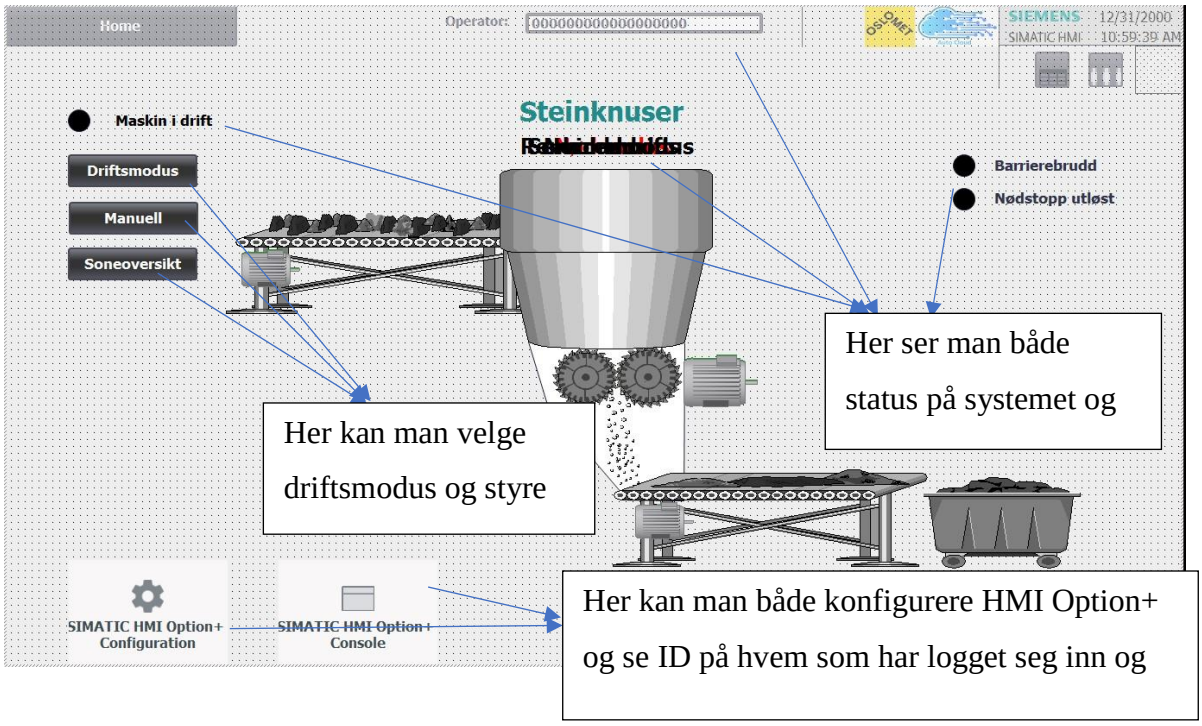
9.1 Skjermbilder

For å logge inn trykker man først logg inn på HMI og deretter skanner man et kort med et unik UID nummer. Hver person har sitt eget kort med et unik UID nummer i kortet. Etter at brukeren har logget inn kommer man inn på hovedmenyen. Øverst til høyre på skjermen kan man se navnet på den som er logget inn.



