Niilo Rinne

Automaatiojärjestelmän modernisointi ja kyberturvallisuuden tehostaminen

PLC- ja WinCC-päivitys NIS2-direktiivin vaatimukset huomioiden

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkö- ja automaatiotekniikka

Insinöörityö

22.8.2024

Tiivistelmä

Tekijä:	Niilo Rinne
Otsikko:	Automaatiojärjestelmän modernisointi ja kyberturvallisuuden tehostaminen
Sivumäärä:	23 sivua
Aika:	22.8.2024
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Sähkö- ja automaatiotekniikka
Suuntautumisvaihtoehto:	Automaatiotekniikka
Ohjaajat:	Lehtori Tuomas Leppänen

Tämä insinöörityö käsittelee biokaasulaitoksen automaatiojärjestelmän modernisointia keskittyen erityisesti valvomon ja PLC-ohjelman päivitykseen sekä kyberturvallisuuden parantamiseen. Työssä toteutettiin WinCC-valvomojärjestelmän migraatio versiosta 7.3 versioon 8.0 sisältäen siirtymisen WebNavigator-pohjaisesta järjestelmästä WebUX-pohjaiseen ratkaisuun. PLC-ohjelmaan tehtiin muutoksia liittyen murskauslinjan päivitykseen, mikä vaati ohjelman version päivittämistä ja toiminnallisuuden muokkaamista.

Kyberturvallisuuden osalta työssä perehdyttiin NIS2-direktiivin vaatimuksiin ja IEC 62443 -standardisarjaan painottaen erityisesti datan salausta automaatiojärjestelmissä.

Työn tuloksena biokaasulaitoksen automaatiojärjestelmä päivitettiin vastaamaan paremmin nykyaikaisia vaatimuksia.

Avainsanat: WinCC, STEP 7, NIS2, verkkopohjaiset valvomot

Abstract

Author:	Niilo Rinne
Title:	Automation system modernization and cybersecurity enhancement
Number of Pages:	23 pages
Date:	22 August 2024
Degree:	Bachelor of Engineering
Degree Programme:	Electrical and Automation Engineering
Specialisation option:	Automation technology
Instructors:	Tuomas Leppänen, Senior Lecturer

This engineering thesis addresses the modernisation of the automation system of a biogas plant, focusing specifically on the upgrade of the control room and PLC program, as well as enhancing cybersecurity.

The project involved migrating the WinCC control system from version 7.3 to version 8.0, including the transition from a WebNavigator-based system to a WebUX-based solution. Waste crushing line PLC program version was updated, and functionality modified.

In terms of cybersecurity, the work explored the requirements of the NIS2 Directive and the IEC 62443 standard series, with a particular emphasis on data encryption within automation systems.

As a result of this work, the biogas plant's automation system was upgraded to better meet modern standards.

Keywords: WinCC, STEP 7, NIS2, Web-based monitoring systems

Sisällys

1 Johdanto

Tämä insinöörityö käsittelee biokaasulaitoksen automaatiojärjestelmän modernisointia. Työn tavoitteena on päivittää olemassa olevan automaatiojärjestelmän keskeisiä komponentteja sekä tarkastella ja parantaa sen kyberturvallisuutta, myös silmällä pitäen EU:n NIS2-direktiiviä. Koska kyseessä on jätteenkäsittelylaitos, tulevaisuudessa se tulee kuulumaan NIS2-direktiivin piiriin.

1.1 Työn tavoitteet ja menetelmät

Työn päätavoitteet ovat seuraavat:

1. Euroopan unionin tietoturvaa koskevaan NIS2-direktiiviin tutustuminen. Tarkoituksena on selvittää, mitä uusi direktiivi tarkoittaa käytännössä ja tuleeko sen mukana uusia teknisiä vaatimuksia.

2. Valvomo-ohjelmiston versionpäivitys ja siirtyminen pois vanhentunutta teknologiaa käyttävistä WebNavigator -pohjaisista käyttöliittymistä.

3. Ohjelmoitavan logiikan ohjelmamuutos.

Työssä on käytetty seuraavia menetelmiä:

1. Kirjallisuuskatsaus: Perehdytään alan kirjallisuuteen, manuaaleihin, standardeihin ja direktiiveihin.

2. Tapaustutkimus: Tutkitaan biokaasulaitoksen nykyistä automaatiojärjestelmää, ja pyritään tunnistamaan mahdollisia muutostarpeita.

3. Automaatiojärjestelmän päivitys ja migraatio: Toteutetaan versionpäivitykset ja ohjelmamuutokset.

1.2 Työn tilaaja

Insinöörityön tilaajana toimii suomalainen biokaasun tuotantolaitos, joka tuottaa biojätteestä ajoneuvojen käyttövoimaksi sopivaa biokaasua. Toimeksiantaja on pyytänyt pysyä nimettömänä, joten tästä syystä yritykseen viitataan jatkossa nimellä työn tilaaja tai toimeksiantaja. Lisäksi laitoksen tietoturvaa käsitellään työssä siinä laajuudessa kuin se on julkisessa dokumentissa tarkoituksenmukaista. Arkaluontaiset aiheet, niin tietoturvan kuin tuotantoprosessin näkökulmasta, on rajattu työn ulkopuolelle.

1.3 Työn rakenne

Työ jakautuu kahteen pääosioon: teoriaosuuteen ja käytännön toteutukseen. Teoriaosuudessa käsitellyt aiheet luovat pohjan käytännön toteutukselle.

Teoriaosuudessa perehdytään seuraaviin aiheisiin:

1. Siemensin tuotteet: Koska työssä käytetään pääasiassa Siemensin tuotteita, teoriaosuudessa perehdytään näihin tuotteisiin.

2. Käyttöliittymävaihtoehdot: WinCC WebNavigator -pohjaisten käyttöliittymien korvaaminen on yksi projektin tavoitteista. Teoriaosuudessa tarkastellaan eri vaihtoehtoja tämän toteuttamiseksi.

3. NIS2-direktiivi: EU:n NIS2-direktiivi asettaa uusia vaatimuksia järjestelmän turvallisuudelle. Teoriaosuudessa käsitellään tämän direktiivin sisältöä ja pyritään luomaan käsitys, mitä tämä direktiivi muuttaa käytännössä ja täyttääkö järjestelmä nykyisellään tai päivityksen jälkeen tekniset vaatimukset.

4. Kryptografia: NIS2-direktiiviä koskevassa kappaleessa huomataan kryptografian olevan yksi toimenpide kyberturvallisuusriskien hallitsemiseksi. Teoriaosuudessa perehdytään datan salaukseen ja miten sen voi käytännössä toteuttaa tietoliikenteessä käyttäen sertifikaatteja.

Soveltava osuus keskittyy käytännön näkökulmaan. Osuuden kappaleissa WinCC-migraatio ja Logiikkapäivitykset käydään läpi muutostarvetta, toteutusta ja käyttöönottoa.

2 Siemensin teollisuuden automaatiotuotteet

2.1 Siemensin rooli teollisuuden automaatiossa

Siemens AG on yksi maailman johtavista teknologiayrityksistä ja merkittävä toimija teollisuusautomaation alalla, erityisesti Euroopassa. Yrityksen juuret ulottuvat vuoteen 1847, jolloin saksalainen keksijä ja insinööri Werner von Siemens perusti yrityksen yhdessä liikekumppaneidensa kanssa. (Siemens 2024.)

