Tampereen yliopisto

Paavo Asikainen

VERKONVALVONTA TEHDASYMPÄRIS-TÖSSÄ

Kandidaatintyö
Informaatioteknologian ja viestinnän tiedekunta (ITC)
Juha Vihervaara
Elokuu 2022

TIIVISTELMÄ

Paavo Asikainen: Verkonvalvonta tehdasympäristössä
Kandidaatintyö
Tampereen yliopisto
Tieto- ja sähkötekniikan kandidaattiohjelma
Elokuu 2022

Automaatio on merkittävä osa modernia yhteiskuntaa, ja sen tarpeen lisääntyminen on saanut aikaan nopean automaatioverkkojen kehityksen muun muassa prosessiteollisuudessa. Kun automaatioverkot laajenevat ja kriittiset järjestelmät siirtyvät verkkoon, niiden ylläpito on entistä haastavampaa. Verkonvalvonnan päätehtävänä on tuottaa tietoa verkon tilasta, jotta verkon ylläpito on helpompaa ja resurssit voidaan hyödyntää tehokkaammin. Automaatioverkkojen toimintaperiaatteet ja ominaispiirteet luovat erilaisia vaatimuksia verkonvalvonnalle sekä verkonvalvontaohjelmistoille. Kandidaatintyön tavoitteena on esitellä automaatioverkkojen ja UPM Kymin sellutehtaan asettamia vaatimuksia verkonvalvonnalle, sekä selvittää avoimen lähdekoodin verkonvalvontaohjelmisto Zabbixin soveltuvuutta sellutehtaan automaatioverkon valvontaan. Kandidaatintyö on tehty toimeksiantona UPM Kymin sellutehtaalle.

Työn teoriaosuudessa tutustutaan Ethernet-pohjaisten lähiverkkojen tekniikoihin ja rakenteisiin sekä automaatioverkkojen ominaispiirteisiin. Lisäksi teoriaosuudessa käsitellään verkonvalvonnan hyötyjä, pääelementtejä, nykypäivän tekniikoita ja protokollia sekä yleisiä vaatimuksia automaatioverkkojen näkökulmasta. Työn tutkimusosassa selvitetään UPM Kymin sellutehtaan verkonvalvonnan nykytilaa sekä millaisia vaatimuksia ja tavoitteita verkonvalvonnalle asetetaan. Verkonvalvontaohjelmisto Zabbixin arkkitehtuuria, toimintaperiaatteita ja ominaisuuksia verrataan asetettuihin vaatimuksiin.

Työssä havaittiin, että automaatioverkkojen hierarkkinen ja heterogeeninen rakenne, tiukat luotettavuus- ja reaaliaikavaatimukset sekä tietoturva asettaa merkittävimmät yleiset vaatimukset verkonvalvonnalle. UPM Kymin sellutehdas painottaa vaatimuksissaan verkonvalvontaohjelmiston helppokäyttöisyyttä, saavutettavuutta, käyttöönoton helppoutta, yhteensopivuutta sekä ohjelmiston tietoturvallista käyttöä. Oleellisimpien toimintojen osalta vaatimuksiksi esitetään vikojen havainnointia ja selvitystä sekä kerätyn datan visualisointia. Zabbixin monipuoliset ominaisuudet vastaavat hyvin esitettyihin vaatimuksiin. Näitä ominaisuuksia ovat selainpohjainen käyttöliittymä, kattavat mahdollisuudet datan keräämiseen, laajennettavuus, ennakoiva vikojen havainnointi ja reaaliaikaiset topologiakartat. Zabbixin monipuoliset ominaisuudet ja UPM Kymin sellutehtaan automaatioverkon laajuus voivat kuitenkin vaikeuttaa ohjelmiston käyttöönottoa.

UPM Kymin sellutehtaalla ei tällä hetkellä ole käytössä yhtenäistä toimintatapaa tai ohjelmistoa automaatioverkon valvontaan. Täten kandidaatintyön pohjalta Zabbixin käyttöönottoa UPM Kymin sellutehtaan automaatioverkon valvontaan voidaan suositella. Verkonvalvonnan avulla voidaan helpottaa verkon ylläpitoa sekä verkkosuunnittelua, jotka ovat avainasemassa automaatioverkon korkean palvelunlaadun saavuttamiseksi. Automaatioverkon korkea palvelunlaatu takaa sellutehtaan tuotantoprosessin tehokkaan hallinnan, jolloin lopputuotteen valmistus toteutuu turvallisesti ja kustannustehokkaasti.

Avainsanat: Prosessiteollisuus, Automaatioverkko, Verkonvalvonta, FCAPS, SNMP, Zabbix

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

ALKUSANAT

Idea kandidaatintyöhön tuli viime vuonna ollessani kesätöissä UPM Kymin sellutehtaalla. Tänä kesänä opintojeni ollessa sopivassa vaiheessa, työ päästiin viimein toteuttamaan. Suuret kiitokset Petri Kuitikalle ja Matias Puraselle kandidaatintyön mahdollistamisesta sekä tuesta työn loppuun saattamiseksi. Kiitos kuuluu myös työn ohjaajalle ja tarkastajalle Juha Vihervaaralle mutkattomasta työn ohjaamisesta. Lopuksi haluan kiittää läheisiäni ja ystäviäni kaikesta tuesta niin opinnoissa kuin vapaa-ajallakin.

Kouvolassa, 11.8.2022

Paavo Asikainen

SISÄLLYSLUETTELO

1. JOHDANTO 1
2. VERKOT 2
2.1 TCP/IP-protokollaperhe 2
2.2 Ethernet-verkot 4
2.3 Lähiverkkotopologiat 5
2.4 Automaatioverkot 8
3. VERKONHALLINTA 12
3.1 FCAPS-viitemalli 12
3.2 Verkonvalvonta 14
3.3 Verkonvalvonnassa käytettävät tekniikat 15
3.3.1 Simple Network Management Protocol, SNMP 15
3.3.2 MIB-tietokanta 17
3.3.3 Internet Control Message Protocol, ICMP 18
3.3.4 Remote Network Monitoring, RMON 19
3.3.5 NetFlow 19
4. ZABBIX 21
4.1 Zabbixin arkkitehtuuri 21
4.2 Zabbixin ominaisuudet 22
5. UPM KYMIN SELLUTEHDAS TOIMINTAYMPÄRISTÖNÄ 26
5.1 Verkonvalvonnan nykytila 27
5.2 Vaatimukset ja tavoitteet verkonvalvonnalle 28
6. YHTEENVETO 32
LÄHTEET 34

LYHENTEET JA MERKINNÄT

API	Application Programming Interface, ohjelmointirajapinta.
CAN	Campus Area Network, kampusverkko.
DNS	Domain Name Service, nimipalvelujärjestelmä.
FCAPS	Fault, Configuration, Accounting, Performance and Security, Verkonhallinnan viitemalli.
GPLv2	General Public License version 2, avoimen lähdekoodin ohjelmistojen julkaisuun tarkoitettu lisenssi.
ICMP	Internet Control Message Protocol, verkkojen virhe-, ohjaus- ja testisanomia välittävä protokolla.
IETF	Internet Engineering Task Force, verkkoprotokollien standardardoinnista vastaava organisaatio.
IP	Internet Protocol, verkkokerroksen internet-protokolla.
ISO	International Organization for Standardization, kansainvälinen standardisoimisjärjestö.
ITU-T	ITU Telecommunication Standardization Sector, kansainvälisen televiestintäliiton televiestinnän standardisoimissektori.
LAN	Local Area Network, lähiverkko.
LTS	Long Term Support, pitkäaikaisen tuen versio.
MAC	Medium Access Control, IEEE 802 standardin mukainen verkkoliikenteestä vastaava protokolla.
MAN	Metropolitian Area Network, Kaupunkiverkko.
OID	Object ID, MIB-tietokannan objektien yksiselitteinen tunnus.
PAN	Personal Area Network, likiverkko.
RMON	Remote Network Monitoring, verkon etämonitorointi.
SMI	Structure of Management Information, MIB-tietokannan standardoitu rakenne.
SNMP	Simple Network Management Protocol, verkonhallinnassa käytettävä protokolla.
SNMPv1	Simple Network Management Protocol version 1, SNMP-Protokollan ensimmäinen versio.
SNMPv2c	Community-based Simple Network Management Protocol version 2, SNMP-Protokollan toisen version yhteisöjulkaisu.
SNMPv3	Simple Network Management Protocol version 3, SNMP-Protokollan kolmas ja uusin versio.
SNOW	UPM ServiceNOW, laitetietokanta.
TCP	Transmission Control Protocol, yhteydellinen ja luotettava kuljetuskerroksen protokolla.
TCP/IP	Transmission Control Protocol / Internet Protocol, verkkojen tiedonsiirrossa käytettävä protokollaperhe.
TLS	Transport Layer Security, tiedonsiirron salauksesta vastaava protokolla.
UDP	User Datagram Protocol, yhteydetön ja epäluotettava kuljetuskerroken protokolla.
WAN	Wide Area Network, laajaverkko.

1. JOHDANTO

Automaatio on merkittävä osa modernia yhteiskuntaa, ja sen tarpeen lisääntyminen on saanut aikaan nopean automaatioverkkojen kehityksen muun muassa prosessiteollisuudessa. Kun automaatioverkot laajenevat ja kriittiset järjestelmät siirtyvät verkkoon, niiden ylläpito on entistä haastavampaa. Verkonvalvonnan päätehtävänä on tuottaa tietoa verkon tilasta, jotta verkon ylläpito on helpompaa ja resurssit voidaan hyödyntää tehokkaammin esimerkiksi verkkosuunnittelussa ja ongelmatilanteen sattuessa. Vaikka verkonvalvonta on avainasemassa verkkojen ylläpidossa, mielletään se tärkeydestään huolimatta usein ylimääräiseksi toiminnoksi tietoliikennetekniikassa.

Automaatioverkkojen toimintaperiaatteet ja ominaispiirteet luovat erilaisia vaatimuksia verkonvalvonnalle sekä verkonvalvontaohjelmistoille. Tämän työn tavoitteena on esitellä millaisia vaatimuksia automaatioverkot sekä UPM Kymin sellutehdas asettavat verkonvalvonnalle. Työssä selvitetään miten avoimen lähdekoodin verkonvalvontaohjelmisto Zabbix vastaa näihin vaatimuksiin ja määritellään, soveltuuko Zabbix UPM Kymin sellutehtaan automaatioverkon valvontaan. Lisäksi työssä kuvataan automaatioverkkojen ominaispiirteitä, nykypäivän verkonvalvontatekniikoita ja verkonvalvontaohjelmistojen toimintaperiaatteita. Työ on toteutettu toimeksiantona UPM Kymin sellutehtaalle.

Kandidaatintyö koostuu seuraavista osista. Luvussa kaksi tutustutaan Ethernet-pohjaisiin lähiverkkoihin liittyviin tekniikoihin ja rakenteisiin, jotka ovat oleellisia työn kannalta. Lisäksi käsitellään automaatioverkkojen ominaispiirteitä ja merkittävimpiä eroja perinteisiin verkkoihin verrattuna. Luvussa kolme siirrytään verkonhallinnan FCAPS-viitekehyksen kautta käsittelemään verkonvalvontaa. Luvussa tulee ilmi verkonvalvonnan pääelementit, tekniikat, protokollat sekä yleiset vaatimukset automaatioverkkojen näkökulmasta. Luvut kaksi ja kolme muodostavat kandidaatintyön teoriaosuuden.

Työn luvussa neljä tutustutaan Zabbix -verkonvalvontaohjelmiston arkkitehtuuriin, toimintaperiaatteisiin sekä ominaisuuksiin verkkojulkaisujen ja dokumentaation pohjalta. Luvussa viisi selvitetään UPM Kymin sellutehtaan verkonvalvonnan nykytilaa, sekä millaisia vaatimuksia ja tavoitteita verkonvalvonnalle asetetaan. Näitä vaatimuksia verrataan Zabbixiin ominaisuuksiin. Luvut neljä ja viisi muodostavat haastatteluihin ja (sisäisiin) selvityksiin perustuvan kandidaatintyön tutkimusosuuden. Luku kuusi sisältää yhteenvedon kandidaatintyöstä sekä esittelee johtopäätökset Zabbixin soveltuvuudesta ja hyödyntämisestä UPM Kymin sellutehtaan automaatioverkon valvonnassa.

2. VERKOT

Yleisellä tasolla verkko tarkoittaa joukkoa toisiinsa yhteydessä olevia ihmisiä tai laitteita, jotka kykenevät jakamaan informaatiota toisilleen [1]. Tietoliikennetekniikassa verkolla tarkoitetaan siirtotien, kuten kaapelin tai radiotien, välityksellä yhdistettyjä laitteita, jotka pystyvät kommunikoimaan keskenään [2]. Verkko koostuu päätepisteistä, joiden välillä olevat solmut, esimerkiksi verkkolaitteet, välittävät informaation lähteeltä määränpäähän siirtoteitä pitkin. Tyypillinen verkko sisältää useita eri päätepisteitä, jotka yhdistyvät siirtotein ja on yleistä, että verkot yhdistyvät myös toisiin verkkoihin tai sisältävät aliverkkoja. Täten verkot ovat lopulta kokoelma eri laitteita ja ohjelmistoja, jotka mahdollistavat tiedonsiirron päätepisteeltä toiselle. [1][3]

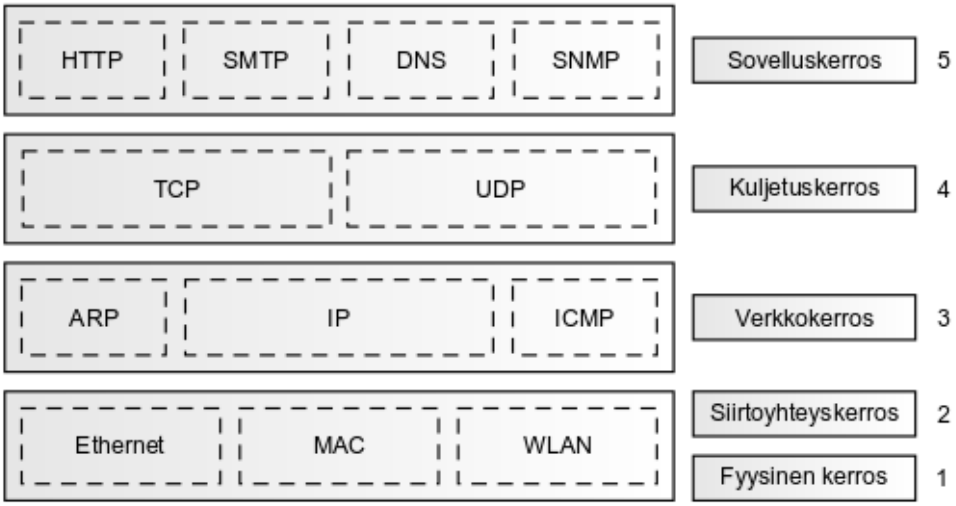
Verkkoja voidaan luokitella niiden koon ja maantieteellisen kattavuuden mukaan. Pienimmästä suurimpaan nämä luokat ovat likiverkko PAN (Personal Area Network), lähiverkko LAN (Local Area Network), kampusverkko CAN (Campus Area Network), kaupunkiverkko MAN (Metropolitan Area Network) sekä laajaverkko WAN (Wide Area Network). Likiverkko käsittää yhden ihmisen ulottuvilla olevat laitteet, ja sen laajuus on noin kymmenen metriä. Lähiverkko kattaa pienen maantieteellisen alueen, kuten kodin, toimiston tai rakennuksen. Nykyiset lähiverkkototeutukset perustuvat usein Ethernet-tekniikkaan. Kampusverkko yhdistää lähiverkkoja keskenään tietyn organisaation alueella, kuten kampuksella tai tehtaalla. Kaupunkiverkko yhdistää useita lähi- tai kampusverkkoja keskenään rajoittuen kaupunkien alueelle. Laajaverkko kattaa suuren maantieteellisen alueen, kuten useita kaupunkeja tai valtioita. [3] Tässä työssä käsitellään verkkoja lähi- ja kampusverkkojen tasolla.

