Sikker kommunikasjon og sertifikathåndtering i byggautomasjon med Tailscale og OPC UA



Figur : Illustrasjon av Wago PLS og HMI skjem. Hentet fra wago.com

Avsluttende rapport skrevet av Espen Klippenberg Bø

Dato: 19.04.2025

# Sammendrag

Denne rapporten dokumenterer et prosjekt som opprinnelig hadde som mål å automatisere OPC UA-sertifikathåndtering i byggautomasjonssystemer for å forbedre sikkerhet og effektivitet. Prosjektet fokuserte på en WAGO CC100 PLS programmert i Codesys 3.5, og implementering av OPC UA-kommunikasjon.

Underveis i arbeidet ble det oppdaget at WAGO CC100 ikke har innebygd støtte for Global Discovery Server (GDS), som er en kritisk komponent for sentralisert sertifikathåndtering. Dette førte til en revidering av problemstillingen, med fokus på bruk av VPN for å sikre kommunikasjon mellom PLS og SCADA-system, samt automatisert oppdatering av sertifikater for nettsiden til PLS-en.

Prosjektet resulterte i en løsning hvor Tailscale VPN ble brukt for å sikre kommunikasjon mellom PLS og SCADA. Det ble utviklet et skript for automatisk installasjon av Tailscale på WAGO CC100 samt et skript for oppdatering av sikkerhetssertifikater for HTTPS. Disse tiltakene sikrer en kryptert kommunikasjonskanal og reduserer behovet for manuell sertifikathåndtering.

Rapporten beskriver metodevalg, testoppsett og de tekniske utfordringene som ble møtt. Videre diskuteres alternative løsninger og anbefalinger for framtidig utvikling.

Figur : Bilde som illustrerer et sammendrag – Generert Bing image creator

# Revisjonshistorikk

|  |  |  |  |
| --- | --- | --- | --- |
| Dato | Versjon | Beskrivelse | Forfattere |
| <05/03/25> | <0.1> | Første versjon | Espen Klippenberg Bø |
| <08/03/25> | <0.2> | Andre versjon | Espen Klippenberg Bø |
| <10/03/25> | <0.3> | Tredje versjon | Espen Klippenberg Bø |
| <17/03/25> | <0.4> | Fjerde versjon | Espen Klippenberg Bø |
| <17/04/25> | <0.5> | Femte versjon | Espen Klippenberg Bø |
| <19/04/25> | <0.6> | Sjette versjon | Espen Klippenberg Bø |

# Akronymer og definisjoner

|  |  |
| --- | --- |
| API | Et grensesnitt som lar ulike programmer eller systemer kommunisere og utveksle data på en standardisert måte. (application programming interface) |
| BACnet Secure Connect (BACnet/SC) | En sikker kommunikasjonsprotokoll for bygningsautomasjon som bruker TLS-kryptering for å beskytte datautveksling mellom enheter i BACnet-nettverk over IP. |
| Byggautomasjon | Integrert styring, overvåkning og optimalisering av tekniske systemer i bygg, som ventilasjon, varme, lys og sikkerhet, for å sikre energieffektiv drift og et optimalt inneklima. |
| CA-tjenester | Systemer som utsteder, verifiserer og administrerer digitale sertifikater for å sikre autentisering og kryptering i elektronisk kommunikasjon. |
| Codesys | Programmvare for programmering av PLSer og HMI paneler. |
| Databaser | Strukturerte systemer for lagring, organisering og søk av data, som gjør det mulig å effektivt håndtere og gi tilgang til store mengder informasjon. |
| Driftsansvarlige | Personer som overvåker og styrer den daglige driften av tekniske installasjoner, som ventilasjon, varme og sikkerhetssystemer, for å sikre optimal ytelse og stabilitet. |
| e!COCKPIT | WAGOs ***e!****COCKPIT*-automatiseringsprogramvare |
| Eiendomsforvaltere | Administrerer og vedlikeholder bygninger og tekniske systemer, og er ansvarlige for økonomisk og operasjonell forvaltning av eiendommer for eiere eller investorer. |
| Eiendomseiere | Enkeltpersoner eller selskaper som eier bygninger og infrastruktur, og har økonomisk og strategisk interesse i effektiv drift, vedlikehold og sikkerhet av sine eiendommer. |
| HMI | Brukerinterfacer for å vise data og kontrollere systemet. Lokal skjerm. (human-machine interface) |
| IIoT | Et nettverk av sammenkoblede enheter, maskiner og sensorer som samler inn, utveksler og analyserer data i sanntid for å optimalisere produksjon, drift og vedlikehold. |
| IT-ansvarlige | Har ansvaret for drift, vedlikehold og sikkerhet av IT-infrastruktur, inkludert nettverk, servere og datasystemer, for å sikre stabil og sikker digital drift. |
| KNX | En global standard for bygningsautomasjon som gir enkel kommunikasjon mellom ulike produsenter og systemer som belysning, varme, persienner og sikkerhet. |
| KNX Secure | |  | | --- | |  |   En sikkerhetsutvidelse for KNX- protokollen som benytter AES-128-kryptering for å sikre kommunikasjon mellom KNX-enheter mot uautorisert tilgang og manipulasjon. |
| OPC UA | En standardisert kommunikasjonsprotokoll for sikker og plattformuavhengig datautveksling mellom industrielle systemer, sensorer og IT-systemer. |
| OT | Refererer til systemer og maskinvare som brukes for å overvåke, styre og automatisere industrielle prosesser, inkludert byggautomasjon, produksjonsanlegg og kritisk infrastruktur. |
| OT-ansvarlige | Personer eller team som har ansvar for drift, vedlikehold og sikkerhet av OT-systemer, med fokus på å sikre stabil, effektiv og sikker drift av industrielle kontrollsystemer og automatiseringsnettverk. |
| PKI-basert | Et system for administrasjon av digitale sertifikater og krypteringsnøkler, som sikrer autentisering, integritet og konfidensialitet i elektronisk kommunikasjon. |
| PLS | En programmerbar logisk styring er en datamaskin som brukes i industrien for å automatisere oppgaver som produksjon og kontroll av for eksempel nivåer i siloer/tanker. PLSen har tatt over oppgavene som hundrevis eller tusenvis av releer gjorde i industrien før og kan programmeres til å gjøre det samme. |
| SCADA | Større overvåkningssystemer som samler og analyserer data fra flere bygningskomponenter. (supervisory control and data acquisition) |
| SD-anlegg | Et system for overvåking, styring og automatisering av tekniske installasjoner i bygg. Består ofte av SCADA-system, ventilasjonsanlegg, PLS-er, sensorer osv. (Sentral driftskontroll anlegg) |
| Sensorer | Måler data som temperatur, luftkvalitet, lysstyrke og trykk. |
| Sikkerhetsansvarlige | Fagpersoner som har ansvaret for å beskytte IT-systemer, bygningsautomasjon og fysiske anlegg mot uautorisert tilgang, cyberangrep og andre sikkerhetsrisikoer. |
| Systemintegratorer | Fagpersoner som designer, implementerer og vedlikeholder automasjonsanlegg som inneholder PLS, HMI, KNX, ventilasjonsanlegg, varmeanlegg og sensorer. |
| UaExpert | Test klientprogram for å teste OPC UA klienter |
| UaGdsConfigurationTool | GDS server og konfigurasjons program |
| Varmesentraler | Sentrale anlegg som produserer og distribuerer varme til et bygg, ofte ved hjelp av varmepumper, fjernvarme eller el/olje-kjeler. |
| Ventilasjonsanlegg | Systemer som regulerer luftkvaliteten i et bygg ved å styre tilførsel og utskifting av luft. |

Figur : Akronymer og tekniske uttrykk med forklarende definisjon

Innhold

[1 Sammendrag 2](#_Toc195973947)

[2 Revisjonshistorikk 3](#_Toc195973948)

[4 Akronymer og definisjoner 4](#_Toc195973949)

[6 Figurer og tabeller 9](#_Toc195973950)

[7 Introduksjon og motivasjon 11](#_Toc195973951)

[8 Problemstilling 12](#_Toc195973952)

[8.1 Uforutsett hendelse 12](#_Toc195973953)

[8.2 Den reviderte problemstillingen ble derfor: 12](#_Toc195973954)

[8.2.1 Delmål: 12](#_Toc195973955)

[9 Teori 13](#_Toc195973956)

[9.1 Teori OPC UA og sikkerhetsmekanismer. 13](#_Toc195973957)

[9.1.2 Automatisert sertifikathåndtering i OPC UA 14](#_Toc195973958)

[9.2 Teori Tailscale Mesh VPN 16](#_Toc195973959)

[9.2.1 Hvordan Tailscale fungerer 16](#_Toc195973960)

[9.2.2 Fordeler med Tailscale 18](#_Toc195973961)

[9.2.3 Ulemper med Tailscale 18](#_Toc195973962)

[*9.2.3.2* *Begrenset lokal kontroll og åpen kildekode* 18](#_Toc195973963)

[9.2.4 Sikkerhetssertifikater i Tailscale 19](#_Toc195973964)

[9.3 Ignition SCADA 20](#_Toc195973965)

[10 Metode 26](#_Toc195973966)

[10.1 Utviklingsprosess 26](#_Toc195973967)

[10.1.1 Testoppsett 26](#_Toc195973968)

[10.2 Original problemstilling med OPC UA 28](#_Toc195973969)

[10.2.1 Evalueringskriterier OPC UA 28](#_Toc195973970)

[10.2.2 Arbeidsprosess manuell sertifikathåndtering 28](#_Toc195973971)

[10.2.3 Arbeidsprosess automatisk sertifikathåndtering 31](#_Toc195973972)

[10.2.4 Uforutsett hendelse 34](#_Toc195973973)

[10.2.5 Uforutsett hendelse og evalueringskriterier 36](#_Toc195973974)

[10.3 Veien videre etter at første problemstilling ikke fungerer 37](#_Toc195973975)

[10.4 Ny problemstilling med Tailscale VPN 37](#_Toc195973976)

[10.4.1 Evalueringskriterier for Tailscale-løsningen 37](#_Toc195973977)

[10.4.2 Arbeidsprosess med Tailscale VPN installasjon på PLS 37](#_Toc195973978)

[10.4.3 Kryptering 47](#_Toc195973979)

[11 Resultater / Produktbeskrivelse 49](#_Toc195973980)

[11.1 Infrastruktur og arkitektur 49](#_Toc195973981)

[11.2 Prosjektoversikt 50](#_Toc195973982)

[12 Diskusjon 52](#_Toc195973983)

[13 Konklusjon og anbefalinger 55](#_Toc195973984)

[13.1 Forstudie rammer 55](#_Toc195973985)

[13.1.1 Forstudierapporten (kap. 5–6) ble følgende definert som mål og rammer 56](#_Toc195973986)

[13.1.2 Prosjektet skal være nyttig for byggautomasjonsbedrifter og redusere driftskostnader og risiko 56](#_Toc195973987)

[13.1.3 Risikohåndtering og fleksibel prosjektstyring 56](#_Toc195973988)

[13.1.4 Kost/nytte 56](#_Toc195973989)

[14 Refleksjon rundt prosessen i prosjektet 58](#_Toc195973990)

[14.1 Hva kunne vært gjort annerledes? 58](#_Toc195973991)

[14.2 Refleksjon over utviklingsprosessen 58](#_Toc195973992)

[15 Hvordan har du håndtert utfordringer? 59](#_Toc195973993)

[16 Hva ville du gjort annerledes om du skulle gjort prosjektet igjen? 60](#_Toc195973994)

[17 Referanser 61](#_Toc195973995)

[18 Vedlegg 1 63](#_Toc195973996)

# Figurer og tabeller

[Figur 1: Illustrasjon av Wago PLS og HMI skjem. Hentet fra wago.com 1](#_Toc195980443)

[Figur 2: Bilde som illustrerer et sammendrag – Generert Bing image creator 2](#_Toc195980444)

[Figur 3: Akronymer og tekniske uttrykk med forklarende definisjon 6](#_Toc195980445)

[Figur 4: Tailscale mesh nettverk 16](#_Toc195980446)

[Figur 5: Tailscale mesh nettverk med subnet-router 17](#_Toc195980447)

[Figur 6: Ignition modul oversikt 20](#_Toc195980448)

[Figur 7: Ignition arkitektur 20](#_Toc195980449)

[Figur 8: Ignition perspective visualisering 21](#_Toc195980450)

[Figur 9: Basis arkitektur https://inductiveautomation.com/ignition/architectures 22](#_Toc195980451)

[Figur 10: Basis arkitektur med redundans 22](#_Toc195980452)

[Figur 11: Utvidet arkitektur med redundans 23](#_Toc195980453)

[Figur 12: Hub & Spoke 24](#_Toc195980454)

[Figur 13: Hub & Spoke med redundans 24](#_Toc195980455)

[Figur 14: IIoT arkitektur 25](#_Toc195980456)

[Figur 15: Cloud hybrid arkitektur 25](#_Toc195980457)

[Figur 16: Ignition logo 26](#_Toc195980458)

[Figur 17: uaExpert logo 26](#_Toc195980459)

[Figur 18: Wago logo 27](#_Toc195980460)

[Figur 19: Codesys logo 27](#_Toc195980461)

[Figur 20: Wago CC100 pls 27](#_Toc195980462)

[Figur 21: Tailscale logo 27](#_Toc195980463)

[Figur 22: Manuell sertifikathåndtering https://reference.opcfoundation.org/Core/Part2/v105/docs/9 28](#_Toc195980464)

[Figur 23: Wago oppsett av OPC UA i nettsiden til PLSen 28](#_Toc195980465)

[Figur 24: Koble seg til PLS 29](#_Toc195980466)

[Figur 25: Oppsett av sikkerhets sertifikat til PLSen i Codesys 3.5 29](#_Toc195980467)

[Figur 26: Oversikt over sikerhetssertifikater i PLS vises i Codesys 3.5 29](#_Toc195980468)