Tässä insinöörityössä käsitellään Siemens SIMATIC -tuoteperheeseen kuuluvia ratkaisuja. Vuonna 1958 perustettu tuoteperhe sisältää laajan valikoiman automaatioratkaisuja, mukaan lukien ohjelmoitavat logiikat ja valvomo-ohjelmat, joissa keskeisiä työkaluja ovat STEP 7 ja WinCC.

2.2 STEP 7

STEP 7 (Steuerungen Einfacher Programmieren 7) on Siemensin kehittämä ohjelmistopaketti, joka toimii työkaluna SIMATIC-sarjan ohjelmoitavien logiikoiden (PLC) konfiguroinnissa ja ohjelmoinnissa. Käytettävät ohjelmointikielet noudattavat EN 61131 -standardia. Ohjelmistopaketti tarjoaa myös versiosta riippuen erilaisia simulointimahdollisuuksia, jotka mahdollistavat ohjelman testaamisen virtuaaliympäristössä. Lisäksi siinä on integroituja diagnostiikkatyökaluja, jotka auttavat vianetsinnässä ja järjestelmän seurannassa.

STEP 7 -ohjelmistosta on useita versioita, jotka voidaan jakaa kahteen ryhmään, SIMATIC Manager ja TIA Portal. SIMATIC Manager oli ensisijainen työkalu ennen TIA Portalin julkaisua. Vaikka TIA Portalista on tullut suositumpi

vaihtoehto uusissa projekteissa, SIMATIC Manager on edelleen laajalti käytössä ja osa PCS 7 -prosessinohjausjärjestelmää.

STEP 7:llä ohjelmoitavat PLC:t toimivat syklisesti toistaen jatkuvasti tiettyä toimintaketjua. Tämä syklinen prosessi koostuu kolmesta pääosasta: tulojen luku, ohjelman suoritus ja lähtöjen kirjoitus.

Syklin alussa PLC lukee kaikkien tulojen tilan ja tallentaa ne prosessikuvaan. Tämä varmistaa, että ohjelma toimii yhtenäisen datasetin kanssa koko syklin ajan. Seuraavaksi PLC suorittaa käyttäjän luoman ohjelman, joka koostuu erilaisista ohjelmalohkoista. Organisaatiolohkot (OB) määrittävät ohjelman rakenteen ja suoritusjärjestyksen. Toimintalohkot (FB) sisältävät toistuvasti käytettäviä ohjelman osia omalla datamuistillaan, kun taas funktiot (FC) suorittavat toistuvia tehtäviä ilman omaa muistia. Datalohkot (DB) varastoivat ohjelman käyttämää dataa.

Syklin lopussa ohjelman suorituksen tulokset kirjoitetaan lähtöihin, ja PLC päivittää fyysisten lähtöjen tilan prosessikuvan mukaisesti. Tämä syklinen prosessi toistuu jatkuvasti, tyypillisesti millisekunneissa, riippuen PLC:n suorituskyvystä ja ohjelman monimutkaisuudesta. Syklinen toiminta takaa, että PLC reagoi muutoksiin nopeasti ja ennustettavasti.

2.3 WinCC

Siemensin WinCC-ohjelmistoperhe sisältää useita versioita. WinCC on kehittynyt ajan myötä ja markkinoilla on ollut aiempia versioita, jotka ovat poistuneet aktiivisesta tuotevalikoimasta. Perinteinen niin sanottu Classic WinCC on nykyään versiossa 8.0. Toinen erillinen WinCC on WinCC OA. Näiden lisäksi on TIA Portaliin integroituja versioita, kuten Comfort, Advanced, Professional ja Unified.

WinCC Open Architecture (OA), entiseltä nimeltään PVSS, on itävaltalaisen yrityksen ETM professional control GmbH kehittämä. Vuonna 2007 ETM:stä tuli Siemens AG:n omistama tytäryhtiö. WinCC OA:n avulla voidaan rakentaa

valvomojärjestelmiä, jotka ovat valmistajasta ja alustasta riippumattomia. Tämä mahdollistaa esimerkiksi Linux-ympäristön käytön, mikä poikkeaa Siemensin tyypillisestä Windows-pohjaisuudesta ja suljetummasta ekosysteemistä. Se on siis nimensä mukaan avoin järjestelmä, joka on suunniteltu erityisesti suuren mittakaavan monimutkaisiin sovelluksiin ja projekteihin. (ETM 2024.)

WinCC Unified on Siemensin uusi, vuonna 2020 julkaistu järjestelmä. Unified on uudelleen rakennettu WinCC, joka perustuu nykyaikaiseen verkkoteknologiaan, kuten HTML5, SVG ja javascript. Unified mahdollistaa operoinnin kirjautuneena verkkoselaimella. Myös uudet SIMATIC HMI Unified -paneelit eroavat aiemmista Siemensin HMI-paneeleista käyttäessään verkkoteknologiaa. Paneelit ovat myös siirtyneet Linux-pohjaisiksi Windowsista. Unified on nousemassa vahvasti esille, ja Siemens vaikuttaa sitoutuneelta sen kehitykseen, paneeleiden kehityksen osalta pääpaino onkin siirtynyt Unifiediin.

Työhön kuuluu WinCC V7/8-migraatio, joka tehdään versiosta 7.3 versioon 8.0. Siemens itse esittelee järjestelmän seuraavasti:

> SIMATIC WinCC V7 SCADA -ohjelmisto on innovatiivinen, skaalautuva prosessin visualisointijärjestelmä, jossa on lukuisia suorituskykyisiä toimintoja automatisoitujen prosessien valvontaan kaikilla teollisuudenaloilla. Olipa kyseessä sitten yhden käyttäjän järjestelmä tai hajautettu monikäyttäjäjärjestelmä, jossa on redundantteja palvelimia. Järjestelmä tarjoaa käyttäjälle täydelliset SCADA-toiminnot prosessien visualisointitehtäviin, aina uusimpiin älykkäänteollisuuden ratkaisuihin. Järjestelmän toiminnallisuutta voidaan laajentaa ja mukauttaa juuri sinun tarpeisiisi WinCC V7:n lisävarusteiden avulla. WinCC Add-ons lisävarusteiden ja yleisten SCADA-vaihtoehtojen avulla. (Siemens 2018.)

3 Verkkopohjaiset valvomot

3.1 Mikä on verkkopohjainen valvomo

Verkkopohjaisten valvomoiden yleistymiseen on useita syitä. Ilmiö heijastaa laajempaa trendiä, jossa teknologiaa siirretään yhä enemmän verkko- ja pilvipohjaiseen ympäristöön. Kun tehdään verkkopohjaista valvomoa, yksi

suurimmista hyödyistä on selaimen käyttö käyttöliittymänä. Kun päätelaitteelta ei vaadita kuin nykyaikainen selain, tämä tuo joustavuutta. Usein valvomot vaativat ohjelmien asennusta ja ovat tästä syystä tyypillisesti riippuvaisia myös Windows-käyttöjärjestelmästä. Selainpohjaisia käyttöliittymiä taas voidaan käyttää helposti eri käyttöjärjestelmillä, mukaan lukien Unix-pohjaiset Linux-, Android- ja iOS-laitteet.

