

Jani Sydänlammi

# **AUTOMAATIOJÄRJESTELMÄN TOIMIN- NALLINEN RISKIKARTOITUS**

Uhat ja niihin varautuminen

Teknisten tieteiden tiedekunta  
Kandidaatintyö  
Joulukuu 2022

# TIIVISTELMÄ

Jani Sydänlammi: Automaatiojärjestelmän toiminnallinen riskikartoitus  
Kandidaatintyö  
Tampereen yliopisto  
Automaatiotekniikan kandidaatin –tutkinto-ohjelma  
Joulukuu 2022

---

Mitattavaa tietoa on paljon. Tiedon mittaaminen, analysointi ja varastointi kehittyvät koko ajan. Automaatiojärjestelmät keskittyvät omalta osaltaan sähköiseen tiedonkeruuseen, indikointiin ja toiminnalliseen ohjaukseen.

Työn tarkoituksena on käsitellä olemassa olevaa automaatiojärjestelmää ja sen eri osien kriittisyyttä sekä analysoida mahdollisia riskejä sen käytettävyydessä ja haavoittuvaisuudessa. Tarkoituksena on myös esittää haasteisiin mahdollisia ratkaisuja ja vikaindikointimenetelmiä.

Kyberturvallisuudesta ollaan koko ajan tietoisempia. Sen uhat tiedostetaan paremmin ja niitä varten luodaan strategioita ja kyberhaavoittuvaisuutta testataan ajoittain. Se on tullut pinnalle, kun tietovuodoista on uutisoitu.

Järjestelmän kahdentaminen on varteenotettava ratkaisu kaikille automaatiojärjestelmän osille. Virtualisointi ja virtuaaliympäristön luonti lisäävät myös vikasietoisuutta ja pienentävät järjestelmän riskiä lamaanantua täysin.

Avainsanat: Automaatiojärjestelmä, kyber, verkko, kriittisyys.

# ABSTRACT

Jani Sydänlammi: Functional risk mapping of the automation system  
Bachelor's thesis  
Tampere University  
Bachelors Degree  
December 2022

---

There is a lot of measurable information. Measuring, analyzing and storing data is constantly evolving. For their part, automation systems focus on electronic data collection, indication and functional control.

The purpose of this work is to address the existing automation system and the criticality of its various parts, as well as to analyze potential risks in its usability and vulnerability. It is also intended to present possible solutions to problems and fault indication methods.

There is a growing awareness of cybersecurity. Its threats are better recognized and strategies are created for them, and cyber vulnerabilities are tested from time to time. It has surfaced when data leaks have been reported.

Duplication of the system is a viable solution for all parts of the automation system. Virtualization and the creation of a virtual environment also increase fault tolerance and reduce the risk of the system being completely paralyzed.

Keywords: automatin system, kyber, network

# SISÄLLYSLUETTELO

1. JOHDANTO .....	1
2. AUTOMAATIOJÄRJESTELMÄ .....	2
2.1 Tutkittava järjestelmä .....	3
2.2 Valvomosovellusjärjestelmä (SCADA) .....	4
2.3 Virtuaalikoneet ja palvelimet.....	4
2.4 Ala-asetat ja laitteet.....	5
2.4.1 Siemens S7-1200 .....	5
2.4.2 TIA-Portal .....	6
2.5 Yhteydet ja liikennöinti-protokollat .....	7
2.5.1 Ethernet-verkko .....	8
2.5.2 4G-OpenVPN.....	8
2.5.3 GPRS .....	8
2.5.4 Radioliikenne .....	9
3. KYBERTURVALLISUUS.....	10
3.1 Tietoturva järjestelmän eri osissa .....	10
3.1.1 Järjestelmän palomuri .....	10
3.1.2 DMZ-verkon rooli .....	11
3.1.3 Virtuaalikoneiden tietoturva.....	11
3.1.4 Ala-asettien tietoturva .....	12
3.2 Tasojen kriittisyys.....	12
3.3 Automaatiolaitteiden näkyvyys .....	13
3.4 Muut uhat.....	14
4. YHTEENVETO.....	15
LÄHTEET .....	16

## LYHENTEET JA MERKINNÄT

CPU	Central Processing Unit, logiikan keskusyksikkö
DMZ	Demilitarisoitu alue
GPRS	General Packet Radio Service, GSM-verkon tiedonsiirtopalvelu
IP	Internet Protocol
I/O	Input/Output, järjestelmän luku ja kirjoitustoiminnot
MPLS	Multiprotocol Label Switching
OS	Object Server, objektipalvelin
PLC	Ohjelmoitava logiikka
REM	Remote, etäyhteys
SCADA	Supervisory Control and Data Acquisition
SRV	serveri, palvelin
TCP	Transmission Control Protocol
TIA	Totally Integrated Automation
VM	Virtual Machine, virtuaalikone
VPN	Virtual Private Network
<i>Hz</i>	taajuus

# 1. JOHDANTO

Yhteiskunta on yhä riippuvaisempi tiedosta. Tarkemmin tiedon sähköisestä muodosta eli ykkösistä ja nolista sekä analogisista mittauksista. Automaatiojärjestelmät toimivat tällä tiedolla. Ne keräävät dataa mittauksista, käyttävät sitä tietoa ja varastoivat sitä.