[Figur 27: Koble uaExpert til PLSen, og legg inn sertifikatet fra PLS inn uaExpert sin Trusted Certifikate. 30](#_Toc195980469)

[Figur 28: Flytt sertifikatet til uaExpert inn i PLSen sin Trusted Certificates. 30](#_Toc195980470)

[Figur 29: Kryptert kommunikasjon imellom PLS og uaExpert fungerer. 30](#_Toc195980471)

[Figur 30: Automatiserte sertifikathåndteringen https://reference.opcfoundation.org/Core/Part2/v105/docs/9 31](#_Toc195980472)

[Figur 31: Skjermbilde fra manualen til UaGDS https://www.unified-automation.com/ 31](#_Toc195980473)

[Figur 32: Skjermdump. Pull configuration for servers 32](#_Toc195980474)

[Figur 33: Skjermdump fra txxxxxxxx-OPCUA-Server-0en-1.pdf 33](#_Toc195980475)

[Figur 34: Discord. NFEA OPC UA #arkitektur-og-konnektivitet Post: OPC UA Global Discovery Server 34](#_Toc195980476)

[Figur 35: wago community svar på spørsmål om OPC UA GDS push https://www.wago.community/t/opc-ua-certificates/1614/6 35](#_Toc195980477)

[Figur 36: E-post fra Wago Norge support 35](#_Toc195980478)

[Figur 37: Tailscale download https://tailscale.com/download 37](#_Toc195980479)

[Figur 38: Installasjonsskript fra Tailscale 38](#_Toc195980480)

[Figur 39: Installasjonsskript jeg har laget https://raw.githubusercontent.com/espenbo/Sikker-kommunikasjon-og-sertifikath-ndtering-i-byggautomasjon-med-Tailscale-og-OPC-UA/refs/heads/main/Skript/InstallTailscale.sh 39](#_Toc195980481)

[Figur 40: : Status side Tailscale 40](#_Toc195980482)

[Figur 41: Codesys koblet til Tailscale IP adresse 40](#_Toc195980483)

[Figur 42: Testet kommunikasjon imellom PLS og UaExpert via Tailscale VPN 41](#_Toc195980484)

[Figur 43: PLS sertifikat lagt inn på Ignition 41](#_Toc195980485)

[Figur 44: Oppsett av OPC UA kommunikasjon i Ignition. Søk etter PLSen 41](#_Toc195980486)

[Figur 45: Funnet PLS 41](#_Toc195980487)

[Figur 46: Liste over støttede kommunikasjons metoder 42](#_Toc195980488)

[Figur 47: Vise sertifikat og velge om man skol stole på den eller ikke 43](#_Toc195980489)

[Figur 48: Viser valgte innstillinger for kommunikasjon med PLS 43](#_Toc195980490)

[Figur 49: Vise at kommunikasjonen er oppe 44](#_Toc195980491)

[Figur 50: Flytte sertifikater i PLSen 44](#_Toc195980492)

[Figur 51: Flytte sertifikater ligger i Trusted 44](#_Toc195980493)

[Figur 52: Oversikt i Ignition over tilkoblede OPC UA servere 44](#_Toc195980494)

[Figur 53: Oversikt i Ignition over tilkoblede OPC UA servere 45](#_Toc195980495)

[Figur 54: Kjøre skriptet på PLSen for å få sikkerhets sertifikat til webserveren https://github.com/espenbo/Sikker-kommunikasjon-og-sertifikath-ndtering-i-byggautomasjon-med-Tailscale-og-OPC-UA/blob/main/Skript/update\_tailscale\_certificates.sh 45](#_Toc195980496)

[Figur 55: Sikker kommunikasjon med HMI på PLS 46](#_Toc195980497)

[Figur 56: Nå har man sikkerhets sertifikat på webserveren 46](#_Toc195980498)

[Figur 57: Tailscale status – viser direkte kryptert forbindelse mellom PLS og SCADA med WireGuard protokoll 47](#_Toc195980499)

[Figur 58: Visning av gyldig HTTPS-sertifikat på PLSens webgrensesnitt 47](#_Toc195980500)

[Figur 59: Viser sikker tilkobling av PLS mot Ignition 48](#_Toc195980501)

[Figur 60: Ignition SCADA viser aktiv og sikker OPC UA-forbindelse med PLS (Sign & Encrypt) 48](#_Toc195980502)

[Figur 61: OPC UA-klienten viser at kommunikasjon med PLS er signert og kryptert med sertifikatbasert autentisering 48](#_Toc195980503)

[Figur 62: Oversikt i Ignition over tilkoblede OPC UA servere 49](#_Toc195980504)

[Figur 63: Oversikt over Storm elektro sin infrastruktur 51](#_Toc195980505)

# Introduksjon og motivasjon

Jeg er ansatt i Storm Elektro AS, et selskap som leverer elektro- og automasjonstjenester. I min rolle som prosjektingeniør innen byggautomasjon arbeider jeg med utvikling av nye systemer, drift og vedlikehold av infrastruktur, programmering av PLS og SCADA-systemer, samt idriftsettelse av tekniske installasjoner.

Motivasjonen for dette prosjektet kommer fra utfordringene knyttet til sikker sertifikathåndtering i OPC UA-baserte byggautomasjonssystemer. Med stadig økende krav til fjernaksess og cybersikkerhet er det kritisk å sikre autentisering og kryptering mellom enheter. Hovedhensikten er å utvikle en automatisert metode for OPC UA-sertifikathåndtering for å forbedre driftssikkerhet og redusere manuelle oppgaver.

Under arbeidet med prosjektet fant jeg ut at alle funksjonene ikke er støttet i firmwaren til Wago PLSen (CC100), så jeg måtte forandre hvordan jeg skulle få til en sikker og kryptert kommunikasjon imellom PLSer og scadasystemet. Jeg har jobbet videre med en tailscale løsning.

Under arbeidet med prosjektet oppdaget jeg at WAGO CC100 PLSen jeg benyttet ikke støtter alle nødvendige OPC UA-funksjoner for fullautomatisk sertifikathåndtering via GDS. Dette tvang meg til å justere retningen i prosjektet. I stedet for å bygge på full OPC UA-integrasjon med GDS, valgte jeg å jobbe videre med en alternativ løsning med Tailscale VPN for å sikre kommunikasjonen mellom PLS og SCADA. Samtidig laget jeg et skript for å kunne oppdatere HTTPS-sertifikatene til PLS-en automatisk, noe som fortsatt bidrar til å oppnå målet om høyere sikkerhet og lavere behov for manuell innsats.

Rapporten er strukturert sånn at den først presenterer bakgrunn og problemstilling, etterfulgt av en gjennomgang av relevant teori knyttet til OPC UA, sertifikathåndtering, VPN og SCADA. Deretter beskrives metoden jeg har brukt, resultatene som er oppnådd, og en vurdering av utfordringer og videre forbedringsmuligheter. Til slutt følger en konklusjon med anbefalinger, samt refleksjon rundt læring og erfaring fra prosjektet.

# Problemstilling

I byggautomasjonssystemer som benytter OPC UA for kommunikasjon mellom komponenter som PLS, HMI og SCADA, er sertifikathåndtering en sentral del av sikkerhetsarkitekturen. Sertifikater brukes for autentisering og kryptert kommunikasjon, men dagens manuelle håndtering – der sertifikater må genereres, installeres, fornyes og tilbakekalles manuelt – er både tidkrevende og utsatt for menneskelige feil. Dette kan føre til økt risiko for driftsavbrudd og svekket cybersikkerhet.

Prosjektet ble i utgangspunktet startet med følgende problemstilling:

***"Hvordan kan en automatisert metode for OPC UA-sertifikathåndtering forbedre sikkerhet og effektivitet i byggautomasjonssystemer?"***

Målet var å undersøke hvordan en sentralisert løsning, kunne håndtere hele livssyklusen til sertifikater – fra utstedelse til fornyelse og tilbakekalling – på en automatisk og sikker måte.

## Uforutsett hendelse

Mens jeg jobbet med prosjektet ble det klart at PLS-en (WAGO CC100) ikke har støtte for GDS eller automatisk håndtering av OPC UA-sertifikater i nåværende firmware. På grunn av dette ble prosjektet justert, med fokus på alternative sikkerhetsmekanismer for å oppnå tilsvarende mål.

## Den reviderte problemstillingen ble derfor:

***"Hvordan kan man bruke VPN for sikker kommunikasjon imellom PLS og Scadasystem, og automatisk oppdatering av sikkerhetssertifikat på nettsiden til PLSen"***

Dette førte til utforskning og implementering av en løsning basert på Tailscale VPN, som sikrer kommunikasjonen mellom SCADA og PLS selv i fravær av innebygd GDS-støtte. Samtidig ble det utviklet en metode for automatisk oppdatering av HTTPS-sertifikater til PLS-en ved hjelp av verktøy som er kompatible med Tailscale.

### Delmål:

* Kartlegge eksisterende praksis og utfordringer ved manuell sertifikathåndtering i OPC UA-miljøer.
* Undersøke teknologier for automatisert håndtering av sertifikater i byggautomasjon.
* Utforske bruk av VPN-teknologi (Tailscale) som et alternativ for sikker kommunikasjon.
* Utvikle og teste et skript for automatisk installasjon og tilkobling av Tailscale på WAGO CC100.
* Implementere automatisert oppdatering av HTTPS-sertifikater på PLS-en via Tailscale.

# Teori

## Teori OPC UA og sikkerhetsmekanismer.

OPC Unified Architecture (OPC UA) ([7], 2025) er en plattformuavhengig, standardisert kommunikasjonsprotokoll som er utviklet for å gi en sikker og pålitelig datautveksling mellom industrielle systemer. OPC UA ble utviklet av OPC Foundation som en videreutvikling av den gamle OPC Classic-protokollen ([14], 2025). Den prøver og løse utfordringene knyttet til kommunikasjon imellom forskjellige produsenter og operativsystemer. Også skal den støtte nye og moderne sikkerhets funksjonene og fleksibilitet som man trenger i en moderne industriell automatisering.

Sikkerhet er en av de viktigste aspektene ved OPC UA, og standarden inkluderer flere sikkerhetsmekanismer for å beskytte datautvekslingen mellom klienter og servere. OPC UA benytter en kombinasjon av autentisering, autorisering, kryptering og sertifikathåndtering for å oppnå dette. ([13], 2025)

#### Sertifikathåndtering og PKI

OPC UA bruker Public Key Infrastructure (PKI) for å håndtere sertifikater som brukes til autentisering og kryptering. Sertifikater sikrer at kun autoriserte enheter kan kommunisere med hverandre, og beskytter mot spoofing-angrep. ([10], 2025)

* Bruk av sertifikater: Enheter må verifisere hverandres identitet ved hjelp av digitale sertifikater utstedt av en betrodd sertifikatautoritet (CA).
* Selvsignerte sertifikater: OPC UA tillater også bruk av selvsignerte sertifikater, men dette krever at klienten manuelt stoler på sertifikatet.
* Administrasjon av sertifikater: OPC UA inkluderer mekanismer for håndtering av utløpne sertifikater, sertifikatfornyelse og tilbakekalling.

#### Autentisering og Autorisasjon

For å sikre at kun legitime brukere og systemer får tilgang til OPC UA-servere, støtter protokollen flere autentiseringsmekanismer. ([10], 2025)

* Brukernavn og passord: En grunnleggende autentiseringsmetode hvor klienter må oppgi brukernavn og passord for å få tilgang.
* X.509-sertifikater: OPC UA støtter bruk av X.509-sertifikater for autentisering. Dette gir et høyere sikkerhetsnivå enn brukernavn og passord.
* Active Directory (AD) og andre identitetstjenester: OPC UA kan integreres med AD eller andre eksterne autentiseringssystemer for rollebasert tilgangskontroll.

Når en bruker eller enhet er autentisert, håndteres autorisasjon gjennom tilgangskontrollmekanismer som definerer hvilke operasjoner en klient har lov til å utføre på serveren.

#### Kryptering og Signering

For å beskytte data som sendes mellom klient og server, benytter OPC UA sterke kryptografiske mekanismer. ([10], 2025)

* Transportlagsikkerhet (TLS): OPC UA bruker Transport Layer Security (TLS) for å sikre dataoverføringer over nettverk.
* Ende-til-ende-kryptering: Alle meldinger mellom klient og server kan krypteres ved hjelp av asymmetrisk eller symmetrisk kryptering.
* Digitale signaturer: Alle meldinger signeres digitalt for å sikre integritet og hindre uautoriserte modifikasjoner.

#### Bruk av Sikre Kommunikasjonsprofiler

OPC UA spesifiserer forskjellige sikkerhetsprofiler som definerer hvilke sikkerhetsmekanismer som skal brukes i ulike scenarioer. ([10], 2025)

* Anonymous Authentication: Ingen autentisering kreves (brukes ofte for åpne systemer).
* Sign-and-Encrypt: Dataene signeres og krypteres for å beskytte både integritet og konfidensialitet.
* Basic256/Basic256Sha256: Krypteringsalgoritmer for sikker kommunikasjon.
* AES-GCM: En nyere standard for sikker kryptering.

#### Sikkerhetsoppdateringer og Tilbakekalling av Tilgang

* Sikkerhetsoppdateringer: OPC UA har innebygde mekanismer for å oppdatere sertifikater og algoritmer som brukes til kryptering.
* Tilbakekalling av tilgang: Administrasjonssystemer kan tilbakekalle sertifikater hvis en enhet blir kompromittert.

### Automatisert sertifikathåndtering i OPC UA

OPC UA Global Discovery Server (GDS) er en viktig komponent i OPC UA-økosystemet som forenkler administrasjonen av sertifikater og enhetsoppdagelse i industrielle nettverk. GDS er designet for store distribuerte systemer hvor mange OPC UA-enheter må autentisere og kommunisere sikkert med hverandre. ([11], 2025)

#### OPC UA GDS har to hovedfunksjoner

Global Discovery: Den fungerer som et sentralt register der OPC UA-klienter og servere kan registrere seg og oppdage andre enheter i nettverket.