Verkkopohjaiset valvomot tarjoavat myös kätevän tavan etäkäyttöön, kun tavallisesti etäkäyttö on tehty ottamalla laitoksen tietokone hallintaan. Verkkopohjaisella valvomolla tämän voi tehdä liittymällä laitoksen lähiverkkoon ja avaamalla valvomo-ohjelman selaimessa. Vaihtoehtoinen harvinaisempi ratkaisu on asettaa valvomo laajaverkkoon, kuten internetiin, mikä mahdollistaa pääsyn myös lähiverkon ulkopuolelta.

3.2 SIMATIC WinCC 7/8 -verkkopohjaiset valvomot

3.2.1 WebNavigator

WinCC WebNavigator on lisäosa, joka on käytettävissä SIMATIC WinCC tai WinCC Runtime Professionalia käyttäessä. WebNavigator mahdollistaa tehtaiden ohjauksen ja valvonnan laajaverkon tai lähiverkon kautta. WebNavigatorin käyttöä varten on konfiguroitava verkkopalvelin, johon verkkoasiakkaat ottavat yhteyttä. WebNavigator toimii Microsoftin Internet Information Services (IIS) -palvelimen päällä. Operoitavia verkkoasiakkaita voi olla jopa 150, WebNavigator perustuu ActiveX-kehysohjelmaan, jonka takia se vaatii selainta käyttäessä Internet Explorer -tai Edge-selaimen Internet Explorer -tilassa. Toinen vaihtoehto on käyttää WinCC Viewer RT -ohjelmaa, joka on tietokoneella asennettava ohjelma, ja vaatii Windows-pohjaisen tietokoneen. (Siemens 2022.)

3.2.2 WebUX

WebUX on WebNavigatorin tapaan verkkopohjainen valvomoratkaisu, mutta se eroaa merkittävästi toimintaperiaatteidensa osalta. Kuva 1 osoittaa näitä eroja,

esimerkiksi WebUX toimii html5- ja SVG-standardien mukaisesti. Lähes kaikki nykyaikaiset selaimet tukevat näitä standardeja, mikä tekee WebUX:ista laite- ja käyttöjärjestelmä riippumattoman.

WebUX on aiemmin ollut huomattavasti rajoittuneempi toiminnaltaan verrattuna WebNavigatoriin, mutta uusimman WinCC 8.0 -julkaisun mukana myös WebUX:iin on tullut päivityksiä, jotka tekevät siitä nyt soveltuvamman myös monimutkaisiin järjestelmiin. WebUX-verkkopalvelin toimii, kuten WebNavigatorikin, Microsoftin IIS-palvelimen päällä.

WebUX-näkymä määritetään käyttäjien mukaan, kullekin käyttäjille annetaan aloitusnäyttö ja määritetään oikeudet. Tämä mahdollistaa esimerkiksi mobiililaitteelle oman käyttäjän tekemisen, jolle voidaan määrittää räätälöity näkymä pienemmällä ja paremmin mobiililaitteelle sopivalla resoluutiolla. WebUX:iin siirtymisen tai testaamisen kynnystä madaltaa sen mahdollisuus käyttää WebNavigator-lisenssejä. Lisenssejä on kahdenlaisia, monitorointiin ja operointiin. (Siemens 2014.)

Distinction WebUX - WebNavigator

WebUX	WebNavigator
Based on generally established web standards	Based on ActiveX technology from Microsoft
Can be used with any browser	Only supports Microsoft Internet Explorer
Can be used for a large number of devices regardless of the operating system, for example, tablets, computers and smartphones	Can only be used with Windows computers
Does not require a client installation	Requires a client installation
Standard user rights are sufficient	Requires administrator rights for installation

Kuva 1. WebUX ja WebNavigator -tekniikoiden vertailu. WebUX perustuu nykyaikaisiin standardeihin, tukee kaikkia selaimia ja laitteita käyttöjärjestelmästä riippumatta. WebNavigator puolestaan perustuu Microsoftin ActiveX-teknologiaan, tukee vain Internet Exploreria Windows-tietokoneilla tai vaatii asiakasohjelman asennuksen sekä järjestelmänvalvojan oikeudet asennukseen. (Siemens 2014.)

4 Tietoturva

Historiallisesti tietoturva automaatiojärjestelmissä on saattanut jäädä huomiotta, ehkä sen merkitystä ei olla täysin ymmärretty tai sitä ei pidetty oleellisena.

Tämä suhtautuminen tulee osittain myös siitä, että automaatiojärjestelmät ovat olleet usein suljettuja ja niitä on näin ollen pidetty turvallisena. Tänä päivänä tietoturvaan kiinnitetään enemmän huomiota, erityisesti kun automaatioverkot yhdistyvät entistä useammin internettiin. Tämä tapahtuu usein etäkäytön tai muiden tarpeiden vuoksi. Yhteys internettiin lisää automaatiojärjestelmien alttiutta erilaisille tietoturvauhille.

Automaatiojärjestelmien tietoturvaan kiinnitetään erityisesti huomiota, kun kyseessä on kriittistä infrastruktuuria. Muutos johtuu automaatiojärjestelmien lisääntymisestä infrastruktuurissa ja tietoisuuden kasvusta maailmalla olleista automaatiojärjestelmiin kohdistuneista kyberhyökkäyksistä. Näistä tunnetuimpia ovat Ukrainan sähköverkkoihin kohdistuneet hyökkäykset ja Stuxnet.

Stuxnetistä kiinnostavan aiheen kannalta tekee sen jonkinasteinen kohdistuminen valvonta- ja ohjausjärjestelmiin, jotka käyttävät Siemensin SIMATIC-ohjelmistoja. Euroopan unionin kyberturvallisuusviraston ENISAN julkaiseman raportin mukaan Stuxnet hyödyntää useita haavoittuvuuksia Windows-käyttöjärjestelmässä tarttuakseen kohteeseen ja levitäkseen. Tartunta tapahtuu USB-asemien tai avoimien verkkojakojen kautta. Haittaohjelmaan kuuluu rootkit-komponentti, joka piilottaa sen sisällön saastuneissa WinCC-järjestelmissä. Saastunutta järjestelmää voi yleensä ohjata etänä hyökkääjän toimesta, mikä käytännössä tarkoittaa, että hyökkääjä saa täyden hallinnan kohteena olevasta laitoksesta. (ENISA 2010.)

4.1 NIS

4.1.1 NIS2-direktiivi

Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 (14.12.2022) toimenpiteistä, joilla pyritään saavuttamaan korkea yhteinen kyberturvallisuuden taso unionissa ja jolla muutetaan asetusta (EU) N910/2014 ja direktiiviä (EU) 2018/1972 sekä kumotaan direktiivi (EU) 2016/1148. (Euroopan parlamentti ja neuvosto, 2022.)

Direktiivi siis korvaa edeltäjänsä, ja sen päätavoitteena on vahvistaa kyberturvallisuuden tasoa kriittisillä ja tärkeillä sektoreilla ja yhdenmukaistaa kyberturvallisuusvaatimuksia EU:n jäsenvaltioiden välillä esimerkiksi laajentamalla alkuperäisen direktiivin soveltamisalaa kattamaan nyt useampia sektoreita. Sektorit jaetaan keskeisiin ja tärkeihin toimijoihin, joista keskeisillä toimijoilla on tiukemmat kriteerit.