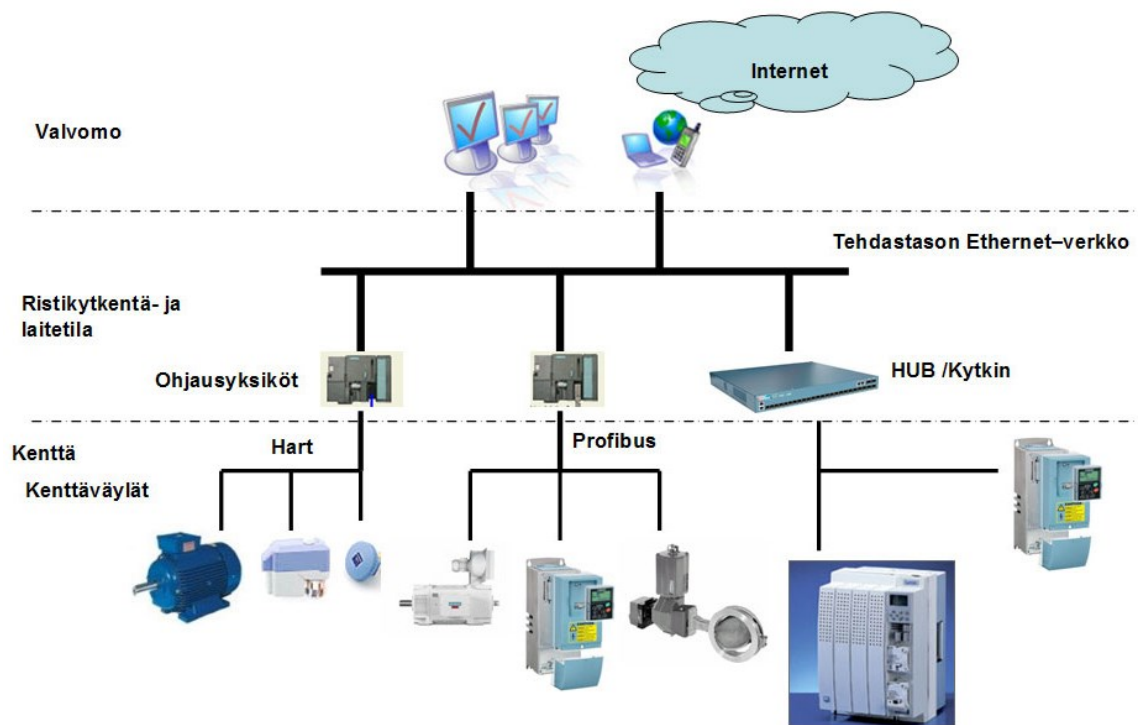
Automaatiojärjestelmät ovat kaikki yksilöllisiä ja räätälöityjä juuri kyseiseen tarpeeseen. Usein niissä on samoja peruseriaatteita, kuten jonkin suureen mittaaminen ja tällä tiedolla jonkin toisen suureen ohjaaminen. Automaation taso vaihtelee täysin autonomisesta järjestelmästä ihmisen kontrolloimaan järjestelmään, jota automaatio tukee datalla ja sen indikoinnilla.

Tässä työssä tarkastellaan erästä toiminnassa olevaa laajaa automaatiojärjestelmää. Työssä järjestelmää puretaan osakokonaisuuksiin ja näitä kokonaisuuksia tarkastellaan kriittisyyden ja toimintaan vaikuttavien riskien näkökulmasta. Riski- ja kriittisyysluokittelulla havainnollistetaan järjestelmän haavoittuvuutta. Tähän haavoittuvuuteen esitetään myös mahdollisia ratkaisuja sen parantamiseksi tai minimoimiseksi.

Aluksi perehdytään yleisesti automaatiojärjestelmiin ja niiden ominaisiin piirteisiin. Seuraavaksi tutustutaan automaatiojärjestelmien kyberturvallisuuteen yleisesti. Yleisten osuuksien jälkeen seuraavat kappaleet käsittelevät kohteena olevaa automaatiojärjestelmää. Järjestelmä jaetaan osakokonaisuuksiin ja sitä tarkastellaan eri riskien kannalta. Tämän jälkeen pohditaan ratkaisuja riskien pienentämiseen ja toimintavarmuuden maksimointiin. Yhteenvedossa pohditaan kohdejärjestelmän riskienhallinnan tasoa selvitettyjen tietojen perusteella.

## 2. AUTOMAATIOJÄRJESTELMÄ

Yleisesti automaatiojärjestelmä rakennetaan osista. Osia ovat esimerkiksi mittalaitteet, logiikat ja tietokoneet. Järjestelmä voi olla kooltaan suuri, kuten kunnallistekniset valvonta- ja ohjausjärjestelmät, tai pieni, kuten yksittäinen ohjelmoitava logiikka. Hiemankin isompi automaatiojärjestelmä jaetaan hierarkkisesti tasoihin. Tasojen nimityksiä voivat olla valvomotaso, ohjausyksikkötaso ja kenttätaso. Hierarkkisesta automaatiojärjestelmästä on hyvä esimerkki kuvassa 1 [1]. Siinä ylimmälle tasolle sijoittuvat valvomotietokoneet ja sieltä on liityntä Internetiin. Toiselle tasolle on sijoitettu toimilaitteita kontrolloivat ohjelmoitavat logiikkayksiköt. Kommunikointi logiikoiden ja valvomon välillä on toteutettu sisäisellä Ethernet-verkolla. Alimmalla kentälaitetasolla ovat yksittäiset toimilaitteet, jotka ohjaavat ja vaikuttavat prosessiin. Laitteiden kommunikointi voidaan toteuttaa erilaisilla väyläratkaisuilla, I/O-kaapeloinnilla tai langattomasti.

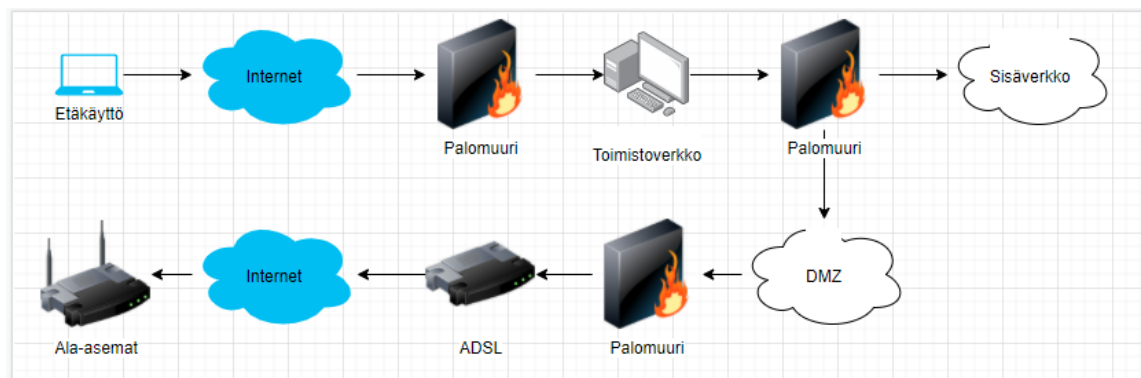


**Kuva 1 Esimerkki tasoihin jaetusta automaatiojärjestelmästä**

Automaatiojärjestelmän reaaliaikaisuus on nykyään tärkeää. Sen saavuttamiseksi järjestelmä on usein kytkettävä Internetiin, ainakin mikäli järjestelmä on laaja. Reaaliaikaisuuden lisäksi järjestelmän tulee olla luotettava ja varmatoiminen sekä tietoturvallinen.