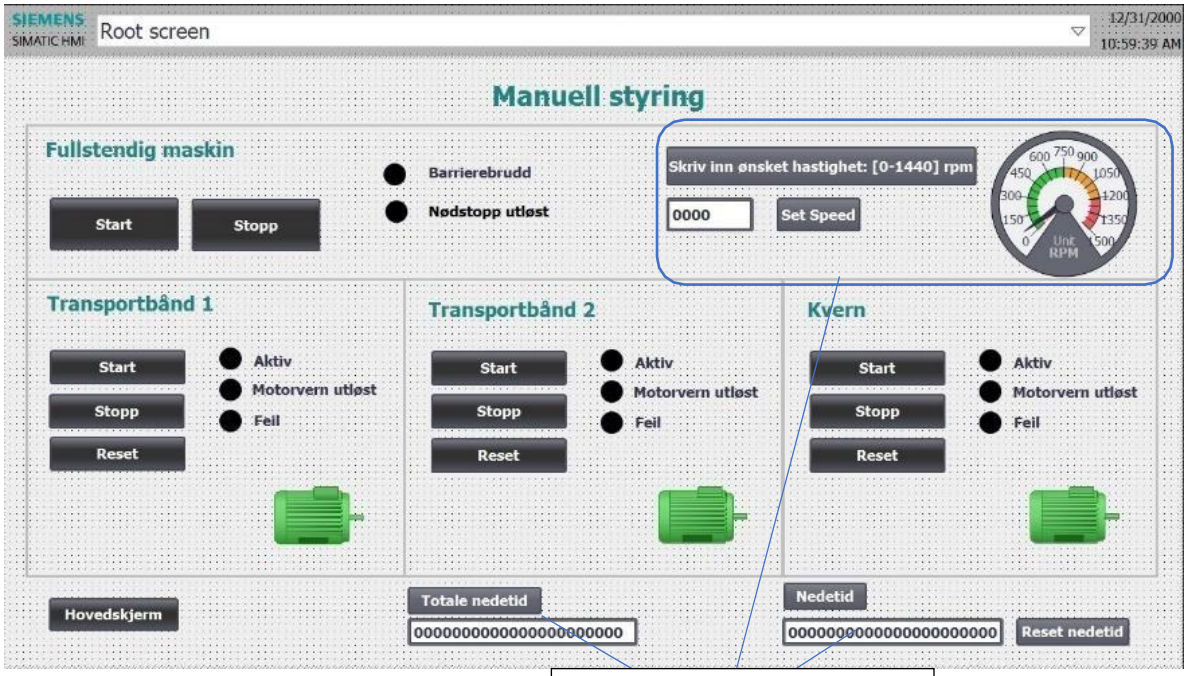
Figur 25 Innlogging

Etter å ha logget inn vil man komme til steinknuser siden hvor man kan se driftsstatus og kan velge driftsmodus, se soneoversikt og styre maskinen manuelt. Vi skal ikke på detaljer på hvordan man gjør dette i og med at det er gjort av forrige årets studenter og de har skrevet en detaljert brukermanual på det de har gjort.



Figur 26 Steinknuser oversikt

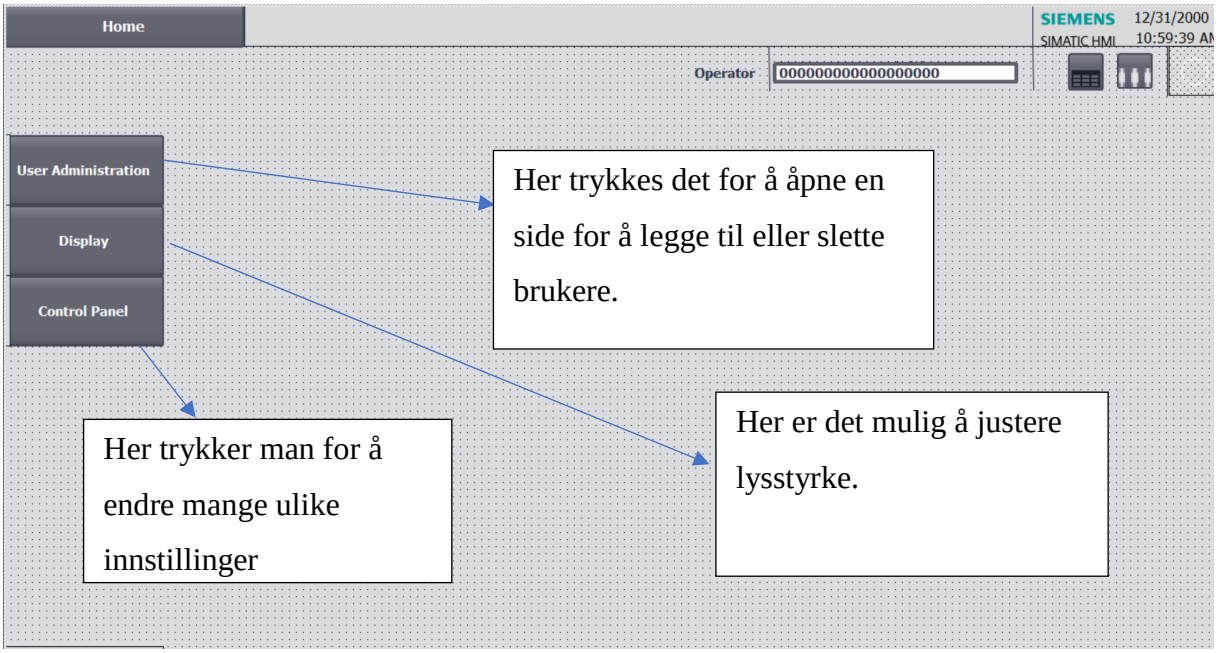
Etter at bruker har valgt «Manuell styring» kan brukeren kontrollere transportbånd 1 og 2, kvern og stille inn hastighet på kvern. Transportbånd 1 og 2 og kvern kan kontrolleres ved å trykke «start» og «stop». Bruker trykker «reset» dersom det har skjedd en feil i systemet og maskinen må startes på nytt etter å ha blitt reparert. Det gir også informasjon om nedetid og totale nedetid med mulighet for resetting av nedetid.