Automatisert Sertifikathåndtering: Den administrerer utstedelse, fornyelse, validering og tilbakekalling av sertifikater ved hjelp av Public Key Infrastructure (PKI).

Automatisert Sertifikathåndtering i OPC UA GDS

For å sikre at enheter kan kommunisere sikkert, håndterer OPC UA GDS hele sertifikatlivssyklusen:

1. Utstedelse av sertifikater:
   1. Når en ny OPC UA-server eller klient kobles til nettverket, kan den automatisk be om et sertifikat fra GDS.
   2. GDS genererer eller henter et sertifikat fra en betrodd Certificate Authority (CA) og distribuerer det til enheten.
2. Fornyelse av sertifikater:
   1. Sertifikater har en begrenset gyldighetstid. GDS overvåker utløpsdatoer og sørger for automatisk fornyelse av sertifikater før de utløper.
   2. Dette forhindrer at kommunikasjonen brytes på grunn av utløpte sertifikater.
3. Tilbakekalling av sertifikater:
   1. Hvis en enhet kompromitteres eller ikke lenger skal ha tilgang til nettverket, kan GDS tilbakekalle sertifikatet og oppdatere Certificate Revocation List (CRL).
   2. Dette hindrer at uautoriserte enheter kan kommunisere med andre OPC UA-komponenter.
4. Distribusjon av Trusted Certificate List:
   1. GDS holder en oppdatert liste over godkjente sertifikater og distribuerer denne til alle registrerte enheter.
   2. Dette sikrer at kun sertifikater utstedt av en betrodd CA blir akseptert i nettverket.

## Teori Tailscale Mesh VPN

Tailscale ([19], 2025) er et moderne mesh-VPN som bruker WireGuard-protokollen ([25], 2025) for å koble sammen enheter på en sikker og enkel måte. Tradisjonelle VPN-løsninger krever en sentraliserte VPN-servere og avanserte nettverkskonfigurasjoner, Tailscale lar alle enheter koble seg direkte til hverandre (peer-to-peer) med en enkle autentiserings- og autorisasjonsmekanismer.

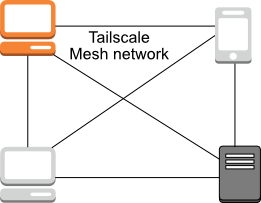
Tailscale forenkler nettverkstilkobling ved at de bruke en skybasert koordineringsserver til å etablere og administrere forbindelser mellom alle enhetene som er koblet til nettverket. Det gjør det enkelt å opprette private, sikre nettverk mellom enheter uten behov for å konfigurere brannmurer, åpne porter eller bruke statiske IP-adresser.

### Hvordan Tailscale fungerer

#### WireGuard-basert kryptering

Tailscale bygger på WireGuard-protokollen ([27], 2025), som er kjent for sin høye ytelse, lav latens og sterke sikkerhet. Alle tilkoblinger mellom enheter er kryptert ende-til-ende, noe som gjør at ingen kan avlytte trafikken.

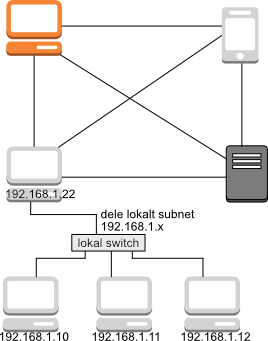
#### Mesh-arkitektur

I tradisjonelle VPN-er går all trafikken gjennom en sentral server. Tailscale lager istedenfor en direkte forbindelse mellom enhetene. Da får man bedre ytelse og mindre forsinkelser. ([23], 2025)

Figur : Tailscale mesh nettverk

#### Subnet-router:

Tailscale enheter kan også brukes som subnet routere slik at de kan dele sitt lokale subnet til resten av tailscale nettverket eller deler av nettverket. ([17], Subnet routers, 2025)



Figur : Tailscale mesh nettverk med subnet-router

#### Brukerautentisering via Oauth/SSO/OIDC

Tailscale integreres med identitetsleverandører som Google, Microsoft, GitHub og Okta for enkel innlogging og administrasjon av brukere. ([9], 2025) ([28], 2025)

#### NAT-traversering

Tailscale håndterer automatisert NAT-traversering, noe som betyr at enheter kan kommunisere med hverandre selv om de er bak ulike rutere eller brannmurer. ([22], 2025)

#### Sentralt administrasjonsgrensesnitt

Administratorer kan kontrollere tilgangsregler, legge til eller fjerne enheter, samt overvåke nettverksaktivitet via en webportal. ([6], 2025)

#### Sikkerhetsmodeller med ACL-er

Tailscale lar brukere definere tilgangskontrollister (ACL-er) for å styre hvem som kan kommunisere med hvilke enheter. ([8], 2025)

### Fordeler med Tailscale

#### Enkel implementering

Tailscale kan settes opp på minutter uten behov for avanserte nettverkskonfigurasjoner.

Man får en sikker og privat forbindelse der all trafikk er ende-til-ende-kryptert, og ingen tredjepart (inkludert Tailscale) kan lese dataene som går over nettverket.

#### Ressursbruk bruk og hastighet

Tailscale bruker wireguard protokollen som er svært effektivt og har lav CPU- og minnebruk sammenlignet med andre VPN-protokoller som OpenVPN og IPSec. Flere test har også vist at wireguard er overfører raskere en for eksempel openvpn. ([29] Mann, 2025)

### Ulemper med Tailscale

#### *Avhengighet av skybasert kontrollplane*

Tailscale bruker en skybasert koordineringsserver for å etablere og vedlikeholde tilkoblinger mellom noder. Det betyr at man må ha internettforbindelse til Tailscales sin server for å etablere nye forbindelser og holde forbindelsen oppe.

#### Begrenset lokal kontroll og åpen kildekode

Selv om Tailscale bygger på WireGuard, som er åpen kildekode, er Tailscales kontrollplaner og enkelte funksjoner proprietære. Det gir mindre innsyn og fleksibilitet sammenlignet med helt åpen kildekode løsninger.

#### *Kompatibilitet med industrielle protokoller*

Byggautomasjon bruker ofte protokoller som BACnet, Modbus, OPC UA og KNX. Disse protokollene er ofte følsomme for latency og krever multicast eller broadcast (f.eks. for BACnet Who-Is/I-Am). Siden Tailscale ikke støtter multicast eller broadcast over mesh-nettverket, må man bruke andre tjenester som BBMD server ([29] Fisher, 2025) eller edge server ([5], 2025) for å kommunisere over nettverket.

#### *Kompleksitet med subnet routing og ACL-konfigurasjon*

Tailscale støtter subnet routing, men det krever manuell konfigurering av ruterroller og kan bli komplisert i større nettverk med mange segmenter. ACL-er må også konfigureres riktig for å sikre riktig tilgang. Feilkonfigurasjoner kan enten føre til manglende kommunikasjon eller for åpne nettverket.

#### Ikke støttet av alle propioritære OS

Alle leverandører av operativsystem til byggautomasjon støtter ikke installasjon av 3-partsprogrammer eller installasjon av Tailscale. Derfor er det ikke mulig og installere Tailscale på alle enheter som brukes i et byggautomasjonsanlegg.

### Sikkerhetssertifikater i Tailscale

I tillegg til kryptert kommunikasjon over Tailscale nettverket, kan Tailscale håndtere sikkerhetssertifikater gjennom Tailscale programmet. ([15], 2025)

#### Automatisk utstedelse av TLS-sertifikater:

Tailscale kan generere og administrere TLS-sertifikater for maskiner i nettverket, slik at du kan bruke HTTPS på interne tjenester. Tailscale kan utstede og fornye sertifikater automatisk, de er laget for \*.tailnet-miljøet slik at sertifikatene knyttes opp mot DNS navnet hosten har i ditt Tailscale nettverk. ([18], 2025)

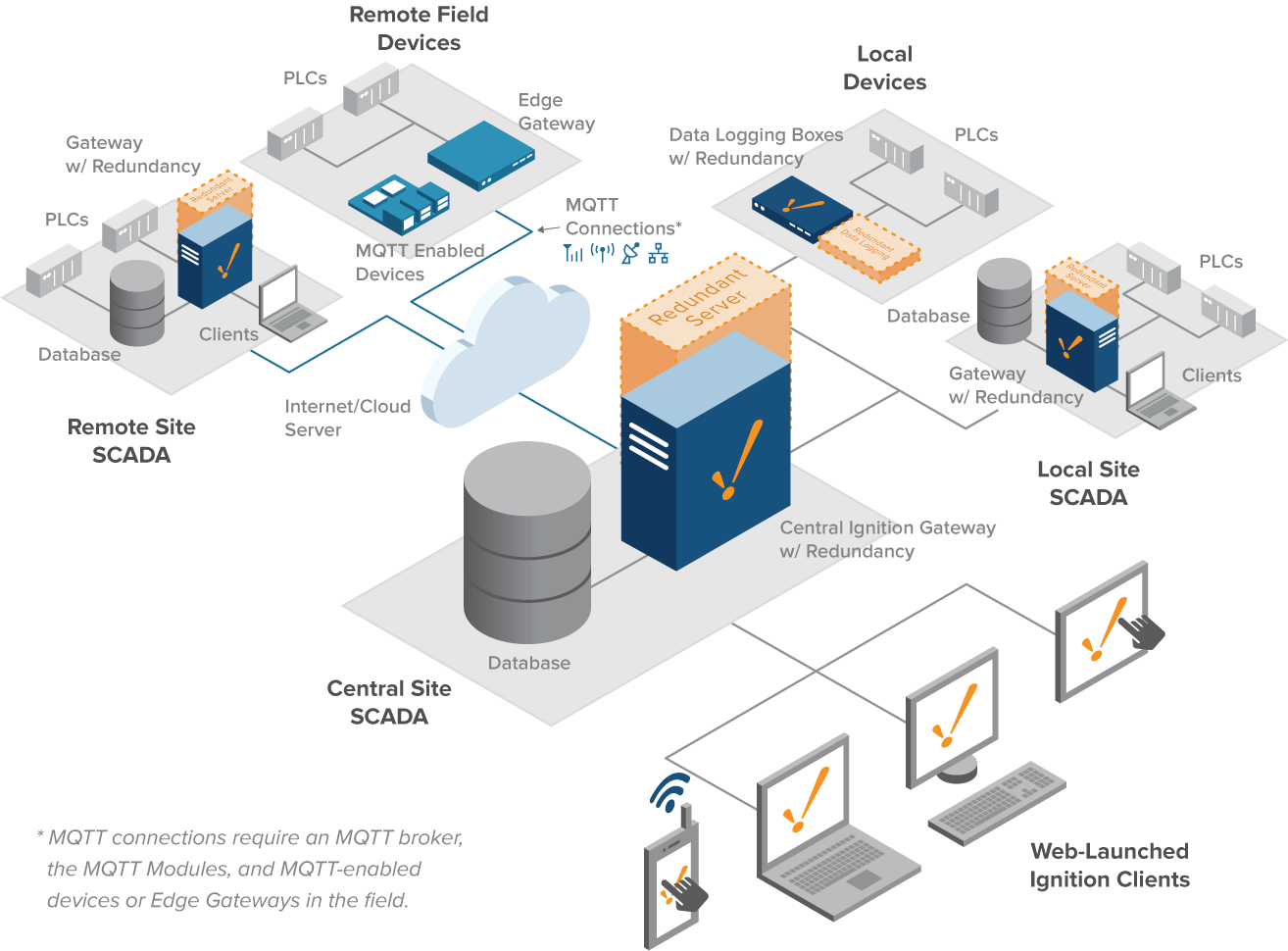
## Ignition SCADA

Ignition SCADA, er utviklet av Inductive Automation, det er en moderne Supervisory Control and Data Acquisition (SCADA)-plattform designet for industriell overvåking, kontroll og dataanalyse. ([24], 2025)

A screenshot of a computer program

AI-generated content may be incorrect.Plattformen er modulbasert, det betyr at brukerne kan velge hvilke funksjoner de ønsker å benytte. Ignition Gateway fungerer som systemets kjerne og kan administreres via en nettleser. Ignition støtter flere kommunikasjonsprotokoller, som OPC UA, MQTT, Modbus, BACnet, SNMP og REST API-er. Ignition kan derfor enkelt integreres med både moderne og eldre industrielle systemer. ([4], 2025)

Figur : Ignition modul oversikt

Ignition har også en innebygget OPC UA-serveren. I har den støtte for forskjellige database som SQL, IBM DB2, historikklagringsfunksjoner brukerne muligheten til å lagre og analysere data direkte i databaser som MySQL, Microsoft SQL Server , PostgreSQL, Oracle Express database og Azure osv. Dette gjør at bedrifter kan kjøre avanserte analyser og generere rapporter basert på både sanntidsdata og historiske data. ([12], 2025)

Figur : Ignition arkitektur

A screenshot of a computer

AI-generated content may be incorrect.Til visualisering bruker Ignition to hovedmoduler: Vision og Perspective. Vision er en desktop-applikasjon designet for industrielle operatører som krever pålitelig og rask dataoppdatering i et kontrollromsmiljø. Perspective er en moderne HTML5-basert løsning som gir tilgang til SCADA-data via nettlesere og mobile enheter, noe som gjør det mulig å overvåke og kontrollere systemer fra hvor som helst i verden. Dette gjør Ignition til en av de mest fleksible og tilpasningsdyktige SCADA-løsningene på markedet.

Figur : Ignition perspective visualisering

Sikkerhet er en viktig faktor i alle automasjons plattform, og Ignition har en rekke innebygde sikkerhetsmekanismer. Plattformen støtter TLS-kryptering, Single Sign-On (SSO), Active Directory-integrasjon og rollebasert tilgangskontroll (RBAC), det gjør at man kan ha full kontroll over hvem som kan få tilgang til systemene. Ignition kan oppfylle strenge sikkerhetskravene som ofte kreves i kritisk infrastruktur, som byggautomasjon, energiproduksjon, vann- og avløpssystemer og transportnettverk.