2.1 TCP/IP-protokollaperhe

TCP/IP (Transmission Control Protocol / Internet Protocol) -protokollaperhe mahdollistaa tiedonsiirron verkossa. Se määrittelee joukon sääntöjä, jotka kertovat kuinka informaatio tulee muotoilla, osoittaa, lähettää, reitittää ja toimittaa lähteeltä oikeaan määränpäähän. [3] Protokollaperhe saa nimensä kahdesta tärkeimmästä protokollastaan, mutta se sisältää useita muitakin protokollia [4].

TCP/IP pohjautuu viiteen kerrokseen, joilla jokaisella on oma tehtävänsä tiedonsiirrossa. Nämä kerrokset alhaalta ylöspäin ovat fyysinen kerros (physical layer), siirtoyhteyskerros (data link layer), verkkokerros (network layer), kuljetuskerros (transport layer) ja sovelluskerros (application layer). Tätä kerrosjaottelua ei kuitenkaan noudateta erityisen

tarkasti, vaan TCP/IP:n ajatellaan enemmänkin koostuvan eri protokollista, jotka asettuvat päällekkäin hyödyntäen toistensa tarjoamia palveluja. Löyhä kerrosajattelu ja TCP/IP:n joustavuus ilmenee siten, että kerroksia on mahdollisuus yhdistää tai ohittaa kokonaan tiedonsiirrossa. [4] Kuvasta 1 ilmenee protokollaperheen kerrokset sekä kunkin kerroksen protokollia.



Kuva 1. *TCP/IP kerrokset ja protokollat, muokattu lähteestä [4].*

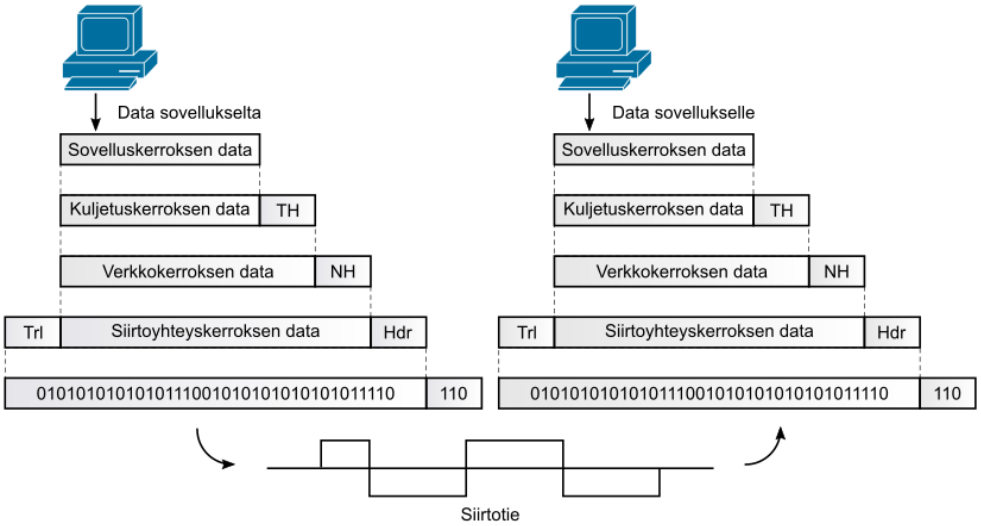
Kaksi alinta kerrosta ovat fyysinen kerros ja siirtoyhteyskerros [4]. Fyysinen kerros sisältää menetelmät bittivirran välittämiseen siirtotiellä [5]. Se siis määrittelee siirtotietä koskevat mekaaniset, fyysiset ja käytännölliset ominaisuudet. Fyysisen kerroksen yläpuolella olevan siirtoyhteyskerroksen päätehtävä on kuljettaa kehykset yksittäiseltä verkkolaitteelta toiselle hyödyntäen laitteiden fyysisiä osoitteita, eli MAC (Medium Acces Control) -osoitteita. Samalla se osaltaan vastaa vuon- ja virheenhallinnasta sekä väylänvarauksesta, jotka mahdollistavat tehokkaan tiedonsiirron. Käytettyjä tekniikoita kahdella alimmalla kerroksella ovat esimerkiksi Ethernet-tekniikka ja MAC-protokolla. TCP/IP ei kuitenkaan määrittele erityisen tarkasti alimmilla kerroksilla käytettyjä tekniikoita. [4]

Seuraavat kaksi kerrosta ovat verkkokerros sekä kuljetuskerros. Verkkokerroksen IP (Internet Protocol) -protokolla on vastuussa kehysten reitittämisestä verkon päästä päähän parasta mahdollista reittiä pitkin huomioiden verkon tilan, kuten ruuhkautumisen. Reitittäminen tapahtuu laitteiden IP-osoitteiden avulla. Verkkokerroksen tehtäviin kuuluu myös muun muassa ruuhkan- sekä virheenhallinta. Neljännellä kerroksella sijaitsevan kuljetuskerroksen tavoitteena on toimittaa kehyksen data kohdelaitteessa oikealle sovellusprosessille porttinumeroiden avulla. Se siis vastaa kanavoinnista sekä tiedonsiirron luotettavuudesta halutulla laatutasolla. Kuljetuskerroksella on käytössä kaksi erilaista protokollaa. TCP (Transmission Control Protocol) -protokolla, josta TCP/IP-protokollaperhe on saanut nimensä, tarjoaa luotettavaa ja yhteydellistä tiedonsiirtopalvelua, kun

taas UDP (User Datagram Protocol) -protokolla tarjoaa yhteydetöntä ja epäluotettavaa tiedonsiirtoa. [4]

Ylimpänä muiden TCP/IP-protokollaperheen kerrosten ja käyttäjän välissä on sovelluskerros. Tämän kerroksen eri protokollat, kuten verkonhallintaprotokolla SNMP (Simple Network Management Protocol) ja nimipalvelu DNS (Domain Name Service), toteuttavat tietoliikenteen sovelluskohtaiset palvelut. Sovelluskerros vastaa asiakas- ja palvelinprosessien toiminnasta ja hyödyntää alempien kerrosten protokollien tarjoamia tiedonsiirtopalveluja. [4]

TCP/IP-protokollaperheen jokaisen kerroksen protokolla kommunikoi toisen laitteen saman kerroksen protokollan eli vastinolionsa kanssa. On kuitenkin huomattava, että näitä laitteita yhdistää fyysinen siirtotie. Täten vastinolioiden suora kommunikointi ei ole mahdollista, vaan informaatio kulkee lähteessä sovelluskerrokselta alas fyysiselle kerrokselle ja vastaavasti vastaanottopuolella alhaalta fyysiseltä kerrokselta ylös sovelluskerrokselle. Alkuperäisen informaation kulkiessa kerroksia alaspäin, jokainen kerros lisää kehykseen otsikon eli vastinoliolleen välitettävän tiedon. Vastaanottopuolella jokainen kerros käsittelee sille kuuluvan tiedon ja poistaa otsikon kehyksestä. [4] Kuvassa 2 esiteltynä datan rakenne ja kulku protokollakerrokselta toiselle.



Kuva 2. *Datan rakenne ja kulku kerrokselta toiselle.*

2.2 Ethernet-verkot

Ethernet-tekniikka on ehdottomasti yleisimmin käytetty tekniikka langallisissa lähiverkkototeutuksissa. Se määrittelee TCP/IP-protokollaperheen fyysisen kerroksen ja siirtoyhteyskerroksen toiminnallisuuksia. Ethernet-tekniikka on määritelty IEEE:n (Institute of Electrical and Electronics Engineers) 802.3-standardissa. Se on suhteellisen pitkän his-

toriansa aikana kehittynyt huomattavasti ja standardointi on edelleen aktiivista. Menestyksensä Ethernet-tekniikka on ansainnut yksinkertaisella toteutuksellaan, luotettavuudellaan ja kustannustehokkuudellaan. [5]

Ethernet-verkkoja voidaan toteuttaa erilaisilla menetelmillä ja tekniikoilla. Jaettuun siirtotiehen perustuvissa Ethernet-verkoissa verkon päätelaitteet ovat kytketty toisiinsa jaetun kaapelin tai keskittimen (hub) välityksellä. Keskitin on passiivinen verkkolaite, joka lähettää vastaanottamansa lähetyksen kaikille verkon muille laitteille. Näissä ratkaisuissa päätelaitteen lähettämä lähetys on siis kaikkien muiden päätelaitteiden vastaanotettavissa. Koska käytössä on jaettu siirtotie, useamman päätelaitteen lähettäessä dataa samanaikaisesti verkossa tapahtuu törmäys. Täten siirtotie on varattava vain yhden päätelaitteen käyttöön kerrallaan CSMA/CD (Carrier Sensing Multiple Access with Collision Detection) -protokollalla. Väylänvarausprotokollan avulla päätelaite kuuntelee siirtotietä ja aloittaa lähetyksen, jos se on vapaa. On myös mahdollista, että useampi päätelaite sattuu aloittamaan lähetyksen lähes samanaikaisesti. Tällöin väylänvarausprotokolla havaitsee törmäyksen, ilmoittaa siitä verkkoon ja toipuu törmäyksestä. [5]

Ethernet-verkkoja voidaan toteuttaa myös kytkemällä verkon päätelaitteet toisiinsa kytkimen välityksellä. Kytkin on aktiivinen verkkolaite, joka opettelee verkon rakennetta ja välittää vastaanottamansa lähetyksen vain kohteena olevalle päätelaitteelle. Kytkimet siis jakavat verkon osiin, jolloin törmäyksiä ei ilmene eikä verkonvarausprotokollaa myöskään tarvita. Täten verkon tehokkuus, luotettavuus ja ennakoitavuus paranee. Nykyiset lähiverkkototeutukset perustuvat pitkälti kytkinpohjaisiin Ethernet-verkkoihin, mutta jaettuun siirtomediaan pohjautuvat Ethernet-verkot ovat myös satunnaisesti käytössä. [6]

2.3 Lähiverkkotopologiat

Verkon topologialla tarkoitetaan rakennetta, jolla verkon laitteet ovat yhdistetty toisiinsa [7]. Topologiat voidaan luokitella kolmeen luokkaan, jotka ovat fyysinen topologia physical topology), looginen topologia (logical topology) sekä signaalitopologia (signal topology). Fyysinen topologia kuvaa verkon solmujen ja siirtoteiden fyysiset kytkennät. Looginen topologia ilmaisee verkon yhteyksien näennäiset kulkureitit, kun taas puolestaan signaalitopologia ilmaisee verkon yhteyksien todelliset kulkureitit. Fyysinen ja looginen topologia mukailevat pitkälti toisiaan, mutta signaalitopologia voi erota muista edellä mainituista huomattavasti. [3]

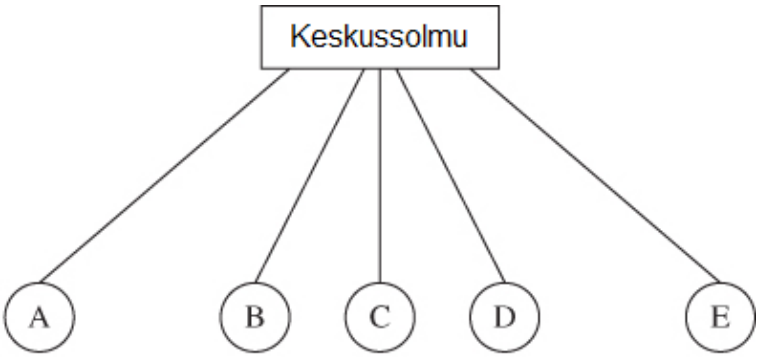
Kaikista yksinkertaisimmillaan topologia voi muodostua kahdesta laitteesta ja niitä yhdistävästä siirtotiestä. Verkoissa topologiat ovat kuitenkin monimutkaisia, koska niissä esiintyy useita erilaisia kytkentöjä. Topologioita voidaan jakaa kytkentöjensä mukaan eri

ryhmiin, joista tyypillisimmät ovat väylätopologia (bus topology), tähtitopologia (star topology), rengastopologia (ring topology), mesh-topologia (mesh topology), puutopologia (tree topology) sekä hybriditopologia (hybrid topology). [7]

Väylätopologiassa kaikki verkon laitteet on kytketty samaan yhteiseen siirtotiehen haaroittimilla. Väylään kytketyt laitteet ovat hierarkkisesti samanarvoisia, ja ne voivat kaikki seurata verkkoliikennettä ja osallistua siihen. [6] Väylätopologiassa on yleensä vaatimuksena väylän päiden päättäminen, jotta signaalit eivät heijastu väylän päästä takaisin. Väylätopologiassa verkon resurssit jaetaan laitteiden kesken tehden siitä toteutukseltaan kustannustehokkaan, mutta toisaalta rajoittaen verkon luotettavuutta ja suorituskykyä. [8] Laitteiden samanarvoisuus aiheuttaakin väylätopologian suurimmat ongelmat, jotka liittyvät väylänvaraukseen. Verkossa syntyy helposti törmäyksiä useiden laitteiden lähettäessä dataa samanaikaisesti, ja verkon on toivuttava näistä törmäyksistä erilaisin menettelyin. [7] Väylätopologia sisältääkin juuri tästä syystä suhteellisen vähän laitteita [8]. Kuvassa 3 esiteltynä väylätopologia.