## 2.1 Tutkittava järjestelmä

Työssä tutkittava automaatioverkko on oikea käytössä oleva järjestelmä. Järjestelmä on kuvattu pääpiirteittäin kuvassa 2. Järjestelmässä on yrityksen oma toimistoverkko, joka on eristetty Internetistä, DMZ-verkosta ja muusta järjestelmästä palomuurien avulla.



**Kuva 2 Tutkittavan järjestelmän pääpiirteet**

Toimisto- ja automaatioverkkoon voidaan ottaa etäyhteys internetin välityksellä palomuurin läpi. Järjestelmä linkittyy internetiin myös toisessa päässä. Kaikki ala-asemat kommunikoivat sen kautta järjestelmään.

Jokainen ala-asema koostuu 4G-reitittimestä ja ohjelmoitavasta logiikasta. Ohjelmoitavat logiikat ovat Siemens S7-1200 sarjaa. Ala-asemilla on yksilöityjä digitaalisia ja analogisia mittauksia, joita se välittää automaatioverkkoon.

Järjestelmä voidaan jakaa osiin tai tasoihin. Järjestelmässä on siis valvomo, jota voidaan käyttää etäyhteydellä, ala-asemat eli kenttätaso, joiden toimintaa seurataan. Näiden välissä järjestelmässä on kaikki datan käsittelyyn liittyvät palvelut ja palvelimet.

## 2.2 Valvomosovellusjärjestelmä (SCADA)

Tutkittavassa automaatiojärjestelmässä laitteet ovat maantieteellisesti hajautettuna. Tiedon hankintaa ja hallintaa tehdään kuitenkin keskitetysti. Tätä valvomosovellusjärjestelmää kutsutaan SCADA-järjestelmäksi. SCADA tarkoittaa ”Supervisory Control and Data Acquisition”. Automaatiojärjestelmän valvomo-ohjelmiston tärkeimmät ominaisuudet ovat ohjelmoitavien logiikoiden toiminnan ohjaus ja valvonta. [2] Tässä tapauksessa toimintaa ohjaamalla ja valvomalla hallitaan suurta prosessia.

Lähteessä kaksi [2] myös mainitaan, että tyypillisimpiä hajautettuja SCADA-järjestelmäkäyttäjiä ovat infrastruktuurijärjestelmät, kuten jätevesijärjestelmät, energianjakeluverkot, kaasulinjat ja muut vastaavat verkot. Näissä keskitetty ohjausjärjestelmä sijaitsee ohjauspalvelimessa ja kommunikaatio reititetään oman suojatun aliverkon kautta. Ohjausjärjestelmä toimii mittausten perusteella ja tallentaa ala-asemien tiedot lokipalvelimelle.

Tallennettua tietoa voidaan esittää trendeinä ja raporteina ja niiden perusteella tehdään isojakin investointeja. Järjestelmä toimii myös kunnossapidon tärkeänä työkaluna välittämällä hälytyksiä ja muuta toiminnalle kriittistä tietoa.

## 2.3 Virtuaalikoneet ja palvelimet

Virtualisointi mahdollistaa, että yksi fyysinen palvelinlaite voi pitää sisällään useita virtuaalisia palvelimia. Eli virtualisoinnissa erotetaan fyysinen laite sovelluksista. Tämä tarkoittaa parhaimmillaan fyysisten laitteiden minimaalista määrää ja yhteensopivuusongelmien vähenemistä. [3]

Tutkittavan järjestelmän valvomo ja lähiverkko ovat palomuurien kautta yhteydessä toimistoverkkoon ja Internetiin. Lähiverkko ja valvomo ovat keskenään IP (Internet Protocol) -verkossa, jossa jokaisella verkon laitteella on oma henkilökohtainen IP-osoitteensa. Lähiverkko on rakennettu virtuaalikoneista ja palvelimista. Jokaisella verkon laitteella on oma tehtävänsä. Taulukossa 1 on esitelty muutamia verkon laitteita ja niiden tehtäviä.

**Taulukko 1 Tutkittavan verkon laitteita**

Palvelin/laite	Mikä	Tehtävä
GR	Kehityskone	Ohjelmointiympäristö
OS	Objektipalvelin	IO-liikennöinti
Historian	Lokipalvelin	IO- ja muu historiadata

REMSRV	Etäkäyttöpalvelin	Etäkäyttö

Jokainen verkon kone on suojattu käyttäjätunnuksella ja salasanalla. Lisäksi koneilla on kyber- ja virusturvat.

Virtuaalisointi tekee järjestelmästä vikasietoisemman. Vikasietoisuutta saadaan aikaiseksi kopioimalla virtuaalikoneet säännöllisesti toiselle koneelle. Vielä edistyneemmän tason vikasietoisuutta tarjoaa virtualisointiympäristö, joka toimii klusteri-tyyppisesti ja toipuu automaattisesti vikatilanteista [4].