Direktiiviä sovelletaan kaikkiin julkisiin ja yksityisiin toimijoihin, jotka täyttävät tai ylittävät keskisuuruisen yrityksen ehdot ja toimivat unionissa. Direktiivi koskee myös tiettyjä toimijoita koosta riippumatta, kuten kriittisten palvelujen tarjoajia, joiden toiminnan häiriöt voivat vaikuttaa merkittävästi yhteiskuntaan, talouteen tai turvallisuuteen. (Euroopan parlamentti ja neuvosto, 2022, 3 artikla.)

Jäsenvaltioiden on annettava ja julkaistava direktiivin noudattamisen edellyttämät säännökset viimeistään 17. päivänä lokakuuta 2024 (Euroopan parlamentti ja neuvosto, 2022, 41 artikla). Jäsenvaltioiden on siis implementoitava direktiivin vaatimukset kansalliseen lainsäädäntöön, luotava kansallinen kyberturvallisuusstrategia ja perustettava tai nimettävä toimivaltaisia viranomaisia valvomaan direktiivin noudattamista.

4.1.2 Raportointivelvoitteet

NIS2-direktiivi asettaa jäsenvaltioille velvoitteen varmistaa, että keskeiset ja tärkeät toimijat ilmoittavat merkittävistä poikkeamista viipymättä kansalliselle CSIRT-yksikölle tai toimivaltaiselle viranomaiselle. Ilmoitus on tehtävä ilman aiheetonta viivytystä ja viimeistään 24 tunnin kuluessa poikkeaman havaitsemisesta. Toimijoiden tulee toimittaa päivitetty poikkeamailmoitus 72 tunnin sisällä ja lopullinen raportti kuukauden kuluessa. Poikkeama katsotaan merkittäväksi, jos se aiheuttaa tai voi aiheuttaa vakavan häiriön palveluiden toiminnassa tai merkittäviä taloudellisia tappioita, sekä jos se vaikuttaa muihin ihmisiin tai organisaatioihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. (Euroopan parlamentti ja neuvosto, 2022, 23 artikla.)

4.1.3 10 Toimenpidettä

21. Artiklassa esitetään kymmenen toimenpidettä kyberturvallisuusriskien hallitsemiseksi:

a) Riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat.

b) Poikkeamien käsittely.

c) Toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta.

d) Toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat.

e) Verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen.

f) Toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta.

g) Perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus.

h) Toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvitessa salauksen käyttöä.

i) Henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta.

j) Tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.

Toimenpiteissä painotetaan paljon käytäntöjen kehittämistä. Näiden käytäntöjen avulla havaittaisiin poikkeamat ja reagoitaisiin ennalta suunnitellusti.

Toimenpiteissä mainitaan myös toimitusketjun turvallisuus, josta puhutaan enemmän artiklassa 24. Artiklan sisältö tarkoittaa, että jäsenvaltiot voivat vaatia keskeisiä ja tärkeitä toimijoita käyttämään määrättyjä tieto- ja viestintätekniikan palveluita. Toimenpiteissä mainitaan myös kryptografia eli datan salaaminen.

4.1.4 Huomioita direktiivistä

NIS2-direktiivi tuo mukanaan raportointivelvoitteita keskeisille ja tärkeille toimijoille, ja näiden velvoitteiden laiminlyönti voi johtaa merkittäviin sakkoihin. Huomionarvoista on, että direktiivissä ei juurikaan määritellä yksityiskohtaisia teknisiä vaatimuksia. Edellisessä kappaleessa esitellyt 10 toimenpidettä direktiivistä kuitenkin löytyy, ja niitä tulee soveltaa tarpeen mukaan.

Teoriaosuuden lopuksi perehdytään vielä kolmeen näistä kymmenestä toimenpiteestä: kryptografiaan, käyttäjähallintaan ja monivaiheiseen tunnistautumiseen. Lisäksi teoriaosuuteen sisältyy yleiskatsaus IEC 62443 -standardisarjaan, jota pidetään keskeisenä ohjenuorana operatiivisten teknologioiden verkkojen osalta, kun halutaan määritellä tarkempia teknisiä vaatimuksia.

4.2 Datan salaus

Yksi tehokkaimmista tietoturvakäytännöistä on tietoliikenteensalaus, joka toimii työkaluna tiedon turvaamisessa. Salausprosessissa tiedot muunnetaan epäselväksi merkkijonoksi, joka puretaan salaisella avaimella takaisin alkuperäiseen muotoon. Se estää ulkopuolisia osapuolia lukemasta ja ymmärtämästä tiedonsiirron sisältöä. Nykypäivänä lähes kaikki Internetin käyttäjät hyödyntävät HTTPS-yhteyttä. Ennen HTTPS-protokollan yleistymistä verkkoliikenne perustui pääasiassa HTTP-protokollaan.

HTTP (Hypertext Transfer Protocol) on sovelluskerroksen protokolla hypermedia-asiakirjojen, kuten HTML:n, välittämiseen. Se on suunniteltu verkkoselaimien ja verkkopalvelimien väliseen viestintään, mutta sitä voidaan käyttää myös muihin tarkoituksiin. HTTP noudattaa klassista asiakas-palvelin-

mallia, jossa asiakas avaa yhteyden tehdäkseen pyynnön ja odottaa kunnes saa vastauksen. HTTP on tilaton protokolla, mikä tarkoittaa, että palvelin ei säilytä tilaa kahden pyynnön välillä. Kun asiakas haluaa kommunikoida HTTP:n avulla, se avaa TCP-yhteyden palvelimeen. Tämä on avoin yhteys, eli tieto liikkuu asiakkaan ja palvelimen välillä juuri sellaisena, kuin asiakas tai palvelin sen lähettää. (MDN Web Docs, 2023.)

Tästä syystä protokollasta kehitettiin turvallisempi versio HTTPS (Hypertext Transfer Protocol Secure). Se käyttää pääasiassa TLS (Transport Layer Security) -salausta varmistaakseen, että tiedot ovat suojattuja. Kaikki nykyaikaiset selaimet tukevat TLS-protokollaa, ja ne vaativat palvelinta toimittamaan pätevän digitaalisen varmenteen vahvistaakseen identiteettinsä turvallisen yhteyden luomiseksi.

Digitaaliset varmenteet eli sertifikaatit ovat keskeinen osa kryptausta. Ne toimivat virtuaalisina henkilöllisyystodistuksina verkkosivustoille ja palvelimille. Sertifikaatit sisältävät tietoja, kuten kenelle se on myönnetty, julkisen avaimen, käytetyn salausalgoritmin, voimassaoloajan ja sertifikaatin allekirjoittajan. Internetissä sertifikaatit on usein allekirjoitettu luotettavan varmenteenmyöntäjän toimesta (Certificate Authority, CA). Jos tarkastellaan osoitteen https://www.google.com tämänhetkistä sertifikaattia, myöntäjä on Google Trust Services LLC, se käyttää SHA-256 salausalgoritmia ja vanhenee 4.3.2024.