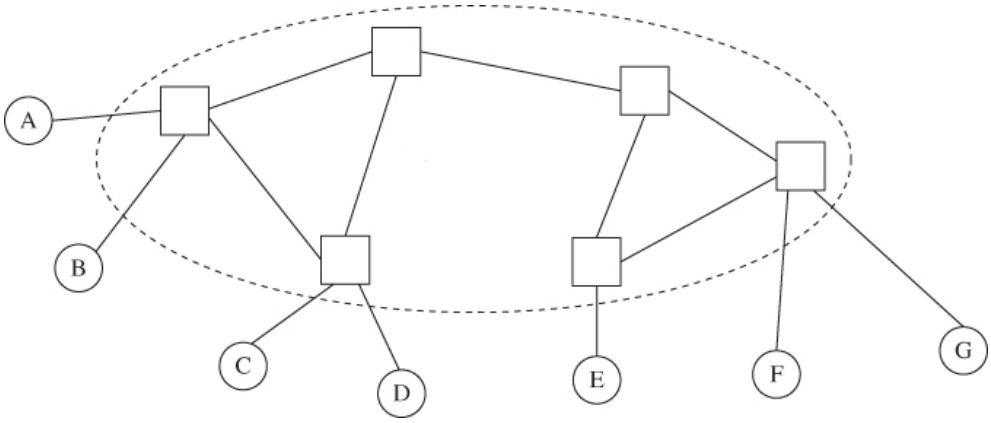
Kuva 3. *Väylätopologia.*

Tähtitopologiassa verkon ympäröivät solmut on kytketty yhteen keskussolmuun. Jokaisella verkon solmulla on siis pisteestä-pisteeseen yhteys keskussolmuun, täten verkon solmut voivat olla yhteydessä toisiinsa vain keskussolmun välityksellä. Tämä kuitenkin tarkoittaa sitä, että yhteyden katketessa solmun ja keskussolmun välillä yhteys verkon muihinkin solmuihin katkeaa. [3] Verkon keskussolmu voi olla passiivinen, esimerkiksi keskitin, joka lähettää vastaanottamansa lähetyksen jokaiseen solmuun. Yleisimmin verkon keskussolmussa on käytössä aktiivinen verkkolaite, esimerkiksi kytkin, joka välittää liikenteen haluttuun suuntaan vähentäen verkon kuormitusta [7][8]. Kuvassa 4 on esitetty tähtitopologia.



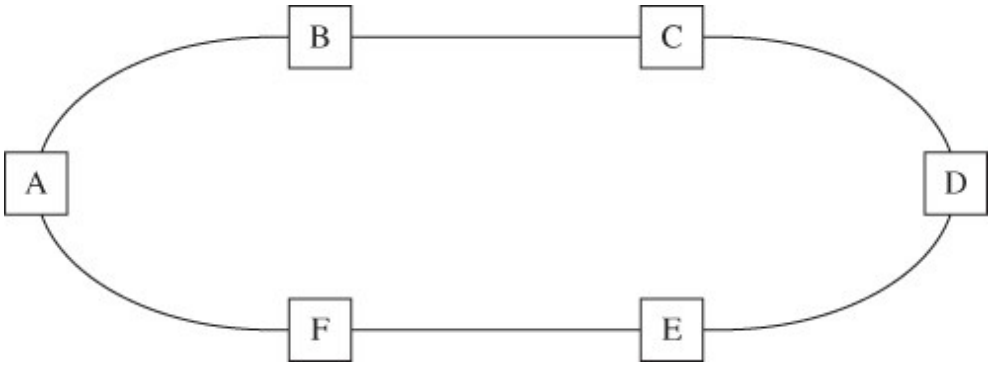
Kuva 4. *Tähtitopologia.*

Mesh-topologiaa käytetään maksimoimaan verkon kriittisten laitteiden käytettävyys ja luotettavuus [8]. Mesh-topologia voidaan toteuttaa osittaisena, jossa vähintään kahdella verkon solmulla on suora yhteys vähintään kahteen muuhun verkon solmuun, tai täydellisenä, jossa kaikki verkon solmut ovat kytketty suoraan toisiinsa [3]. Koska solmujen välillä on useita yhteyksiä, yhden yhteyden katkeaminen tai laitevikakaan ei välttämättä vaikuta verkon käytettävyyteen [8]. Kuvassa 5 ilmenee osittainen mesh-topologia.



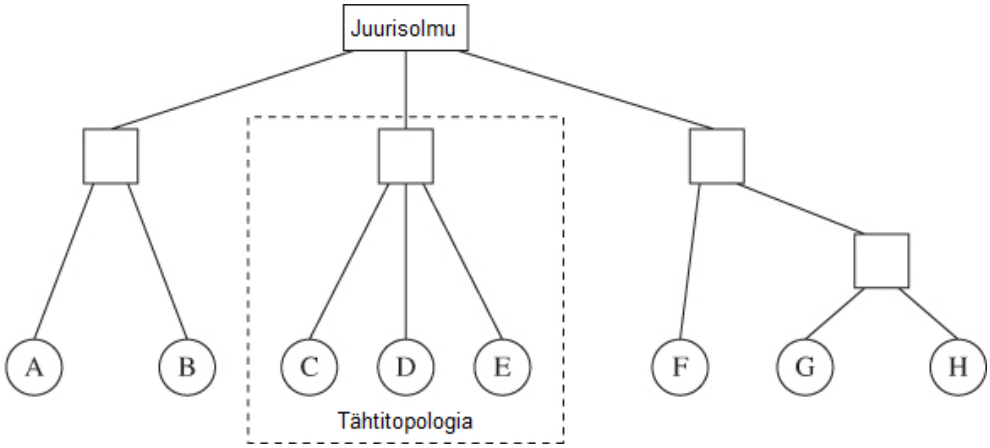
Kuva 5. *Osittainen mesh-topologia.*

Rengastopologiassa verkon solmut kytketään toisiinsa nimensä mukaisesti renkaan muotoon. Tällöin jokaisella verkon solmulla on kaksi viereistä solmua renkaassa. [3] Yleensä rengastopologia on rakennettu kytkimistä, joihin verkon muut solmut yhdistyvät [8]. Tiedonsiirto rengastopologiassa voidaan toteuttaa eri tavoin. Liikenne voi kulkea renkaassa vain tiettyyn suuntaan. Tämä kuitenkin aiheuttaa sen, että verkon kahden viereisen solmun välinen liikenne voi joutua kiertämään koko renkaan. Toinen tapa on käyttää rinnakkaisia renkaita, joiden liikenne kulkee eri suuntiin. [7] Rengastopologian solmujen ylimääräiset yhteydet parantavat verkon luotettavuutta, koska yksi katkennut yhteys ei vielä kaada verkkoa, vaan liikenteelle löytyy vaihtoehtoinen reitti [8]. Kuvassa 6 ilmenee rengastopologia



Kuva 6. *Rengastopologia.*

Puutopologia kytkee yhteen verkon solmuja hierarkkisesti [8]. Puutopologiassa verkon juurisolmu on kytketty yhteen tai useampaan hierarkkisesti alempana olevaan solmuun. Nämä solmut voivat puolestaan olla kytkettynä edelleen hierarkkisesti alempiin solmuihin muodostaen puumaisen rakenteen. [3] Verkon solmut voivat haarautua eri tavoin ja rakentua muiden topologioiden mukaisista kytkennöistä. Tällöin kyseessä on hybriditopologia, joka on kahden tai useamman eri topologian yhdistelmä. Hybriditopologioita ilmenee, kun verkon eri osat yhdistyvät toisiinsa siten, ettei rakenteesta ilmene selkeästi yhtä tiettyä määritettyä topologiaa. [8] Kuvassa 7 esiteltynä puutopologia.



Kuva 7. *Puutopologia.*

2.4 Automaatioverkot

Automaatiojärjestelmillä tarkoitetaan hajautettuja järjestelmiä, jotka koostuvat mittauksista sekä niiden pohjalta toteutettavista hallinta- ja ohjauspäätöksistä fyysisille laitteille. Automaatio on merkittävä osa modernia yhteiskuntaa. Se integroituu nykyään useisiin prosesseihin sekä laitteisiin, kuten sähkön- ja lämmöntuotantoon, tehtaisiin sekä kodinkoneisiin. Nykyaikaiset automaatiojärjestelmät rakennetaan tietoliikenneverkkojen ja ohjelmistojen avulla. [9]

Olennaisena osana automaatioverkkoja on Ethernet-tekniikan hyödyntäminen automaatiojärjestelmien eri tasoilla [10]. Ethernet-tekniikkaa on pystytty kehittämään automaation tarpeita huomioiden, ja kustannustehokkuutensa, laajan saatavuutensa sekä suuren tiedonsiirtonopeutensa ansiosta se soveltuu hyvin automaatioverkkoihin [6]. Automaatioverkkojen toimintaperiaatteiden ymmärtäminen vaatii laajaa tietämystä, koska ne sisältävät useita eri tekniikoita, protokollia sekä standardeja. Automaatioverkot ovat siis luoneet uudenlaisen verkkoympäristön, joka vaikuttaa perinteisten verkkojen kaltaiselta sisältäen kuitenkin useita erilaisia vaatimuksia. [10]

Vaikka automaatioverkkojen viimeaikainen integraatio Ethernet-tekniikan parissa on häivyttänyt rajaa automaatioverkkojen sekä perinteisten verkkojen välillä, on niillä lähtökohtaisesti suuria eroavaisuuksia ja erilaisia vaatimuksia. Suurin eroavaisuus näiden kahden välillä on se, että automaatioverkot ovat yhdistettynä jonkinlaisiin fyysisiin laitteisiin ja automaatioverkkoja käytetään reaalimaailman toimintojen hallintaan sekä monitorointiin. Yhteys reaalimaailmaan johtaa esimerkiksi erilaisiin painotuksiin palvelunlaadussa (quality of service) automaatioverkkojen ja perinteisten verkkojen välillä. [10] Taulukossa 1 on esiteltynä tyypillisimmät eroavaisuudet verkkojen välillä.

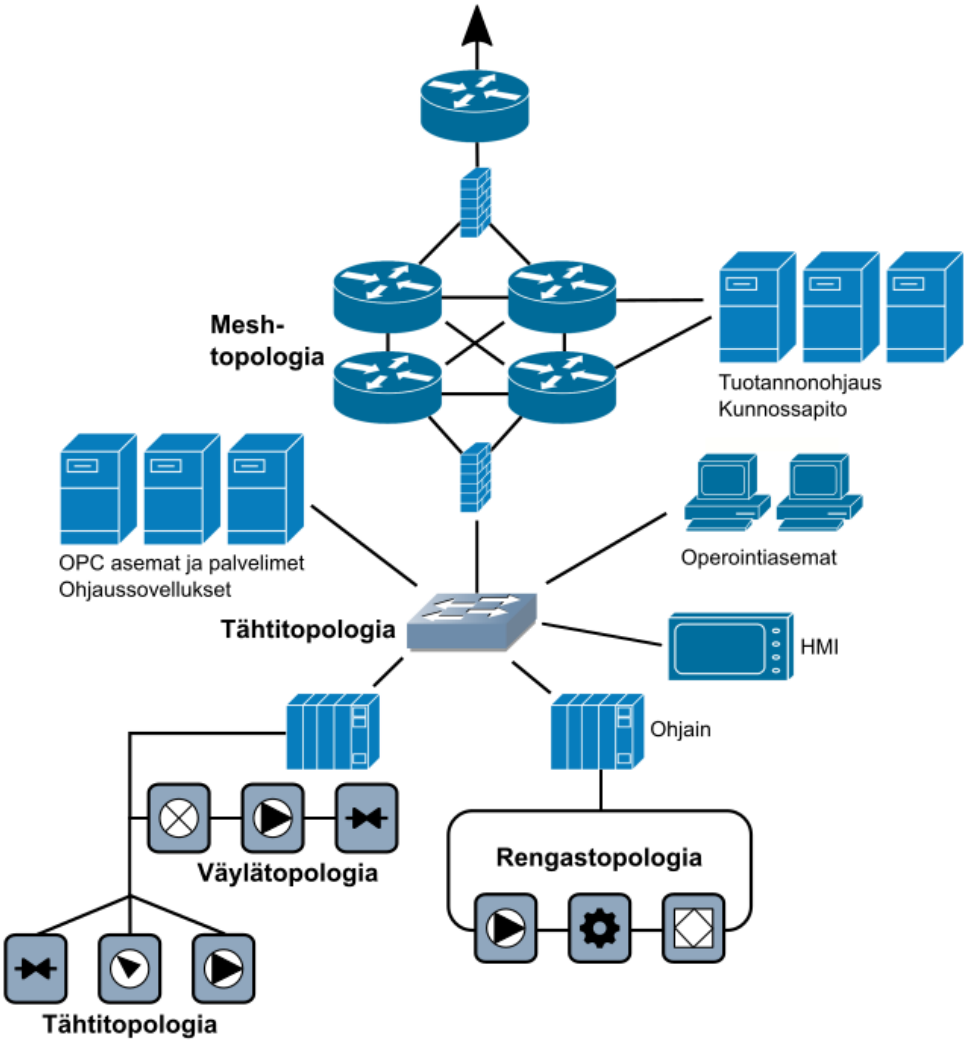
Taulukko 1. *Automaatioverkkojen ja perinteisten verkkojen eroavaisuudet, muokattu lähteestä [10].*

	Automaatioverkko	**Perinteinen verkko**
Päätarkoitus	Fyysisten laitteiden hallinta	Tiedonsiirto ja -käsittely
Sovellusalue	Tuotanto, prosessiteollisuus, infrastruktuuri	Yritykset ja kotitaloudet
Hierarkia	Syvä, toiminnallisesti erotultu, sisältää useita protokollia ja standardeja	Matala, integroitu hierarkia, sisältää yhtenäiset protokollat ja standardit
Vikaantumisen vakavuus	Korkea	Matala
Vaadittava luotettavuus	Korkea	kohtalainen
Vasteaika	250 µs – 10 ms	50+ ms
Ennakoitavuus	Korkea	Matala
Tiedon koostumus	Pieniä paketteja, jaksottainen ja jaksoton liikenne	Suuria paketteja, jaksoton liikenne
Ajallinen eheys	Vaaditaan	Ei vaadita
Operointiympäristö	Monipuoliset olosuhteet	Siisti ympäristö, usein tarkoitettu herkille laitteille

Kuten jo aiemmin on todettu, automaatioverkkojen päätarkoituksena on fyysisten laitteiden hallinta. Automaatioverkkojen sovellusalueena on usein tuotantolaitokset, prosessiteollisuus ja infrastruktuuri. Perinteiset verkot puolestaan keskittyvät tiedonsiirtoon ja -käsittelyyn erityisesti yrityksissä ja kotitalouksissa. Automaatioverkkojen sovellusalueella on usein monipuoliset olosuhteet. Esimerkiksi valvomoissa ja laitetiloissa on siistit

sekä kontrolloidut olosuhteet, mutta tuotantotiloissa on puolestaan usein haastavat olosuhteet, jotka voivat sisältää esimerkiksi kuumuutta, kosteutta, pölyä ja tärinää. Perinteisissä verkoissa laitteet ovat lähtökohtaisesti siistissä ympäristössä. [10]

Automaatioverkoilla on syvempi arkkitehtuurinen rakenne kuin perinteisillä verkoilla. Perinteiset verkot voivat koostua yksittäisistä lähiverkoista, jotka yhdistyvät laajaverkkoon, kun taas pienetkin automaatioverkot sisältävät vähintään kolmesta neljään kerrosta. Esimerkiksi alimmalla tasolla kenttälaitteet on kytketty ohjausjärjestelmiin, ja seuraavalla tasolla ohjausjärjestelmät yhdistyvät keskenään. Tämän yläpuolella on käyttäjärajapinta, operointiasemia ja palvelimia. Kaikista ylimpänä sijaitsee ulkoiseen tiedonsiirtoon tarkoitettu verkko. On myös tyypillistä, että eri hierarkkiatasoilla on käytössä erilaisia protokollia ja standardeja. [10] Kuvassa 8 on esiteltynä esimerkkikuva automaatioverkon hierarkkisesta rakenteesta.



