Riku Immonen

Teollisuusautomaatiojärjestelmien ja teollisen internetin kyberturvallisuus

pro gradu -tutkielma
4. maaliskuuta 2019

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA

Tekijä: Riku Immonen
Yhteystiedot: riku.j.immonen@jyu.fi
Puhelinnumero: +358445992254
Ohjaaja: Timo Hämäläinen
Työn nimi: Teollisuusautomaatiojärjestelmien ja teollisen internetin kyberturvallisuus
Title in English: Cyber security for the Industrial Control Systems and the Industrial Internet of Things
Työ: pro gradu -tutkielma
Sivumäärä: 75 + liitteet
Tiivistelmä: Tämä teollisuusautomaatiojärjestelmien ja teollisen internetin kyberturvallisuutta käsittelevä tutkielma kartoittaa teollisuusyrityksiin kohdistuvia kyberuhkia sekä toimintatapoja ja menetelmiä, joilla näistä uhkista voidaan selvitä ilman suurempia menetyksiä. Tutkielman yhtenä tavoitteena oli suunnnitella ja toteuttaa tilaajayritykselle kyberturvallinen IIoT-arkkitehtuuriratkaisu, jolla teollisuuslaitoksista pystyttäisiin siirtämään dataa pilveen turvallisesti, tehokkaasti ja luotettavasti. Sama IIoT-arkkitehtuuriratkaisu olisi lisäksi kyettävä implementoimaan kaikkiin yrityksen teollisuuslaitoksiin, jotta erilaisten IIoT-ratkaisujen määrä, mutta samalla myös kyberuhkat, pystyttäisiin minimoimaan ja pitämään hallinnassa.

Tutkielmassa kartoitettiin aluksi kirjallisuuskatsauksen menetelmin teollisuusautomaatiojärjestelmien kyberturvallisuuden erityispiirteitä, haavoittuvuuksia ja kyberturvallisuusratkaisuja. Tämän jälkeen suunniteltiin optimaalinen konstruktio eli IIoT-arkkitehtuuriratkaisu, joka pitää sisällään IIoT-sovellukset, -tiedonsiirtoverkot, tiedonsiirtoprotokollat ja tietoturvan, joilla pystytään siirtämään dataa tehokkaasti, mutta myös torjumaan kirjallisuuskatsauksessa selvitetyt kyberuhkat. Lopuksi IIoT-arkkitehtuuriratkaisu implementoitiin teollisuuslaitokselle ja pilveen, ja sen toimivuus testattiin käytännössä.

Tutkielman yhteenvetona voidaan todeta, että ratkaisu toimi tehdasympäristössä hyvin ja pienet datamäärät saatiin siirrettyä automaatiojärjestelmästä ja sensorinoodeista luotettavasti pilveen. Tulevaisuudessa on kuitenkin pystyttävä siirtämään ja käsittelemään dataa vieläkin enemmän, koska tekoälysovellukset vaativat koko ajan suurempia datamääriä. Kasvavat datamäärät voivatkin tulevaisuudessa tehdä IIoT-järjestelmän rajapinnoista pullonkauloja. IIoT-rajapintojen kuormitustestaus onkin tutkielmalle luonnollinen jatkotutkimusaihe.
Avainsanat: Teollisuusautomaatiojärjestelmät, teollinen internet, kyberturvallisuus

Abstract: This master's thesis on cyber security for the industrial control systems (ICS) and the industrial internet of things (IIoT) explores cyber threats against industrial companies, and practices and methods to overcome these cyber threats without major losses. One of the aims of the study was to design and implement a cybersecure IIoT architecture for the subscriber company that can be used to transfer data from ICS to the cloud safely and reliably. In addition, the same IIoT architecture should be able to be implemented in all industrial plants in order to minimize and manage the number of different IIoT solutions, but also threatening cyber threats.

The thesis first explored the special features of cyber security in automation systems, such as vulnerabilities and cyber security methods. This was followed by an optimal construction, the IIoT architecture, which includes IIoT applications, data transmission networks, data transfer protocols and data security to transfer data efficiently, but also to eliminate cyber threats identified in the literature review. Finally, the IIoT architecture was practically implemented at an industrial plant and the cloud where its functionality was tested.

In conclusion, the architecture worked well in the factory environment and with small data volumes. Data packets were reliably transferred from the automation system and sensor nodes to the cloud. However, in the future, it will be necessary to be able to transfer and process data even more, because artificial intelligence applications require continuous higher data volumes. In the future, IIoT interfaces can become bottlenecks in the system. Therefore, the load testing of the IIoT interfaces is a natural subject for further research.

Keywords: Industrial control systems, ICS, industrial internet of things, IIoT, cyber security

Sanasto

ABP	Activation By Personalization
AES	Advanced Encryption Standard
AMQP	Advanced Message Queuing Protocol
AS	Application Server
CA	Certificate Authority
CPU	Central Processing Unit
CSET	Cyber Security Evaluation Tool
CSIRT	Computer Security Incident Response Team
CMRI	Complex Malicious Response Injection
CRC	Cyclic Redundancy Code
CSRF	Cross-Site Request Forgery
CSS	Chirp Spread Spectrum
CVE	Common Vulnerabilities and Exposures
CVFR	Common Vulnerability Reporting Framework
CVSS	Common Vulnerability Scoring System
CSV	Comma-Separated Values
DCOM	Distributed Component Object Model
DCS	Distributed Control System
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNAT	Destination Network Address Translation
DoS	Denial of Services
ECB	Electronic CodeBook
FQDN	Fully Qualified Domain Names
FSK	Frequency Shift Keying
GRC	Governance, Risk and Compliance
HMI	Human Machine Interface