Automaatiosovelluksissa yleinen vaihtoehto CA:n allekirjoittamille sertifikaateille ovat itse allekirjoitetut sertifikaatit (Self-signed Certificate). Tällöin kyseessä on mutuaalinen autentikointi, joka perustuu siihen, että sertifikaatin allekirjoittaja toimittaa sekä palvelimelle että asiakkaalle sertifikaatit.

Siemens tarjoaa työkalun nimeltä Certificate Manager sertifikaattien luomiseen. Tämä mahdollistaa sekä itse allekirjoitettujen sertifikaattien että paikallisen verkon tunnetun varmenteen (CA) sertifikaattien käytön.

TLS-salauksesta puhuttaessa nousee usein esiin termi SHA-256 (Secure Hash Algorithm 256-bit), joka on yksi SHA-2 (Secure Hash Algorithm 2) -perheen algoritmeista, joka on ottanut vahvan aseman monissa tietoturvakäytöissä. Tähän mennessä ei ole tunnettuja tehokkaita hyökkäyksiä SHA-256 vastaan. Paras vaihtoehto sen purkamiseen ilman asianmukaista avainta on raakavoima. Käytännössä tämä siis tarkoittaa alkuperäisen datan arvaamista ja tarkastamista, tuottaako se vastaavan hajautusarvon.

Algoritmin tehokkuus perustuu sen tuottamaan 256 bittiseen hajautusarvoon. Tämä tarkoittaa, että on olemassa kaksi potenssiin 256 eri yhdistelmää, joista hyökkääjän olisi löydettävä oikea. Usein SHA-256-salattujen salasanojenonnistunut purku perustuukin tietokantoihin, joissa on listattuna salasanoja, joista yritetään etsiä oikea. On myös mahdollista käyttää raakavoimaa, mutta salasanan pituuden ylittäessä 12 merkkiä, jos numerot ja erikoismerkit ovat käytössä, ylittää tarvittava laskentateho salasanan murtamiseen kohtuullisessa ajassa melko varmasti hyökkääjän resurssit.

4.3 Käyttäjähallinta ja monivaiheinen tunnistautuminen

Käyttäjänhallinta on kriittinen osa tietojärjestelmien turvallisuutta. Hyvin toteutettuna se mahdollistaa pääsynhallinnan, jossa määritellään käyttäjä- tai ryhmäkohtainen oikeus käyttää tiettyjä järjestelmiä ja resursseja. Tämä sisältää käyttäjien luomisen, oikeuksien määrittämisen ja hallinnan, sekä käyttäjien toiminnan seuraamisen ja dokumentoinnin.

Monivaiheinen tunnistautuminen (MFA), yleensä kaksivaiheinen (2FA) on tarvittaessa tehokas lisä käyttäjänhallintaan. 2FA vaatii käyttäjältä toisen tunnistautumistavan, kuten kertakäyttöisen koodin, joka saadaan tekstiviestillä, sähköpostilla tai autentikointisovelluksen kautta, ennen kuin pääsy järjestelmään myönnetään. Tämä vaikeuttaa luvatonta pääsyä järjestelmään, vaikka käyttäjän salasana olisi vuotanut.

WinCC-järjestelmissä on toki perinteinen mahdollisuus käyttäjäryhmien ja käyttäjien luomiseen, jossa ryhmälle annetaan oikeuksia ja käyttäjät ovat jonkin

ryhmän jäseniä. Kun halutaan parantaa ja keskittää käyttäjänhallintaa, siihen on erillinen työkalu SIMATIC Logon. Sillä voidaan hyödyntää Windowsin käyttäjäryhmiä ja käyttöoikeuksia. Tämä tarkoittaa, että käyttäjä kirjautuu WinCC-järjestelmään samoilla active directory (AD) -tunnuksilla, joita hän käyttää Windowsille kirjautumiseen. SIMATIC Logon tarjoaa myös diagnostiikkatietoja, kuten tapahtumalokin keräämisen, jonka avulla voidaan seurata käyttäjien toimintaa.

WinCC 7/8 -järjestelmään 2FA:n implementointiin ei ole valmiita työkaluja, mutta teknisesti katsottuna tähän on vaihtoehtoja. On mahdollista rakentaa oma ratkaisu tai hyödyntää kolmannen osapuolen palveluja. Yksinkertaisimmillaanhan käyttäjä pakotetaan kirjautumisen jälkeen odottamaan toista autentikointia ennen pääsyä järjestelmään.

Käyttäjänhallinnan ja 2FA:n tarkempi tarkastelu ja toteutus tehdään insinöörityön ulkopuolella, ja näin ollen se puuttuu soveltavasta osuudesta.

4.4 IEC 62443 -standardisarjan yleiskatsaus

IEC 62443 -standardisarja on kehitetty yhteistyössä International Society of Automation (ISA) ja International Electrotechnical Commission (IEC) kanssa. Se on tarkoitettu vastaamaan tarpeeseen parantaa automaation kyberturvallisuutta. Sarja sisältää ohjeita siitä, mitä tulisi tehdä, sekä teknisiä ratkaisuja, jonka lisäksi ne painottavat henkilöstön koulutuksen ja tietoisuuden sekä organisaation sisäisten käytäntöjen merkitystä tietoturvan integroimisessa päivittäiseen toimintaan. (International Society of Automation 2024.)

Standardisarja on suunnattu useille sidosryhmille. Sarjan eri osat vaihtelevat yksityiskohtaisuudeltaan ja kohderyhmältään. Osa standardeista käsittelee teknisiä yksityiskohtia, toiset osat taas maalaavat laajemman kuvan keskittyen organisaatiotason strategioihin ja käytäntöihin. Sarja esittelee useita käsitteitä, kuten verkon segmentointi osiin (zone and conduit model), turvallisuustasot (security levels) ja perusvaatimukset (foundational requirements), joiden avulla

voidaan arvioida ja parantaa IACS-järjestelmien kyberturvallisuutta. (International Society of Automation 2024.)

Vaikka NIS2-direktiivi ei nimenomaisesti mainitse IEC 62443 -standardisarjaa, direktiivissä kuitenkin viitataan muihin kansainvälisiin ISO/IEC-standardeihin. Sarjan useat osat ovat relevantteja NIS2-vaatimusten täyttämisessä operational technology (OT) -verkkojen osalta, samaan tapaan kuin ISO 27001 on information technology (IT) -verkkojen osalta.