Kuva 8. *Esimerkkikuva automaatioverkon rakenteesta, muokattu lähteestä [8].*

Koska automaatioverkot ovat yhdistettynä fyysisiin laitteisiin, verkon vikaantuminen voi aiheuttaa huomattavasti suurempaa vahinkoa kuin perinteisissä verkoissa. Vikatilanne voi johtaa esimerkiksi laitteiston vaurioitumiseen, tuotannonmenetykseen, ympäristövahinkoon tai pahimmillaan hengenmenetykseen. Täten automaatioverkkojen on toimittava luotettavasti. Tämä johtaa automaatioverkkojen tarkkaan reaaliaikavaatimukseen ja ennakoitavuuteen. Prosessien ja kenttälaitteiden toimintanopeus edellyttää, että data käsitellään mahdollisimman nopeasti. Data on myös pystyttävä käsittelemään ennakoitavasti, joka tarkoittaa, että verkon vasteajalla on oltava mahdollisimman pieni varianssi. [10]

Automaatioverkoissa, etenkin sen alimmilla hierarkkiatasoilla, datapaketit ovat pieniä sisältäen vain yksittäistä mittaus- tai kontrollidataa. Tällaiset paketit ovat kooltaan vain joitain kymmeniä bittejä. Mittausdataa näytteistetään ja lähetään säännöllisin väliajoin jaksottaisesti. Kontrollidataa ja hälytyksiä lähetetään puolestaan jaksottomasti niiden ilmetessä epäsäännöllisesti. Automaatioverkoissa vaaditaan myös ajallista eheyttä, jotta tiedetään milloin ja missä järjestyksessä tiedonsiirtotapahtumat ovat tapahtuneet. Perinteisissä verkoissa paketit ovat usein kooltaan vähintään kilobittien luokkaa, ja ne lähetetään best-effort-periaatteella. [10]

3. VERKONHALLINTA

Automaation tarpeen lisääntyminen nyky-yhteiskunnassa on saanut aikaan nopean automaatioverkkojen kehityksen [11]. Lähiverkkojen koon kasvaminen ja kriittisten järjestelmien siirtäminen verkkoon tuo verkkojen käytettävyydelle haasteita [12]. Nämä seikat, sekä aliluvussa 2.3.1 esitellyt automaatioverkkojen ominaispiirteet, lisäävät vaatimuksia tekniikoille, joilla automaatioverkkoja ylläpidetään ja hallitaan [11]. Verkonhallinta on laaja käsite, ja se voidaan määritellä eri tavoin riippuen näkökulmasta. Verkonhallinnalla tarkoitetaan toimintatapoja, menetelmiä sekä teknologioita, joilla voidaan valvoa, hallita ja ylläpitää verkkoja. Merkittävä osa verkonhallinnasta on verkonvalvontaa, mutta lisäksi se sisältää esimerkiksi verkkolaitteiden määrittelyä ja ylläpitoa sekä verkon resurssien jakoa. [13]

Verkonhallinta tarjoaa monia hyötyjä verkkojen toiminnalle. Sen päätehtävänä on varmistaa, että verkon palvelut sekä toiminnot ovat käyttäjien saatavilla asianmukaisella palvelunlaadulla. [14] Lisäksi se esimerkiksi mahdollistaa verkon ylläpitokustannusten pitämisen kurissa sekä verkkolaitteiden tehokkaan käyttämisen parantaen verkon saatavuutta. Tehoton verkonhallinta puolestaan voi johtaa verkon palvelunlaadun heikkenemiseen ja häiriintymiseen, sekä huonoon investointien hyödyntämiseen. Täten verkonhallinta on avainasemassa, jotta verkkoa voidaan hyödyntää mahdollisimman hyvin. Tärkeydestään huolimatta verkonhallinta mielletään usein ylimääräiseksi toiminnoksi tietoliikennetekniikassa eikä verkonhallinnan merkitystä ymmärretä täysin. [13]

3.1 FCAPS-viitemalli

Kansainvälinen standardisoimisjärjestö ISO (International Organization for Standardization) ja kansainvälisen televiestintäliiton televiestinnän standardisoimissektori ITU-T (ITU Telecommunication Standardization Sector) ovat määritelleet FCAPS (Faults, Configuration, Accounting, Performance, Security) -viitemallin selventämään laajaa verkonhallinnan kokonaisuutta [11]. FCAPS jakaa verkonhallinnan viiteen toiminnalliseen alueeseen, jotka ovat vianhallinta (Fault management), kokoonpanon hallinta (Configuration management), käytönhallinta (Accounting management), suorituskyvyn hallinta (Performance management) sekä turvallisuuden hallinta (Security management) [15]. FCAPS on yleisimmin käytetty viitemalli verkonhallinnassa, ja se auttaa luomaan yhteistä terminologiaa, ryhmittelemään eri toimintoja sekä tunnistamaan niiden välisiä yhteyksiä. On kuitenkin muistettava, että kyseessä on käsitteellinen viitemalli, joka sisältää yleistyksiä.

Todellisissa järjestelmissä viitemallin mukaista jaottelua on usein haastavaa noudattaa. [13]

Vianhallinta käsittelee verkossa ilmeneviä vikoja, kuten laite- tai ohjelmistovikoja [13]. Sen tavoitteena on pyrkiä havaitsemaan, ilmoittamaan sekä korjaamaan verkossa ilmeneviä vikoja [12]. Vianhallinta keskittyy siis pitkälti valvomaan verkon tilaa ja reagoimaan erilaisiin hälytyksiin ja ilmoituksiin. Tehokas vianhallinta ja nopea vikatilanteisiin reagoiminen on tärkeää, jotta verkossa ei ilmenisi käyttökatkoksia. Vianhallinta on lähtökohtaisesti reaktiivista toimintaa, eli toimiin ryhdytään vasta kun viat havaitaan. Vika- ja hälytyslokeja analysoimalla on kuitenkin mahdollista havaita kaavoja vikojen ilmaantumisesta ja niiden syy-seuraus-suhteista, mikä mahdollistaa vikatilanteisiin reagoimisen ennakoivasti. [13]

Kokoonpanon hallintaa käytetään verkossa olevien laitteiden asetusten määrittelyyn ja konfigurointiin. Tämä sisältää kokonaan uuden laitteen saattamisen toimintakuntoiseksi verkkoon, kuin myös jo verkossa valmiina olevien laitteiden hallinnan. Kokoonpanon hallinta seuraa verkon rakennetta, ja oleellinen osa kokoonpanon hallintaa on ylläpitää tietokantaa verkossa olevista laitteista sekä niiden konfiguraatioista. Laitteiden ja tietokantojen ajantasainen varmuuskopiointi on myös kokoonpanon hallinnan vastuulla. [13]

Käytönhallinta käsittelee verkon käytön tunnuslukujen mittaamista siten, että verkon käyttöä on mahdollista seurata [12]. Oleellisimmat tunnusluvut ovat verkon todellinen kapasiteetti ja kuinka paljon sitä käytetään. Näitä tietoja voidaan hyödyntää verkon kapasiteettisuunnittelussa sekä sen kustannustehokkaassa ylläpidossa. Verkosta kerättävä tieto on määriteltävä sopivilla termeillä ja yksiköillä, jotka ovat oleellisia kunkin tunnusluvun kannalta. Esimerkiksi verkon käyttöä voidaan mitata megatavuina siirrettyä dataa. Kun tunnuslukuja mitataan oikeilla yksiköillä, niiden käsittely ja analysointi on helpompi toteuttaa tehokkaasti. [13]

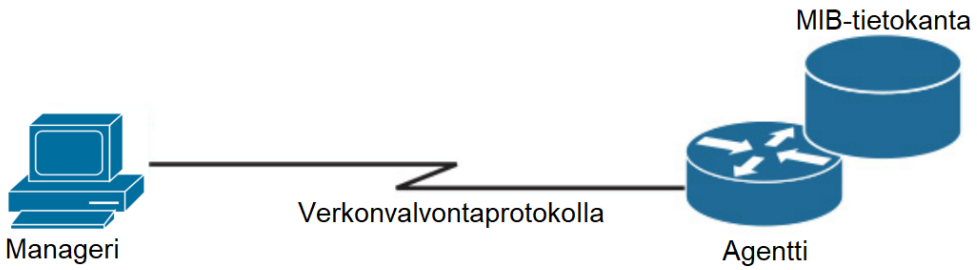
Suorituskyvyn hallinta käsittelee verkon suorituskykyparametrien valvontaa ja hienosäätöä [13], jotta verkon suorituskyky pystytään pitämään hyväksyttävällä tasolla [12]. Valvottavia parametrejä ovat esimerkiksi tiedonsiirtonopeus, viive ja palvelunlaatu. Näiden parametrien avulla luodaan kuvaa verkon nykytilasta ja sen suorituskyvystä. Suorituskykyparametrien muutoksia voidaan tarkastella pidemmällä aikavälillä esimerkiksi kuvaajien avulla. Tällöin saatujen tietojen pohjalta voidaan hienosäätää verkon toimintaa sekä havaita verkon ongelmakohtia, esimerkiksi pullonkauloja. Etenkin suurissa verkoissa suorituskyvyn valvonta voi kuormittaa verkkoa huomattavasti, koska valvottavia laitteita on paljon. [13]

Viimeinen viitemallin osa-alue on turvallisuuden hallinta, joka käsittelee verkon suojaamista erilaisilta sisäisiltä sekä ulkoisilta uhkilta. Turvallisuuden hallinta keskittyy siihen, että verkot sekä laitteet ja ohjelmistot ovat suojattuja ja niihin on pääsy vain valtuutetuilla käyttäjillä. Suuressa osassa turvallisuuden hallintaa on verkkoliikenteen sekä lokitietojen seuranta ja tallennus. Näistä saatuja tietoja analysoimalla voidaan havaita poikkeavaa toimintaa. Turvallisuuden hallinta sisältää erilaisia menetelmiä uhkia vastaan, joita ovat esimerkiksi järjestelmien ja laitteiden suojaus, käyttöoikeuksien hallinta, salasanapolitiikka, verkkoliikenteen rajoittaminen sekä epäilyttävien IP-osoitteiden estäminen. [13]

3.2 Verkonvalvonta

Kaikki FCAPS viitemallissa esittelyt osa-alueet sisältävät erilaisia toimenpiteitä, jotka käsittelevät joko informaation keräämistä ja valvomista verkosta tai konfiguraatioiden ja asetusten hallintaa. Nämä toimenpiteet voidaan jakaa verkonvalvontaan sekä verkonhallintaan. Verkonvalvonta sisältää menetelmät verkon tilan tarkkailuun. Se käsittelee verkon sekä laitteiden suorituskykyparametrien, konfiguraatioiden, tunnuslukujen, vikojen ja hälytysten valvontaa. Verkonhallinta puolestaan sisältää menetelmät verkon sekä verkkoon liitettyjen laitteiden konfigurointiin ja asetusten käsittelyyn. Verkonvalvonta on siis verkonhallinnan osa-alue, joka tuottaa arvokasta tietoa verkon tilasta, jonka perusteella voidaan toteuttaa verkonhallinnan toimenpiteitä. [13]

Verkonvalvonta koostuu kolmesta pääelementistä: verkonvalvontaohjelmistosta, valvottavasta laitteesta ja verkonvalvonnassa käytettävistä protokollista. Verkonvalvontaohjelmistolla toteutetaan verkonvalvonnan toimenpiteitä. Se sijaitsee yleensä tietokoneella tai palvelimella. Valvottava laite on jokin verkossa oleva laite, kuten esimerkiksi kytkin, reititin tai tietokone, jota valvotaan verkonvalvontaohjelmistolla. Verkonvalvontaohjelmiston ja valvottavan laitteen välinen kommunikaatio perustuu lähtökohtaisesti manageri-agentti -arkkitehtuuriin, jossa verkonvalvontaohjelmisto on manageri ja valvottava laite on agentti. Agentti ylläpitää erilaisia tietoja laitteesta, kuten sen määrittely- ja tilatietoja, MIB (Management Information Base) -tietokannassa. Näitä valvottavia tietoja kutsutaan objekteiksi. [3] Manageri lähettää agentille kyselyitä verkonvalvonnassa käytettyjen protokollien, kuten SNMP (Simple Network Management Protocol) -protokollan, välityksellä. Tällöin puhutaan aktiivisesta verkonvalvonnasta. [3][16] Agentti voi myös puolestaan lähettää managerille viestejä ilman erillisiä kyselyitä, jolloin kyseessä on passiivista verkonvalvontaa [16]. Kuvassa 9 on esiteltynä verkonvalvonnan elementit.