## 2.4 Ala-asetat ja laitteet

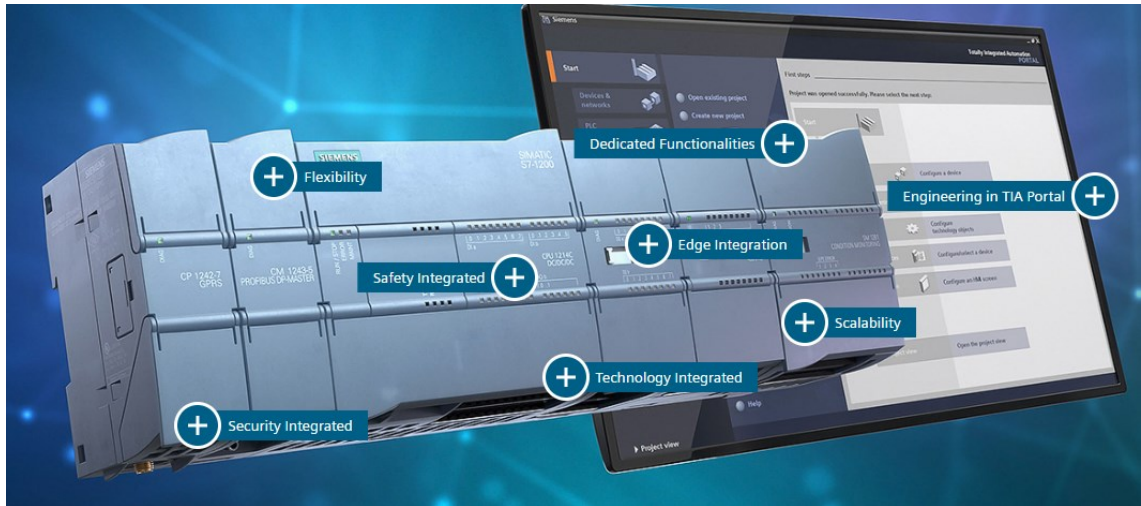
Tutkittavassa järjestelmässä ala-asetat ovat yksittäisiä sähkö- ja automaatiolaitteiden kokonaisuuksia. Tärkeimpiä laitteita ovat ohjelmoitavat logiikat ja liikennöintilaitteet. PLC:t (Programmable logic controller) ovat Siemensin valmistamaa S7-1200 sarjaa. Niiden ominaisuudet kattavat digitaaliset ja analogiset mittaukset sekä –ohjaukset. Asemilta välitetään valvomoon mittausdataa ja hälytyksiä sekä asemia on mahdollista etäohjata.

Ala-asettien ohjausjärjestelmän toteutus logiikalla mahdollistaa hyvän elinkaarenhallinnan ja tarvittaessa kehitystyön verrattuna esimerkiksi releohjaukseen. Siemensillä uusia varaosia on saatavilla rikkoutuneiden tilalle tai laajennustarpeeseen. Lisäksi logiikalla toimivaa ohjelmaa eli koodia on mahdollista muuttaa ja kehittää jälkikäteen. Logiikkaohjelmien yhteneväisyys on tärkeää järjestelmän hallinnan ja ylläpidon kannalta järjestelmän kasvaessa.

Ala-asetilla on logiikan lisäksi Siemensin ohjelmoitava ohjauspaneeli aseman käyttöön-ottoa ja paikallista seuranta varten. Ohjauspaneelilla aseman tilaa on helppo seurata ja asetusrvojen muuttaminen onnistuu ilman ohjelmontikokemusta.

### 2.4.1 Siemens S7-1200

Siemensin S7-1200 sarja on tarkoitettu pienen ja keskitason suorituskykyä vaativiin tehtäviin. Sarjan laitteissa ja lisäosissa on laajasti teknologisia ratkaisuja liikennöintiin ja signaalien keräämiseen. Järjestelmä pystytään kokoamaan tapauskohtaisesti moduuleista. [5] Kuvassa 3 on esitelty mallikokoonpano S7-1200 järjestelmästä.



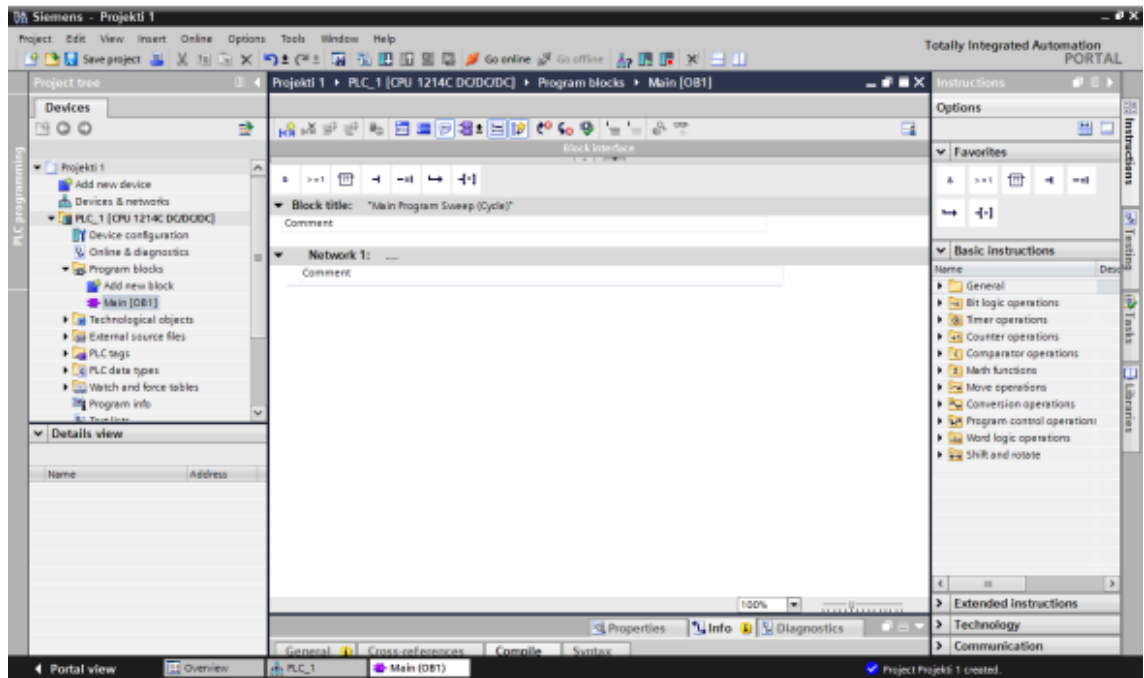
**Kuva 3 S7-1200 logiikka lisämoduuleineen [4]**

Kuvassa 3 on keskellä keskusyksikkö eli CPU (Central Processing Unit). Tämä on logiikan aivot, jossa tehty ohjelma käsittelee kaikki tiedot ja toteuttaa itseään järjestelmällisesti. CPU:n vasemmalla puolella ovat kommunikaatiomodulit. Nämä moduulit mahdollistavat logiikan liikennöinnin eri protokollien (sarjaliikenne, PROFIBUS, Ethernet jne.) kautta. CPU:n oikealla puolella ovat signaaliyksiköt. Näitä ovat digitaali- ja analogiatulo- ja -lähtökortit.