A diagram of a computer network

AI-generated content may be incorrect.A diagram of a computer network

AI-generated content may be incorrect.Det som virkelig skiller Ignition fra andre SCADA-løsninger er skalerbarheten og fleksibiliteten. Systemet kan settes opp i en sentralisert eller distribuert arkitektur, der flere Ignition-servere samarbeider for å håndtere store industrielle systemer. Ignition Edge, en lettvektsversjon av programvaren, kan installeres på fjernlokasjoner for lokal datainnsamling og videresending til hovedsystemet. Dette gjør det enkelt å håndtere både små, lokale automasjonsprosjekter og komplekse globale systemer. ([17], SCADA vs. Ignition, 2025)

Figur 9: Basis arkitektur  
https://inductiveautomation.com/ignition/architectures

Figur : Basis arkitektur med redundans

A diagram of a computer network

AI-generated content may be incorrect.A computer network diagram with blue boxes and a computer

AI-generated content may be incorrect.

Figur : Utvidet arkitektur med redundans

Figur 11: Utvidet arkitektur

A diagram of a computer network

AI-generated content may be incorrect.

Figur : Hub & Spoke

A diagram of a computer network

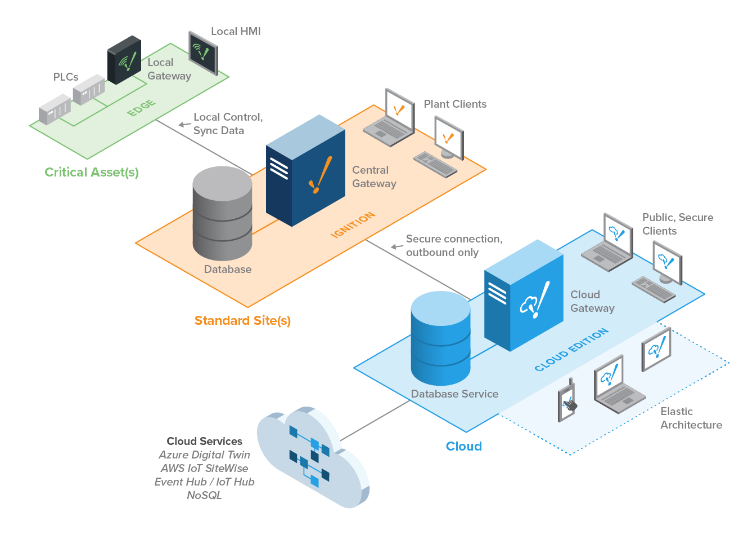
AI-generated content may be incorrect.

Figur : Hub & Spoke med redundans

A diagram of a computer network

AI-generated content may be incorrect.

Figur : IIoT arkitektur



Figur : Cloud hybrid arkitektur

([2], 2025)

# Metode

Dette prosjektet er gjennomført med et testoppsett. Målet har vært å utvikle og teste en løsning for sikker kommunikasjon og sertifikathåndtering i et OPC UA-basert byggautomasjonssystem. Prosjektet har gitt ny informasjon under testing, det har ført til justeringer i både mål og tilnærming.

## Utviklingsprosess

Det er brukt korte utviklingssykluser med hyppig testing. Det er vekslet mellom undersøkelse, konfigurering, skripting og testing i et kontrollert testmiljø. Prosessen kan oppsummeres i følgende hovedfaser:

1. Kartlegging av eksisterende løsning og sikkerhetsutfordringer i OPC UA.
2. Undersøkelse av teknologier for sertifikathåndtering og VPN.
3. Valg og installasjon av verktøy: Tailscale, UaExpert, Ignition SCADA og test-PLS (WAGO CC100).
4. Utvikling av automatiseringsskript for Tailscale-installasjon og HTTPS-sertifikatfornyelse.
5. Testing og evaluering av løsningen i et simulert automasjonsnettverk.

### Testoppsett

For utvikle og teste løsningen under kontrollerte forhold ble det laget et lokalt testmiljø bestående av følgende komponenter:

* Hardware
  + WAGO CC100 PLS (med Codesys 3.5 SP19 Patch 7)
* Software
  + Ignition SCADA
  + Debian Linux-server (for sertifikathåndtering og scripting)
  + Tailscale installert på både PLS og SCADA-maskin
  + UaExpert brukt som testklient for OPC UA-kommunikasjon
  + Bash skrip
* Intern DNS og HTTPS-test via Tailscale sitt .tailnet-domene
* Chatgpt.com for hjelp med feilsøking og lage bash skript

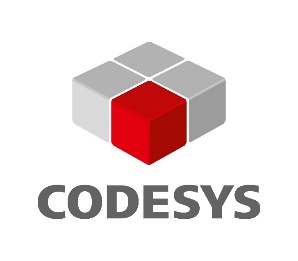
Nettverket ble testet både med og uten VPN aktivert for å evaluere sikkerhet og tilgjengelighet i ulike scenarioer.



Figur : Ignition logo



Figur : uaExpert logo





Figur : Wago logo

Figur : Codesys logo

A close-up of a white electronic device

AI-generated content may be incorrect.

Figur : Wago CC100 pls



Figur : Tailscale logo

## Original problemstilling med OPC UA

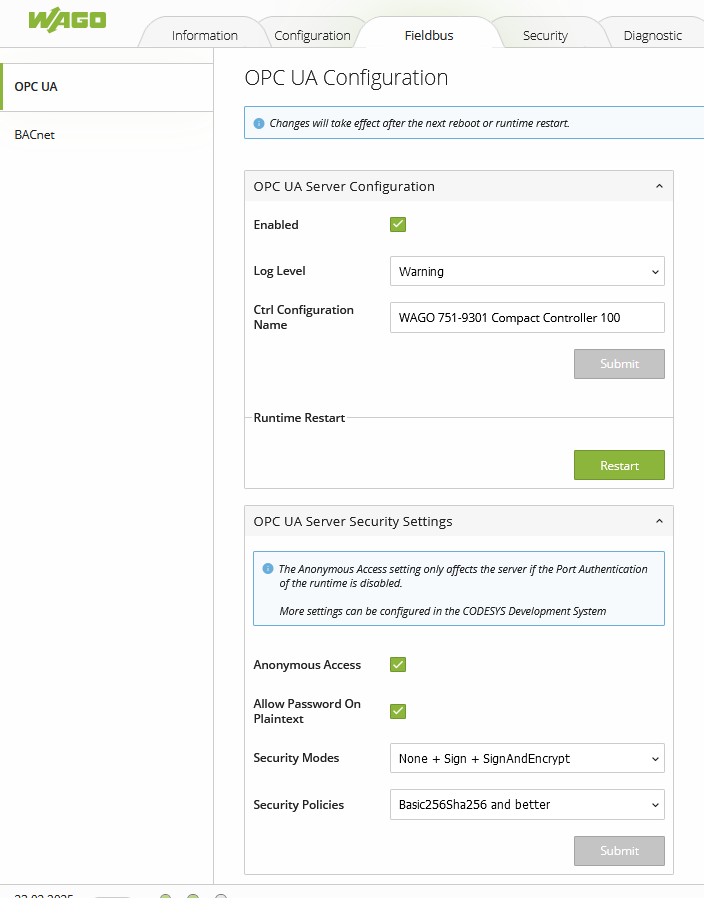
### Evalueringskriterier OPC UA

* Funksjonalitet: Fungerer OPC UA-Sertifikat generering som forventet?
* Sikkerhet: Er kommunikasjonen kryptert (verifisert via TLS)? Beskyttes enhetene mot uautorisert trafikk?
* Automatisering: Kan sertifikatene automatisk oppdateres?
* Robusthet: Hva skjer dersom en enhet restarter eller mister forbindelse?

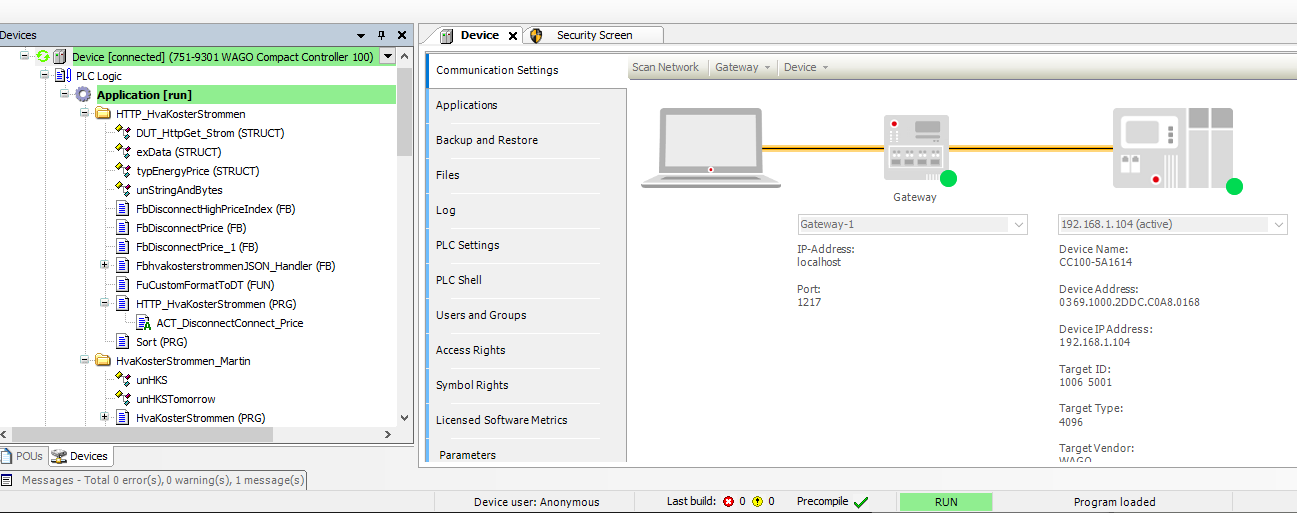
### A diagram of a software AI-generated content may be incorrect. Arbeidsprosess manuell sertifikathåndtering

Figur 22: Manuell sertifikathåndtering  
https://reference.opcfoundation.org/Core/Part2/v105/docs/9

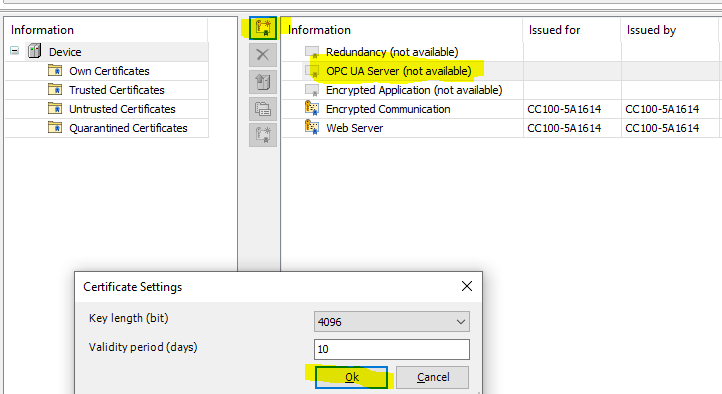
1. Konfigurasjon av OPC UA-server og sertifikathåndtering i Codesys.



Figur : Wago oppsett av OPC UA i nettsiden til PLSen

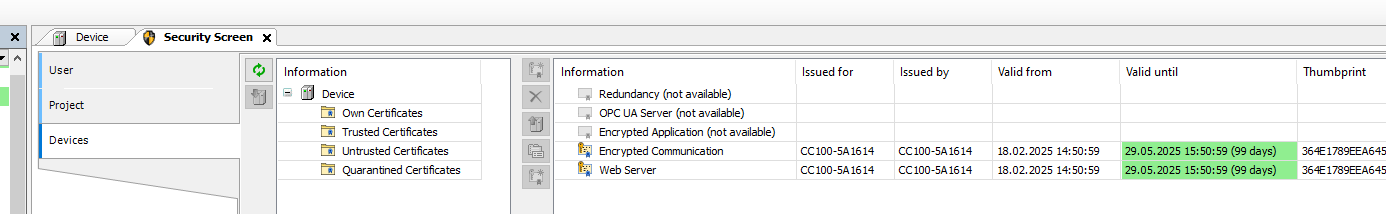
1. Koble seg til PLSen.

Figur : Koble seg til PLS

1. Generere nytt OPC UA sertifikat.

Figur : Oppsett av sikkerhets sertifikat til PLSen i Codesys 3.5

1. Oversikt over sertifikater.



Figur : Oversikt over sikerhetssertifikater i PLS vises i Codesys 3.5

1. Koble uaExpert til wago PLSen for og teste om kommunikasjonen fungerer over kryptert linje, sikkerhetssertifikatet fra PLSen må legges inn i uaExpert.

A screenshot of a computer

AI-generated content may be incorrect.

Figur : Koble uaExpert til PLSen, og legg inn sertifikatet fra PLS inn uaExpert sin Trusted Certifikate.

1. A screenshot of a computer

   AI-generated content may be incorrect.Flyttet sertifikatet fra uaExpert fra Quarantined Certificates til Trusted Certificates i PLSen

Figur : Flytt sertifikatet til uaExpert inn i PLSen sin Trusted Certificates.

1. A screenshot of a computer

   AI-generated content may be incorrect.Testet at kommunikasjon fungerer

Figur : Kryptert kommunikasjon imellom PLS og uaExpert fungerer.

Jeg hadde litt utfordringer med og å få generert nye sertifikater. Jeg måtte oppdatere firmware på PLSen og passe på at PLSen var tilkoblet en NTP server (klokke server) slik at jeg var sikker på at klokka på PLSen var helt riktig.