HIDS	Host-based Intrusion Detection System
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
I/O	Input/Output
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
IDS	Intrusion Detection Systems
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IT	Information Technology
JS	Join Server
JSON	JavaScript Object Notation
LAN	Local Area Network
LoRaWAN	Long Range Wide Area Network
LPWAN	Low Power Wide Area Network
LRC	Long Range Controller
LRR	Long Range Relay
MFCI	Malicious Function Code Injection
MPCI	Malicious Parameter Command Injection
MSCI	Malicious State Command Injection
MQTT	Message Queuing Telemetry Transport
NS	Network Server
NIDS	Network Intrusion Detection System
NMRI	Naive Malicious Response Injection
NPB	Network Packet Broker
NX	Non-eXecutable
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OS	Operating System
OT	Operational Technology

OTAA	Over The Air Activation
OWASP	Open Web Application Security Project
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PoC	Proof of Concept
QoS	Quality of Service
RAM	Random Access Memory
REST	REpresentational State Transfer
RDP	Remote Desktop Protocol
RSPAN	Remote Switched Port Analyzer
RSSI	Received Signal Strength Indicator
RTOS	Real Time Operating System
RTU	Remote Terminal Unit
SaaS	Software as a Service
SASL	Simple Authentication and Security Layer
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SNR	Signal to Noise Ratio
SOC	Security Operations Center
SNAT	Source Network Address Translation
SPAN	Switched Port Analyzer
SQL	Structured Query Language
SSH	Secure SHell
SSL	Secure Sockets Layer
TAP	Terminal Access Point
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAF	Web Application Firewall
XML	Extensible Markup Language
XSS	Cross-Site Scripting

Sisältö

1 Johdanto

Kriittisiin infrastruktuurikohteisiin kohdistuvien kyberhyökkäysten määrä on noussut viimeisen vuosikymmenen aikana niin paljon, että kyberturvallisuudesta on tullut keskeinen huolenaihe teollisuusautomaatio- ja valvontajärjestelmien käyttäjien ja myyjien keskuudessa. Näillä strategisilla kyberhyökkäyksillä pyritään häiritsemään teollista valmistustoimintaa monista eri syistä. Tällaisia syitä voivat olla esimerkiksi taloudelliset, poliittiset, kilpailulliset tai sosiaaliset syyt. Jopa ihmisten henkilökohtaiset kaunat, jotain tiettyä teollisuusyritystä kohtaan, ovat olleet riittävä syy tehdä kyberhyökkäys tätä toimijaa vastaan. On myös havaittu, että teollisuuden uudet automaatiojärjestelmät ovat yhä haavoittuvampia erilaisille hyökkäyksille. Syinä tähän voivat olla automaatiojärjestelmien etäkäytön yleistyminen, ja niissä käytettyjen komponenttien käyttäminen myös teollisuuden ulkopuolella, jolloin niiden haavoittuvuudetkin ovat jo ennätetty kartoittaa ja ne ovat yleisesti tiedossa. Toisaalta teollisuuslaitoksissa on myös liian vähän teollisiin IT-järjestelmiin erikoistuneita kyberturvallisuusasiantuntijoita, eivätkä teollisuuden loppukäyttäjät kykene aina itse tunnistamaan tietoverkkoihin liittyviä riskejä. [15] Onkin yleistä, että tietoturva on käytössä lähinnä toimistoverkkojen ja internetin yhteydessä, mutta tietoturva-asiantuntijat eivät useinkaan ymmärrä kaikkia teknisiä eroja liiketaloudellisten tietoturvakysymysten ja teollisuudessa käytettyjen automaatiojärjestelmien toiminnan välillä. Vastaavasti automaatioasinatuntijat tuntevat hyvin automaatiojärjestelmien ongelmat, mutta heidän tietoturvatietämys on usein vielä vähäistä. Teollisuusautomaatiojärjestelmät ovatkin yleensä vielä tietoturvan hallintajärjestelmien ulkopuolella, ja niiden kyberturvallisuus onkin jätetty yksinomaan automaatioasiantuntijoiden hoidettavaksi. Uhkien ja haavoittuvuuksien lisääntyessä olisikin alettava tarkastelemaan ja suojaamaan teollisuuden käyttämiä tietoverkkoja ja automaatiojärjestelmiä kyberhyökkäysten varalta. [5] Tämä on ajankohtaista etenkin nyt, kun uudet IoT-teknologiat ja -verkot ovat vasta saapumassa teollisuusympäristöön. Teollisuusyrityksien olisikin syytä tarkastella myös käyttöönotettavien teknologioiden määrää ja kokonaisuutta, jotta ne pystyisivät kontrolloimaan kyberriskejä myös tulevaisuudessa.

1.1 Kirjallisuuskatsaus

Tämän tutkielman kirjallisuuskatsausta varten haettiin kirjallisuutta eri hakupalveluista, kuten: Google Scholar, Finna ja ACM Digital Library -hakupalveluista. Pääasiallisina hakusanoina toimivat: industrial control systems cyber, industrial control systems security, ICS cyber, ICS security, automation systems cyber ja automation systems security. Lisäksi tietoa haetaan myös teollisuusautomaatiojärjestelmien alatyypeillä ja eri kenttäväylätyypeillä: DCS cyber, PLC cyber, RTU cyber, SCADA cyber, Modbus cyber, CAN cyber ja Profibus cyber. Näillä hakusanoilla saadaan syvennettyä tietämystä eräistä yleisimmistä automaatiojärjestelmistä. Hakusanojen lisäksi tutkielmassa tullaan käyttämään forward search -hakumenetelmää, jotta saadaan myös kaikkein tuorein tutkimus mukaan tutkielmaan. Lähteiden tärkeimpinä valintaperusteina toimivat niiden relevanttius ja uutuusarvo. Näiden kriteerien perusteella, sana "cyber" soveltuu kirjallisuuden hakuun paremmin kuin sana "security", koska "cyber" -sana ei esiinny kovin usein eteenkään vanhemmissa artikkeleissa, koska kyberturvallisuus on kuitenkin suhteellisen uusi tutkimusalue.