## 2.4.2 TIA-Portal

Logiikan ohjelmointityökaluna käytetään TIA-Portalia. TIA-Portal on Siemensin kehittämä ohjelmisto STEP-7:n pohjalta. TIA-Portalin ja STEP-7:n muutokset ovat pääosin ulkoasullisia, koska kyseessä on oikeastaan saman ohjelman uudempi versio [6]. TIA-Portal:sta on tarjolla tänä päivänä versio V17.

Ohjelmoinnissa lähdetään liikkeelle komponenttien kokoonpanosta ja konfiguraatiosta. Kun haluttu kokoonpano on tehty, aloitetaan varsinainen ohjelmointi. Ohjelmointikieliä on kolme erilaista LAD (ladder diagram), FBD (function block diagram) ja STL (symbol table).



**Kuva 4 TIA-Portal:n ohjelmointinäköymä [5]**

Ohjelmoimalla luodaan järjestelmälle halutut toiminnot. TIA-Portal:ssa on käytössä laaja kirjasto valmiita logiikkaoperaatioita, ajastimia, laskureita ja vertailijoita. Kun ohjelma on valmis, se ladataan logiikalle ja testataan.

## 2.5 Yhteydet ja liikennöinti-protokollat

Tutkittavassa järjestelmässä on ollut useita eri liikennöinti-protokollia. Tiedonsiirtotapoja on pyritty yhtenäistämään järjestelmän ylläpidon ja hallinnan kannalta tehokkaampaan suuntaan. Tärkeänä syynä on ollut myös järjestelmän kyberturvallisuuden parantaminen.

Ala-asemien etäyhteys muodostetaan 4G-reitittimen avulla. Yhteys on tunneloitu OpenVPN-yhteys, joka käyttää ennalta määrättyjä sertifiikaatteja ja salausavaimia. Lisäksi tarvitaan kaupallinen data SIM-kortti ja operaattorin tukiasemia Internet-yhteyttä varten.

Ala-aseman laitteilla on kaikilla omat IP-osoitteensa. Tällä tavoin ala-asemat yksilöidään järjestelmän näkökulmasta. Nämä kaikki tiedot ovat tärkeitä dokumentoitavia.

Tutkittavan järjestelmän yksi käytöstä poistettu liikennöinti-protokolla on radioliikenne. Toinen poistuva liikennöinti-protokolla on GPRS-järjestelmä. Kun tiedonsiirtojärjestelmiä otetaan pois käytöstä, järjestelmästä saadaan purettua myös paljon muutakin siihen kuuluvaa tekniikkaa, kuten palvelimia, lähettämiä ja antennia.

## 2.5.1 Ethernet-verkko

Yleisin tutkittavan järjestelmän protokolla on TCP/IP. Kyseisessä protokollassa osoitteistetaan laitteet, käytetään aliverkon peitteitä ja yhdyskäytäviä. Kyseinen tiedonsiirtotapa on yhteensopiva useiden eri laitevalmistajien kesken.

TCP/IP protokollassa TCP määrittää, kuinka applikaatiot luovat kommunikointikanavia verkon yli. TCP myös hallitsee, kuinka viesti on purettu pienempiin osiin ennen välittämistä ja miten se kootaan oikeassa järjestyksessä kohdeosoitteessa. [7]

IP määrittää kunkin paketin osoitteen ja reitin päästäkseen oikeaan paikkaan. Jokainen yhdyskäytävälaite tarkistaa IP-osoitteet määrittääkseen minne välittää paketin tai viestin. [7]

## 2.5.2 4G-OpenVPN

Järjestelmän kaikkien ala-asemien liikenne pyritään saamaan 4G-protokollan taakse. Tässä liikennöintitavassa ala-asemalle asennetaan 4G-mobiiliyhteyttä käyttävä modeemi. Modeemiin on konfiguroitu VPN-tunnelointi, luotu sertifikaatit ja salausavaimet ja annettu oma IP-osoitealue.

VPN-protokollia on viisi erilaista [8]:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunnel Protocol (L2TP/IPSec)
- OpenVPN
- Secure Socket Tunneling Protocol (SSTP)
- Internet Key Exchange version 2 (IKEv2)

VPN mahdollistaa turvallisen ja salatun yhteyden julkisen verkon yli. 4G-version tästä tekee mobiilidatayhteys. Yhteys internetiin luodaan operaattorin palveluntarjoajan datayhteyden kautta. VPN-yhteys luodaan tietokoneella pyörivälle VPN-palvelulle, jonka kautta päästään liikennöimään objektipalvelimille.

## 2.5.3 GPRS

GPRS (General Packet Radio Service) on GSM-verkossa toimiva data SIM-kytkentäinen palvelu. GPRS-tekniikka on periaatteessa vanhempi versio verrattuna uudempiin 3G- ja 4G-tekniikoihin.

GPRS on yksi ensimmäisistä tekniikoista, joka mahdollistaa liittymän IP-verkkoihin mistä ja milloin tahansa. Vanhentunutta teknologiaa GPRS:stä tekee sen hitaat tiedonsiirtonopeudet nykystandardien mukaan. [9]

## **2.5.4 Radioliikenne**

Radioliikenne on ollut myös käytössä ala-asemien liikennöinnissä ja etävalvonnassa. Radioliikennöintiin tarvitaan radioliikennöintilupa tietyille taajuusalueille. Liikennöintiin käytetty taajuusalue on satoja MHz. Lisäksi radioliikenne on toimintavarmuudeltaan riippuvainen sääoloista sekä antennien ja mastojen näkyvyyksistä.