Kuva 9. *Verkonvalvonnan elementit, muokattu lähteestä [17].*

Verkonvalvonnalle sekä verkonvalvontaohjelmistolle voidaan asettaa automaatioverkkojen näkökulmasta yleisiä vaatimuksia. Kuten tässäkin työssä on tullut ilmi, automaatioverkkoja on kooltaan sekä tyypiltään erilaisia, ja ne sisältävät erilaisia tekniikoita, protokollia ja laitteita. Verkonvalvontaohjelmistojen tulee siis skaalautua kullekin verkolle sopivaksi, ja niiden on sovelluttava erityisesti heterogeenisille verkoille. Koska automaatioverkot keskittyvät fyysisten laitteiden hallintaan ja ne integroituvat kriittisiin prosesseihin, verkonvalvontaohjelmiston ei tulisi kuormittaa verkkoa, jotta automaatioverkkojen korkea luotettavuus sekä tarkat reaaliaikavaatimukset saavutetaan. Verkonvalvontaohjelmistojen tietoturvaominaisuudet on myös oltava asianmukaisella tasolla, jotta ulkopuolinen ei pääse automaatioverkon tietoja sisältävään dataan käsiksi. [14]

3.3 Verkonvalvonnassa käytettävät tekniikat

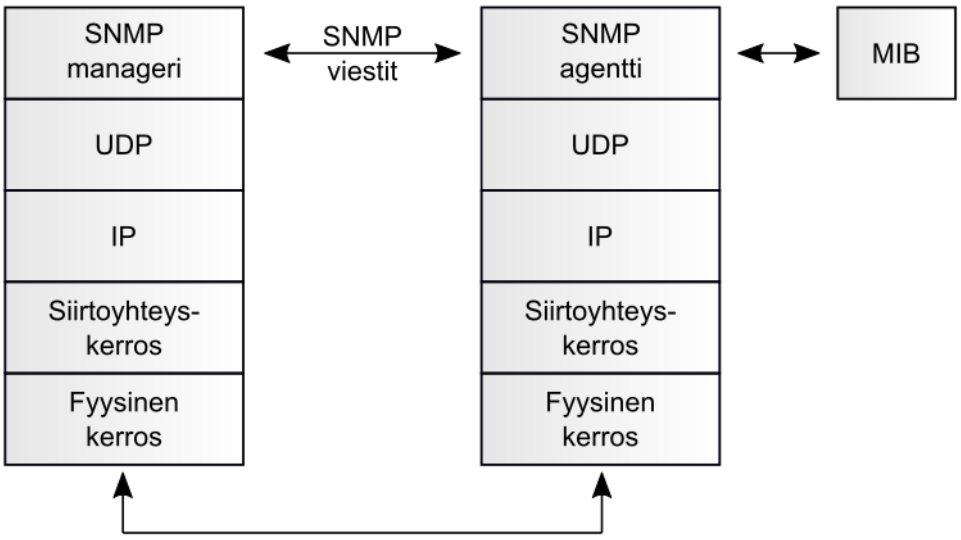
3.3.1 Simple Network Management Protocol, SNMP

SNMP-protokolla on kaikista tunnetuin ja eniten käytetty verkonhallintaprotokolla. Sitä käytetään erityisesti verkonvalvontaohjelmistoissa mahdollistamaan managerin ja agentin välinen kommunikaatio. [17] Alun perin internet-protokollien standardoinnista vastaava organisaatio IETF (Internet Engineering Task Force) määritteli SNMP-protokollan ja MIB-tietokannan 1980-luvun loppupuolella. [13] Ajatuksena oli kehittää standardisoitu tietokanta, joka sisältää tietoja yksittäisestä TCP/IP-verkossa olevasta laitteesta ja valvoa näitä tietoja yksinkertaista SNMP-protokollaa käyttäen [17]. Nykyisin lähtökohtaisesti jokaiselta laitteelta löytyy valmiiksi tuki SNMP-protokollan käyttöön [18]. SNMP-protokollan yksinkertaisuus ja helppokäyttöisyys onkin suurimpia syitä sen suosiolle [2].

SNMP protokolla sisältää erilaisia viestityyppejä. Verkonvalvontaohjelmisto, eli SNMP manageri, lähettää kyselyjä valvottavassa laitteessa olevalle SNMP agentille käyttäen ”Get Request”, ”GetNext Request” sekä ”GetBulk Request” -viestejä. Edellä mainittuihin viitataan yleisesti kyselyviesteinä. SNMP Agentti vastaa näihin kyselyihin käyttäen ”Get Response” -viestiä, joka sisältää halutun informaation. Kyselyviestit ovat siis pyyntövaste-pareja. Managerin on mahdollista konfiguroida MIB-tietokannan valvottavia tietoja

käyttäen ”Set” -viestiä. Agentin on myös mahdollista lähettää ilmoituksia managerille käyttäen ”Trap” ja ”Inform” -viestejä. Näillä ansaviesteillä ilmoitetaan, kun jokin MIB-tietokannan objekti ylittää tietyn raja-arvon tai saavuttaa jonkin tilan. [17]

SNMP-protokolla hyödyntää kuljetuskerroksen UDP-protokollaa managerin ja agentin välisessä tiedonsiirrossa. UDP onkin sopiva valinta pyyntö-vaste-parien viestintään, koska se on yhteydetön eikä muodosta päästä-päähän yhteyttä managerin ja agentin välille. Täten UDP kuormittaa verkkoa vähemmän kuin TCP-protokolla, mikä on tärkeää verkonvalvonnassa. UDP:n yhteydettömyys tekee siitä epäluotettavan protokollan, koska paketteja ei kuitata protokollatasolla. Verkonvalvontaohjelmiston vastuulle siis jää määrittää, onko paketit tulleet perille. Tämä toteutetaan yleensä yksinkertaisella aikakatkaisulla. Kyselyviesteille epäluotettavuus ei ole niinkään ongelma, koska pahimmillaan verkonvalvontaohjelmisto ei saa vastausta. Ansaviestien osalta tilanne on hieman erilainen. Jos ”Trap” -viesti ei saavu ikinä perille, verkonvalvontaohjelmisto ei voi tietää, että viestiä on koskaan lähetetty. Agentti ei myöskään osaa lähettää sitä uudelleen koska ”Trap” -viestissä kuittausta ei odoteta, toisin kuin ”Inform” -viestissä, jota voidaan hyödyntää kriittisemmissä ilmoituksissa. [19] Kuvasta 10 ilmenee SNMP-protokollan sijoittuminen TCP/IP-protokollaperheessä.



Kuva 10. *SNMP-protokolla TCP/IP-protokollaperheessä, muokattu lähteestä [5].*

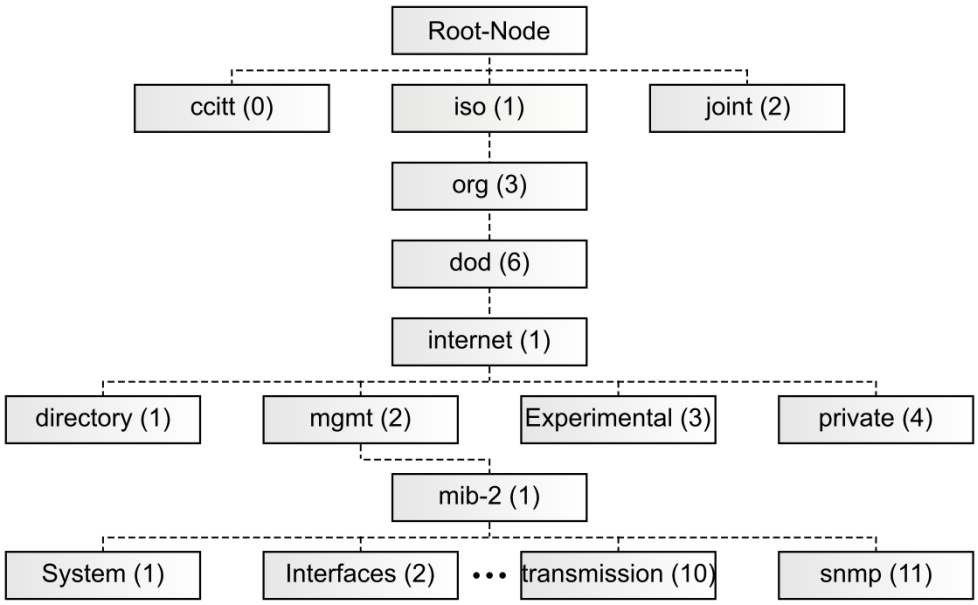
SNMP-protokollalla on kolme eri versiota, joita kaikkia käytetään vielä nykyäänkin. Ensimmäinen ja alkuperäinen versio tunnetaan nimellä SNMPv1 (Simple Network Management Protocol version 1). Se on toteutukseltaan kaikista yksinkertaisin ja helpoin ottaa käyttöön. SNMPv1 sai aikanaan suurta suosiota, mutta sen eräät osa-alueet osoittautuivat liiankin yksinkertaisiksi. Esimerkiksi SNMPv1 on tehoton käsittelemään suurta määrää informaatiota ja sen mitättömät tietoturvaominaisuudet saavat sen alttiiksi erilaisille uhkille. Näitä puutteita korjaamaan kehitettiin seuraava versio SNMPv2c (Community-

based Simple Network Management Protocol version 2). Se paransi monia ominaisuuksia aiemmasta versiosta. Ennen kaikkea sen suorituskykyominaisuudet ovat paremmat kuin SNMPv1:n. Lisäksi se kykenee keräämään ja käsittelemään suuria määriä informaatiota. SNMPv2c ei kuitenkaan tuonut toivottuja parannuksia tietoturvaominaisuuksiin. SNMP-protokollan viimeisin versio SNMPv3 (Simple Network Management Protocol version 3) toi parannuksia tietoturvaan, jotka puuttuivat kummaltakin aiemmalta versiolta. SNMPv3 sisältää menetelmät viestien salaamisen ja autentikoimiseen. Täten SNMPv3 on vähemmän alttiina uhkille ja viestinnän osapuolet voivat varmistua toisistaan. [13]

3.3.2 MIB-tietokanta

MIB-tietokannassa on esitettynä valvottavien laitteiden objektit, eli esimerkiksi määrittely- ja tilatiedot. Rekisteröityjä objekteja on olemassa yli tuhat, ja ne voivat olla yleisiä tai laitekohtaisia. MIB-tietokanta määrittelee yksityiskohtaisesti objektien merkitykset ja toiminnot, sekä niiden väliset suhteet. Valvottavassa laitteessa oleva agentti ylläpitää MIB-tietokantaa sekä välittää objektien sisältämiä tietoja managerille. MIB-tietokanta on siis olennainen osa verkonvalvontaa. [4]

MIB-tietokannalle on määritelty standardoitu rakenne SMI (Structure of Management Information), joka mahdollistaa objektien tehokkaan ja yksiselitteisen käsittelyn. Rakenteeltaan MIB-tietokanta on puumainen sisältäen eri hierarkkiatasoja. MIB-objektit sijaitsevat rakenteen alimmalla hierarkiatasolla haarassa, joka on lähtöisin ISO:sta. Puurakenteen jokainen haara sisältää nimen ja numeron lukuun ottamatta rakenteen juurta. [4] Haaroissa olevien numerojen avulla jokaiselle objektille voidaan määrittää yksiselitteinen OID (Object ID) -tunnus [19]. Kuvassa 11 on esitetty MIB-tietokanta. Objektit laitteen määrittelyistä löytyy haaran alta, jonka OID-tunnus on 1.3.6.1.2.1.1.



Kuva 11. *MIB-tietokanta, muokattu lähteestä [19].*

3.3.3 Internet Control Message Protocol, ICMP

ICMP (Internet Control Message Protocol) -protokolla on TCP/IP-protokollaperheen verkkokerroksella sijaitseva protokolla, jota käytetään verkoissa ilmenevien ongelmien raportointiin. Se keskittyy muun muassa siihen, että pääseekö data sille tarkoitettuun määränpäähänsä ajallaan. ICMP-protokollan tehtävänä on siis välittää tiedonsiirtotapahtumiin liittyviä virhe-, ohjaus- ja testisanomia. ICMP-sanomia seuraamalla saadaan verkonvalvonnan kannalta tietoa verkon sekä sen laitteiden tilasta. ICMP-protokollaa voidaan myös hyödyntää verkon vikojen diagnosointiin käyttäen sen ping- ja traceroute-toimintoja. [4]

ICMP-protokollan ping-toiminto on yleisimmin käytetty menetelmä selvittämään, onko kohdelaite tavoitettavissa. Se hyödyntää toiminnassaan ”Echo” ja ”Echo Reply” -sanomia. [3] Jos kohdelaite on saavutettavissa, ping-toiminto ilmoittaa kuinka kauan sanomilla kesti saavuttaa kohdelaite ja palata takaisin lähteelle. Ping-toiminnolla saa siis myös tietoa verkon vasteajasta. Traceroute-toiminto tarjoaa mahdollisuuden tarkempaan verkon diagnosointiin. Sen avulla voidaan selvittää kahden laitteen välinen reitti verkossa hyödyntäen ICMP-protokollan virhesanomia. [4] Selvitetystä reitistä saadaan tietoa verkkoa rajoittavista tekijöistä, kuten vikaantuneista laitteista [3].

3.3.4 Remote Network Monitoring, RMON

Suurissa verkoissa, joissa on paljon laitteita, SNMP-protokollan pyyntö-vaste-parit voivat kuormittaa verkkoa sekä verkonvalvontaohjelmistoa huomattavasti. Etenkin verkkosegmentti, jossa verkonvalvontaohjelmisto sijaitsee voi kuormittua pahiten, koska kaikki verkonvalvontaliikenne kulkee sen kautta. Verkonvalvontaliikennettä aiheutuu erityisesti verkon vikatilanteen ilmetessä, jolloin agentit lähettävät ansaviestejä. RMON (Remote network Monitoring) -lyhenteellä tunnettavan verkon etämonitoroinnin avulla voidaan vähentää sekä jakaa verkonvalvonnasta aiheutuvaa kuormitusta. [14]

Verkon etämonitorointi perustuu verkon jakamiseen eri segmentteihin. Yleensä reitittimeen tai kytkimeen sijoitettava laite- tai ohjelmistopohjainen välityspalvelin valvoo ja analysoi verkkosegmenttiä paikallisesti. Välityspalvelin välittää tarpeellisen informaation verkonvalvontaohjelmistolle hyödyntäen SNMP-protokollan viestejä. Täten verkonvalvontaohjelmiston ei tarvitse lähettää kyselyitä kaikille verkon laitteille, vaan se voi olla yhteydessä vain välityspalvelimiin. Erityisesti käytössä ovat ”Trap” ja ”Inform” -viestit, joita välityspalvelin lähettää havaitessaan tavallisesta poikkeavaa toimintaa segmentillään. [14]

Verkon etämonitorointi tarjoaa verkonvalvonnalle monia etuja. Tärkeimpänä tietenkin, että se vähentää ja jakaa verkonvalvonnasta aiheutuvaa kuormitusta verkonvalvontaohjelmiston segmentistä tasaisesti muualle verkkoon. Lisäksi se parantaa verkon luotettavuutta, koska verkonvalvontaliikenteen ei tarvitse kulkea niin pitkää matkaa kerrallaan verkossa välityspalvelimien ansiosta. Yksittäisiä segmenttejä voidaan myös valvoa tarkemmin ja jatkuvammin pienemmän kokonsa ansiosta. Tämä mahdollistaa paremman tilastoinnin sekä vianilmaisun. [14]

3.3.5 NetFlow

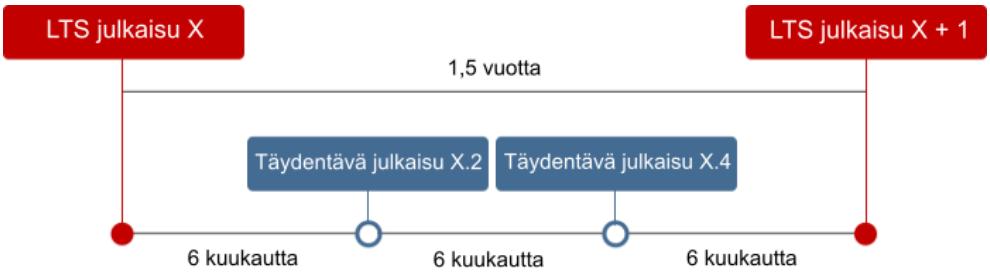
NetFlow on virtaustekniikoihin pohjautuva verkonvalvontaprotokolla, jota käytetään keräämään suuria määriä dataa verkkoliikenteestä. Kerättyä dataa analysoimalla saadaan tietoa verkon käytöstä ja suorituskyvystä. Sen avulla voidaan selvittää esimerkiksi, miten verkon käyttö jakautuu eri laitteiden kesken, mistä verkon liikenne koostuu tai onko verkossa pullonkauloja. Teoriassa vastaavan datan voisi kerätä verkosta käyttäen SNMP-protokollaa, mutta etenkin suurissa verkoissa ongelmaksi ilmenee informaation laajuus ja lukemattomista kyselyistä aiheutuva verkon tehoton käyttö. [13]