Kirjallisuutta löytyy aiheesta hyvin, tutkielman yhtenä päälähteenä käytän vuonna 2015 tehtyä Oxana Andreevan ym. tutkimusta [6], jossa on etsitty ja selvitetty teollisuusautomaatiojärjestelmien erityyppisiä haavoittuvuuksia ja peilattu niitä erityyppisiin automaatiokomponentteihin. Tässä tutkimuksessa on selvitetty automaatiokomponentteihin liittyviä kyberriskejä, joita on haettu yleisistä haavoittuvuustietokannoista. Lopputuloksena on saatu aikaan erittäin hyvin tiivistetty raportti, jonka tulokset ovat mielenkiintoisia, mutta myös jokseenkin ennalta-arvattavia. Tuloksista näkyy selvästi, että uusimmat ja nykyaikaisimmat teollisuusautomaatiokomponentit ovat myös kaikkein riskialttiimpia erilaisille kyberhyökkäyksille. Oxana Andreevan ym. tutkimuksessa käsiteltyihin eri haavoittuvuustyyppeihin löytyy tarkempia ja syvällisempiä tietoja Viestintäviraston [56] ja Massachusetts Institute of Technology:n (lyh. MIT) sivuilta [37]. Water information sharing and analysis center:in vuonna 2016 julkaistussa raportissa: "10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks" [57] kuvataan suoraan parhaita käytäntöjä, joita teollisuusautomaatiojärjestelmien kyberturvallisuuden parantamiseksi voidaan soveltaa. Tästä raportista löytyy erilaisia yleisiä suosituksia, kuten: tietoa automaatiojärjestelmien segmentoinnista, työntekijöiden tietoturvakoulutuksesta ja yrityksen tietoverkkokomponenttien inventoimisesta. Hakusanoilla löytyy myös National Institute of Standards and Technology:n, NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Secu-

rity, joka on luultavasti eniten viitattu artikkeli, tai oikeastaan ohjekirja, joka liittyy teollisuusautomaatiojärjestelmien kyberturvallisuuteen. Artikkelia [50] on viitattu Google Scholar:in mukaan yhteensä 775 kertaa. Ernst & Young:ilta löytyi laaja tutkimus [54], joka kantaa nimeä: "Path to cyber resilience: Sense, Resist and React", ja sen aineisto on kerätty vuosina 2016-2017. Tämä tutkimus on survey-tutkimus, jossa on kysytty yritysjohtajien mielipiteitä tietoturvaan liittyen. Aiheesta löytyy vanhempiakin tutkimuksia, kuten Joe Weissin kirjoittama artikkeli: "Assuring Industrial Control System Cyber Security" [58] vuodelta 2008.

1.2 Tutkimusaihe ja -kysymykset

Tämän tutkielman tutkimusaihe on teollisuusautomaatiojärjestelmien ja teollisen internetin (IIoT) kyberturvallisuus. Tutkimuskysymyksinä toimivat:

1. Mitkä kyberuhat ja haavoittuvuudet liittyvät teollisuuden käyttämiin automaatiojärjestelmiin ja -laitteisiin?
2. Mitkä ovat parhaat käytännöt teollisuuslaitosten hyvän kyberturvallisuustilanteen takaamiseksi?
3. Millä tiedonsiirto-, tietoturva- ja IoT-tekniikoilla saadaan rakennettua teollisuusyritykselle optimaalinen ja kyberturvallinen IIoT-arkkitehtuuri?

1.3 Tutkimusmetodi

Tässä tutkielmassa käytetään tutkimusmetodina konstruktiivista tutkimusotetta – suunnittelututkimusta. Työssä on tarkoituksena kehittää teollisuusyritykselle paras mahdollinen IIoT-arkkitehtuuriratkaisu, joka skaalautuu suuren konsernin tarpeisiin. Ratkaisun tulee sopia useisiin erilaisiin käyttötarkoituksiin, kuten prosessidatan ja langattoman IoT-datan siirtämiseen. Ratkaisun tulee täyttää myös tiukat tietoturvakriteerit, joiden pohjalle yrityksen kyberturvallisuus rakentuu. Tutkielmassa kartoitetaan aluksi automaatiojärjestelmiin kohdistuvat kyberriskit ja haavoittuvuudet, jonka jälkeen kerrotaan käytännöistä, joilla kyberriskejä voidaan pienentään ja poistaa. Lopuksi kerrotaan tilaajayritykselle suunnitellusta IIoT-arkkitehtuuriratkaisusta, joka on suunniteltu erityisesti luotettavuuden ja tietoturvan näkökulmista.