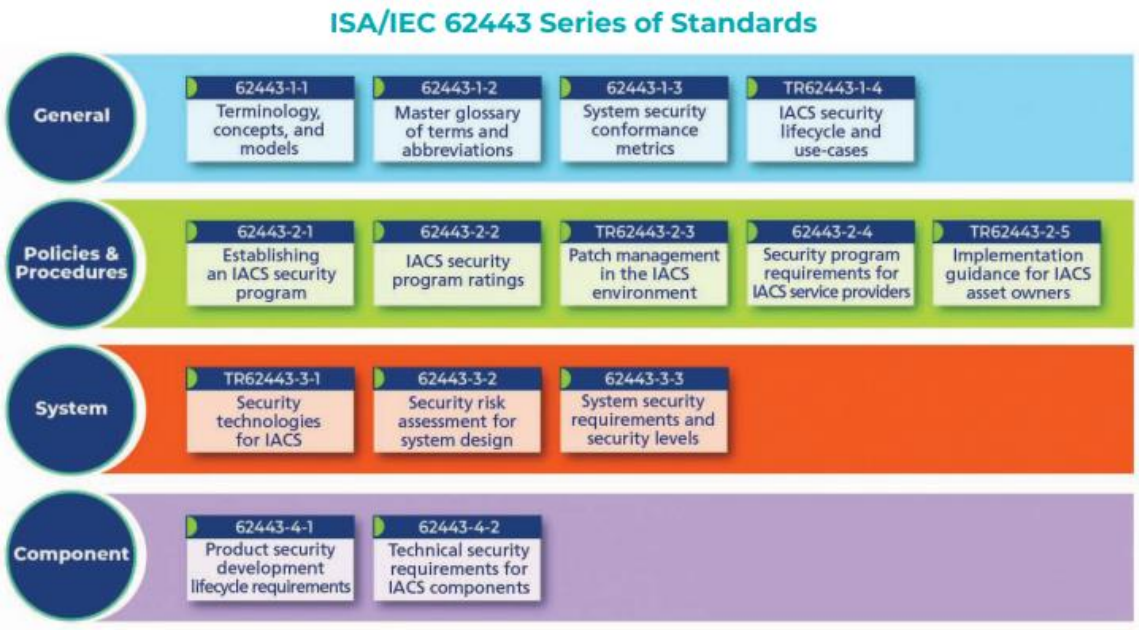
NIS2 näkökulmasta kaikista relevanteimmat osat voisivat olla:

1. IEC 62443-2-1: Osa käsittelee IACS (Industrial Automation and Control Systems) turvallisuushallintajärjestelmän vaatimuksia.

2. IEC 62443-2-2: Osa käsittelee keinoja IACS turvallisuushallintajärjestelmän arvioimiseen.

3. IEC 62443-3-2: Osa keskittyy järjestelmän suunnittelun turvallisuusriskien arviointiin.

4. IEC 62443-3-3: Osa määrittelee järjestelmän turvallisuusvaatimukset ja turvallisuustasot.



Kuva 2. ISA/IEC 62443 -standardisarjan yleiskatsaus. Sarjan 14 osaa on jaettu neljään pääryhmään: Yleiset standardit (General), Käytännöt ja menettelytavat (Policies & Procedures), Järjestelmä (System), ja Komponentit (Component). (International Society of Automation 2024, Figure 2.)

5 WinCC-migraatio

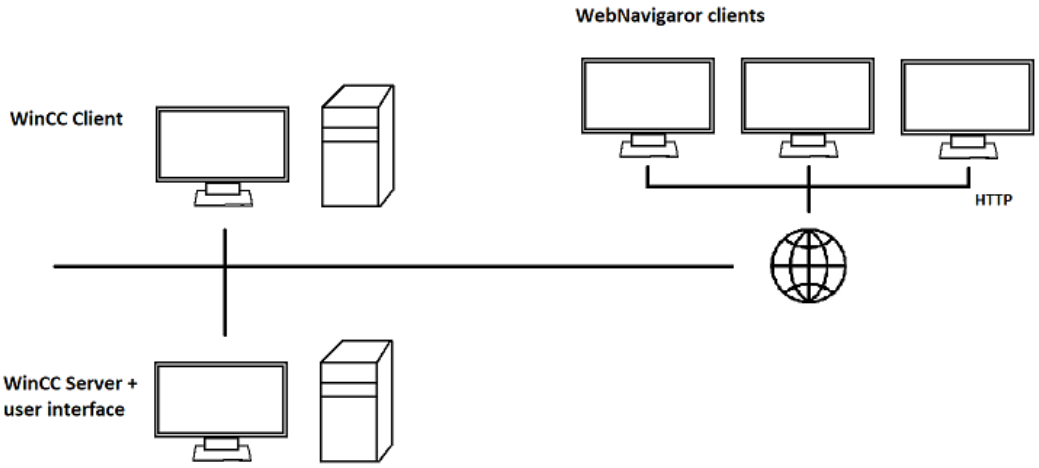
5.1 Lähtökohdat ja tavoitteet

Biokaasulaitoksella on WinCC 7.3, jossa on WebNavigator-verkkopalvelin ja käyttöliittymiä. Projektissa päädyttiin pitämään verkkopohjaiset käyttöliittymät, mutta ne muutettaisiin käyttämään WebUX:ia. Tämä on kustannustehokas tapa korvata WebNavigator, kun vanhat lisenssit voidaan antaa WebUX:in käyttöön, joten lisenssikustannuksia ei siltä osin synny. Myös WinCC 8.0 tuomat WebUX-päivitykset tekevät siitä nykyisin hyvän vaihtoedon verkkopohjaiselle valvomolle ja kehityssuunta näyttäisi, että myös tulevaisuuden versiopäivityksissä tähän panostettaisiin.

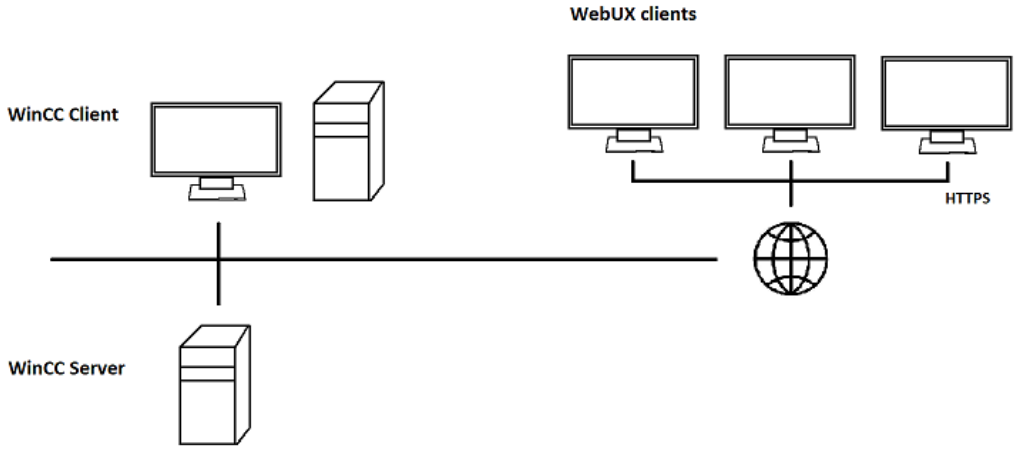
Tämä kuitenkin tarkoittaa, että on oleellista tehdä päivitys versioon 8.0, jolloin WebUX tukee C-skriptejä ja Customized object -toiminnallisuutta. Versiopäivitys myös nostaa järjestelmän käyttöikää. Siemens on sitoutunut pitämään version aktiivisessa tuotevalikoimassa ainakin vuoden 2031 maaliskuulle asti.

Verkkoliikenteen kommunikoinnissa siirrytään HTTPS-protokollaan. Tämä edellyttää sertifikaattien luomista ja WebUX:in konfigurointia käyttämään protokollaa.

Alkuperäiseen järjestelmään kuuluu yhteensä viisi käyttöliittymää, yksi WinCC RT -asiakas ja kolme WebNavigator-verkkoasiakasta, myös palvelinkonetta käytetään käyttöliittymänä. Päivityksen yhteydessä palvelinkone on tarkoitus siirtää sähkötilaan ja käyttää prosessinohjaukseen WinCC RT -asiakasta ja verkkoasiakkaita.