### A diagram of a software application AI-generated content may be incorrect. Arbeidsprosess automatisk sertifikathåndtering

Figur : Automatiserte sertifikathåndteringen  
https://reference.opcfoundation.org/Core/Part2/v105/docs/9

1. Konfigurasjon av OPC UA-server og sertifikathåndtering i Codesys, likt som i prossesen over.
2. Installere UaGDS som er en GDS server fra Unified Automation.
3. A screenshot of a computer

   AI-generated content may be incorrect.Følg installasjon instruksene som følger med UaGDS fra Unified Automation. ([3], 2025)

Figur : Skjermbilde fra manualen til UaGDS  
https://www.unified-automation.com/

1. A screenshot of a computer

   AI-generated content may be incorrect.Oppsett av ‘Pull configuration for servers’. Klienter eller server som støtter ‘Pull’ fra GDS server. ([16], 2025)

Figur 32: Skjermdump. Pull configuration for servers

1. A screenshot of a computer

   AI-generated content may be incorrect.Oppsett Wago 750-8xxx OPC Ua Server. (txxxxxxxx-OPCUA-Server-0en-1.pdf, 2020)

Figur : Skjermdump fra txxxxxxxx-OPCUA-Server-0en-1.pdf

1. Bruke GDS for sentralisert sertifikathåndtering.
2. Testing og validering av sikker kommunikasjon.
3. Feilsøking gjennom testing, supporthenvendelser, forumdiskusjoner og iterativ justering av løsningen.

### Uforutsett hendelse

Gjennomførte flere tester for å se om jeg kunne automatisk oppdatere sertifikatet slik som er beskrevet av OPC-UA Foundation ([11], 2025). Og i wago dokumentasjon jeg hadde funnet. (txxxxxxxx-OPCUA-Server-0en-1.pdf, 2020)

A screenshot of a chat

AI-generated content may be incorrect.Kontaktet Wago Norge, Discord #NFEA OPC UA og <https://www.wago.community> for å få hjelp med feilsøking på hvorfor sertifikathåndteringen fungerte slik jeg hadde forstått at det skulle fungere.

Figur : Discord. NFEA OPC UA #arkitektur-og-konnektivitet Post: OPC UA Global Discovery Server

Feilsøking og kommunikasjon med de forskjellige support linjene ga med til slutt svaret.

A screenshot of a computer

AI-generated content may be incorrect.I WAGO Community-forumet la jeg ut en detaljert beskrivelse av problemet, inkludert feilmeldingen jeg fikk i UaExpert: 'Reading the server CertificateGroups returned error BadNodeIDUnknown'. Flere brukere foreslo ulike tilnærminger, men ingen av disse fungerte. Etter videre undersøkelser fikk jeg til slutt bekreftet fra WAGO Tyskland at GDS-støtte ikke ville være tilgjengelig før tidligst 2026.

Figur : wago community svar på spørsmål om OPC UA GDS push  
https://www.wago.community/t/opc-ua-certificates/1614/6

A screenshot of a computer

AI-generated content may be incorrect.På Discord diskuterte jeg også problemstillingen med andre som jobber med OPC UA, og det ble foreslått å benytte en alternativ løsning basert på VPN.

Figur : E-post fra Wago Norge support

### Uforutsett hendelse og evalueringskriterier

En uforutsett hendelse fikk en stor betydning for prosjektets. WAGO CC100 PLS, som programmeres med Codesys 3.5, støtter ikke OPC UA Pull-funksjonen. Etter omfattende testing og kontakt med WAGO Norge og internasjonale brukermiljøer ble det klart at denne funksjonen kun er tilgjengelig i WAGOs eldre OPC UA-server basert på e!COCKPIT-plattformen, og at støtte for Pull i Codesys-varianten av WAGO CC100 først forventes i fremtidige firmwareversjoner (tidligst 2026).

Det gjør at den opprinnelige problemstillingen – ***"Hvordan kan en automatisert metode for OPC UA-sertifikathåndtering forbedre sikkerhet og effektivitet i byggautomasjonssystemer?"*** – ikke kan gjennomføres med maskinvaren som er valgt. Derfor ble det nødvendig å justere prosjektets mål og metode. Fokuset ble i stedet rettet mot alternativ sikkerhetsarkitektur.

## Veien videre etter at første problemstilling ikke fungerer

Siden softwaren som brukes på Wago sin CC100 ikke støtter GDS server med mulighet til og automatisk oppdatering av sikkerhetssertifikatene, måtte jeg finne en annen løsning for å skape en sikker kommunikasjon imellom PLSen og Scada serveren som kunne enkelt oppdateres og vedlikeholdes.

Tailscale er en type mesh-VPN som støtter ulike operativsystemer og prosessorarkitekturer. Jeg satte meg inn i hvordan Tailscale fungerer, og startet testing for å se om denne programvaren kunne brukes til å sikre kommunikasjonen.

## Ny problemstilling med Tailscale VPN

### Evalueringskriterier for Tailscale-løsningen

* Funksjonalitet: Er det stabil kommunikasjon imellom PLS og Scada over VPN? Støtter Tailscale OPC UA og https trafikk?
* Sikkerhet: Er kommunikasjonen kryptert (verifisert via TLS)? Beskyttes enhetene mot uautorisert trafikk?
* Automatisering: Kan sertifikatene automatisk oppdateres?
* Robusthet: Hva skjer dersom en enhet restarter eller mister forbindelse?

### Arbeidsprosess med Tailscale VPN installasjon på PLS

1. Kartlegge utfordringer med installasjon av Tailscale på PLS
2. Utvikle et script som kan installere Tailscale på PLSen
3. Test kommunikasjon mellom PLS og uaExpert via VPN
4. Test kommunikasjon mellom PLS og Ignition via VPN
5. Utvikle et script som kan automatisk hente sertifikat som kan brukes på nettsiden på PLSen
6. Teste og validere løsningen i simulerte scenarier

Tailscale har installasjons skript for blant annet Linux

A screenshot of a computer

AI-generated content may be incorrect.

Figur 37: Tailscale download  
https://tailscale.com/download

Jeg lastet det ned og kjørte skriptet på PLSen.

A screenshot of a computer

AI-generated content may be incorrect.Men det klarte ikke å installere Tailscale på PLSen. Tailscale lager også static binaries filer som kan brukes. <https://pkgs.tailscale.com/stable/#static>

Figur : Installasjonsskript fra Tailscale

Jeg testet med manuell installasjon av riktig fil og fikk kontakt.

Manuell installasjon er ganske tungvint så jeg laget et nytt installasjons skript som bygger på Tailscale sitt skript. Ligger som vedlegg.

A screenshot of a computer program

AI-generated content may be incorrect.

Figur : Installasjonsskript jeg har laget  
https://raw.githubusercontent.com/espenbo/Sikker-kommunikasjon-og-sertifikath-ndtering-i-byggautomasjon-med-Tailscale-og-OPC-UA/refs/heads/main/Skript/InstallTailscale.sh

A screenshot of a computer

AI-generated content may be incorrect.

Figur : : Status side Tailscale

Jeg fant PLSen på nettsiden til Tailscale. Fant IP adressen til PLSen på VPN nettverket.

A computer screen shot of a computer

AI-generated content may be incorrect.

Figur : Codesys koblet til Tailscale IP adresse

Brukte denne IP adressen til og koble meg til PLSen med Codesys 3.5

A screenshot of a computer

AI-generated content may be incorrect.

Figur : Testet kommunikasjon imellom PLS og UaExpert via Tailscale VPN

A screenshot of a computer

AI-generated content may be incorrect.Testet kommunikasjonen mellom PLS og UaExpert via Tailscale VPN nettverk.

Figur : PLS sertifikat lagt inn på Ignition

A screenshot of a computer

AI-generated content may be incorrect.Legg Ignition sertifikatet inn på PLSen, og legg PLS sertifikatet inn på Ignition.

Figur : Oppsett av OPC UA kommunikasjon i Ignition. Søk etter PLSen

A screenshot of a computer error message

AI-generated content may be incorrect.Neste test er og koble PLSen til Ignition scada systemet

Figur : Funnet PLS

A screenshot of a phone

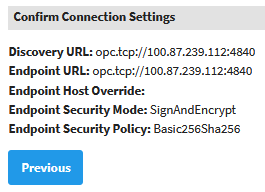
AI-generated content may be incorrect.

Figur : Liste over støttede kommunikasjons metoder

A screenshot of a computer

AI-generated content may be incorrect.

Figur : Vise sertifikat og velge om man skol stole på den eller ikke



Figur : Viser valgte innstillinger for kommunikasjon med PLS

A screenshot of a chat

AI-generated content may be incorrect.

Figur : Vise at kommunikasjonen er oppe

A screenshot of a computer

AI-generated content may be incorrect.

Figur : Flytte sertifikater i PLSen

I codesys 3.5 og flytte Sertifikat fra karantene til sertifikater som man stoler på.

A screenshot of a computer

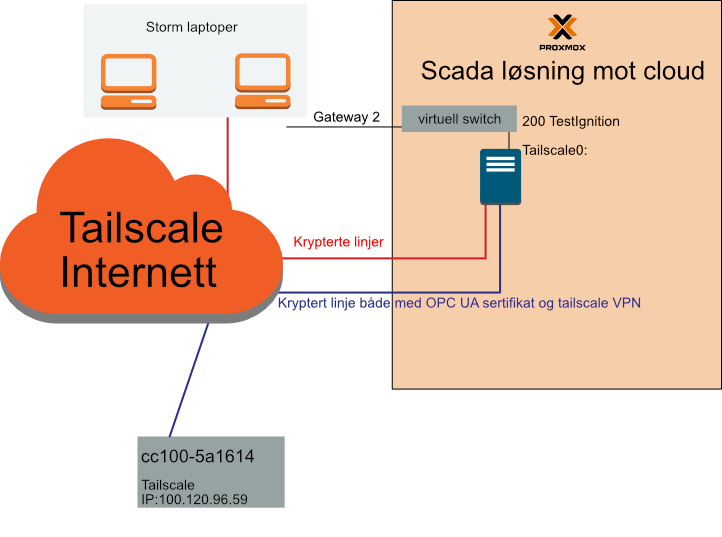
AI-generated content may be incorrect.

Figur : Flytte sertifikater ligger i Trusted

A screenshot of a computer

AI-generated content may be incorrect.Da har vi en oversikt over sertifikater som PLSen stoler på

Figur : Oversikt i Ignition over tilkoblede OPC UA servere

Infrastukturen baserer seg på Tailscale VPN løsningen sammen med OPC UA sertifikat som brukes mellom Ignition og PLSen når de kommuniserer.

Figur : Oversikt i Ignition over tilkoblede OPC UA servere

En PC kan logge seg til Ignition serveren og se på visualiseringen på scada serveren, eller man kan koble seg til PLSen.

A black screen with white text

AI-generated content may be incorrect.For å få sertifikater som fungerer på nettsidene til PLSen bruker jeg Tailscale sin sertifikat tjeneste. Jeg har laget et skript for å hente sertifikat og flytte dem til riktig plass på PLCen.

Figur : Kjøre skriptet på PLSen for å få sikkerhets sertifikat til webserveren  
https://github.com/espenbo/Sikker-kommunikasjon-og-sertifikath-ndtering-i-byggautomasjon-med-Tailscale-og-OPC-UA/blob/main/Skript/update\_tailscale\_certificates.sh

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

Figur : Sikker kommunikasjon med HMI på PLS

Figur : Nå har man sikkerhets sertifikat på webserveren

### Kryptering

A screenshot of a computer

AI-generated content may be incorrect.

Figur : Tailscale status – viser direkte kryptert forbindelse mellom PLS og SCADA med WireGuard protokoll

Trafikken mellom PLS og SCADA går over Tailscale som bruker Wireguard protokollen for å lage et VPN-nettverk som krypterer all trafikk automatisk, uavhengig av applikasjonstype. ([20], 2025)

A screenshot of a computer

AI-generated content may be incorrect.

Figur : Visning av gyldig HTTPS-sertifikat på PLSens webgrensesnitt

A screenshot of a computer error

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

Figur : Viser sikker tilkobling av PLS mot Ignition

Figur : Ignition SCADA viser aktiv og sikker OPC UA-forbindelse med PLS (Sign & Encrypt)

Figur : OPC UA-klienten viser at kommunikasjon med PLS er signert og kryptert med sertifikatbasert autentisering

Forbindelsen mellom Ignition SCADA og PLS er kryptert på to nivåer: først gjennom WireGuard-basert Tailscale VPN, som sikrer at alle datapakker mellom enhetene er kryptert på transportnivå, og deretter gjennom OPC UA sin egen sikkerhetsprotokoll med TLS, X.509-sertifikater og "Sign & Encrypt"-policy. Skjermbilder fra både UaExpert og Ignition bekrefter at denne sikkerheten er aktiv, og Tailscale grensesnittet dokumenterer at kommunikasjonen går over en kryptert, direkte kanal.

# Resultater / Produktbeskrivelse

Målet med prosjektet har vært å sikre kommunikasjon mellom en WAGO CC100 PLS og Ignition SCADA-systemet. Siden CC100 mangler støtte for Global Discovery Server (GDS), måtte jeg finne en alternativ løsning. Løsningen er basert på Tailscale VPN for kryptert datatrafikk og automatisk oppdatering av sikkerhetssertifikater for HTTPS ved hjelp av Tailscale sine innebygde funksjoner.

Løsningen gjør det mulig å ha sikker kommunikasjon både for OPC UA og for tilgang til PLSens innebygde webgrensesnitt.

## Infrastruktur og arkitektur

Den tekniske løsningen er bygd opp som vist i bilde over.

Figur 56: Infrastruktur for sikker kommunikasjon mellom SCADA og PLS via Tailscale VPN

* PLS-enheten cc100-5a1614 er tilkoblet Tailscale-nettverket med en privat IP-adresse.
* En Ignition SCADA-instans kjører på en Proxmox-server, også koblet til Tailscale via tailscale0.
* En Storm-laptop kan aksessere både SCADA-serveren og PLS-en via sikre linjer over Tailscale.
* A computer screen with a cloud and text

  AI-generated content may be incorrect.Kommunikasjonen er kryptert både via VPN (Tailscale) og OPC UA-sertifikater der det er støttet.