Konstruktiivisen tutkimusotteen tieteellinen kontribuutio on herättänyt ajan saatossa paljon keskustelu. Sen luonne onkin aina ollut hieman ristiriitainen, ja siitä on tutkimusmenetelmänä kirjoitettu lukuisia artikkeleita. Konstruktiivisen tutkimuksen arvostelijat kokevatkin usein ongelmalliseksi juuri sen, että ihmisen keksimät konstruktiot ovat usein liian kaukana luonnon itsensä muovaamista tieteen lainalaisuuksista, koska konstruktiot ovat todellakin vaan synnytetty jotakin käytännön tarvetta silmällä pitäen. Seuraavassa kappaleessa esitetty Kari Lukan ajatus tiivistää kuitenkin hyvin konstruktiivisen tutkimusotteen luonteen ja suhteen tutkimukseen.

> *"Konstruktiivinen tutkimusote on innovatiivisia konstruktioita tuottava metodologia, jolla pyritään ratkaisemaan reaalimaailman ongelmia ja tällä tavoin tuottamaan kontribuutioita sille tieteenalalle, jossa sitä sovelletaan. Tämän tutkimusotteen ydinkäsite, (uusi) konstruktio, on abstrakti käsite, jolla on suuri, itse asiassa loputon määrä mahdollisia toteutumia. Kaikki ihmisen luomat artefaktit, kuten mallit, diagrammit, suunnitelmat, organisaatiorakenteet, kaupalliset tuotteet ja tietojärjestelmämallit, ovat konstruktioita. Niille on tunnusomaista se, että ne eivät ole löydettyjä, vaan ne keksitään ja kehitetään. Kehittämällä konstruktion, joka poikkeaa kaikesta jo olemassa olevasta, luodaan jotain aivan uutta: uudenlaiset konstruktiot itsessään kehittävät uutta todellisuutta."* [30]

Konstruktiivisen tutkimuksen tieteellinen kontribuutio voidaan saavuttaa kahdella eri tavalla: 1. Kehitetyn uuden konstruktion toimivuuden todentaminen alkuperäisessä case-ympäristössä lisää tietämystä jo olemassa olevaan aiempaan kirjallisuuteen. 2. Käytetään jo olemassa olevaa tietämystä soveltavan empiirispainotteisen tutkimusprosessin syötteenä, ja analysoidaan taas tutkimusprosessin päätteeksi tämän alkuperäisen tietämyksen suhdetta saavutettuun kontribuutioon. [30] Seuraavassa luettelossa on lueteltu konstruktiivisen tutkimuksen vaiheet. [46]

1. Potentiaalisen ongelman etsiminen, jossa on myös tutkimusnäkökulmaa.
2. Perustavanlaatuisen ymmärryksen hankkiminen aiheesta.
3. Teoriaan perustuvan ratkaisun innovointi.
4. Ratkaisun implementointi ja testaus käytännössä.
5. Ratkaisun käyttömahdollisuuksien selvitys.
6. Teoreettisen yhteyden ja kontribuution esittäminen.

1.4 Automaatio- ja toimistotietojärjestelmien erot

Automaatio- ja toimistotietojärjestelmien IT-suunnittelu ja -toiminta eroavat toisistaan vieläkin monessa asiassa. Automaatiojärjestelmällä hallitaan fyysistä maailmaa ja toimistotietojärjestelmällä dataa. Järjestelmien riskit ja prioriteetit ovat erilaisia. Kun tietoturvallisuuden peruskäsitteitä ovat: luotettavuus, eheys ja saatavuus, niin automaatiojärjestelmien kanssa operoivat henkilöt perustavat ajatuksensa "turvallisuus ensin"ajattelulle. Tässä tapauksessa turvallisuudella tarkoitetaan nimenomaan automaatiojärjestelmien fyysistä turvallisuutta, koska niissä on paljon riskejä, jotka liittyvät ihmisten, omaisuuden ja ympäristön fyysiseen turvallisuuteen. Automaatio- ja toimistotietojärjestelmiä käyttävillä ja kehittävillä henkilöillä on myös omat organisaationsa, ja niissä työskentelevät henkilöt kehittävät ja tukevat vain omia järjestelmiään. [20]

Toimistotietojärjestelmien suunnittelijat ovat yleensä tietotekniikan asiantuntijoita, ja he näkevät hyökkääjän tietojärjestelmän "vihollisena" , joten he suunnittelevatkin turvatarkastuksia ja valvontajärjestelmiä tämän uhkakuvan pohjalta. Automaatiojärjestelmien suunnittelijat ovat taas sähkö- ja automaatioasiantuntijoita, jotka yrittävät selvittää eri automaatiojärjestelmissä tapahtuvia virhetiloja. Tämän vuoksi automaatiosuunnittelijat yrittävät pitää automaatiojärjestelmät niin yksinkertaisina ja toimintavarmoina kuin vain pystyvät. Tämä toimintatapa johtaa erittäin luotettaviin, mutta harmillisesti myös kyberhyökkäyksille erittäin alttiisiin tietoverkkoihin. Luotettavan, turvallisen ja joustavan suorituskyvyn turvaaminen saattaa estää sellaisten tietoturvatyökalujen käyttämisen, joilla voidaan taata täydellinen tietoturva koko teollisuusautomaatiojärjestelmälle. Tietokoneiden rajallinen laskentakapasiteetti voi olla myös yksi este tietoturvatyökalujen käytölle. Tämä johtaa kompromisseihin suorituskyvyn, turvallisuuden ja kyberturvallisuuden välillä. Kaikki nämä erot johtavat helposti ristiriitoihin, kun tehdään yhteistyötä automaatio- ja toimistotietojärjestelmiä kehittävien organisaatioiden välillä, koska eroja on niin teknisissä yksityiskohdossa kuin toimintakulttuureissakin. [58]