Radioliikenne on lisäksi häirinnälle altis. Samalla taajuusalueella ollessaan viestejä voi häiritä. Häirintää voi tehdä esimerkiksi lähettämällä väärennettyjä viestejä verkkoon.

## 3. KYBERTURVALLISUUS

Havainnot viimevuosina tehdyistä kyberhyökkäyksistä ovat lisääntyneet huomattavasti. Kyberturvallisuus on otettava vakavasti ja yhteiskuntakriittisessä ympäristössä siihen on varauduttava mahdollisimman hyvin. Myös kriittisissä ympäristöissä toimivien henkilöiden ohjeistus ja toimintamallit pitää olla tarkasti ohjeistettu, ettei käyttäjäperäisiä turvallisuus-uhkia tapahdu. Automaatioteollisuuden toimintakriittisyys ja sen toiminnan varmistaminen suojatamalla kyberuhilta on oltava jatkuvan kehityksen alla.

Laajassa automaatiojärjestelmässä on oltava korkeatasoinen helposti ylläpidettävä tietosuojaus verkon osille ja laitteistoille, joiden oma tietoturvaso ei riitä. Tällaisen suojauksen suunnittelussa on otettava huomioon, että suojattavan laitteiston tietoturva toimii lähes täysin lisäsuojauslaitteiston varassa.

Paraskaan varautuminen ei välttämättä estä tietomurtoa, mutta se voidaan havaita ja siihen voidaan reagoida nopeasti. Kyberturvallisuutta on tunnistaminen, ehkäisy ja varautuminen.

### 3.1 Tietoturva järjestelmän eri osissa

Tietoturvahyökkäysten riski on nykyään todellinen. Järjestelmään voidaan yrittää murtautua etänä internetin välityksellä. Tämä on todennäköisin tapa, miten järjestelmää uhaataan ja minkälaisiin uhkiin tulisi varautua.

Tietoturvan toteutustapa järjestelmän eri osissa vaihtelee. Joka osassa se on kuitenkin tärkeää. Tietoturvan tärkein tehtävä on pitää liikennöinti salattuna ja ulkopuolisten pääsy tietoihin estettynä.

#### 3.1.1 Järjestelmän palomuuuri

Hyökkääjän pääsyn järjestelmään estää palomuuuri. ADSL-modeemipohjainen palomuuuri on haittaohjelmalle ohjelmistopohjaista palomuuria haastavampi ohittaa tai sammuttaa.

Hyvätkään palomuurit eivät välttämättä estä liikenteen tunnelointia, jolloin toimistoverkossa olevien koneiden suojaus korostuu.

Automaatiojärjestelmän verkkotopologia on ratkaisevassa asemassa tietoturvallisuuden kokonaisarviointissa. Oikein suunniteltu tietoverkko ja oikein sijoitetut palomuurit antavat jo itsessään askeleet kohti turvallisempaa järjestelmää.

Palomuurin ohi päästessään hyökkääjän tai haittaohjelman on mahdollista saada jokin kohdelaite kokonaan haltuunsa. Tämä tarkoittaa, että jokainen järjestelmän laite tulisi suojata erikseen. Järjestelmän muiden laitteiden suojauksia on käsitelty seuraavissa kappaleissa.

### **3.1.2 DMZ-verkon rooli**

DMZ-verkko on tärkeässä osassa kyberturvallisuuden kohdalla varsinkin, kun puhutaan etäyhteyksistä ja kaukovalvonnan toteutuksesta. DMZ-verkko toimii aliverkkona, joka yhdistää yrityksen järjestelmän turvattomampaan alueeseen, kuten Internetiin. DMZ toimii käytännössä lisäturvallisuuserroksena.

Turvalliset ja valvotut yhteydet näkevät ja saavat pääsyn DMZ-alueella oleville koneille. Järjestelmän muu osa on turvassa palomuurin takana. Palomuri valvoo ja erottaa liikennettä DMZ-alueen ja sisäverkon välillä. Yleensä käytetään myös palomuuria suojaamaan DMZ-verkkoa näkymästä kaikkialle ulkoiseen Internetiin. [10]

### **3.1.3 Virtuaalikoneiden tietoturva**

Palomuurien sisällä järjestelmässä on useita virtuaaliservereitä. Virtualisointi mahdollistaa, että fyysinen tietokone on erotettu sovelluksesta luomalla virtuaalikone (VM). Tämä on vikasietoisempi ja vakaampi ympäristö kriittisille sovelluksille. Vähentää tehokkaasti fyysisten koneiden tarvetta ja helpottaa koko järjestelmän ylläpitoa ja suojaamista. Virtuaaliseen koneeseen on kuitenkin suhtauduttava aivan kuten fyysiseenkin koneeseen. Samat uhat on otettava huomioon molemmissa. Toisaalta virtuaalikoneet voivat olla riskialttiimpia, koska yksi heikosti suojattu virtuaalikone alustalla voi aiheuttaa vakavan tietoturvariskin koko alustalle.

Virtuaalikoneiden tietoturvaa käsitellään Reubenin julkaisussa [11]. Hän mainitsee saman asian, että virtuaalikoneiden tietoturva on kriittinen osa IT-ympäristöä, koska yksikin tietoturvaton kone voi vaarantaa sen kokonaan. Virtuaalikoneissa pitää hänen mukaansa kiinnittää erityistä huomiota siihen, ettei mahdollisella tunkeutujalla yhdelle koneelle

päästyään ole pääsyä toisille koneille. Pahimmassa tapauksessa virtuaalikoneella pyörivä haittaohjelma pystyy ohittamaan virtuaalisen tason ja pääsemään käsiksi isäntäkoneeseen. Toinen hyvin haitallinen skenaario hänen mukaansa on, että saastunut isäntäkone toimii yhdyskäytävänä muihin virtuaalikoneisiin.