Figur : Oversikt i Ignition over tilkoblede OPC UA servere

## Prosjektoversikt

I prosjektet ble det utviklet og validert en løsning der Tailscale benyttes som et virtuelt, mesh nettverk for å knytte sammen tre sentrale noder: en CC100 PLS, en Ignition SCADA-server som kjører på en virtuell maskin i Proxmox, og en utviklingsmaskin (Storm laptop). Alle nodene kobles til det samme Tailscale-nettverket, og hver enhet får en unik IP-adresse innenfor Tailscale sitt private adresseområde. Det tillater direkte, kryptert kommunikasjon mellom enhetene, uten behov for NAT-konfigurasjon, port forwarding eller bruk av statiske IP-adresser.

Det ble det utviklet et skript for automatisk installering av Tailscale. InstallTailscale.sh

Et sentralt resultat i prosjektet har vært integrasjonen mellom PLS og SCADA. På grunn av begrensninger i WAGO CC100 – spesielt mangel på støtte for GDS (Global Discovery Server) – kunne ikke automatisk sertifikathåndtering for OPC UA benyttes. Dette ble løst ved at man manuelt genererte sertifikater med lang holdbarhet i CODESYS-miljøet på PLS-en, som deretter ble overført og importert til Ignition sin sertifikatdatabase. For å etablere en fungerende OPC UA-tilkobling måtte både server- og klientsertifikater utveksles og godkjennes manuelt. Etter at sertifikatene var riktig importert, ble det opprettet en forbindelse fra Ignition til PLSen med OPC UA protokollen. Dataen i PLSen kan da leses og visualiseres i SCADA-miljøet. Ulempen med manuelt genererte sertifikat er at de tidkrevende å oppdatere dem. Derfor ble den laget med lang holdbarhet. I tillegg er kommunikasjonen allerede kryptert over VPN kommunikasjonen til Tailscale.

Det ble det utviklet et skript update\_tailscale\_certificates.sh for automatisk håndtering av HTTPS-sertifikater på CC100-enheten. Tailscale tilbyr en innebygd funksjon for å utstede TLS-sertifikater signert av Let's Encrypt, knyttet til enhetens Tailscale-DNS-navn. Ved å bruke tailscale cert-kommandoen er det mulig å hente ned gyldige sertifikater uten noen form for manuell konfigurasjon. Det ble laget et bash-skript som identifiserer enhetens DNS-navn basert på Tailscale-status, laster ned sertifikatet og den tilhørende nøkkelen, kombinerer disse til en .pem-fil, og oppdaterer lighttpd-serverens konfigurasjon. Skriptet håndterer også symlinking av sertifikatfilene for enkel drift og sørger for at sertifikatene automatisk fornyes før de utløper. Dette sikrer at WebVisu alltid er tilgjengelig over HTTPS uten manuelle inngrep.

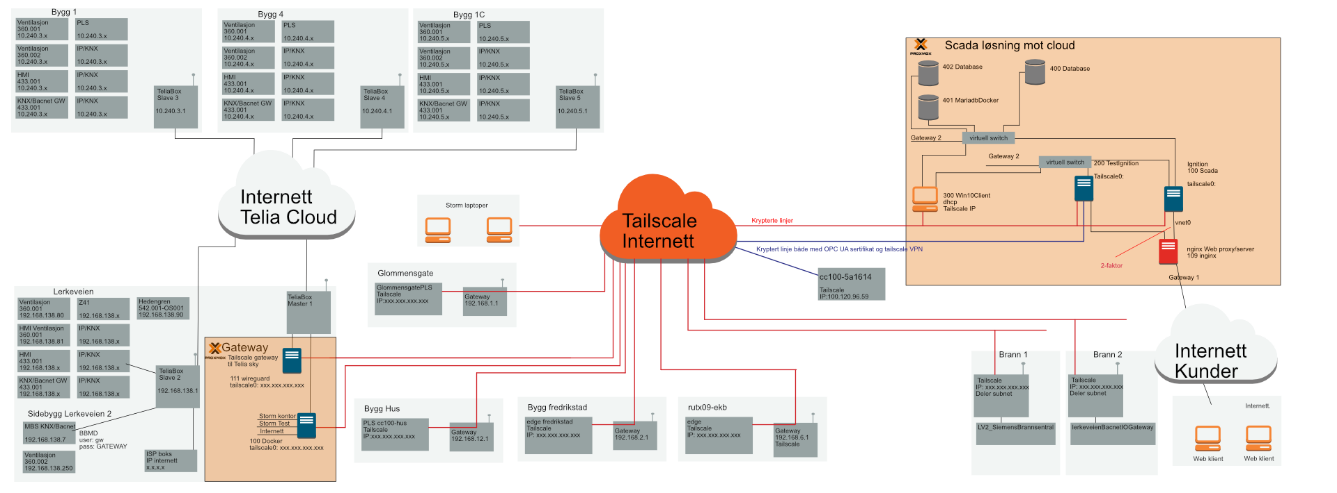
Kommunikasjonen mellom PLS og SCADA går utelukkende via krypterte linjer, både over Tailscale og i applikasjonslaget via OPC UA-sertifikater. En utviklingsmaskin kan koble seg til systemet via Tailscale og får tilgang til både webgrensesnitt og SCADA-gateway.

Gjennom testing ble det bekreftet at løsningen fungerer som ønsket. Ignition kunne lese data fra PLS-en, og WebVisu er tilgjengelig fra eksterne klienter uten at det er nødvendig å åpne porter i brannmurer eller konfigurere VPN manuelt.

Når man bruker Tailscale reduserer man vesentlig behovet for nettverksadministrasjon, og automatiseringen av HTTPS-sertifikater gjorde løsningen robust og egnet for produksjonsmiljø.

En svakhet i løsningen er at OPC UA-sertifikater fortsatt må håndteres manuelt. Dette er en konsekvens av maskinvarebegrensninger på CC100 og vil kunne løses i fremtidige prosjekter når codesys og CC100 får støtte for dette, eller ved å velge en PLS som støtter GDS. Likevel har løsningen vist seg praktisk og driftssikker i testmiljøet, og den kan lett overføres til andre industrielle settinger hvor sikker fjernkommunikasjon er nødvendig.

Prosjektet har resultert i en ferdig implementert og testet arkitektur for sikker dataflyt mellom edge-enhet og SCADA-system. Resultatet inkluderer både programkode, skript for vedlikehold og dokumentasjon som gjør det mulig å drifte og videreutvikle systemet. Løsningen er robust mot tap av internettforbindelse, og støtter både tilkobling for drift og for videre programmering og konfigurasjon av PLS-en via fjernaksess.



Figur : Oversikt over Storm elektro sin infrastruktur

Deler av løsningen er tatt i bruk av Storm elektro med flere PLS koblet til en Ignition server.

# Diskusjon

I dette prosjektet har det blitt tydelig at automatisert sertifikathåndtering i OPC UA er et område som fremdeles ikke er fult støttet av alle PLS-leverandører. Selv om OPC UA-standarden åpner for høy grad av sikkerhet og fleksibilitet gjennom blant annet Global Discovery Server (GDS) og sertifikatbasert autentisering, er det fortsatt store variasjoner i hvor godt dette er implementert i praksis. I dette tilfelle var det opprinnelige målet å få på plass en helautomatisk løsning for sertifikathåndtering mellom en WAGO CC100 PLS og et Ignition SCADA-system. Etter grundig testing og kontakt med både leverandør og brukermiljøer viste det seg at CC100 mangler støtte for nødvendige GDS-funksjoner, og at dette tidligst vil bli tilgjengelig i fremtidige versjoner av CODESYS.

Denne begrensningen gjorde at prosjektets fokus måtte forandres. Det ble i stedet rettet mot å finne alternative, men sikre løsninger for kommunikasjon og sertifikathåndtering. Det valgt å ta i bruk Tailscale VPN og manuell sertifikathåndtering for OPC UA, kombinert med en automatisert løsning for HTTPS-sertifikater for PLSens innebygde webserver. Det viser hvor viktig det er med fleksibilitet i utviklingsprosjekter.

|  |  |  |
| --- | --- | --- |
| Kriterium | Opprinnelig løsning (GDS) | Ny løsning (Tailscale + manuell OPC UA) |
| Automatisering | Høy grad av automatisering ved støtte av GDS i PLS | Automatisk HTTPS, men manuell OPC UA-håndtering |
| Krav til støtte i maskinvare | Krever full støtte for GDS i PLS | Krever Linux-kompatibilitet og mulighet for installasjon av 3-parts program |
| Fremtidsrettethet | Følger OPC UA-visjonen sin visjon | Følger ikke OPC UA visjonen. Tailscale bruker wireguard protokoll som er GPL basert noe som gjør den åpen og tilgjenglig |
| Tilgjengelighet | Begrenset til GDS-støttede plattformer | Tailscale fungerer på de fleste arkitekturer og OS |
| Tilpasning | Lite fleksibel, ikke støttet av alle PLSer | Høy grad av fleksibilitet, skript kan tilpasses. Ikke støttet av alle PLSer |
| Driftssikkerhet | Potensielt høy ved støtte i PLS | Høy, god støtte av standard IT-miljøer |

En av de største styrkene i løsningen er bruken av Tailscale som et alternativ til tradisjonelle VPN-løsninger. Dette reduserte behovet for kompliserte brannmurregler og nettverkskonfigurasjoner, og sørget for kryptert kommunikasjon mellom PLS, SCADA og utviklingsmaskin uten at det var nødvendig å gjøre endringer i den lokale nettverksinfrastrukturen. Tailscale sitt brukergrensesnitt og administrasjonsverktøy gjør det enkelt å overvåke tilkoblinger og kontrollere tilgang, og dette ble raskt en stabil og pålitelig løsning.

En annen positivt funksjon er automatiseringen av HTTPS-sertifikathåndteringen for webserveren på PLSen. Ved å benytte Tailscale sin cert-funksjon og et egendefinert bash-skript, ble det mulig å hente ut gyldige TLS-sertifikater fra Tailscale sitt API og bruke dem direkte i lighttpd-konfigurasjonen på PLS-en. Dette fungerer sømløst og gir sikker tilgang til WebVisu over HTTPS, helt uten manuell innsats etter første oppsett. Løsningen ble validert og fungerte stabilt gjennom flere testsykluser.

**Fordel ved skript for automatisk oppdatering av https sertifikat**

* Det gjør det mulig å installere Tailscale på en PLS som ikke har pakkehåndtering.
* Det forenkler vedlikehold av HTTPS-sertifikater gjennom automatisering.
* Det gjør løsningen skalerbar til andre enheter med lik plattform.
* Det reduserer tid brukt på manuelle oppgaver og senker risikoen for feil.
* Det bidrar til standardisering og repeterbarhet på tvers av installasjoner.

Den største utfordringen i prosjektet var sertifikathåndteringen i OPC UA. Det viste seg at mangelen på GDS-støtte ikke bare forhindret automatisert utveksling av sertifikater, men også gjorde feilsøking langt mer krevende. I praksis krevde dette at jeg manuelt opprettet sertifikater, flyttet dem mellom klient og server, og validerte kommunikasjonen i begge retninger. Feilmedinger fra for eksempel UaExpert eller Ignition var ofte generiske, og det var vanskelig å vite nøyaktig hvilken del av sertifikatkjeden som lagde problemene. Flere ganger ble sertifikater slettet å opprette pånytt for å prøve å finne feilen.

Feilsøkingen ble gjort lettere med hjelp fra fagmiljøer, spesielt WAGO Norge, WAGO Tyskland, NFEA Discord-kanaler og WAGO Community. Likevel tok det lang tid før jeg fikk bekreftet at det ikke var GDS støtte.

**Hva som kan forbedres**

* Tidlig verifisering av maskinvarestøtte kunne ha redusert feilsøking og spart tid.
  + Det vil være lurt å teste andre PLSer som har innebygd støtte for GDS, enten i nyere CODESYS-versjoner eller andre leverandører. Det kan gjøre det mulig å lage en fullautomatisert løsning for OPC UA-sertifikater, noe som vil gi mindre risiko for feil.
* Evaluering av OPC UA-sikkerhet i praktiske bruksområder.
  + Det bør gjennomføres en mer omfattende evaluering av OPC UA-kommunikasjon i ulike driftsmiljøer, inkludert sikkerhetsvurderinger, ytelsestester og simulering av feilsituasjoner. Dette vil bidra til å styrke forståelsen for hvordan protokollen oppfører seg i praksis og hvordan ulike komponenter (som SCADA, PLS og VPN) samhandler under reelle forhold.
* Feilmeldingene i OPC UA-miljøet (spesielt UaExpert og Ignition) kunne vært mer presise og hjelpsomme.
* Tailscale sin støtte for multicast/broadcast er begrenset.
  + Enkelte protokoller som KNX og Bacnet vanskelig å bruke uten workaround som BBMD eller edge-server.
* Manuell håndtering av OPC UA-sertifikater er tidkrevende og sårbart for menneskelige feil, løsningen med lang holdbarhet på sertifikatet er ikke optimalt.
  + Når GDS-støtte blir tilgjengelig i CODESYS og for WAGO CC100 eller lignende maskinvare, bør den eksisterende infrastrukturen bygges videre med integrert GDS. Dette vil gjøre det mulig å migrere til en helautomatisk løsning, slik som opprinnelig tiltenkt.
* Grensesnittet i Codesys for sertifikathåndtering kunne vært mer brukervennlig og automatisert.
* PLSen støtter ikke pakkehåndtering
  + apt, yum eller tilsvarende løsning er ikke støttet av PLSen, slik støtte ville gjort det enklere å administrere pakkeoppdateringer.
* Tailscale-klienten burde ha en pakke laget og testet for Wago PLSer.
* Sikkerhetslogging og overvåkning av VPN-aktivitet kunne vært mer integrert i SCADA eller sentral logg.
  + Tailscale har støtte for API kommunikasjon der man kan hente ut mere informasjon som kan visualiseres og overvåkes av Ignition Scada.
* Videreutvikling og dokumentasjon av automatiseringsskript
  + De skriptene som er laget i dette prosjektet for installasjon og sertifikathåndtering bør videreutvikles, testes og dokumenteres enda bedre. En forbedret brukeropplevelse og enklere distribusjon vil gjøre det lettere å standardisere sikkerhetsrutiner på tvers av ulike installasjoner.
* Opprettelse av malverk og anbefalte praksiser for sikker fjernaksess
  + Prosjektets erfaringer kan danne grunnlaget for etablering av standardiserte prosedyrer for sikker fjernaksess til PLS og SCADA-systemer i byggautomasjon. Dette kan inkludere retningslinjer for bruk av VPN, sertifikathåndtering, logging og tilgangskontroll.