Automaatio- ja toimistotietojärjestelmillä oli aluksi todella vähän yhteisiä laitteita ja ohjelmistoja, koska molemmissa oli käytössä omat tietoliikenneprotokollat. Tämän vuoksi automaatiojärjestelmät olivat melko hyvin eristettyjä järjestelmiä. Nykyään Ethernet- ja TCP/IP-pohjaiset laitteet kuitenkin korvaavat vanhaa tekniikkaa, koska ne ovat edullisia ja laajasti saatavilla. Tämä aiheuttaa ongelmia ja vaaratilanteita kyberturvallisuuden näkökulmasta. Teollisuusautomaatiojärjestelmissä on alettu käyttämään myös standardeja tietokoneita, käyttöjärjestelmiä ja verkkopro-

tokollia, joilla pystytään luomaan järjestelmille esimerkiksi uusia etäkäyttöominaisuuksia. Tämä heikentää automaatiojärjestelmien eristystä. Vaikka markkinoilla onkin tietoturvaratkaisuja, joilla pystytään käsittelemään juuri näitä etäkäyttöjen tietoturvaongelmia, niin silti näitä ohjelmia joudutaan usein räätälöimään tapauskohtaisesti, kun ne otetaan käyttöön teollisuusautomaatiojärjestelmissä ja tehdasympäristössä. [50]

Taulukko 1.1: Automaatio- ja toimistotietojärjestelmien erot [50]

Kategoria	*Toimisto*	*Automaatio*
Suorituskyky-vaatimukset	-Ei reaaliaikainen -Vasteaika normaali -Korkea läpisyöttö -Viiveet ja niiden heilunta sallitaan -Ei kriittisiä hätätoimintoja -Voidaan asettaa tiukka kulunvalvonta	-Reaaliaikainen -Vasteaika kriittinen -Vaatimaton läpisyöttö -Viiveitä ei sallita -Kriittiset hätätoiminnot -Kulunvalvonta voi olla tiukka, mutta koneiden käyttö täytyy turvata
Saatavuus ja luotettavuus vaatimukset	-Uudelleenkäynnistys mahdollista -Saatavuushäiriöt ovat joissakin tapauksissa hyväksyttyjä	-Uudelleenkäynnistys ei aina mahdollista -Saatavuushäiriöt eivät ole hyväksyttyjä -Alasajot joudutaan suunnittelemaan
Riskinhallinta-vaatimukset	-Hallitaan dataa -Datan luotettavuus ja eheys tärkeää -Vikaherkkyys ei ole niin kriittinen -Hetkellinen alasajo sallittua	-Hallitaan fyysisiä toimintoja -Turvatoiminnot kriittisiä -Alasajot eivät ole sallittuja -Suurimmat riskitekijät liittyvät säädoksien rikkomiseen (ympäristöriskit, henkilöiden, omaisuuden ja tuotannon turvaaminen)

Kategoria	*Toimisto*	*Automaatio*
Järjestelmän toiminta	-Perinteiset käyttöjärjestelmät -Päivitetään automaattisesti	-Sovelluskohtaiset käyttöjärjestelmät, joissa ei ole usein vielä tietoturvaa -Päivitetään valmistajan toimesta, koska ovat spesiaaleja
Resurssirajoitukset	-Suuret resurssit -Kolmannen osapuolen tietoturvasovelluksia voidaan tukea	Automaatiojärjestelmän resurssit eivät aina riitä tukemaan kolmannen osapuolen tietoturvasovelluksia
Yhteydet	-Standardit tietoliikenneprotokollat -Langallisia ethernet-verkkoja, joissa voi olla joitain langattomia osia	-Monia standardeja ja sovelluskohtaisia tietoliikenne- ja väyläprotokollia -Pääosin langallisia verkkoja -Langattomat verkot yleistyy
Muutoksenhallinta	-Ohjelmistomuutokset suoritetaan aika ajoin käyttäen hyvää tietoturvapolitiikkaa	-Ohjelmistomuutokset täytyy testata hyvin, että järjestelmän eheys pystytään takaamaan -Automaatiojärjestelmässä voidaan käyttää käyttöjärjestelmiä, joita ei enää tueta
Tukitoiminnot	-Monipuoliset tukitoiminnot	-Tukitoiminnot tulevat yhdeltä toimittajalta
Laitteiden elinikä	3-5 vuotta	10-15 vuotta
Komponenttien sijoittelu	-Komponenttien luokse pääsee helposti	- Komponentit eristettyjä ja sijaitsevat hankalissa paikoissa

Taulukossa 1.1 on esitetty yhteenveto automaatio- ja toimistotietojärjestelmien eroavaisuuksista kyberturvallisuuden näkökulmasta.

2 Automaatiojärjestelmien haavoittuvuudet

Ensimmäiset julkisesti saatavilla olevat tiedot automaatiokomponenttien haavoittuvuuksista ovat peräisin vuodelta 1997, jolloin julkaistiin kaksi haavoittuvuutta. Siitä lähtien vuosittain paljastuneiden haavoittuvuuksien määrä on kasvanut merkittävästi. Esimerkiksi vuonna 2010 julkaistiin 19 haavoittuvuutta, ja vuonna 2015 niitä julkaistiin jo 189 kappaletta. Vuosina 2010-2012 haavoittuvuuksien määrä kasvoi jyrkästi, mikä heijasteli tutkijoiden ja teollisuusautomaatiojärjestelmien omistajien lisääntyvää kiinnostusta teollisuusautomaatiojärjestelmien kyberturvallisuutta kohtaan. Löydettyjen uusien haavoittuvuuksien lukumäärä on sittemmin alkanut tasaantua hieman yli 150 tapaukseen vuodessa. [6]