Figur 27 Manuell styring

Disse er endringene vi har lagt til

For å unngå at uvedkommende for tilgang til anlegget er det en regel om at man alltid må logge seg ut etter bruk. Hvis brukeren glemmer dette, vil det etter 60 minutter med inaktivitet skje en automatisk utlogging. Man kan også velge å ha en annen løsning der man må holde kortet mot kortleseren hele tiden for å holde seg innlogget, og med en gang kortet tas vekk fra kortleseren, logger brukeren seg ut. På grunn av at vi ikke har en kortholder til kortleseren valgte vi ikke denne løsningen.



Figur 28: Display

Under «user administration» er det mulig for administrator å legge til eller slette brukere. Dette kan kun administratorene gjøre. De ulike brukerne har altså ulike sikkerhetsnivå.

Under «control panel» er det mange ulike innstillinger. Her kan man endre på f.eks. utloggingsprosessen, der man velger om man skal trykke «logg ut» på skjermen eller logges ut med en gang kortet fjernes fra kortleseren.

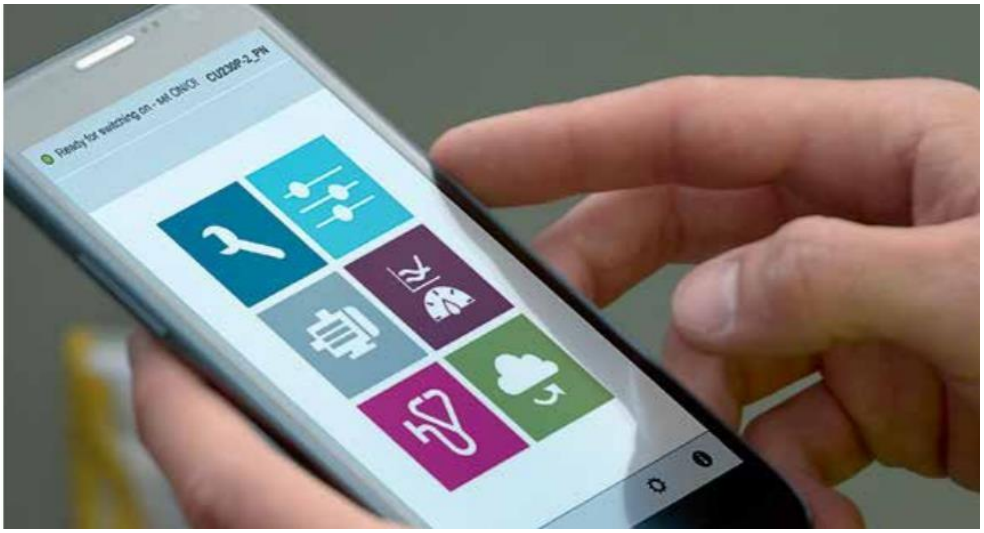
Under “Display” er det mulig å justere lysstyrken på skjermen.