Virtuaalikoneiden tietoturvan etuina fyysisiin koneisiin voidaan pitää myös sitä, että ylläpitäjät voivat asettaa tietoturva-asetuksia, jotka koskevat kaikkia virtuaalikoneita. Keskitetty hallinta auttaa varmistamaan, että kaikkien järjestelmän osien tietoturva on ajan tasalla.

### **3.1.4 Ala-asemien tietoturva**

4G kaukovalvontayhteyksissä käytetyn OpenVPN-protokollan VPN-tunnelin salauksen murtaminen on todella vaativaa ja todella hidasta. Salauksessa käytettyjen avainten varastaminen on myös uhkakuva. Se missä ja miten avaimia säilytetään, nousee vahvaan rooliin. Kaukovalvonnassa käytetty SSL/TLS –salaus on salaukseltaan tehokkaampi kuin muut aiemmat teknologiat.

Uhkana on myös ala-asemille murtautuminen. Ala-asemilla käytössä murtohälytystieto, mutta hyökkääjän mahdollista saada logiikka täysin haltuunsa. Tätä varten tarvitsee oikean tiedonsiirtokaapelin pc:n ja logiikan välille ja ohjelmiston tietokoneessa. Tällöin ala-asema voidaan esimerkiksi pysäyttää ilman, että siitä tulee tieto valvomoon.

Tukiaseman radioliikenteeseen hyökätessään ja Modbus-protokollan tuntiessaan hyökkääjän mahdollista ohjata taajuuden takana olevia ala-asemia ja estää hälytykset järjestelmään.

## **3.2 Tasojen kriittisyys**

Järjestelmän tasojen kriittisyyttä voidaan arvioida sen perusteella, kuinka ison tiedonsiirtokatkoksen järjestelmän osan vioittuminen aiheuttaa. Tutkittavassa järjestelmässä tärkeintä on tilannekuvan säilyttäminen ja toiminnan varmistaminen. Tätä varten kentältä saatua tietoa käytetään, jotta voidaan ennakoida ongelmatilanteita, puuttua niihin ja seurata sekä ennustaa järjestelmän toimintaa.

Yksittäisen ala-aseman kriittisyys ei siis järjestelmän kannalta ole kovin korkea, koska sen vikaantuessa vain se kyseinen asema on yhteyskatkolla. Yksittäiset ala-asetat voivat kuitenkin olla keskenään kriittisempiä tai vähemmän kriittisiä.

Joten järjestelmän kriittisimmät osat löytyvät ylempää järjestelmätasolta. Aiemmin taulukossa 1 esitellyistä järjestelmän osista kehityskone ja historiapalvelin eivät ole kaikkein kriittisimpiä. Kehityskoneen palvelun estyessä järjestelmään ei voi tehdä muutoksia, mutta etäyhteyksien ja toiminnan valvonnan pitäisi onnistua. Historiapalvelin taas nimensä mukaan tallentaa dataa ja esittää sitä. Sen estyminen vaikuttaisi valvomossa trendien ja historiatietojen seurantaan ja tallentumiseen, mutta sen hetkinen tilannekuva pysyisi yllä.

Kriittisimpiä osia ovat siis koneet ja palvelimet, joiden kautta liikennöinti muodostuu. Näitä ovat VPN-palvelin ja objektipalvelimet. Mikäli jonkun niistä yhteydet estyvät tai katkeavat, kaikki kyseisen palvelimen avulla muodostuvat yhteydet katkeavat. Tämä tarkoittaisi useita kymmeniä ja jopa satoja yhteyskatkoksia tarkasteltavassa järjestelmässä. Pahimmassa tapauksessa lähes koko järjestelmän tiedonsiirron ja päivittymisen katkeamista.

Kriittisiä järjestelmän osia ovat myös palomuurit ja kytkimet. Palomuurien tai kytkimien fyysinen vioittuminen tai toimimattomuus johtaisi kaiken liikennöinnin katkeamiseen kyseisen laitteen läpi. Pahimmassa tapauksessa siis hyvin laajoja yhteyskatkoja.

### **3.3 Automaatiolaitteiden näkyvyys**

Automaatiolaitteiden suojaus voi olla usein heikkoa eikä niiden tietoliikenne välttämättä edes salattua. Tähän voi olla syynä se, että ei tunnisteta salaamattomuuden ja näkyvyyden uhkia. Isoin syy saattaa kuitenkin olla se, että yhteydet ja toiminta halutaan pitää mahdollisimman vikavapaana. [2]

Automaatiolaitteiden löytyvyydestä Internetistä on tehty tutkimus vuonna 2013. Tämän tutkimuksen tarkoituksena oli selvittää, kuinka paljon kriittisiä SCADA-, kontrolli- ja tehdasautomaatiojärjestelmiä on löydettävissä ja löytyykö niistä tunnettuja haavoittuvuuksia. Tutkimuksen tekivät Aalto-yliopiston tutkijat Seppo Tiilikainen ja Jukka Manner ja he löysivät 2915 Suomessa sijaitsevaa automaatiolaitetta, joihin olisivat pystyneet ottamaan yhteyden julkisen Internetin avulla [12].

### 3.4 MPLS-verkko

Automaatioverkon liikennettä tunneloidaan järjestelmässä myös Multi-Protocol Label Switching-tekniikalla. MPLS on alusta erilaisille sovelluksille ja datan siirtoon. MPLS on suhteellisen vanhaa tekniikkaa 1990-luvun lopulta. MPLS-tekniikan luotettavuudesta käydään nykyään keskustelua.