Toisin kuin SNMP-protokolla, NetFlow ei lähetä kyselyitä verkkoon, vaan valvoo ja kerää tietoa verkossa jo valmiina olevasta datasta, joka ”virtaa” verkkolaitteiden läpi. Virtauk-

sella (flow) tarkoitetaan paketteja, jotka kuuluvat samaan tiedonsiirtotapahtumaan. Kaikilla virtaukseen kuuluvilla paketeilla on siis samat tunnistetiedot, ja virtaus voidaan tunnistaa yksiselitteisesti. Näitä tietoja ovat lähde- ja kohdeosoite, porttinumerot, käytetty kuljetuskerroksen protokolla, palvelunlaatu ja liitäntä. Virtauksesta kerätystä datasta koostetaan erillinen virtaustietue (flow record). Se sisältää muun muassa virtauksen tunnistetiedot, alku- ja loppuajan sekä kuinka monta pakettia ja bittiä virtauksessa oli. Kun virtaustietue on saatu valmiiksi, se välitetään verkonvalvontaohjelmistolle käsiteltäväksi ja analysoitavaksi. [20]

4. ZABBIX

Zabbix on avoimeen lähdekoodiin perustuva yritystason verkonvalvontaohjelmisto. Se on julkaistu ja jaettu GPLv2 (General Public License version 2) -lisenssin mukaisesti, eli Zabbixin lähdekoodi on vapaasti jaettavissa ja yleisön saatavilla [21]. Zabbixin kehitti Alexei Vladishev, joka on nykyisin ohjelmistoa ylläpitävän Zabbix SIA/LLC -yrityksen perustaja sekä toimitusjohtaja [22]. Vaikka Zabbix itsessään on ilmainen, Zabbix SIA/LLC tarjoaa erilaisia koulutuksia sekä teknistä tukea ohjelmiston käyttäjille [23]. Ensimmäinen versio Zabbixista julkaistiin vuonna 2001. Siitä lähtien Zabbixista on julkaistu puolentoista vuoden välein LTS (Long Term Support) -versio, johon tarjotaan viiden vuoden tuki. LTS-versioihin tulee puolen vuoden välein kaksi täydentävää päivitystä. Uusin versiojulkaisu on numeroltaan 6.2. [24] Kuvassa 12 on esitettynä Zabbixin julkaisukierto ja versionumeroinnin perusta.



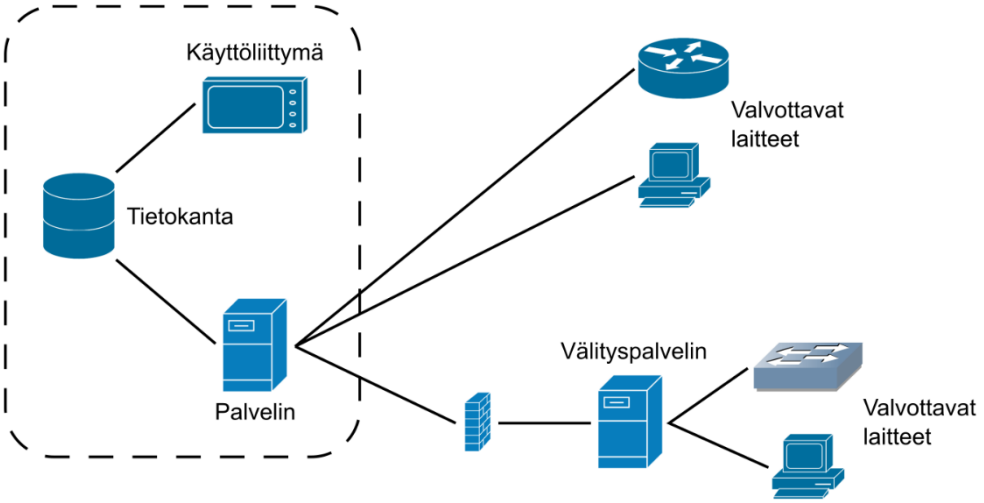
Kuva 12. *Zabbixin julkaisukierto ja versionumerointi, muokattu lähteestä [24].*

4.1 Zabbixin arkkitehtuuri

Zabbix voidaan määritellä hajautetuksi verkonvalvontaohjelmistoksi, jolla on keskitetty selainpohjainen käyttöliittymä [25]. Se koostuu viidestä eri pääkomponentista, jotka ovat palvelin, tietokanta, käyttöliittymä, välityspalvelin (proxy) ja agentti [21]. Zabbixin arkkitehtuurinen rakenne on joustava, ja se on laajasti muokattavissa kullekin järjestelmälle sopivaksi erilaisilla konfiguraatioilla [25].

Zabbixin keskeisin elementti on palvelin [21]. Se suorittaa tietojen keräämisen verkosta eri menetelmin hyödyntäen esimerkiksi SNMP- ja ICMP-protokollia tai Zabbix agenttia, joka asennetaan valvottavalle laitteelle [25]. Kerätyn datan perusteella palvelin suorittaa halutut toiminnot, jotka käyttäjä on määritellyt käyttöliittymässä. Kaikki verkosta kerätyt ja analysoidut tiedot tallennetaan Zabbixin tietokantaan, johon sekä palvelin että käyttöliittymä ovat yhteydessä. Tietokanta sisältää myös ohjelmiston konfiguraatiotiedot [21]. Palvelin, käyttöliittymä ja tietokanta sijaitsevat lähtökohtaisesti samalla laitteella, esimerkiksi virtuaalikoneella. Jos Zabbixilla valvotaan erityisen suurta verkkoa, voidaan nämä

kolme elementtiä hajauttaa jokainen omalle laitteelle, jolloin kuormitus tasaantuu [26]. Kuten verkonvalvonnan tekniikoiden käsittelyssä tuli ilmi, välityspalvelimia voidaan hyödyntää jakamaan palvelimen kuormitusta. Välityspalvelimien käyttö mahdollista myös skaalautumisen. Tällöin välityspalvelin kerää verkosta dataa palvelimen puolesta ja välittää tarvittavat tiedot eteenpäin palvelimelle. Välityspalvelin on myös hyödyllinen palomuurien yhteydessä, koska tällöin palomuurisäännöt tarvitsee määrittää vain palvelimen ja välityspalvelimen välille. [21] Kuva 13 havainnollistaa Zabbixin arkkitehtuuria.



Kuva 13. *Zabbixin arkkitehtuuri, muokattu lähteestä [26].*

4.2 Zabbixin ominaisuudet

Zabbix tarjoaa lukuisia työkaluja ja menetelmiä muun muassa verkon, laitteiden ja ohjelmistojen parametrien sekä tilan valvontaan [27]. Zabbix kerää verkosta dataa kysely- sekä ansaviestien avulla. Kerättyä dataa voidaan visualisoida eri tavoin ja verkossa ilmenevistä vioista on mahdollista määrittää hälytyksiä. Hälytykset ilmenevät Zabbixin selainpohjaisessa käyttöliittymässä ja niitä voidaan lähettää myös esimerkiksi verkon käyttö- ja kunnossapitohenkilöille. Zabbixin selainpohjainen käyttöliittymä mahdollistaa ohjelmiston käytön mistä tahansa paikasta käsin. Näin Zabbixia voidaan hyödyntää nopeaan vikojen paikallistamiseen ja korjaamiseen varmistaen järjestelmän vakaan toiminnan. [21]

Zabbix sisältää erilaisia menetelmiä helpottamaan sen käyttöönottoa ja datan keräämistä. Ohjelmistolla on mahdollista skannata tietyin väliajoin verkkoa halutulla IP-alueella ja löytää verkosta valvottavat laitteet. Tämä onnistuu hyödyntämällä eri protokollilta sekä agenteilta saatuja tietoja. Uusi verkkoon liitetty laite, jossa on Zabbix agentti, voi myös itse lähettää palvelimelle rekisteröimispyynnön, jotta sitä voidaan valvoa. Koska

monet valvottavat laitteet, kuten reitittimet ja kytkimet, ovat identtisiä tai melko samanlaisia, on niillä myös samanlaiset valvottavat tiedot. Valvottaville laitteille voidaankin siis asettaa valmiiksi määriteltyjä malleja. Se määrittelee, mitä tietoja kustakin laitteesta valvotaan ja miten niitä käsitellään. Mallit helpottavat valvonnan käyttöönottoa ja ylläpitoa. Zabbix pystyy myös mukauttamaan valvottavia kohteita vastaamaan valvottavan laitteen sen hetkistä tilaa. Se esimerkiksi voi tunnistaa reitittimen aktiiviset portit ja valvoa vain niitä. [21]

Verkonvalvonnassa voidaan hyödyntää Zabbix agentteja ja SNMP agentteja. Agentin valintaan vaikuttaa kuinka yksityiskohtaisia tietoja halutaan kerätä sekä millainen laite on kyseessä. [21] Zabbix agentti on C-kielellä ohjelmoitu ulkoinen ohjelmisto, joka asennetaan valvottavalle laitteelle. Se kerää tietoja valvottavalta laitteelta ja välittää havainnot palvelimelle. Zabbix agentin etuja ovat sen tehokkuus ja monipuolisuus. Sillä voidaan valvoa useita eri laitteita ja alustoja. Sen pieni resurssienkulutus mahdollistaa vaivattoman ja laajan tietojen keräämisen verkosta ja verkkoon liitetyistä laitteista. [28] Laitteita, joille ei ole mielekästä tai mahdollista asentaa Zabbix agenttia, voidaan valvoa käyttäen jo valmiiksi asennettua SNMP agenttia. Tällaisia laitteita ovat muun muassa reitittimet ja kytkimet. [21] SNMP-protokollan toimintaa ja ominaisuuksia on käsitelty kappaleessa 3.3.1. Kumpikin agentti tukee aktiivisia tarkastuksia eli kyselyviestejä sekä passiivisia tarkastuksia eli ansaviestejä. Kyselyitä voidaan lähettää säännöllisesti tietyin aikavälein tai kellonajoin. [17][21] Zabbixilla on myös mahdollista suorittaa yksinkertaisia tarkastuksia ilman agenttien käyttämistä. Näillä yksinkertaisilla tarkastuksilla voidaan esimerkiksi selvittää, onko verkkopalvelut saatavilla hyödyntäen TCP-protokollan tarjoamia toimintoja tai selvittää onko laitteita tavoitettavissa käyttäen ICMP-protokollan Ping-toimintoa. [29]

Triggerit ovat loogisia lausekkeita, jotka arvioivat kerättyä dataa ja ylläpitävät tietoa järjestelmän senhetkisestä tilasta. Triggereiden avulla voidaan määritellä hälytyksille kynnysarvoja. Kun kynnysarvo ylitetään, triggeri laukeaa antaen hälytyksen tai muuttaen tilan ongelmaksi. Triggerit ovat olennainen osa vikojen havainnointia reaaliaikaisesti. [21] Vikoja on mahdollista havainnoida ennakoivien triggereiden ja koneoppimisen avulla jo ennen kuin vikoja ilmenee. Tämä on mahdollista analysoimalla historiadataa ja tekemällä laskelmia erilaisten algoritmien avulla. Tällöin vikatilanteisiin, kuten laitteen muistin loppumiseen tai verkon ruuhkautumiseen, on mahdollista reagoida ennakoivasti, ennen kuin vikoja sekä ongelmia ilmenee. [21][30] Vikatilanteissa verkon käyttö- ja kunnossapitohenkilöille on mahdollista lähettää ilmoituksia esimerkiksi sähköpostin, kännykän tai erilaisten kommunikointipalveluiden, kuten Teamsin, välityksellä. Tällöin käyttöliittymää

ei tarvitse jatkuvasti seurata, vaan oikeat henkilöt saavat joustavasti tarvittavat ilmoitukset. [21]

Koska Zabbix käsittelee paljon dataa ja valvottava verkko sisältää paljon laitteita, ei ole tarkoituksenmukaista seurata sitä vain numeroin ja tunnuksin. Zabbix tarjoaa menetelmät datan visualisointiin eri tavoin, mikä onkin tärkeä ominaisuus verkonvalvonnassa. Trendit mahdollistavat tehokkaan tavan tarkkailla dataa tietyllä aikavälillä, etsiä ongelmia ja saada selville, milloin jokin vikatilanne on alkanut. Yksinkertaiset trendit mahdollistavat yksittäisen tiedon seuraamisen helposti, kun taas ad-hoc trendillä voi vertailla useampaa tietoa keskenään. Trendejä sekä kaavioita voi kustomoida monipuolisesti vastaamaan haluttuja tarpeita. Kustomoitavat kaaviot ja trendit jäävät aina talteen, jolloin niitä on helppo tutkia myös myöhemmin. [21] Verkkoon liitetyt laitteet voidaan esittää visuaalisesti kustomoitavilla reaaliaikaisilla topologiakartoilla. Reaaliaikaisuus ilmenee siten, että esimerkiksi verkossa esiintyvät vikatilanteet voidaan asettaa näkymään topologiakartassa ja sen avulla vika voidaan paikantaa helposti. Topologiakarttoja on mahdollista rakentaa hierarkkisesti, ja niiden välille voidaan luoda yhteyksiä. [31]

Zabbixin käyttöliittymässä tärkeässä roolissa on työpöytä (Dashboard). Se rakentuu erilaisista widgeteistä, jotka ovat suunniteltu näyttämään haluttua informaatiota. Widgetit voivat sisältää muun muassa koosteita, listauksia, topologiakarttoja, trendejä, kaavioita tai aika- ja paikkatietoja. Työpöytä on siis täysin kustomoitavissa erilaisia tarpeita ajatellen, ja niitä voi olla määriteltynä useita. Työpöydän tavoitteena on ilmaista verkon tila ja sen olennaiset tiedot helposti yhdellä näytöllä. [21] Kuvassa 14 on esitettynä esimerkkikuva Zabbixin työpöydästä.