10 G120 Smart WiFi Access

Siemens ønsket at vi skulle teste ut det nye programmet, Sinamics G120 Smart Access, og vi installerte det derfor på driven. Sinamics G120 Smart Access er en modul som gjør det mulig å koble seg trådløst til driven på alle bærbare enheter. Gjennom tilkobling til Wi-Fi, transformerer du din mobil eller laptop om til et virtuelt operatørpanel. Da kan du fra telefonen din få inn sanntidsdata som motorfart, spenning, temperatur, du kan dele data til andre enheter eller justere parametere. En av de største fordelene med denne løsningen er muligheten til å trådløst koble seg til anlegg med plassering som gjør fysisk tilgang til anlegget vanskelig.

10.1 Installering

Set-up av programmet er en rask prosedyre. Det er ingen app som må lastes ned for å få tilgang fra mobile enheter. For installasjon følges et enkelt steg for steg manual. Se vedlegg [12.002 – SINAMICS G120 Smart Wifi Access] for manualen. Etter installasjonen er fullført kobles en ny enhet raskt til ved å koble seg til Wi-Fi og deretter skrive inn IP-adressen i nettleseren. Dersom du har flere smart access moduler i anlegget er det mulig å endre navn på hver moduls Wi-Fi, slik at du har oversikt over hvilket Wi-Fi som tilhører hvilken modul. Du kan også endre passord.



Figur 29: Viser bildet av hvordan nettsiden ser ut på G120 Smart Wifi Access [17]

10.2 Bruk

Grunnleggende idriftsettelse

Under modulen Basic Commissioning kan du igangsette driven ved å angi data som fart på motoren og tilkobling. Du kan også velge «restore to factory settings» dersom du ønsker å resette programmet.

Kontrollpanel

Under «Control panel» kan du sette motordata som maksfart, minimumsfart og maks akselerasjon når settpunkt for fart endres.

Parametere

Under «parameters» har du oversikt over parameter verdier som fart, spenning, strøm, temperatur m.m. For å finne riktig parameter kan du søke etter og filtrere parametere. Du kan endre parameterverdier og lagre relevante parameterverdier til drive eller til Smart Access Module i en tilpasset liste. Det er også mulig å resette alle eller spesifikke parametere tilbake til fabrikkinnstillinger.

Diagnostisering

Under «diagnostics» kan brukeren få oversikt over alle de siste feil og alarmer i anlegget. Du kan også sjekke status på alle inputs og outputs og status bits.

Back-up

Under “Back-up and restore” kan du ta back-up av parameterverdier og laste det ned. Under «restore» kan du laste opp, laste ned slette eller gjenopprette eksisterende filer.

Overvåking

Under “Monitoring” kan du få oversikt over data som fart, spenning, settpunkt, temperatur m.m.

10.3 Styrker og svakheter

Fordelen med programmet er at det er enkelt og raskt å få tilgang til anlegget i stedet for å måtte koble seg til gjennom PC. Dersom anlegget har en plassering som gjør fysisk tilgang til anlegget vanskelig, er det en fordel å raskt kunne bruke programmet til å koble seg til. Anlegget kan for eksempel være plassert i et område som har risikoer som eksplosjonsfare, der du må følge strenge sikkerhetsrutiner for å få tilgang. Å heller kunne koble seg trådløst til fra telefonen i slike situasjoner kan derfor være en stor fordel.

En av svakhetene er at programmet ikke har nok kapasitet til å brukes i store anlegg. Da kan du altså ikke styre eller bruke commissioning, men du har fortsatt mulighet til å overvåke parameterne i anlegget.

Ved rask og enkel tilgang til anglegget økes også risikoen for at uvedkommende får tilgang til anlegget. Uvedkommende trenger nemlig kun Wi-Fi passord og IP adresse for å få tilgang. Da får hackere for eksempel mulighet til å endre motorfart eller endre på andre parametere i anlegget.

11 Diskusjon

11.1 MindSphere

Vi har laget et dashbord som det er mulig å se verdier direkte fra PLS-systemet. Disse verdiene kan man se fra MindSphere-plattformen – det vil si at de er tilgjengelig hvor enn du er i verden.