Muutamat tietoturva-alan yhteisöt ovat kehitelleet standardeja, joilla pystytään luokittelemaan ja pisteyttämään eri haavoittuvuuksia. Näitä standardeja ovat ainakin yleisesti tunnettujen haavoittuvuuksien raportointikehys CVRF, web-järjestelmien haavoittuvuuksiin keskittyvä OWASP, haavoittuvuuksien pisteytysjärjestelmä CVSS, joka on ilmainen ja avoin teollisuusstandardi, jolla voidaan pisteyttää ja arvioida haavoittuvuuksien vakavuutta. Lisäksi on vielä CVE, joka on listaus yleisesti tunnetuista haavoittuvuuksien ja altistuksien nimistä ja yksityiskohdista. CVE tarjoaa myös vertailumenetelmän yleisesti tunnetuille kyberhaavoittuvuuksille ja -altistuksille. CVE:tä ylläpitää US Department of Homeland Security - Yhdysvaltojen kotimaan turvallisuusvirasto. [8]

2.1 Haavoittuvuustyypit

Automaatiokomponenteissa on tietoturvallisuuden näkökulmasta omat hyvät puolensa, mutta myös uudentyyppisiä haavoittuvuuksia on havaittu. Yleisesti voidaan kuitenkin sanoa, että automaatiojärjestelmiä ja -verkkoja uhkaavat saman tyyppiset haavoittuvuudet kuin muitakin tietojärjestelmiä ja -verkkoja. Kaikkein yleisin haavoittuvuustyyppi teollisuusautomaatiojärjestelmissä on, vuonna 2015 tehdyn Oxana Andreevan ym. tutkimuksen [6] mukaan, puskurin ylivuoto. Näiden löydösten osuus oli 9 % kaikista samana vuonna löydetyistä haavoittuvuuksista. Toisella ja kolmannella sijalla olivat kovakoodatut kirjautumistiedot ja XSS-tyyppinen haavoit-

tuvuus, joita molempia oli 7 % kaikista löydetyistä haavoittuvuuksista. Näitä haavoittuvuustyyppejä seurasi autentikoinnin ohitukset ja CSRF-tyyppinen haavoittuvuus, joita molempia oli 5 % haavoittuvuuksista. [6]

2.1.1 Puskurin ylivuodot

Puskurin ylivuoto on ohjelmavirhe, joka pääsee tapahtumaan silloin, kun tietokoneohjelmalla tallennetaan dataa muistiin. Kun tallennettavan datan määrä kasvaa liian suureksi, suhteessa muistipaikan kokoon, niin osa tiedoista tallentuu varatun muistialueen ulkopuolelle. Kirjoittaminen varatun muistialueen ulkopuolelle tyhjentää aiemmin muistissa olleet tiedot ja kaataa ohjelman tai aiheuttaa haitallisen koodin suorittamisen. Pääsyynä ylivuotojen olemassaololle on C ja C++ -kielten kaltaiset matalantason ohjelmointikielet, joita on käytetty pitkään eri automaatiolaitteissa ja -sovelluksissa. Nämä ohjelmointikielet ovat käytössä etenkin sulautetuissa järjestelmissä, tietoliikennekomponenteissa, automaatiokomponenteissa ja IoT-laitteissa. Automaatiojärjestelmät ja IoT-laitteet ovat kyberturvallisuuden näkökulmasta erittäin riskialttiita, koska ne ovat usein liitettyinä sellaisiin koneisiin, joiden kaappaus voi aiheuttaa vakavia ongelmia henkilöiden, rakennusten ja esineiden fyysiselle turvallisuudelle.

Ongelman C-kielen kohdalla aiheuttaa erityisesti sen muistinkäsittelyominaisuudet, jotka sallivat ohjelmoijille monia eri vapauksia kirjoittaa ja hallita muistipaikkoja sekä pino- ja kekorakenteita. Hyökkääjä voi esimerkiksi yrittää saada muitiosoittimet haltuunsa ylikirjoittamalla muistipaikat jollain keksityllä paluuosoitteella. Tämän jälkeen aliohjelman käsittely siirtyy jonnekin hyökkääjän tahtomaan muistipaikkaan, ja sitten alkaa tapahtua ei-toivottuja asioita, kuten tiedostojen siirtoa, oikeuksien hallinnan riistoa tai mitä tahansa hyökkääjä keksiikin. Tällaiset toimet vaativat kuitenkin myös haitallisen koodin suorittamista, joka voidaan estää käyttämällä NX-muistia. Tämän jälkeen hyökkääjä pystyy vain kaatamaan ohjelman puskurin ylivuodon avulla. Puskurin ylivuodot voidaan kuitenkin ehkäistä myös kokonaan käyttämällä tiettyjä menetelmiä. Tällaisia menetelmiä ovat: virheiden välttäminen C-kieltä koodattaessa, koodausvirheiden löytäminen työkalujen avulla ja turvallisten ohjelmointikielien, kuten Javan, Pythonin tai C#:in käyttäminen. Koko ohjelmointikielen vaihtaminen ei ole yleensä taloudellisesti järkevää, ja tämän takia joudutaan tyytymään usein kahteen ensimmäiseen menetelmään. Haittoja voidaan myös pienentää, yksi työkalu tällaiseen on kanarialinnun (eng. canary) käyttäminen. Kanarialintu voi olla esimerkiksi jokin luku, joka tallennetaan pi-