Det er tydelig at det fortsatt er et gap mellom OPC UA sin spesifikasjon og hva som faktisk er støttet av tilgjengelig hardware idag. Tailscale VPN gir sikker kommunikasjon, men er ikke beskrevet i løsningen til OPC UA. Etter hvert som det kommer oppdateringer til Codesys og Wago softwaren vil støtten til OPC UA sine muligheter bli bedre.

# Konklusjon og anbefalinger

Prosjektet har demonstrert at det er mulig å etablere sikker og driftssikker kommunikasjon mellom en WAGO CC100 PLS og Ignition SCADA ved å benytte Tailscale VPN som et alternativ til fullstendig PKI-basert, automatisk sertifikathåndtering i OPC UA. Selv om det opprinnelige målet – å utvikle en helautomatisk løsning for OPC UA-sertifikater – ikke kunne realiseres grunnet begrenset støtte for Global Discovery Server (GDS) i den aktuelle maskinvaren, har prosjektet resultert i en fungerende og fleksibel løsning som kan brukes i virkelige industrielle miljøer.

Løsningen basert på Tailscale VPN viste seg å være både enkel å implementere og robust i bruk. Den eliminerer mange av utfordringene knyttet til tradisjonell nettverkskonfigurasjon, som behovet for port forwarding, statiske IP-adresser og komplekse brannmurregler. I tillegg gir Tailscale muligheten for sikker, ende-til-ende-kryptert kommunikasjon, samt innebygd funksjonalitet for utstedelse av TLS-sertifikater som kan benyttes på webservere.

Ved å benytte Tailscale sitt sertifikattjeneste kombinert med et egendefinert skript, ble det mulig å sikre HTTPS-kommunikasjon til WebVisu-grensesnittet på PLSen. Denne delen av løsningen er fullstendig automatisert og sørger for at sertifikater fornyes før de utløper, uten at det kreves manuell innsats. Det gjør løsningen skalerbar og praktisk, selv i større systemer med mange PLSer.

Det er ikke nødvendig å bruke OPC UA sertifikater når Tailscale VPN løsningen allerede bruker Wireguard protokollen ([1], 2025) som gjør at kommunikasjonen er kryptert over Tailscale sitt mesh nettverk.

Det fortsatt nødvendig med manuell håndtering av OPC UA-sertifikater mellom SCADA og PLS. Dette representerer en svakhet i løsningen, men er i dette tilfellet en uunngåelig konsekvens av begrenset støtte i firmware og programvare. Det understreker viktigheten av å verifisere funksjonalitet og støtte i valg av utstyr tidlig i et prosjektforløp.

På tross av denne begrensningen har prosjektet gitt verdifulle erfaringer og innsikt i hvordan moderne VPN-teknologi og automatiserte prosesser kan brukes for å oppnå høyere grad av sikkerhet og enklere drift i byggautomasjonssystemer. Løsningen er allerede i bruk internt hos Storm Elektro, og den viser potensial til videre anvendelse i andre prosjekter.

## Forstudie rammer

Prosjektets opprinnelige problemstilling ble forandret som følge av manglende støtte for Global Discovery Server (GDS) i WAGO CC100. Den nye metoden som består av Tailscale VPN har i stor grad oppfylt målene, rammene og intensjonene som ble definert i forstudierapporten. Den opprinnelige målsetningen om å forbedre sikkerheten i OPC UA-basert byggautomasjonanlegg gjennom automatisert sertifikathåndtering er fortsatt sentral i løsningen, selv om teknisk gjennomføring er forandret.

Ved bruk av Tailscale som sikkerhetslag og automatisering av HTTPS-sertifikater gjennom skript, blir det en praktisk og gjennomførbar løsning med dagens tekniske begrensninger. Det er utviklet og testet en metode for å sikre kommunikasjon mellom PLS og SCADA, og løsningen er både skalerbar, dokumentert og validert i et kontrollert testmiljø.

Løsningen oppfyller kravene til sikkerhet, autentisering og vedlikeholdbarhet, og løser de samme effektmålene: å redusere manuell innsats, øke driftssikkerheten og sikre kontinuerlig kryptert kommunikasjon. Kost/nytte-forholdet er også ivaretatt, løsningen krever lite ekstra utstyr og Tailscale er gratis for små prosjekter. Dette gjør løsningen mer realistisk å teste før det implementeres i dagens byggautomasjonsanlegg enn en løsninger som forutsetter funksjoner som ennå ikke er støttet i dagens maskinvare.

Prosjektet har fulgt de avgrensninger og risikohensyn som ble definert i forstudierapporten. Det ble presisert at testing skulle foregå i simulert miljø, at alternative løsninger måtte vurderes dersom teknisk støtte manglet, og at man ikke skulle utvikle ny CA-infrastruktur, men integrere med eksisterende systemer.

### Forstudierapporten (kap. 5–6) ble følgende definert som mål og rammer

* Prosjektmål: Automatisert håndtering av OPC UA-sertifikater.
* Effektmål: Økt sikkerhet, redusert manuelt arbeid, kontinuerlig kryptering.
* Resultatmål: En testet og fungerende metode for sertifikatoppdatering.
* Delmål: Evaluere eksisterende praksis og lage en løsning som er kompatibel med WAGO PLS.

Metoden ble forandret fra GDS-basert løsning til en Tailscale basert løsning. Prosjektet har levert en løsning som løser kjerneproblemet: Sikker kommunikasjon.

### Prosjektet skal være nyttig for byggautomasjonsbedrifter og redusere driftskostnader og risiko

Løsningen med Tailscale:

* Reduserer behovet for manuell nettverkskonfigurasjon.
* Gir kryptert kommunikasjon mellom PLS og SCADA.
* Har et automatisert oppsett for HTTPS på PLSen via skript.
* Gir muligheten til å bruke OPC UA sertifikater i tilegg.

Løsningen er rimelig og egnet for reell bruk, noe som var ett av suksesskriteriene.

### Risikohåndtering og fleksibel prosjektstyring

* Dokumentere manglende GDS-støtte i WAGO CC100.
* Endre fokus til en løsning som fungerer med dagens maskinvare.
* Levert en ferdig og testet løsning med dokumentasjon.

### Kost/nytte

Løsningen som ble utviklet i prosjektet representerer et godt forhold mellom kostnad og nytte, spesielt siden det ble utfordringer med opprinnelig planlagt løsning basert på GDS.

Ved å bruk Tailscale (gratis for 3 brukere med inntil 100 enheter) er det mulig å sikre kommunikasjonen mellom PLS og SCADA uten behov for kostbare lisensierte VPN-løsninger, dedikerte brannmurbokser, eller komplekse nettverksoppsett. Dette reduserer både anskaffelseskostnader og driftskostnader, særlig for små og mellomstore byggautomasjonsanlegg. Ved behov for flere brukere må man betale per bruker. ([21], 2025)

Det ble utviklet et egendefinert skript for automatisert installasjon av Tailscale og for oppdatering av HTTPS-sertifikater på PLSens webserver. Dette fjerner behovet for manuell håndtering av TLS-sertifikater etter første oppsett, og reduserer dermed driftsbelastning, tid brukt på vedlikehold og risiko for feilkonfigurasjoner.

Selv om manuell OPC UA-sertifikathåndtering fortsatt kan gjennomføres, kreves ikke OPC UA sertifikater for å oppnå kryptert kommunikasjon. Oppsettet som ble laget i prosjektet fungerer godt med dagens teknologi.

Løsningen er også fleksibel og lett å gjenbruke i fremtidige prosjekter. Skriptene som ble utviklet kan enkelt tilpasses andre WAGO-enheter eller distribueres til andre installasjoner, noe som gir langsiktig nytteverdi.

Totalt sett gir løsningen høy funksjonell verdi til lav økonomisk kostnad, og utgjør et godt kompromiss mellom det ideelle og det praktisk gjennomførbare, gitt dagens tekniske forutsetninger.

# Refleksjon rundt prosessen i prosjektet

Arbeidet med dette prosjektet har vært både utfordrende og lærerikt. Selv om den opprinnelige målsettingen med fullautomatisert sertifikathåndtering ikke var mulig å gjennomføre på grunn av manglende støtte i WAGO CC100 PLS-en, har prosjektet gitt en annen løsning basert på Tailscale VPN og automatisk HTTPS-sertifikatfornyelse.

En viktig erfaring fra prosjektet har vært betydningen av å kartlegge tekniske begrensninger i valgt maskinvare tidlig i prosessen.

Jeg startet prosjektet med å sette meg inn i OPC UA-standarden og hvordan den håndterte sertifikathåndtering, prosjektet var basert på at PLSen støttet GDS. Først etter omfattende testing og kommunikasjon med leverandøren fant vi ut at denne PLSen ikke støttet GDS, men det hadde vært det i PLSer basert på e!Cockpit. Dette understreker hvor viktig det er å teste sentrale funksjoner i praksis og innhente detaljert dokumentasjon om utstyret før man definerer teknisk retning.

Prosjektet vist hvor viktig det er å være fleksibel og åpen for justeringer av problemstillingen underveis. Da det opprinnelige målet viste seg å være urealistisk innenfor rammen av prosjektet, ble problemstillingen justert til å fokusere på en alternativ sikkerhetsløsning. Det gjorde det mulig å fortsatt oppnå målet om å styrke sikkerheten i byggautomasjonsnettverket, selv om det ble gjort på en annen måte enn først planlagt.

En annen ting prosjektet viser er hvor stor verdi det er å ha et godt samarbeid med fagpersoner og bransjeeksperter. Gjennom dialog med kollegaer, leverandører og veileder fikk jeg tips og hjelp til å feilsøke og teste løsninger.

Dette hjalp til så prosjektet kunne fortsette selv om det var noen tekniske utfordringene.

Prosjektet har også gitt meg verdifull praktisk erfaring med VPN-teknologi, automatisering av installasjonsprosesser og sertifikathåndtering, som er direkte relevant for fremtidig arbeid innen byggautomasjon og industriell IT-sikkerhet. Jeg har også fått styrket min forståelse for hvordan moderne SCADA-løsninger og sikkerhetsmekanismer må spille sammen for å møte dagens krav til fjernaksess og cybersikkerhet.

Til slutt har dette prosjektet lært meg viktigheten av strukturert dokumentasjon og kontinuerlig testing, og at selv et delvis endret prosjekt kan gi verdifulle resultater – så lenge man er tilpasningsdyktig og bevisst på hva man lærer underveis.

## Hva kunne vært gjort annerledes?

Hvis jeg skulle gjort prosjektet på nytt, ville jeg sjekket bedre om GDS var støttet på CC100 PLSen. Det ville spart meg for mye tid og frustrasjon. Jeg ville også ha planlagt mer tid til testing og feilsøking.

## Refleksjon over utviklingsprosessen

Gjennom arbeidet med prosjektet erfarte jeg hvor viktig det er å kartlegge tekniske begrensninger i forkant. Hadde jeg visst at WAGO CC100 ikke støttet GDS, kunne jeg valgt en annen PLS eller et annet prosjekt. Samtidig fikk jeg mye feilsøkingserfaring og lærte mye mens jeg feilsøke og prøvde og finne en løsning.

Jeg lagde egne skript for installasjon og sertifikathåndtering som kan brukes i andre prosjekter. Det viser hvordan man kan automatisere komplekse prosesser og bygge løsninger som er både sikre og enkle å drifte. I tillegg fikk jeg testet hvordan Ignition SCADA fungerer sammen med OPC UA-klienter over VPN, noe som har lært meg hvordan dette kan gjøres i større byggautomasjonsanlegg.

# Hvordan har du håndtert utfordringer?

For å håndtere utfordringene som oppstod underveis, har jeg brukt flere strategier:

1. **Testing og feilsøking:** Jeg brukte verktøy som UaExpert for å overvåke OPC UA-sertifikathåndtering og teste kommunikasjon mellom PLS og SCADA-systemet. Dette hjalp meg med å identifisere hvor problemer oppstod.
2. **Ekstern støtte og samarbeid:** Jeg kontaktet Wago support, postet spørsmål på Wago Community-forumet og diskuterte utfordringene i Discord NFEA OPC UA-gruppen. Dette ga meg mange gode tilbakemeldinger som jeg jobbet videre med, spesielt feilsøking rundt GDS-støtte i Codesys var hjelp fra andre veldig verdifullt.
3. **Litteratur og dokumentasjon:** Jeg undersøkte OPC UA-dokumentasjon, inkludert OPC Foundation sine spesifikasjoner, og testet metoder for sertifikatoppdatering beskrevet i Codesys-dokumentasjonen.
4. **Iterativ tilpasning av løsningen:** Da jeg oppdaget at Wago CC100 ikke støttet GDS, justerte jeg problemstillingen for å fokusere på VPN-basert sikker kommunikasjon og automatisk oppdatering av sertifikater for nettsiden til PLSen.
5. **Installasjon av Tailscale på PLS:** Installasjonen av tailscale på PLS er ikke automatisert. Jeg fant en binary fil som kunne kjøres på PLSen. Men alt måtte gjøres manuelt. Laste ned filen, pakke de ut, flytte dem, lage oppstarts skript osv. Ble en del testing for å få det riktig.
6. **Automatisering med skript:** Når jeg hadde fått Tailscale til å fungere manuelt på PLSen lagde jeg et Shell-skript for å installere Tailscale på PLS-en, det kan også oppdatere sertifikater automatisk, slik at sikkerhetsinfrastrukturen ble mer robust.
7. **Sikkerhetsertifikater på webserveren til PLSen:** Tailscale har en løsning for å generere sikkerhetssertifikater, men de må også plasseres på riktig plass i PLSen slik at de brukes av webserveren. Jeg laget et skript for å løse dette etter at jeg hadde funnet ut hvordan det skulle gjøres manuelt.