MPLS-tekniikassa datapaketeille annetaan "leima". Näin määritellään, miten paketin tulee liikkua ennalta määritettyjen yhteyksien ylitse. Koska datan liikkuminen on ennalta määritettyä se on myös nopeaa, koska IP-hakuja ei tarvitse suorittaa joka vaiheessa. Ruuhkautumista MPLS välttää jakamalla verkkopyynnöt eri reittien väliin. MPLS voi ohjata liikennettä myös vaihtoehtoista reittiä pitkin välttääkseen katkoksia. [13]

MPLS-tekniikan huonona puolena on dataliikenteen suhteellisen kallis hinta verrattuna internet-liikenteeseen. Kyberturvallisuuden kannalta kriittinen ominaisuus on, että se ei salaa liikennettä.

### 3.5 Muut uhat

Konkreettisenä lisäuhkana on ala-asemille murtautuminen. Maantieteellisesti hajautettuna niitä on paljon ja hyvin laajalla alueella. Asemilla on käytössä murtohälytystieto.

Ala-asemalle murtautuessaan asemalle pystyy aiheuttamaan ilman liikennöintitietämystäkin yhteyskatkon. Tämän jälkeen esimerkiksi sähkökatkon tekeminen onnistuu. Sähkökatko aiheuttaa toimintakatkoksen, josta voi aiheutua julkista haittaa. Ethernet-liikennöintiä ymmärtävän on myös mahdollista saada ala-asemalta IP-osoitealueita selville.

## 4. YHTEENVETO

Työn tavoitteena oli tarkastella olemassa olevaa järjestelmää ja etsiä sen toiminnan kannalta kriittisimpiä osia. Työn tavoite täyttyi siltä osin, että järjestelmän kriittisimmät osat saatiin haarukoitua liikennöintiä käsitteleviin järjestelmän osiin. Yksittäisen aseman liikennöinti ei ole järjestelmän toimivuuden kannalta kriittistä, mutta satojen asemien objektipalvelimet ovat.

Järjestelmässä on automaatiojärjestelmän toimivuuteen vaikuttavia komponentteja ja automaatiolaitteilta ala-asemilta aina sisäverkkoon asti. Tietoturva on heikointa kenttätasolla mutta paranee tultaessa ylöspäin järjestelmätasolle.

Ala-asemilla tapahtuvat laiterikot tai yhteyshäiriöt vaikuttavat vain kyseisen aseman yhteyteen. Kriittisimpien yksittäisten asemien yhteydet olisi hyvä varmentaa varayhteyksillä. Kaikkien ala-asemayhteyksien päivitys radio- ja GPRS-liikennöinnistä 4G-liikennöintiin OpenVPN protokollalla on iso harppaus kyberturvan parannuksessa ja laitteiden suojauksessa.

Kun lähes kaikki yhteydet toimivat samalla periaatteella, järjestelmän yhteyksien kannalta kriittisimpien osien eli VPN- ja objektipalvelimien kahdennusta tai kuorman jakamista useammille kannattaa harkita. Isona varmuustekijänä järjestelmien varmuuskopiointi säännöllisin väliajoin.

DMZ-verkon kytkimet ovat tärkeässä osassa DMZ-verkon toiminnassa ja sitä myöten etäyhteyksien ja kaukovalvonnan kyberturvallisuuden toteutuksessa. hyvässä verkko-ohjelmistoprojektissa verkkokytkimiä valvotaan. Verkkokytkimien toiminnan seuranta voi tehdä porttikohtaisesti (liikennetasot, käyttö, kaistanleveys). Tätä valvontaa voisi hyödyntää antamaan jonkinlaisen hälytyksen, kun esimerkiksi käyttö saavuttaa asetetun korkean rajan.

# LÄHTEET

- [1] EDU opetushallituksen sähkötekniikan oppimateriaali. Saatavissa: [http://www03.edu.fi/oppimateriaalit/kunnossapito/sahkotekniikka\\_a2\\_automatiojarjestelma.html](http://www03.edu.fi/oppimateriaalit/kunnossapito/sahkotekniikka_a2_automatiojarjestelma.html)
- [2] T. Tiitinen, Tietoturvallisuuden haasteet Internetiin kytketyssä teollisessa automaatiojärjestelmässä, Diplomityö, Tampereen Teknillinen Yliopisto, 2014.
- [3] Virtualisoinnin tuomat hyödyt: Tapaus Oulun Tietotekniikka, Pro gradu-tutkielma, Oulun Yliopisto, Toni Riekkinen, 2015. Saatavilla: <http://jultika.oulu.fi/files/nbnfioulu-201510072024.pdf>
- [4] ProTrainIT Oy, 2006, 1.14
- [5] Siemens Oy:n verkkosivujen tuote-esittely. Saatavissa: <https://new.siemens.com/global/en/products/automation/systems/industrial/plc/s7-1200.html>
- [6] Opinnäytetyö, Tampereen Ammattikorkeakoulu, Wallenius Henri, 2012. Saatavilla: [https://www.theseus.fi/bitstream/handle/10024/48033/Wallenius\\_Henri.pdf?sequence=1](https://www.theseus.fi/bitstream/handle/10024/48033/Wallenius_Henri.pdf?sequence=1)
- [7] TCP/IP networking explained. Saatavilla: <https://www.techtarget.com/searchnet-working/definition/TCP-IP>
- [8] OpenVPN software. What is a VPN. Saatavilla: <https://openvpn.net/what-is-a-vpn/>
- [9] GPRS. Mikä on GPRS? Saatavilla: <https://fi.eyewated.com/mikae-on-gprs-yleinen-pakettiradiopalvelu/>
- [10] Barracuda, enterprice that secures data from wide range of threats. Saatavilla: <https://www.barracuda.com/glossary/dmz-network>
- [11] Jenni Susan Reuben, A Survey on Virtual Machine Security, Helsinki University of Technology. Saatavilla: <http://www.cs.umd.edu/class/fall2017/cmsc414/readings/vm-security.pdf>
- [12] J. M. Seppo Tiilikainen, Aalto.fi(Suomen automaatioverkkojen haavoittuvuus), 21.3.2013. Saatavissa: <https://research.comnet.aalto.fi/public/Aalto-Shodan-Raportti-julkinen.pdf>
- [13] NordVPN, markkinajohtaja internetin tietoturvan tarjoajista. Saatavilla: <https://nordvpn.com/fi/blog/mps-verkko/>