Kuva 14. *Zabbixin työpöytä [32].*

Zabbix sisältää erilaisia menetelmiä, joilla varmistetaan tietoturva ja verkonvalvonnan luotettavuus. Kaikki liikenne Zabbixin elementtien välillä on salattu käyttäen TLS (Transport Layer Security) -protokollan versiota 1.2 ja 1.3. Zabbix tukee myös sertifikaatteihin ja jaettuun avaimeen perustuvia salausmenetelmiä. Haluttua salaustekniikkaa on mahdollista muuttaa laitetasolla. Zabbix sisältää neljä erilaista käyttäjäroolia, jotka ovat vierailija (guest), käyttäjä (user), järjestelmävalvoja (admin) ja super-järjestelmävalvoja (super-admin). Eri käyttäjäryhmille voidaan asettaa erilaisia käyttöoikeuksia koskien datan käsittelyä ja Zabbixin toimintojen käyttöä työpöydällä. Jokaisesta Zabbixissa tehdystä muutoksesta jää jälki järjestelmän muistiin. Kaikkien Zabbixin käyttäjän tulee olla autentikoituja, sekä jokainen käyttäjä kirjautuu ohjelmistoon omilla tunnuksillaan. [21]

5. UPM KYMIN SELLUTEHDAS TOIMINTAYMPÄRISTÖNÄ

UPM-Kymmene Oyj (lyh. UPM) on eräs maailman johtavista metsäteollisuusyrityksistä. UPM:n historia ulottuu suomalaisen metsäteollisuuden alkuajoille, kun yhtiön ensimmäiset tuotantolaitokset aloittivat toimintansa 1870-luvun alussa. Nykyinen UPM-Kymmene Oyj perustettiin vuonna 1995 Kymmene Oy:n ja Repola Oy:n fuusioituessa. Vuosien saatossa useat merkittävät suomalaiset metsätalousyritykset, kuten Yhtyneet Paperitehtaat, Kymi, Kaukas sekä Kajaani, ovat sulautuneet nykyiseen UPM-konserniin. [33]

UPM jakautuu kuuteen eri liiketoiminta-alueeseen, jotka ovat Fibres, Energy, Raflatac, Specialty Papers, Communication Papers ja Plywood. Tuotteinaan UPM:n tehtaat tuottavat muun muassa sellua, sahatavaraa, energiaa, paperia, puutuotteita ja erilaisia biotuotteita. Vuonna 2021 UPM:n liikevaihto oli noin 9,8 miljardia euroa. Tällä hetkellä UPM työllistää maailmanlaajuisesti noin 17 000 työntekijää, ja yhtiöllä 54 on tuotantolaitosta 12 eri maassa. [34] UPM Fibres sisältää sahatavaran ja sellun tuotannon hyödyntäen yhteistä puuraaka-aineen hankintaketjua. UPM:llä on neljä sellutehdasta, joista kolme on Suomessa ja yksi Uruguayssa, johon on myös valmistumassa viides sellutehdas. Sellutehtaissa tuotetaan havu-, koivu-, ja eukalyptussellua eri käyttökohteisiin. Sellutehtaiden vuosittainen tuotantokapasiteetti on noin 3,7 miljoonaa tonnia. [35]

Kouvolassa Kymijoen rannalla sijaitseva UPM Kymin tehdasintegraatti tuottaa sellua, paperia sekä bioenergiaa [36]. Kymin tehtaiden toiminta sai alkunsa 150 vuotta sitten vuonna 1872, kun alueelle perustettiin Kymin ja Kuusankosken paperitehtaat sekä puuhiomo. Nykyisellä sijainnillaan Kuusaanniemessä tehdasintegraatti on toiminut vuodesta 1964. [37] Kuusaanniemen tehdasalueella toimii UPM Kymin sellutehdas, UPM Communication Papersin Kymin paperitehdas, Kymin Voima Oy:n biovoimalaitos sekä Schaefer Kalk Finland Oy:n karbonaattilaitos. Tehtaiden vuotuinen puunkäyttö on noin 4 miljoonaa kuutiota, ja alueella työskentelee noin 720 UPM:n työntekijää tehtaiden sekä eri tukitoimintojen palveluksessa. [36] Kuvassa 15 on Kymin tehdasintegraatti.

Kuva 15. *UPM Kymin tehdasintegraatti, etualalla sellutehdas [39].*

Kymin sellutehdas on yksi Suomen moderneimmista sellutehtaista viimeaikaisten investointien ansiosta. Tehtaalla tuotetaan sellua kahdella tuotantolinjalla. Se on tuotannollisesti Suomen suurin sellutehdas tuottaen vuosittain noin 870 000 tonnia valkaistua havu- ja koivusellua. Sellutehdas koostuu kuorimosta, keittimet sekä valkaisulaitoksen sisältävästä kuitulinjasta, kuivauskoneesta, talteenottolaitoksesta sekä happilaitoksesta. Puuraaka-aineina ovat koivu, kuusi ja mänty. Selluntuotannon sivutuotteena syntyvää tärpättiä ja mäntyöljyä hyödynnetään biotalouden tuotteisiin. Sellutehdas työllistää noin 250 henkilöä. [38]

5.1 Verkonvalvonnan nykytila

UPM Kymin sellutehtaan (myöh. tehdas, sellutehdas) sähkö- ja automaatiokunnossapidon vastuulla on kaikkien elektronisten ja sähköisten laitteiden kunnossapito koko automaatiojärjestelmän tasolla. Osaston vastuulle kuuluu myös siis automaatioverkon ylläpito. Toimiva automaatiolaitteisto ja niistä saatavat tarvittavat prosessiarvot ovat ehtona tehtaan prosessin tehokkaalle hallinnalle. Tällöin tuotanto on korkeatasoista ja hyvänlaatuisten tuotteiden valmistus onnistuu turvallisesti sekä kustannustehokkaasti. [40]

Nykyinen kehityssuunta tietotekniikan kehittymisen sekä automaatiojärjestelmien verkkoon siirtymisen parissa on tuonut muutoksia sähkö- ja automaatiokunnossapidon toimintaan. Kun prosessia ohjataan valvomosta ja operointiasemilta automaatioverkkoon liitettyjen mitta- sekä säätölaitteiden varassa, niiden toimintavarmuus ja kunnossapidon tärkeys korostuu entisestään. [41] Tämä luo myös tarpeen automaatioverkkojen valvonnalle ja ylläpidolle, jotta se toimii vaaditulla palvelunlaadulla ja mahdolliset viat voidaan havaita sekä korjata.

Kuten luvussa 3 tuli ilmi, verkonhallinta ja täten myös verkonvalvonta koetaan usein ylimääräiseksi toiminnoksi tietoliikennetekniikassa, eikä sen hyötyjä ymmärretä täysin. Sama ilmiö on havaittavissa myös sellutehtaalla. Sähkö- ja automaatiokunnossapidon vastuulla olevassa automaatioverkon ylläpidossa ei ole käytössä yhtenäistä toimintatapaa verkonvalvonnalle. Myöskään erityisesti verkonvalvontaan tarkoitettua ohjelmistoa ei ole käytössä. Automaatioverkkoon liitetyt laitteet ja niiden määrittelytiedot, kuten IP-osoite, fyysinen sijainti ja asennetut sovellukset, ovat kirjattuna SNOW (UPM ServiceNow) -tietokannassa. SNOW sisältää myös tietoja muun muassa laitteiden suojauksesta ja tilasta, eli onko laite verkossa saatavilla vai ei. Koska kyseessä on vain tietokanta, sen tiedot päivittyvät päivien tasolla, eikä sitä voida tehokkaasti hyödyntää verkonvalvonnan näkökulmasta. FCAPS-viitemallin mukaan SNOW käsittelee kokoonpanon valvontaa. Muut viitemallin osa-alueet jäävätkin huomioimatta. Aktiivista verkonvalvontaa ei siis toteuteta. Täten verkossa ilmeneviin ongelmatilanteisiin, kuten verkkokuormituksiin tai laitevikoihin, ei voida reagoida tarvittavalla tasolla. Yleensä ongelmatilanteet havaitaan verkon käyttäjien toimesta, ja vasta silloin vianselvityksen eteen voidaan tehdä toimenpiteitä. Kyseessä on siis reaktiivista toimintaa. Tällaiset ongelmatilanteet vähentävät käyttäjien luottamusta automaatioverkkojen toimintaan.

5.2 Vaatimukset ja tavoitteet verkonvalvonnalle

Sellutehtaan tavoitetilana verkonvalvonnassa on saada toimintaan yksi yhtenäinen järjestelmä, jolla pystytään aktiivisesti toteuttamaan verkonvalvonnan toimenpiteitä osana päivittäistä automaatioverkon ylläpitoa. [42] Tällöin verkossa esiintyviä ongelmia kyetään ehkäisemään ennakoivasti, jopa ennen kuin ne ilmenevät verkon käyttäjille. Parempi tietoisuus verkon tilasta ja mahdollisuus tehokkaampaan verkkosuunnitteluun takaavat varmemman automaatioverkon palvelunlaadun, jota vaaditaan kriittisen tuotantoprosessin ylläpitämiseksi. Zabbix määräytyi tämän työn käsittelyyn sellutehtaan automaatioverkon toimittajan Valmet Automation Oy:n suosituksesta.

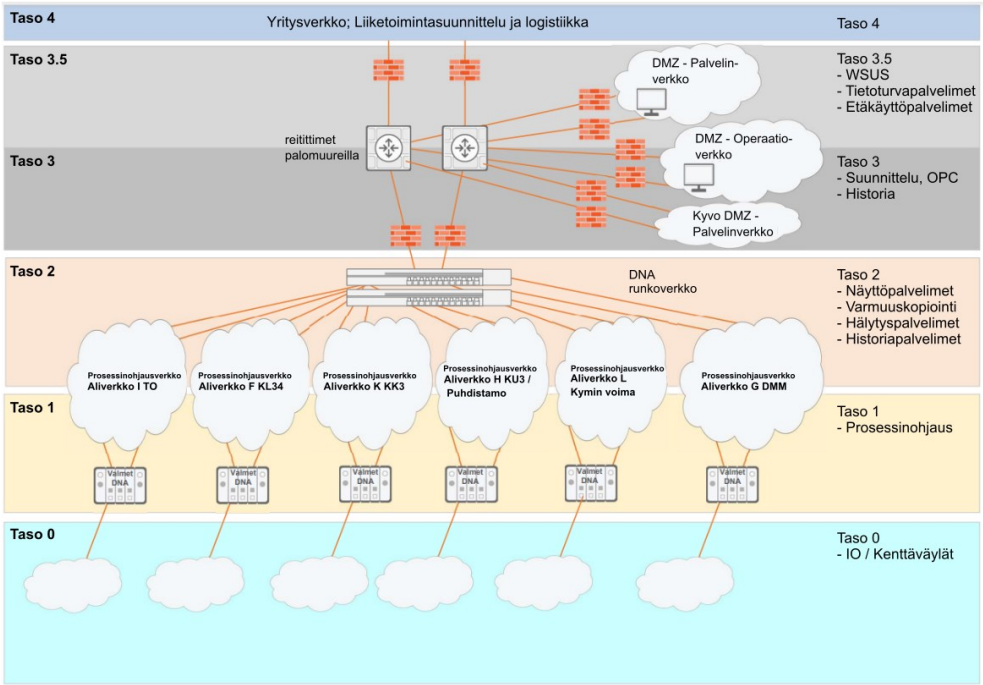
Ehdottomasti tärkeimpänä vaatimuksena tehtaalla verkonvalvontaohjelmistolle on helppokäyttöisyys ja saavutettavuus. Verkonvalvontaohjelmiston täytyy sisältää yksinkertaisen käyttöliittymän, jossa on helposti saatavilla automaatioverkon ylläpidon kannalta tärkeimmät tiedot ja toiminnot. [42] Zabbixin selainpohjainen käyttöliittymä ja täysin kustomoitavissa olevat työpöydät vastaavat tähän vaatimukseen. Työpöydille saa määriteltyä sovellusten avulla olennaiset tiedot, kuten trendit, topologiakartat ja vikailmoitukset. Näiden tietojen pohjalta on mahdollista toteuttaa toimenpiteitä. Selainpohjaisuus mahdollistaa Zabbixin käytön prosessitiloissa kunnossapitohenkilöstön toimesta, kuin myös toimistotiloissa verkon ylläpitäjien toimesta. [21] Zabbix on yleisesti ottaen helppo ja kevyt

ylläpitää verrattuna muihin kilpaileviin verkonvalvontaohjelmistoihin. Sen helppokäyttöiseen ja visuaaliseen käyttöliittymään on panostettu, jotta sen käyttäminen onnistuu verkon ylläpitäjiltä omatoimisesti [43].

Oleellisimmat toiminnot automaatioverkon ylläpidon kannalta, ovat vikojen havainnointi ja selvitys sekä datan visualisointi. Reaaliaikaiset hälytykset esimerkiksi laitevioista tai verkon kuormituksesta mahdollistavat nopean reagoinnin ongelmatilanteiden sattuessa, mitä tällä hetkellä ei ole voitu toteuttaa. [42] Kuten jo luvussa 4 tuli ilmi, Zabbixista löytyy useampikin menetelmä vikojen havainnointiin. Vikojen havainnoinnissa tärkeässä roolissa olevat triggereiden kynnysarvot voidaan määrittää kullekin seuratulle kohteelle yksilöllisesti. Esimerkiksi kytkimen kuormitusta valvottaessa ensimmäinen varoitus voidaan antaa 80 % kohdalla täydestä kapasiteetista Zabbixin käyttöliittymässä. Sen sijaan kriittinen hälytys 90 % kohdalla voidaan lähettää verkon ylläpitäjille vaikkapa sähköpostitse, jotta hälytys menee varmasti perille. Ennakoivat triggerit ja koneoppimiseen perustuvat menetelmät vikatilanteiden ennakoinnissa nousevat myös tärkeään arvoon. Tällöin optimaalisessa tilanteessa epänormaali toiminta voidaan havaita jo ennen triggereitä ja vikatilanteiden ilmenemistä käyttäjälle. Kerätyn datan visualisointi auttaa myös huomattavasti verkon ylläpitäjän kykyä seurata verkon tilaa. Trendidataa visualisointia ja ennakointia varten säilytetään järjestelmässä lähtökohtaisesti yksi vuosi ja kaikkea ohjelmiston sisältämää dataa neljä kuukautta [43]. Visualisoinnissa reaaliaikaiset topologiakartat automaatioverkon rakenteesta mahdollistavat tehokkaan vikojen paikantamisen ja rajaamisen. Tällä hetkellä automaatioverkon topologiasta löytyy yksinkertaisia kuvia ja piirroksia, joten Zabbixin topologiakartta on jo itsessään suuri edistysaskel verkon tilan ja rakenteen ylläpidossa [42].