# Hva ville du gjort annerledes om du skulle gjort prosjektet igjen?

Dersom jeg skulle gjennomført prosjektet på nytt, ville jeg vurdert følgende forbedringer:

1. **Tidligere verifikasjon av krav og begrensninger:** Jeg brukte mye tid på å undersøke GDS-støtte, bare for å oppdage at den ikke var tilgjengelig på CC100. En grundigere forhåndssjekk av hardware- og softwarebegrensninger kunne spart tid.
2. **Mer strukturert feilsøkingsmetodikk:** Jeg kunne laget en mer systematisk testprotokoll tidlig i prosjektet for å unngå å gjenta tester unødvendig.
3. **Alternativ programvare og maskinvare:** Siden GDS-støtte først kommer i Codesys 3.5 SP22, kunne jeg vurdert andre PLS-er eller programvareversjoner som allerede hadde denne funksjonaliteten.
4. **Bedre tidsstyring:** Jeg undervurderte hvor tidkrevende det ville være å feilsøke sertifikathåndtering og OPC UA-kommunikasjon. En mer detaljert milepælsplan kunne hjulpet med å identifisere tidskritiske oppgaver tidligere.
5. **Mere samarbeid med bransjeeksperter tidlig:** Tidlig dialog med personer som har erfaring med OPC UA og sertifikathåndtering kunne gitt meg verdifulle tips om alternative løsninger.

# Referanser

[1]. (2025, April 17). *About wireguard*. Hentet fra tailscale.com: https://tailscale.com/kb/1035/wireguard

[10]. (2025, april 13). *OPC Foundation reference Certificate management*. Hentet fra Certificate management: https://reference.opcfoundation.org/Core/Part2/v104/docs/8

[11]. (2025, april 13). *OPC Foundation reference Global Discovery Server*. Retrieved from https://reference.opcfoundation.org/GDS/v104/docs/6

[12]. (2025, April 13). *OPC UA Integration in Ignition.* Hentet fra Inductiveautomation: https://inductiveautomation.com/resources/video/using-opc-ua-in-ignition

[13]. (2025, April 13). *OPC Unified Architecture – Landingpage*. Retrieved from OPC Foundation: https://opcfoundation.org/about/opc-technologies/opc-ua/

[14]. (2025, april 13). *OPC-Classic*. Retrieved from OPC Foundation: https://opcfoundation.org/about/opc-technologies/opc-classic/

[15]. (2025, april 13). *Provision TLS certificates for internal Tailscale services.* Hentet fra Tailscale: https://tailscale.com/blog/tls-certs

[16]. (2025, april 13). *Pull configuration with administrator account.* Hentet fra Unified-automation: https://documentation.unified-automation.com/uagds/1.1.1/html/sec\_config\_pull\_admin.html

[17]. (2025, April 13). *SCADA vs. Ignition.* Hentet fra Inductiveautomation: https://inductiveautomation.com/why-ignition

[17]. (2025, april 13). *Subnet routers*. Hentet fra Tailscale: https://tailscale.com/kb/1019/subnets

[18]. (2025, april 13). *Set up HTTPS certificates.* Hentet fra Tailscale: https://tailscale.com/kb/1153/enabling-https

[19]. (2025, april 13). Hentet fra Tailscale: https://tailscale.com/

[2]. (2025, April 13). *Common Ignition Architectures.* Hentet fra Inductiveautomation: https://inductiveautomation.com/ignition/architectures

[20]. (2025, April 17). *Tailscale encryption*. Hentet fra tailscale.com: https://tailscale.com/kb/1504/encryption

[21]. (2025, April 17). *Tailscale Pricing*. Hentet fra tailscale.com: https://tailscale.com/pricing

[22]. (2025, april 13). *Terminology and concepts*. Hentet fra Tailscale: https://tailscale.com/kb/1155/terminology-and-concepts?q=NAT-traversering

[23]. (2025, april 13). *Understanding mesh network topology*. Hentet fra Tailscale: https://tailscale.com/learn/understanding-mesh-vpns

[24]. (2025, April 13). *What is Ignition.* Hentet fra Inductiveautomation: https://inductiveautomation.com/ignition

[25]. (2025, april 13). Retrieved from Wireguard: https://www.wireguard.com/

[27]. (2025, april 13). *wireguard protocol*. Hentet fra Wireguard: https://www.wireguard.com/protocol/

[28]. (2025, april 13). *Supported SSO identity providers and OIDC*. Hentet fra Tailscale: https://tailscale.com/kb/1013/sso-providers?q=OIDC

[29] Fisher, D. (2025, April 13). *BACnetIP and BBMDs.* Hentet fra Bacnetexperts: https://bacnetexperts.com/papers/BACnetIP%20and%20BBMDs.pdf

[29] Mann, B. (2025, april 13). *WireGuard vs OpenVPN: 7 Key Differences in 2025*. Hentet fra Cyberinsider: https://cyberinsider.com/vpn/wireguard/wireguard-vs-openvpn/

[3]. (2025, april 13). *Configuration tool for UaGDS.* Hentet fra Unified-automation: https://documentation.unified-automation.com/uagds/1.1.1/html/administration\_sec.html#sec\_admin\_connect\_config

[4]. (2025, April 13). *Ignition User Manual.* Hentet fra Inductiveautomation: https://docs.inductiveautomation.com/

[5]. (2025, april 13). *ignition-edge.* Hentet fra Inductiveautomation: https://page.inductiveautomation.com/ignition-edge

[6]. (2025, april 13). *Manage access*. Hentet fra Tailscale: https://tailscale.com/kb/1350/manage

[7]. (2025, april 13). Retrieved from OPC Foundation: https://opcfoundation.org/

[8]. (2025, april 13). *Manage permissions using ACLs*. Hentet fra Tailscale: https://tailscale.com/kb/1018/acls

[9]. (2025, april 13). *Oauth*. Hentet fra Tailscale: https://tailscale.com/kb/1215/oauth-clients?q=Oauth

txxxxxxxx-OPCUA-Server-0en-1.pdf, [. (2020). *OPC UA Server. Version 1.1.0, FW Version 03.06.09(18), OPC UA Server Version 1.2.5.* WAGO.

Inductive Automation. What is Ignition? Hentet fra https://inductiveautom ([2], 2025)ation.com/ignition

Inductive Automation. Ignition User Manual. Hentet fra https://docs.inductiveautomation.com/

Inductive Automation. Why Ignition is Different. Hentet fra https://inductiveautomation.com/why-ignition

Inductive Automation. MQTT and Ignition. Hentet fra https://inductiveautomation.com/resources/article/mqtt-ignition

Inductive Automation. OPC UA Integration in Ignition. Hentet fra https://inductiveautomation.com/resources/video/using-opc-ua-in-ignition

OPC Foundation. What is OPC UA? Hentet fra https://opcfoundation.org/about/opc-technologies/opc-ua

OPC Foundation. OPC UA Security Overview. Hentet fra https://opcfoundation.org/security

OPC Foundation. OPC UA Part 2: Security Model. Hentet fra https://reference.opcfoundation.org/v104/Core/docs/Part2/

OPC Foundation. Global Discovery Server (GDS). Hentet fra https://opcfoundation.org/about/opc-technologies/opc-ua-gds

Unified Automation. OPC UA GDS Explained. Hentet fra https://www.unified-automation.com/products/ua-runtime-software/uagds.html

Tailscale. Understanding Mesh VPNs. Hentet fra https://tailscale.com/learn/understanding-mesh-vpns

Tailscale. TLS Certificates with Tailscale. Hentet fra https://tailscale.com/blog/tls-certs

Tailscale. Enabling HTTPS. Hentet fra https://tailscale.com/kb/1153/enabling-https

Tailscale. Encryption in Tailscale. Hentet fra https://tailscale.com/kb/1504/encryption

CyberInsider. WireGuard vs OpenVPN – Which is Better? Hentet fra https://cyberinsider.com/vpn/wireguard/wireguard-vs-openvpn

WAGO Community. (2025). OPC UA Certificates – Spørsmål og svar. Hentet fra https://www.wago.community/t/opc-ua-certificates/1614/6

Discord – NFEA OPC UA. (2025). Post om OPC UA Global Discovery Server [Foruminnlegg].

WAGO Norge Support. (2025). E-postkorrespondanse med teknisk støtte.

GitHub. Tailscale Installer Script. Hentet fra https://github.com/tailscale/tailscale/blob/main/scripts/installer.sh

GitHub. Espen Bø – Tailscale installasjonsskript. Hentet fra https://github.com/espenbo/xxx

WAGO. WAGO CC100 PLS-dokumentasjon og produktbilder. Hentet fra https://wago.com

# Vedlegg

## Vedlegg 1 - KI-deklarasjon

KI-deklarasjon for Avsluttende prosjekt.pdf

## Vedlegg 2 - Timeliste

Timeliste.pdf

## Vedlegg 3 - Forstudierapport

Forstudierapport OPCUA.pdf

## Vedlegg 4 - Presentasjon

Sikker kommunikasjon i byggautomasjon med Tailscale og OPC.pptx

## Vedlegg 5 - Møter

Referat møte 29012025.pdf

Møteinkalling OPC UA 17022025.pdf

Referat møte 17022025.pdf

Møteinkalling OPC UA 07042025.pdf

Referat møte 07042025.pdf

Møteinkalling OPC UA 05032025.pdf

Referat møte 05032025.pdf

## Vedlegg 6 - GanttDiagram

GanttDiagram.pdf

gantt\_diagram.py

## Vedlegg 7 - pdf

#### BACnet/IP and BBMDs

BACnetIP and BBMDs.pdf

#### Codesys Roadmap 2025 Q2

Codesys\_Roadmap\_2025\_Q2.pdf

#### 751-9301 Compact Controller 100

m07519301-00000000-0en.pdf

#### Cyber Security for Controller

mxxxxxxxx-CyberSecurity-0en.pdf

#### OPC-UA Security Model for Administrators

OPC-UA\_Security\_Model\_for\_Administrators\_V1.00.pdf

#### WAGO I/O System 750 OPC UA

txxxxxxxx-OPCUA-Server-0en-1.pdf

#### Understanding\_OPC\_eBook

Understanding\_OPC\_eBook.pdf

#### Quickstart Unified Automation

Quickstart\_0.10.2.pdf

## Vedlegg 8 - Bilder

Architecture-Diagram\_database\_cloud.jpg

ArchitectureDiagram-HubandSpoke-Redundant@2x.8a9d70a21cc8.png

ArchitectureDiagram-HubandSpoke@2x.3aff1adf9b76.png

ArchitectureDiagram-ScaleOut-Redundant@2x.c28d58b227a4.png

ArchitectureDiagram-ScaleOut@2x.b3203c9482eb.png

cloud-architecture-diagram.8a784a335965.png

enterprise-scada-architecture.509ea1a50cff.png

flytskjema\_CA.afdesign

flytskjema\_CA.png

iiot-architecture-diagram.e30f8b355256.png

Inductive-Automation-Ignition-Designer-Logo.png

Infrastruktur\_PLS\_Scada.afdesign

Infrastruktur\_Storm\_PLS\_Scada.png

Infrastruktur\_Test\_PLS\_Scada.afdesign

Infrastruktur\_Test\_PLS\_Scada.png

logo\_codesys.jpg

MM-21337-GWA-Display-PFC200.png

opc-ua-fig2.png

OPC-UA-security\_600x400px\_en.png

OPC-UA-security\_600x400px\_en.webp

prinsippskjema\_sdanlegg.afdesign

prinsippskjema\_sdanlegg.png

redundant-scada-architecture-enterprise.cb678254a05d.png

redundant-scada-architecture.a3d7edfbcec6.png

scada-architecture-diagram.8f58be1c22db.png

Sikker kommunikasjon og sertifikathåndtering i byggautomasjon med Tailscale og OPC UA.jpg

Tailscale-Logo-Black.svg.png

tailscale-logo-png\_seeklogo-396927.png

tailscalemeshnetwork.png

tailscalemeshnetworksubnet.png

uaexspert.png

WAGO\_Logo.png

## Vedlegg 9 - Codesys program

PlcLogic

visu

\_cnc

Archive.prj

Effektstyring-AllUsers.opt

Effektstyring-esbo-STORMELEKTRO.opt

Effektstyring.backup

Effektstyring.Device.Application.152aeda7-4222-4b51-a461-b42a3abf8f8b.compileinfo

Effektstyring.Device.Application.xml

Effektstyring.project

Effektstyring\_project.precompilecache

## Vedlegg 10 - UaExpert

cc100-5a1614.uap

## Vedlegg 11 - Skript

gantt\_diagram.py

InstallTailscale.sh

README.md

update\_tailscale\_certificates.sh

## Vedlegg 12 - Sluttbrukerveiledning

Sluttbrukerveiledning\_OPCUA\_Tailscale.pdf

## Vedlegg 13 - E-post

RE Opc UA storm.eml

RE OPC UA.eml

[WAGO Open Source Community] [CODESYS] OPC UA Certificates.eml