nossa paikallismuuttujien ja paluuosoitteen väliin, sitten kun ollaan lopettamassa jokin aliohjelma, ja ollaan palaamassa return-käskyllä paluuosoitteen osoittamaan muistipaikkaan, niin tarkastetaan kanarialintu ensin. Jos kanarialintu on ylikirjoitettu jollain toisella merkkijonolla, niin tiedetään, että ohjelma on saastunut. Ohjelman suorittamista ei tämän jälkeen jatketa. Menetelmän nimi tulee kaivoksissa käytetyistä, kaasuvuotoja valvovista, kanarialinnuista. Puskurin ylivuotoja löydettiin Oxana Andreevan ym. tutkimuksessa yhteensä 17 kappaletta. Aukkoja oli eri automaatiokomponenteista, kuten SCADA-järjestelmistä, HMI-käyttöliittymistä, PLC-logiikoissa ja DCS-järjestelmistä. Neljässä näistä haavoittuvuuksista saavutettiin korkeimmat CVSS-pistemäärät, eli 10 pistettä, joka vastaa suurinta mahdollista kyberuhkaa, tällöin hyökkäys voidaan suorittaa etänä tunnistautumattoman hyökkääjän toimesta. [6] [37]

2.1.2 Kovakoodatut kirjautumistiedot

Kovakoodatut kirjautumistiedot, kuten salasana tai kryptografiset avaimet, luovat tavallisesti merkittävän reiän, jonka avulla hyökkääjä voi ohittaa ohjelmiston ylläpitäjän määrittelemän autentikointimenetelmän. Tämä haavoittuvuus havaittiin Oxana Andreevan ym. tutkimuksessa yhteensä 14:stä eri automaatiokomponentista ja useimmissa tapauksissa se aiheutti korkean kyberriskin. Lähes kaikkia tämän tyyppisiä haavoittuvuuksia voidaan hyödyntää etäyhteyden avulla, vain parissa tapauksessa sitä pystyttiin hyödyntämään ainoastaan paikallisesti. Automaatiolaitteiden salasanat voidaan yksinkertaisesti myös valita tai tallentaan niin huolimattomasti, että hyökkääjän on helppo saada ne selville ja murtautua järjestelmään. Ongelmana on se, että huomattavan suuri ihmisjoukko valitsee salasanansa samasta pienestä salasanojen joukosta, josta salasana on helppo ratkaista raakaan voimaan perustuvalla menetelmällä, jossa kaikki listan salasanat kokeillaan peräkkäin läpi. Raakaan voimaan perustuvilta salasanojen murtamismenetelmiltä voidaan taas suojautua menetelmällä, joka estää tämän vasaroinnin. Tämä tapahtuu estämällä salasanojen loputtomat uudelleen yritykset, asettamalla viive uudelleen yrityksille, jonka jälkeen salasanaa voi vasta kokeilla uudelleen. On tärkeää säädellä arvaustaajuutta, koska salasanojen entropia on niin heikko. Monissa palveluissa on käytössä sääntöjä, joiden mukaan salasanat tulee kirjoittaa. Säännöissä voidaan määritellä salasanoille esimerkiksi pituus ja merkkisääntöjä. Todellisuudessa hyökkääjät voivat kuitenkin myös soveltaa näitä samoja sääntöjä omissa hyökkäyksissään, ja näin säännöt eivät pääse muuntumaan paremmaksi entropiaksi. [6] [38]

2.1.3 XSS-haavoittuvuus

Cross-site scripting (XSS) on haavoittuvuus, jonka avulla hyökkääjä voi injektoida omia skriptejään HTML-pohjaisiin automaatiojärjestelmiin, joiden avulla voidaan varastaa käyttäjätunnistustietoja, evästeitä, kiertää pääsynhallinta, suorittaa käyttäjän manipulointia tai levittää haittaohjelmia. Perinteisillä verkkosivuilla tämä tapahtuu siten, että hyökkääjä voi kirjoittaa esimerkiksi sivun kommenttiosioon mielivaltaista JavaScript koodia, jonka palvelin sitten suorittaa. Nykyaikaisissa HTML-pohjaisissa SCADA-järjestelmissä ja HMI-käyttöliittymissäkin on kohtia, joihin voidaan lisätä haitallista koodia. XSS-haavoittuvuus vaikuttaa erittäin vakavalta, koska sen avulla pystytään suorittamaan lukuisia muita toisen tyyppisiä hyökkäyksiä. XSS-hyökkäykseltä voidaan puolustautua esimerkiksi joissakin selaimissa käyttävän sisäänrakennetun heuristiikan avulla, joka havaitsee XSS-hyökkäykset. Verkkosivustojen ja www-palvelimen tulisi aina tarkistaa huolellisesti käyttäjältä tulevat syötteet. Tiettyjen merkkien tai merkkiyhdistelmien suodattamista ei voi pitää riittävänä, koska tällaisen suodatuksen voi useimmiten kiertää syöttämällä jokin merkkiyhdistelmä, joka sitten kääntyy ohjelmassa toiseksi merkiksi. Myös eri selaimet tulkitsevat käyttäjän antamat merkit ja syötteet eri tavalla, joka tekee XSS-hyökkäyksistä entistäkin ongelmallisempia. Sisällön tarkistamiseen ja suodattamiseen on olemassa erilaisia työkaluja, kuten eri palvelinohjelmistoja ja ohjelmointiympäristöjä. Yksi tapa estää XSS-hyökkäykset on HTTPOnly-evästeiden käyttäminen, jolloin palvelin voi kertoa selaimelle, että asiakkaan puolen JavaScript-koodilla ei pääse käsiksi evästeisiin. XSS-tyyppisiä haavoittuvuuksia esiintyy Oxana Andreevan ym. tutkimuksessa yhteensä 14 kappaletta, joista useimmat olivat SCADA-järjestelmiä. SCADA-järjestelmät ovat suhteellisen uusi järjestelmätyyppi perinteisiin teollisuusautomaatiojärjestelmiin verrattuna, mutta niiden määrä kasvaa koko ajan. SCADA-järjestelmän integrointi muihin järjestelmiin, varsinkin kriittisiin ohjausjärjestelmiin, tulisi aina perusteellisesti suunnitella ja kartoittaa myös tietoturvallisuuden näkökulmasta. [6] [56]