Kuva 3. Vanha WinCC-topologia. Käytössä on WinCC palvelin, asiakas ja kolme sisäverkossa olevaa WebNavigator verkkoasiakasta. Kommunikointi perustuu HTTP-protokollaan.



Kuva 4. Uusi WinCC-topologia. Palvelimen käyttöliittymä on poistettu käytöstä, palvelin on siirretty sähkötilaan ja kommunikointi on vaihdettu HTTPS-protokollaan.

5.2 Migraatio

Kun päivitetään versioon 8.0, migraatio on suositeltavaa tehdä joko suoraan tai vanhemmissa versioissa version 7.3 SE kautta. Tässä tapauksessa alkuperäinen versio on 7.3, joten versiokorotuksen voi tehdä ilman välivaiheita.

Koska projektissa uusitaan palvelinkone, korotus tehdään uudella koneella. Vanha projekti kopioidaan Project Duplicator -lisäohjelmalla. Kun uudella palvelinkoneella on WinCC 8.0, avataan projekti ja tehdään migraatio. Versiokorotuksen jälkeen korjataan mahdollisesti ilmenneet virheet ja tehdään projektiin tarvittavat muutokset, kuten tietokoneen nimi. Tämän jälkeen ohjelman teoriassa tulisi toimia.

Koska migraation yhteydessä otetaan WebUX käyttöön. Projektissa täytyy luoda WebUX-käyttäjä, määrittää objekteille verkkokäyttö ja määrittää WebUX-käyttäjän näkymä.

5.3 Toteutus

WinCC-migraation toteutus sujui pääosin ongelmitta, mutta prosessissa havaittiin muutamia haasteita. Konversiossa ei itsessään ilmennyt virheitä,

mutta kaikki Visual Basic -skriptit eivät migraation jälkeen toimineet vanhaan tapaan. Tämä johtui syntaksimuutoksista, joita migraatiotyökalu tai WinCC:n syntaksintarkistus ei tunnistanut. Lisäksi osa vanhoista visualisointiobjekteista ei ollut yhteensopivia WebUX-ympäristön kanssa.

Visual Basic -skriptien syntaksi päivitettiin manuaalisesti, minkä jälkeen ohjelman toiminta normalisoitui.

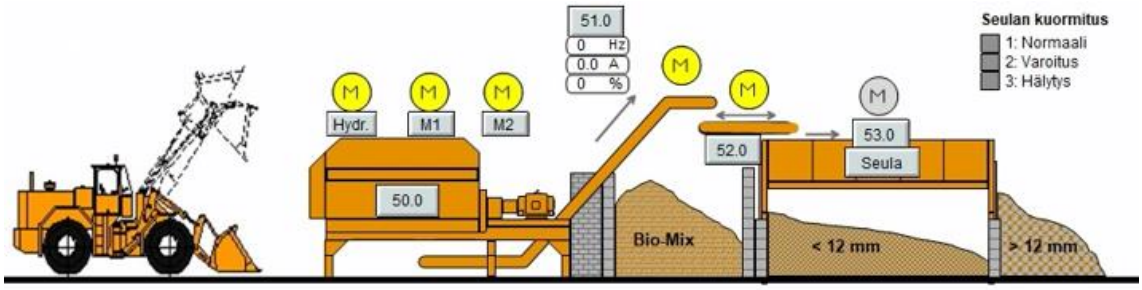
WebUX:ille ei tarvinnut luoda omaa näkymää. Sitä on tarkoitus käyttää pääasiassa tietokoneelta, joten vanha WebNavigator käyttöliittymä on tähän tarkoitukseen sopiva. Ongelmalliset kustomoidut visualisointiobjektit liittyivät tankkien pinnankorkeuden visualisointiin. Nämä objektit korvattiin hieman yksinkertaistaen oletusobjekteilla, joille määritettiin dynaaminen täyttö -toiminto pinnankorkeuden visualisointia varten. Näin visualisointi saatiin toimimaan myös WebUX-näkymässä.

HTTPS-kommunikointia varten luotiin Siemensin Certificate Manager -työkalulla itse allekirjoitetut sertifikaatit, jotka asennettiin manuaalisesti asiakaskoneille. Tämän jälkeen WinCC WebUX Configuration Managerilla konfiguroitiin WebUX käyttämään HTTPS-protokollaa uusilla sertifikaateilla.

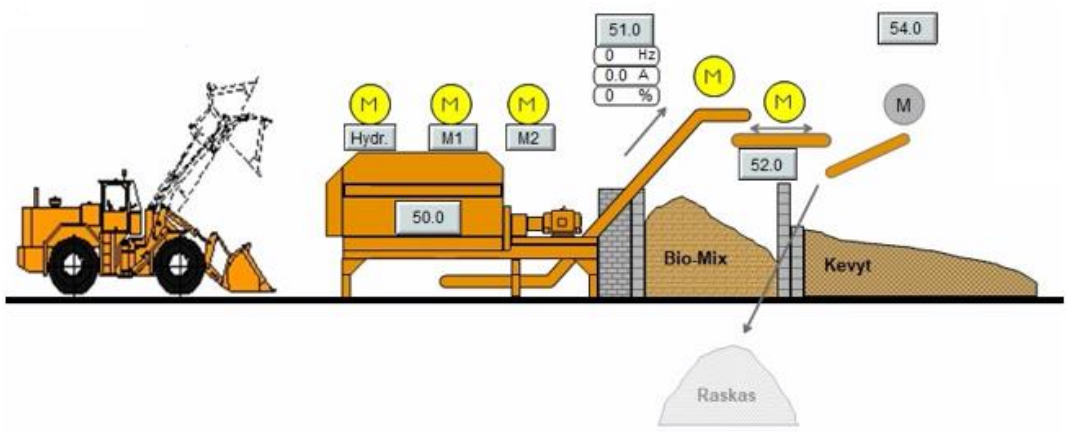
6 Logiikkapäivitykset

6.1 Muutostarve

Biokaasulaitoksen murskauslinjan toiminnallisuutta haluttiin muuttaa. Alkuperäinen linja lajitteli murskatun jätteen kahteen kategoriaan: Bio-Mixiin sekä koon mukaan yli ja alle 12 mm jakeisiin. Kokoon perustuva seulonta poistettiin käytöstä, ja seulonta korvattiin uudella heittimellä. Uusi heitin mahdollistaa jätteen lajittelun painon mukaan.



Kuva 5. WinCC käyttöliittymän näkymä vanhasta murskauslinjasta. Vanhassa linjassa on seula, jolla lajitellaan jätettä koon perusteella.



Kuva 6. WinCC käyttöliittymän näkymä uudesta murskauslinjasta. Seula on korvattu heittimellä, joka lajittelee jätettä painon perusteella.