Eduksi verkonvalvontaohjelmistolle katsotaan sen käyttöönoton helppous sekä yhteensopivuus automaatioverkkoon [42]. Vaikka Zabbixin käyttöliittymä on helppokäyttöinen ja ohjelmisto on vaivaton ylläpitää, voi sen käyttöönotto kuitenkin olla työlästä. Syitä tähän ovat esimerkiksi Zabbixin monipuoliset ominaisuudet sekä sellutehtaan automaatioverkon koko. [43] Tehtaan automaatioverkon rakenne mukailee selkeästi tyypillisiä automaatioverkon piirteitä sekä luvussa 3 esitettyä esimerkkikuvaa. Laajuudeltaan kyseinen verkko voidaan luokitella kampusverkoksi. Sellutehtaan automaatioverkko koostuu kuudesta eri hiearkkiatasosta kenttälaiteista aina yritystason verkkoon. Rakenteessa esiintyy palomuurein eroteltuja kokonaisuuksia sisältäen eri tekniikoita ja toiminnallisuuksia. Automaatioverkko jakaantuu kuuteen eri aliverkkoon mukaillen alueella sijaitsevia laitoksia. Alijärjestelmien välisessä reitityksessä runkona on rengastopologia, jota käsiteltiin aliluvussa 2.3. [44] Kuvassa 16 on periaatteellinen kuva sellutehtaan automaa-

tioverkon rakenteesta. Vaikka Zabbix sisältää useita menetelmiä helpottamaan ohjelmiston käyttöönottoa, se vaatii silti paljon manuaalista määrittelyä. Zabbixin ohjelmointirajapinta API (Application Programming Interface) on hyödynnettävissä käyttöönoton määrittelytoimenpiteissä, ja sen avulla ohjelmistoa voi laajentaa scriptien avulla [43]. Käyttöönotossa Zabbixin yhteensopivuus verkossa käytettävien laitteiden kanssa on tärkeää, jotta kaikki toimii asianmukaisesti. Zabbix sisältääkin esimerkiksi Valmet Automation Oy:n valmiiksi määrittelemiä malleja tehtaan automaatioverkossa olevien ohjelmistojen ja laitteiden, kuten kytkimien, valvontaan [43]. Valmiiksi määritellyillä ja itse kustomoitavilla malleilla yhteensopivuus ja valvonnan monipuolisuus voidaan varmistaa.



Kuva 16. *Sellutehtaan automaatioverkon periaatteellinen rakenne, muokattu lähteestä [44].*

Verkkoon siirtyneet automaatiojärjestelmät ovat alttiita erilaisille uusille kyberuhkille. Automaatioverkon tietoturvaan onkin kiinnitettävä erityistä huomiota, koska se käsittelee kriittistä dataa. Täten Zabbixilta vaaditaan asianmukaiset ja nykyaikaiset tietoturvaominaisuudet, jotta se soveltuu sellutehtaan automaatioverkon valvontaan. [42] Verkonvalvontaohjelmisto on erityisen haavoittuvassa asemassa kyberuhkien näkökulmasta, koska se sisältää valvontadataa koko automaatioverkosta ja sen kautta on mahdollista päästä käsiksi verkon rakenteeseen ja laitteisiin. Zabbix sisältää luvussa 4 esiteltyjä tietoturvaominaisuuksia, kuten salauksen, autentikoinnin ja käyttöoikeusmäärittelyn. Tietoturvaa on myös mahdollista lisätä eri keinoin. Näihin lukeutuu muun muassa palvelimen fyysinen sijainti lukitussa paikassa, ajantasaiset versiopäivitykset, Zabbixin tarjoama tuki

ja verkon suojaus. [8] Zabbixin palvelin sijaitsee yleensä verkon demilitarisoidulla alueella. Sellutehtaan tapauksessa se sijoittuisi kuvan 16 tasoille 3 ja 3.5 erillisen palomuurin taakse. Olennaisena osana tietoturvaa on ohjelmiston ajantasainen päivitys ja uudet versiot, joissa on pitkäaikainen tuki. Ehdottomasti tärkeimpänä ominaisuutena Zabbixin tietoturvassa on käyttää sitä niin sanotussa ”Standalone” -tilassa, jolloin kaikki data käsitellään paikallisesti tehtaan verkon sisällä. [43] Täten verkonvalvontadataa ei kulje tehtaan automaatioverkon ulkopuolelle julkiseen verkkoon.

6. YHTEENVETO

Kandidaatintyön tavoitteena oli esitellä automaatioverkkojen ja UPM Kymin sellutehtaan asettamia vaatimuksia verkonvalvonnalle, sekä selvittää avoimen lähdekoodin verkonvalvontaohjelmisto Zabbixin soveltuvuutta sellutehtaan automaatioverkon valvontaan. Aiheena automaatioverkot sekä verkonvalvonta luovat laajan kokonaisuuden. Aiheen laajuuden ja kandidaatintyön näkökulman kannalta automaatioverkkojen osalta keskityttiin käsittelemään niiden ominaispiirteitä sekä yleisiä vaatimuksia syventymättä enempää automaatioverkkojen tekniikoihin. Verkonvalvonnassa käsiteltiin työn kannalta oleellisia nykypäivän verkonvalvontaohjelmistojen toimintaperiaatteita sekä tekniikoita, joista ehdottomasti yleisimpänä on SNMP. Mielenkiintoisia tutkimuskohteita ovat uudet verkonvalvonnassa hyödynnettävät tekniikat, kuten ohjelmisto-ohjatut verkot sekä koneoppiminen, jotka jäivät työn rajauksen ulkopuolelle. Lähteet käsiteltyihin aiheisiin liittyen ovat pitkälti englanniksi ja julkaisuajankohdiltaan 2000-luvun alusta tähän päivään. Haasteita lähteiden läpikäynnissä tuotti verkonvalvonnan (network monitoring) yläkäsite verkonhallinta (network management), jota käytetään monesti käsitellessä vain verkonvalvonnan osa-aluetta.

Automaatioverkkojen toimintaperiaatteiden ja ominaisuuksien pohjalta verkonvalvonnalle voidaan asettaa yleisiä vaatimuksia. Rakenteeltaan automaatioverkot ovat hierarkkisia ja sisältävät erilaisia tekniikoita, protokollia sekä laitteita. Täten verkonvalvontaohjelmistojen tulee skaalautua ja soveltua laajoille heterogeenisille verkoille. Koska automaatioverkot integroituvat kriittisiin prosesseihin, on verkonvalvonta toteutettava kuormittamatta verkkoa, jotta automaatioverkkojen luotettavuus- ja reaaliaikavaatimukset saavutetaan. Verkonvalvontaohjelmiston tietoturvaominaisuudet on myös oltava asianmukaisella tasolla, koska se käsittelee arkaluontoista dataa automaatioverkosta.

UPM Kymin sellutehtaan tavoitteena on ottaa käyttöön yksi yhtenäinen verkonvalvontajärjestelmä, jota hyödynnetään automaatioverkon ylläpidossa. Tärkeimpänä vaatimuksena verkonvalvontaohjelmistolle on sen helppokäyttöisyys ja saavutettavuus, jotta sitä voidaan hyödyntää tehokkaasti prosessi- sekä toimistotiloissa. Oleellisimpia toimintoja, joita verkonvalvontaohjelmistolta vaaditaan ovat datan visualisointi sekä vikojen havainnointi ja selvitys. Verkonvalvontaohjelmiston omat tietoturvaominaisuudet tulee olla pätevät, ja tehtaalla on varmistettava ohjelmiston tietoturvallinen käyttö. Eduksi verkonvalvontaohjelmistolle katsotaan myös sen käyttöönoton helppous sekä yhteensopivuus tehtaan automaatioverkkoon ja sen laitteisiin.

Kandidaatintyön perusteella voidaan todeta Zabbixin soveltuvan UPM Kymin sellutehtaan automaatioverkon valvontaan. Zabbix sisältää helppokäyttöisen selainpohjaisen käyttöliittymän. Zabbixin monipuoliset ominaisuudet muun muassa ennakoivasta vikojen havainnoinnista aina reaaliaikaisiin topologiakarttoihin vastaavat hyvin automaatioverkkojen sekä sellutehtaan vaatimuksiin. Zabbixin arkkitehtuuri mahdollistaa kattavat vaihtoehdot datan keräämiseen verkosta, sekä ohjelmiston laajennettavuus varmistaa yhteensopivuuden automaatioverkkoon. Monipuoliset ominaisuudet ja automaatioverkon laajuus voivat kuitenkin tehdä ohjelmiston käyttöönotosta haastavaa. Käyttöönoton yhteydessä Zabbixin välityspalvelimien sijoittamista on syytä harkita, jotta verkon kuormitusta voidaan jakaa ja palomuurisäännöt ovat yksinkertaisempi toteuttaa.

Verkonvalvonnan hyötyjä tehdasympäristössä ei voi liikaa korostaa, ja siksi Zabbixin käyttöönottoa UPM Kymin sellutehtaan automaatioverkon valvonnassa voidaan suositella. Verkonvalvonta helpottaa verkon ylläpitoa ja verkkosuunnittelua, jotka ovat avainasemassa automaatioverkolta vaaditun saatavuuden ja korkean palvelunlaadun saavuttamiseksi. Lisäksi resurssit voidaan kohdistaa verkon ongelmakohtiin, jolloin verkon ylläpitokustannukset pysyvät kurissa. Korkealla palvelunlaadulla toimiva automaatioverkko on ehtona sellutehtaan tuotantoprosessin tehokkaaseen ajamiseen, joka takaa korkeatasoisen ja hyvälaatuisen lopputuotteen valmistuksen turvallisesti ja kustannustehokkaasti.

LÄHTEET

[1] O.C. Ibe, Fundamentals of data communication networks, Wiley, 2007, p. 320.

[2] H. Jaakohuhta, Lähiverkot – Ethernet, 4. Uudistettu painos, IT Press, 2005, s. 380.

[3] J. Ding, Advances in network management, Customer resource management, 2016, p. 390.

[4] W. Goralski, The illustrated network, 2nd ed, Morgan Kaufmann, 2017, p 936.

[5] J. Cowley, Communications and networking, Springer, 2007, p 230.

[6] R. Zurawski, Industrial communication technology handbook, 2nd edition. CRC Press, 2017, p. 1756.

[7] K. Granlund, Tietoliikenne, 1. Painos, WSOYpro, 2007, s. 473.

[8] E.D. Knapp, J. Langill, Industrial network security, 2nd edition, Syngress, 2014, p. 460.

[9] J. Seppälä, M. Salmenperä, Towards dependable automation, In M. Lehto, P. Neittaanmäki (eds.), Cyber security: Analytics, technology and automation, Vol 78. Springer, 2015, pp. 229-249.

[10] B. Galloway, G.P. Hancke, Introduction to industrial control networks, In IEEE communications surveys & tutorials, Vol. 15, Iss. 2, IEEE, 2013, pp. 860-880.

[11] A. Kwiecien, K. Opielka, Management of industrial networks based on the FCAPS guidelines, Computer networks 19th international conference, Springer, 2012, pp. 280-288.

[12] M. Puska, Lähiverkkojen tekniikka, 2. Uudistettu painos, Suomen atk-kustannus, 2000, p. 348.

[13] A. Clemm, Network management fundamentals, Cisco press, 2006, p. 552.

[14] M. Subramanian, Network management, 2nd ed, Pearson education India, 2010, p. 724.

[15] G. Barbu, ITIL & FCAPS – network management fundamentals, the 7th international scientific conference “Defense resources management in the 21st century”, 2012, Proquest.

[16] D. Perdices, D. Muelas (eds.), Network performance monitoring with flexible models of multi-point passive measurements, 14th international conference on network and service management (CNSM), 2018, IEEE, pp. 1-9.

[17] W. Odom, CCNA routing and switching ICND2 200-105 official cert guide, Cisco Press, 2016, p. 992.

[18] E. Safrianti, S. Linna Oktaviana (eds.), Real time network device monitoring system with simple network management protocol (SNMP) model, 3rd international conference on research and academic community services (ICRACOS), 2021, IEEE, pp. 122-127.

[19] D. Mauro, K Schmidt, Essential SNMP, 2nd ed, O'Reilly media, 2005, p. 462.

[20] R. Hofstede, P. Celeda (eds.), Flow monitoring explained, from packet capture to data analysis with NetFlow and IPFIX, Vol 16. Iss. 4, IEEE, 2014, pp. 2037-2064.

[21] Zabbix 6.2 documentation, 2022, Saatavissa (viitattu 11.7.2022): https://www.zabbix.com/documentation/current/en/manual

[22] Zabbix About Zabbix LLC, Saatavissa (viitattu 9.7.2022): https://www.zabbix.com/about

[23] Zabbix Technical Support, Saatavissa (viitattu 9.7.2022): https://www.zabbix.com/support

[24] Zabbix Life Cycle & Release Policy, Saatavissa (viitattu 9.7.2022): https://www.zabbix.com/life_cycle_and_release_policy

[25] A.D. Vacche, Mastering Zabbix, 2nd edition, Packt Publishing, 2015, p. 412.

[26] R. Olupus, A.D. Vacche (eds.), Zabbix: enterprise network monitoring made easy, Packt publishing, 2017, p. 1327.

[27] Y.G. Shan, L. Chao (eds.), Research on monitoring of information equipment based on Zabbix for power supply company, 3rd international conference on applied machine learning, IEEE, 2021, pp. 487-491.

[28] Zabbix agent, Saatavissa (viitattu 11.7.2022): https://www.zabbix.com/zabbix_agent

[29] Zabbix agentless monitoring, Saatavissa (viitattu 11.7.2022): https://www.zabbix.com/agentless_monitoring

[30] Zabbix Machine Learning, Saatavissa (viitattu 12.7.2022): https://www.zabbix.com/features#baseline_monitoring

[31] Zabbix Infrastructure Maps, Saatavissa (viitattu 12.7.2022): https://www.zabbix.com/features#maps

[32] Zabbix Visualization, Saatavissa (viitattu 15.7.2022): https://www.zabbix.com/features#visualization

[33] UPM:n juuret ulottuvat 1870-luvulle, Saatavissa (viitattu 13.7.2022): https://www.upm.com/fi/tietoa-meista/yhtion-historia/

[34] UPM-Kymmene Oyj vuosikertomus 2021.

[35] UPM Selluliiketoiminta, Saatavissa (viitattu 13.7.2022): https://www.upm.com/fi/liiketoiminnot/upm-selluliiketoiminta/

[36] UPM Kymi, Saatavissa (viitattu 13.7.2022): https://www.upmpulp.com/fi/upm-kymi/

[37] UPM Kymi 150 vuotta kehityksen virrassa, Saatavissa (viitattu 13.7.2022): https://www.upmpulp.com/fi/upmkymi150/

[38] UPM sellu ja UPM Kymi esittely, UPM-Kymmene Oyj, 2022, Intranet.

[39] UPM Kymi Aerial photo, UPM-Kymmene Oyj, 2018, Intranet.

[40] UPM Maintence Strategy, UPM-Kymmene Oyj, 2014, sisäinen selvitys.

[41] L.D. Goettche, Maintenance of instruments & systems, 2nd ed, ISA – The instrumentation, systems, and automation society, 2005, p. 459.

[42] Matias Puranen, Kehitysinsinööri, UPM-Kymmene Oyj, 2022, haastattelu.

[43] Mikko Tikkala, Senior specialist, Cyber security services, Valmet automation Oy, 2022, haastattelu.

[44] UPM Kymin sellutehtaan automaatioverkon periaatteellinen topologia, UPM-Kymmene Oyj, 2022, sisäinen selvitys.