Fordelene med dashbord er at vi har en kontinuerlig datastrøm som sørger for at man har sanntidsoversikt over KPI'ene som er valgt. Dette gir anleggseier muligheten til å agere ved eventuelt uhell som gjør at PLS-systemet er nede.

En annen fordel er at det er mulig å hente data direkte fra nettet og visualisere dette på applikasjonen. Som eksempel visualiserte vi været i Oslo direkte fra en nettside.

Andre fordeler er at det er oversiktlig og gir muligheten til å lage flere dashbord tilpasset til ulike brukere – det vil si at man kan ha dashbord for økonomi ansvarlig, produksjonsansvarlig osv. Simatic Performance Insight gir deg også muligheten til å ha grensesnitt for advarsel og alarm.

Det gir oss også muligheten til å lage våre egne matematiske variabler direkte i applikasjonen. Det fører til at man ikke trenger å programmere alt på PLS-systemet.

Noen av ulempene til MindSphere og deres applikasjoner er at man av og til blir frakoblet grunnet feilmeldinger i deres system. Vi opplevde at applikasjonen Simatic Performance Insight var nede i to-tre dager grunnet en feilmelding som bare utviklerne kunne løse. Dette kan bli problematisk for anleggseiere dersom det forekommer ofte.

En annen ulempe med Simatic Performance Insight er at applikasjonen er helt ny og dermed er det begrenset med at det bare er mulig å fremstille tall via graf eller tall. Det er for eksempel ikke mulig å vise det frem med sektordiagram, søylediagram osv.

Det er heller ikke mulig å varsle med melding eller mail dersom en av alarmene går, grunnen til dette er at applikasjonen er helt nytt og denne funksjonen er ennå ikke blitt lagt til.

11.2 Cyber Security

Vi har valgt to ulike tiltak for å sikre anlegget. Disse er som nevnt tidligere RFID-kortleser og plugger i PLS-systemet.

11.2.1 RFID-kortleser

Fordelen og grunnen til at vi valgte RFID-kortleser er at det sørger for å oppnå sikkerhetsnivå 2. Det gir ett unikt UID som gjør at bare ansatte med kort kan logge seg inn i systemet og gjøre endringer. I tillegg er det bare administrator som kan endre på brukere og legge til flere brukere, som gir en oversikt over hvem som har tilgang til systemet.

En annen fordel er at man kan se hvem som har logget seg inn og ut, dersom noe uønsket skulle skje, er det mulig å identifisere personen som har vært logget inn sist. For å øke tryggheten så er det lagt inn et back-up-system som automatisk logger seg av systemet etter 60 minutter.

Det finnes andre tiltak som kunne ha sørget for å sikre anlegget enda bedre, men vi er avgrenset til å bruke Siemens sine produkter og vi er økonomisk begrenset, dermed ble denne løsningen den mest optimale.

Ulempene med RFID-kortleser er at ansatte kan bli frastjålet eller miste kortet, dette er et problem i og med at andre kan logge seg inn på systemet. Vi anbefaler derfor at dersom ansatte mister kortet bør det rapporteres til administrator for å slette bruker fortest mulig.

En annen ulempe er at dersom systemet er nede er det ingen andre metoder å logge seg inn på systemet. Dette kan skape problemer og det bør opprettes en annen innloggingsmetode.

11.2.2 Plugger i PLS-systemet

Fordelen med å ha plugger i PLS-systemet er at ingen får tilgang til å koble seg direkte inn til nettverksanlegget. Det vil si at det ikke blir mulig for inntrengere å laste opp virus og andre skadelige programvarer.

Ulempe med plugger at dersom nøkkelen for å åpne disse pluggene ikke er tilstede vil man ikke få mulighet til å bruke inngangs/utgangs-porter på systemet.

En annen ulempe er at de fleste plugger har universal nøkkel – det vil si at det kan være mulig å åpne disse pluggene dersom man har tilgang til denne nøkkelen.

11.3 AOS

Fordeler med programmet er at det gir kunden en rask oversikt over tilgjengelighet på ulike komponenter, samt hvilke komponenter som bør vurderes å ha på lager for å unngå nedetid.