6.2 Vanhan ohjelman tarkastelu ja muutos

Logiikassa olevasta ohjelmasta ei ollut täyttä varmuutta, joten työn ensimmäinen vaihe oli varmistaa, että ohjelman senhetkinen tila vastaa saatavilla olevaa ohjelmaa. Siemensin ohjelmoitavien logiikoiden kanssa tähän hyvä työkalu on online/offline-vertailu. Se ei kuitenkaan ollut mahdollista tässä tapauksessa. Ohjelma oli tehty TIA Portal -versiolla 11, joka on poistunut tuote eikä ole enää saatavissa Siemensin SIOS-portaalista. Myöskään vertailu uudemman ja vanhemman version välillä ei tässä tapauksessa ollut mahdollista, TIA Portal -versiot 11 ja 12 edustavat vanhempaa sukupolvea. Tämä tulee huomioida myös projektin versiota päivittäessä. Versiota 13 vanhemmat projektit tulee aina päivittää version 13 kautta uudempiin.

Tässä tapauksessa kuitenkin logiikan toiminnallisuus on suhteellisen yksinkertainen, joten tarvittaessa vaikka koko ohjelman uudelleenkirjoittaminen pitäisi onnistua suhteellisen ripeästi. Vanhaa ohjelmaa oli mahdollista testata varalogiikalla, joten se voitiin päivittää TIA-versioon 18 ja testata sen toimintaa. Tällä tavoin vanha toimiva ohjelma säilyi alkuperäisessä logiikassa ja oli tarvittaessa palautettavissa käyttöön. Ohjelman toiminnallisuutta tarkastellessa nyt versiossa 18 se todettiin toimivaksi.

6.3 PLC-ohjelmamuutos

Uuden heittimen moottorin toimintalogiikka saatiin suurilta osin vanhan seulan moottorin ohjauksesta. Kun heitintä edeltävä kuljetin on käynnissä, käynnistetään heitin. Suoritetaan linjaston käynnistys ja sammutus askeleittain niin, että jäte kerkeää linjaston loppuun ja kuljettimet tyhjenevät ennen pysähtymistä.

PLC-ohjelmaan muutos tehtiin TIA Portal V18 korotettuun versioon lisäämällä ohjelmaan uusi funktio heittimen ohjausta varten. Ohjelman tulot ja lähdöt korjattiin vastaamaan muutoksia. Tämän jälkeen poistetun seulan toiminta ja siihen liittyneet turhaksi jääneet varoitukset poistettiin käytöstä tai korvattiin uuden heittimen vastaavilla.

6.4 Käyttöönotto

Ohjelmamuutosten jälkeen tehtiin käyttöönotto. Käyttöönotossa testattiin linjaston perustoiminnallisuus, käynnistykset, pysäytykset ja toiminta erikoistilanteessa. Käyttöönotto sujui ongelmitta, joten näin ollen muutokset voitiin jättää tuotantoon.

7 Yhteenveto

Insinöörityön aikana toteutetut PLC- ja WinCC-muutokset osoittivat, että molemmat järjestelmät ovat hyvässä kunnossa tulevaisuuden muutoksia ajatellen. Päivitetyt ohjelmaversiot ovat pitkään tuettuja, mikä takaa järjestelmän ylläpidettävyyden tulevina vuosina. Kyberturvallisuuden näkökulmasta datan salauksen käyttöönotto on askel eteenpäin. Käyttäjänhallinnan ja monivaiheisen tunnistautumisen tarpeellisuutta ja toteutusta tarkasteltiin, ja niiden kehittämistä jatketaan insinöörityön ulkopuolella.

NIS2-direktiivi voi vaikuttaa vaikeaselkoiselta etenkin, kun etsitään konkreettisia teknisiä ohjeistuksia. Siinä puhutaan paljon oikeasuhteisista ja asianmukaisista toimenpiteistä. Tämä ei kuitenkaan ole yllättävää, eihän Euroopan parlamentti ole teknisten yksityiskohtien määrittelijä. Sen sijaan NIS2 nojaa jo olemassa oleviin hyväksi todettuihin käytäntöihin ja standardeihin. NIS2-direktiivin rooli onkin enemmän ohjata ja yhtenäistää toimintatapoja kuin määritellä tarkkoja teknisiä vaatimuksia. Vaatimusten puutteellisuus kuitenkin nojaa paljon tapauskohtaisille tulkinnoille, mikä taas vaikeuttaa järjestelmien analysointia, etenkin tässä vaiheessa, kun ei ole esimerkkitapauksia. Päivitetty järjestelmä kuitenkin noudattaa nyt pääosin vakiintuneita tietoturvakäytäntöjä.

NIS2-direktiivin mukana laajentuneen soveltamisalan vuoksi myös työn tilaaja kuuluu nyt tämän sääntelyn piiriin. Koska tilaaja luokitellaan tärkeäksi toimijaksi NIS2-direktiivin alaisuudessa, se aiheuttaa huomattavasti vähemmän toimenpiteitä kuin jos se olisi määritelty kriittiseksi toimijaksi. Tärkeille toimijoille ei aseteta yhtä tiukkoja ennakkovalvontavaatimuksia, ja niiden järjestelmien turvallisuuden varmistaminen perustuu pääosin jälkikäteisvalvontaan, jota tehdään, jos epäillään puutteita direktiivin noudattamisessa.

Kuitenkin lokakuussa voimaantulevien lakimuutosten osalta on tärkeää perehtyä vaatimuksiin asianmukaisella tasolla ja kehittää toimintatapoja vastaamaan näitä vaatimuksia. Nämä vaatimukset sisältävät mm. 21. artiklassa määritellyt toimenpiteet ja 23. artiklassa määritelty raportointivelvollisuus.

Lähteet

Euroopan parlamentti ja neuvosto, 2022. Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555. Verkkosivu. Saatavissa: <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32022L2555>. [viitattu 31.7.2024]

ENISA, 2010. Stuxnet Analysis. Verkkosivu. Saatavissa: <https://www.enisa.europa.eu/news/enisa-news/stuxnet-analysis>. [viitattu 27.7.2024]

ETM, 2024. Company. Verkkosivu. Saatavissa: <https://www.winccoa.com/company.html>. [viitattu 22.1.2024]

International Society of Automation, 2024. Security of Industrial Automation and Control Systems: An Owerview of ISA/IEC 62443 Standards. PDF. Saatavissa: <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>. [viitattu 30.7.2024]

MDN Web Docs, 2023. An overview of HTTP. Verkkosivu. Saatavissa: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview>. [viitattu 12.2.2024]

Siemens, 2014. WinCC V7.3 SE incl. Update 1 WinCC/WebUX – Documentation. Manuaali. PDF-Dokumentti. Saatavissa: <https://cache.industry.siemens.com/dl/files/351/109479351/att_856147/v1/WebUXenUS_en-US.pdf>. [viitattu 20.1.2024]

Siemens, 2018. SIMATIC WinCC V7. PDF-dokumentti. Saatavissa: <https://assets.new.siemens.com/siemens/assets/api/uuid:eac06c86-f121-48f8-874f-30355aa6b111/DIFA-I10159-00-7600-SIMATIC-WinnCC-V7.pdf>. [viitattu 17.1.2024]

Siemens, 2022. WinCC WebNavigator. Verkkosivu. Saatavissa: <https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10371743#Overview>. [viitattu 18.1.2024]

Siemens, 2024. 1847-1865: Company founding and initial expansion. Verkkosivu. Saatavissa: <https://www.siemens.com/global/en/company/about/history/company/1847-1865.html>. [viitattu 15.1.2024]