En svakhet ved analysen er at programmet ikke vet hvilke komponenter som er nødvendige for at anlegget skal fungere. Det hadde vært nyttig om programmet kunne gi informasjon om dette slik at kunden på forhånd vet hvilke komponenter det er viktig å ha på lager og hvilke komponenter som er mindre viktige. Det er samtidig komplisert å lage et program som kan skille ut hva som er kritiske komponenter ettersom dette kan variere fra anlegg til anlegg.

En annen svakhet er at programmet ikke viser komponentene fra andre leverandører enn Siemens.

Det er heller ingen anbefaling av pris. Siemens kunne for eksempel ha informert om komponenter som er på vei ut av produksjon og anbefalt kunden å kjøpe disse nå. Dette fordi det ofte blir vanskeligere å få tak i disse modellene fordi de blir tatt ut av produksjon.

12 Konklusjon

12.1 MindSphere

For å sikre anlegget til kunden kontinuerlig bruker vi dashbord i SPI. MindSphere har den fordelen at den får en kontinuerlig datastrøm (eksempelvis KPI-er som er valgt) fra PLS-systemet som kan visualiseres på visualiseringsapplikasjoner i MindSphere, for eksempel SPI eller FM. Dette gir anleggseier mulighet til å se driftsstatusen for anlegget og agere hvis uønskede nedetid oppstår. Dette sikrer at anlegget til kunden er kontinuerlig i drift. MindSphere har muligheten til å lage flere dashbord til ulike brukere som eksempelvis økonomi- og produksjonsansvarlig. Dette gjør det enkelt å tilpasse dashbordene til ulike kundegruppers behov. Simatic Performance Insight gjør det mulig å aktivere en alarm når et gitt grensesnitt er nådd slik at brukeren får en advarsel dersom noe er galt med anlegget.

Som nevnt tidligere er ulempen med MindSphere og dets applikasjoner at man av og til blir frakoblet grunnet feilmeldinger i systemet. I tillegg er ikke systemet mobilvennlig.

Slik vi ser det er MindSphere fortsatt i utviklingsfasen. Vi anbefaler derfor at det jobbes mer med å sørge for at systemet ikke har nedetid og at MindSphere-plattformen gjøres mer brukervennlig for mobil. I tillegg bør SPI oppgraderes med følgende funksjoner:

- utsendelse av SMS eller mail dersom alarm blir aktivert
- økt mobilvennlighet
- flere graftyper som eksempelvis søylediagram, sektordiagram osv.
- videreutvikling av brukervennlig manual

MindSphere er en god løsning når det gjelder å sikre en kontinuerlig overvåking av anlegget og for å kunne se dataene i sanntid. Dette fører til at anleggseier til enhver tid har kontroll over anlegget slik at driften opprettholdes.

12.2 Cyber Security

I denne delen av oppgaven gjennomførte vi en grundig risikoanalyse av anlegget, og det ble bestemt at anlegget skal sikres på sikkerhetsnivå 2. På nivå 2 er det vedtatt at RJ45 plugger skal implementeres i anlegget. Pluggene gjør det vanskeligere for andre å koble seg inn i nettverksinngangene til PLS-systemet. Det kreves en nøkkel for å låse ut pluggene.

Det er også vedtatt at det kreves et log-in system for å koble til anleggets HMI. Det er derfor implementert en RFID-kortleser som krever et fysisk nøkkelkort for å få tilgang til HMI. Dette gjør at man får oversikt over hvem som har tilgang til HMI, og at systemet logger UID-nummeret til kortene som blir brukt - det blir altså mulig å finne ut hvem som har vært logget inn på systemet dersom noen av de ansatte skulle velge å sabotere systemet.

Kontrollrommet er inngjerdet og har kameraovervåkning. Dette beskytter anlegget mot uønskede personer. Ved å følge standarden IEC62443 minsker man sannsynligheten for at anlegget opplever dataangrep, noe som kan spare bedriften for betydelige beløp.

I tiden fremover vil flere selskaper oppleve å bli utsatt for uønsket angrep. For å forhindre slike angrep må standardene videreutvikles og dette er et arbeid som vil pågå kontinuerlig. Vi anbefaler derfor at Siemens fokuserer på Cyber Security og utvikler god kompetanse på området.

12.3 AOS

AOS-rapporten gjør det mulig å få oppdateringer om levetiden og leveringsrisikoen til de kritiske komponentene i anlegget. Det gir også mulighet til å se varelageret der delene befinner seg slik at man får kjennskap til om lageret trenger påfyll. Dette fører til at det alltid er mulig å skifte ut slitne deler slik at risikoen for driftsstans og unødvendig dødtid blir så liten som mulig. Dette sparer anleggseieren for unødvendige kostnader og tidsbruk.

En videreutvikling av AOS kan være at programmet på forhånd gir informasjon om hvilke av anleggets «livsviktige» komponenter som må skiftes ut for å unngå driftsstans og pris indikator på hvor mye det kan koste anleggseier å kjøpe ny eller oppgradere systemet. Det bør også gi informasjon om mindre viktige komponenters tilstand, slik at anleggseier ikke trenger å fokusere på mindre viktige komponenter som ikke vil føre til driftsstans.

Slik AOS-rapporten er i dag kan den brukes til å få oversikt over komponenter i anlegget og på varelager, og i tillegg få oppdatering over hvilke deler som bør skiftes ut.

13 Kilder

[1] Siemens. (u.å). This is MindSphere. Retrieved from https://new.siemens.com/global/en/products/software/mindsphere.html

[2] BBC. (2018, 15. februar). UK and US blame Russia for 'malicious' NotPetya cyber-attack. Retrieved from https://www.bbc.com/news/uk-politics-43062113

[3] NDLA. (2018, 5. april). Felles standarder. Retrieved from https://ndla.no/subjects/subject:6/topic:1:182078/topic:1:168371/resource:1:166429

[4] NEK. (2016, 1. august). IEC62443-serien. Retrieved from https://www.nek.no/manedens-standard-august-2016/

[5] Rausland, M., & Utne, I. B. (2009). *Risikonalyse -teori og metoder* (2 ed.). Bergen: Fagbokforlaget.

[6] Parmenter, D. (2015). Key Performance Indicator. 7-7. Retrieved from https://jadoobi.com/wp-content/uploads/2018/03/Parmenter-David-Key-performance-indicators-_-developing-implementing-and-using-winning-KPIs-Wiley-2015.pdf **[Lagt til som Vedlegg nr. 31]**

[7] NDLA. (2018, 18. september). Kvalitetssikringsprosessen. Retrieved from https://ndla.no/subjects/subject:28/topic:1:58274/resource:1:123674

[8] FM45, FELTMONTERT C5E/B RJ45 PLUGG. Retrieved from https://i2.wp.com/westec.no/wp-content/uploads/2018/04/R320374.jpg?fit=350%2C253&ssl=1

[9] Siemens. (u.å). A Breaking-down Picture of MindSphere. Retrieved from http://w2.siemens.com.cn/stories/StoryShow/FindStory/137?culture=enUS&sourceId=1

[10] Tek. Ordbok. Retrieved from https://www.tek.no/ordbok?letter=S

[11] IP-Calculator. (2005). Retrieved from http://jodies.de/ipcalc?host=192.168.1.1&mask1=24&mask2=

[12] Siemens. (2017). RFID systems SIMATIC RF1060R Retrieved from https://www.siemens-pro.ru/docs/rfid/BA_RF1060R_76_en-US.pdf **[Lagt til som Vedlegg nr. 24]**

[13] Siemens. (2019). SIMATIC HMI Option+. Retrieved from https://cache.industry.siemens.com/dl/files/400/109754400/att_970495/v2/109754400_SimaticHmiOptionPlus_V20_DOC_en.pdf **[Lagt til som Vedlegg nr. 27]**

[14] Siemens. Asset Optimization Services. Retrieved from https://cache.industry.siemens.com/dl/files/772/90001772/att_764045/v2/Asset_Opt_Services_Customer_Presentation_en.pdf **[Lagt til som Vedlegg nr. 30]**

[15] Tecno PLC. IOT INDUSTRIAL MINDSPHERE Y TCS UNEN FUERZAS. Retrieved from http://www.tecnoplc.com/iot-industrial-mindsphere-tcs/

[16] Blaja Automation Portal. Retrieved from https://www.blaja.cz/ruzne/identifikacni-system-rfid-spolecnosti-siemens.html

[17] Siemens. (u.å). SINAMICS G120 Smart Access. Retrieved from https://www.industry.usa.siemens.com/drives/us/en/electric-drives/ac-drives/standard-drives/sinamics-g120-vector-drive/Documents/SINAMICS_G120-Smart_Access-brochure.pdf **[Lagt til som Vedlegg nr. 28]**

[18] STANDARD, I. (2019). "IEC 62443-2-1." Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program: p. 42-46. **[Konfidensielt]**

[19] STANDARD, I. (2019). "IEC 62443-2-1." Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program: p. 36. **[Konfidensielt]**

[20] STANDARD, I. (2019). "IEC 62443-2-1." Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program: p. 56. **[Konfidensielt]**

[21] Siemens (2019). "IEC62443 Compliance Asessment." p. 11. **[Konfidensielt]**

[22] STANDARD, I. (2019). "IEC 62443-2-1." Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program: p. 43. **[Konfidensielt]**

[23] Siemens (2019). "IEC62443 Compliance Assessment " Example Questions from Standard IEC62443-3-3 and IEC 62443-2-1: p. 4-10. **[Konfidensielt]**

[24] STANDARD, I. (2019). "IEC 62443-2-1." Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program: p. 46-52. **[Konfidensielt]**

[25] STANDARD, I. (2019). "IEC 62443-2-1." Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program: p. 52. **[Konfidensielt]**

[26] STANDARD, I. (2019). "IEC 62443-2-1." Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program: p. 54. **[Konfidensielt]**

[27] STANDARD, I. (2019). "IEC 62443-2-1." Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program: p. 55-56. **[Konfidensielt]**

[28] STANDARD, I. (2019). "IEC 62443-2-1." Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program: p. 56-70. **[Konfidensielt]**

[29] E24. (2019). "Cyberangrep koster opptil 450 millioner." Retrieved from https://e24.no/boers-og-finans/norsk-hydro/cyberangrep-har-kostet-hydro-opptil-450-millioner/24612353?fbclid=IwAR0GCONbL2mPoKhMH7qUu9GdDLkhid_WM7uZD1uisml88U7gdtlnlYzhWFI

14 Vedlegg

[0] 03.001 – HMI brukermanual(forrigeårets studenter)

[1] 04.000 - Kundens kravspesifikasjon

[2] 04.001 - Leverandørens designspesifikasjon

[3] 04.002 - DesignavKontrollrom

[4] 04.003 - AOS

[5] 04.004 - Sjekkliste

[6] 04.005 - Avviksrapport

[7] 04.006 - KontrollromEtterTiltak

[8] 04.007 - Utstyrsliste modell

[9] 05.006 - Flytskjema Økonomi

[10] 05.007 - Flytskjema Produksjon

[11] 05.008 - Flytskjema Status

[12] 05.009 - Frekvensomformer

[13] 05.010 - Simatic Performance Insight

[14] 06.000 - Cyber Security IEC62443 Håndbok

[15] 06.030 – Motor

[16] 07.006 - CompressedMLFB

[17] 02.000 - Cyber - Sec. - IEC62443_v2 **[Konfidensielt]**

[18] 02.001 - IEC 62443_2_1 **[Konfidensielt]**

[19] 02.002 - IEC 62443_3_3 **[Konfidensielt]**

[20] 02.003 - IEC62443_Report_EN_Example_Obfuscated_v1.0 **[Konfidensielt]**

[21] 02.004 - IEC62443 **[Konfidensielt]**

[22] 02.005 - Spm Assessment Restricted **[Konfidensielt]**

[23] 12.002 - RF1060R USB reader 6GT28316AA50_datasheet_en

[24] 12.003 - RFID_SIMATIC_1060R

[25] 12.004 - User login with RFID Card Reader

[26] 12.005 - Manual_MindSphere_GettingStarted_en

[27] 12.006 - Simatic HMI option+

[28] 12.010 - SINAMICS G120 Smart Access brosjyre

[29] 12.011 - SINAMICS G120 Smart Access installering

[30] 13.000 – AOS

[31] 13.001 – KPI_Bok_D.P