2.1.4 CSRF-haavoittuvuus

Cross-site request forgery (CSRF) haavoittuvuus on olemassa, jos verkkopalvelin on suunniteltu niin, että se ottaa vastaan asiakkaan HTTP-pyynnön, mutta ei varmista millään suojamekanismilla, että kysely on lähetetty asiakkaan toimesta ja tarkoituksella. CSRF-hyökkäyksessä hyökkääjä itse asiassa vaan käyttää uhrin oikeuk-

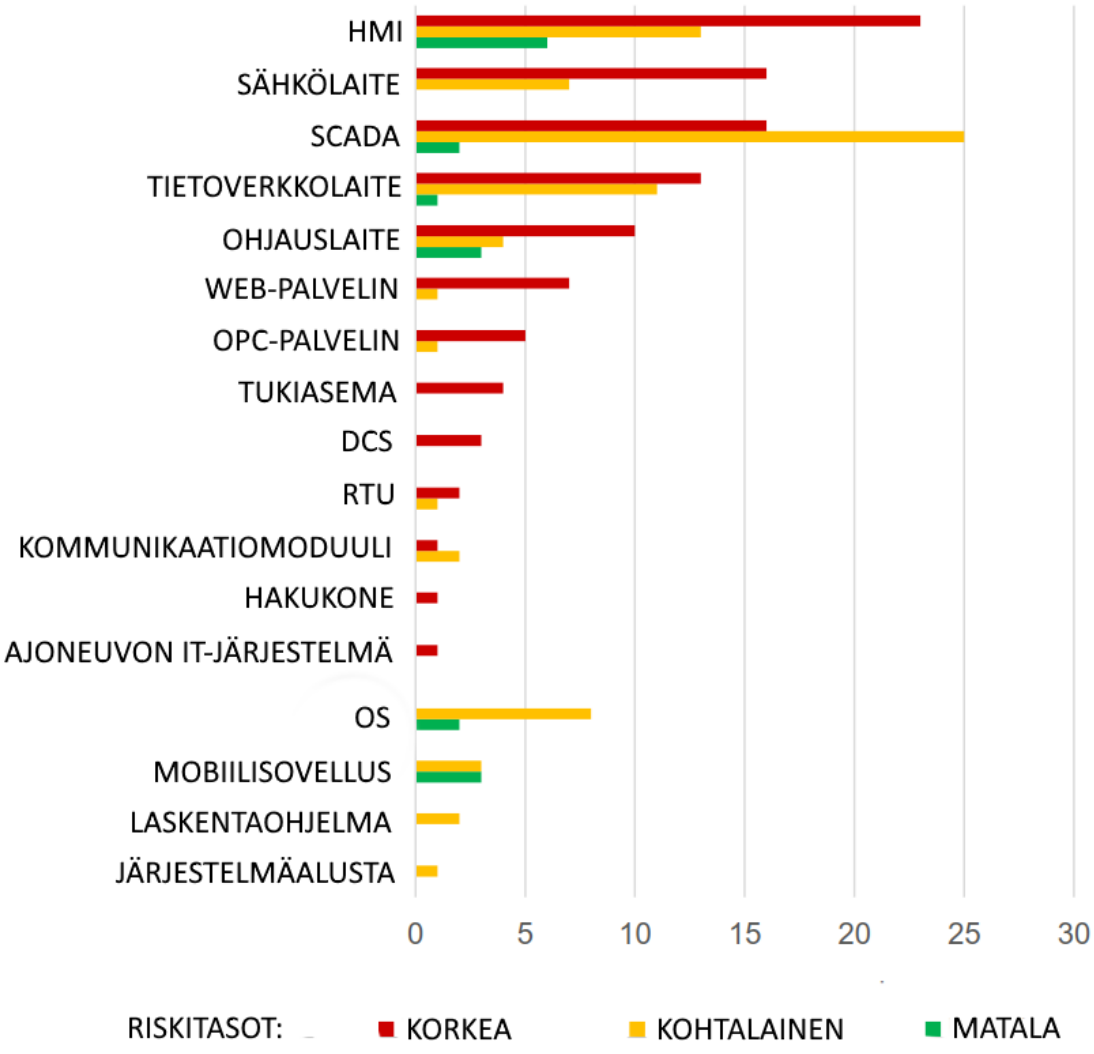
sia hyväkseen, että pääsee lähettämään varmennettuja HTTP-pyyntöjä verkkopalvelimelle. Verkkopalvelin kuitenkin käsittelee näitä aitoina autentikoituina HTTP-pyyntöinä. Hyökkääjän pitää myös tietää, mitkä HTTP-pyynnöt aiheuttavat halutut toiminnot palvelimella. Hyökkääjä voi tehdä hyökkäyksensä URL-osoitteen, kuvan latauksen tai XMLHTTP–pyyntöjen kautta, kun käyttäjä vierailee epäilyttävillä verkkosivuilla. CSRF-hyökkäys voi johtaa tietojen menettämiseen tai haitallisen koodin suorittamiseen. [6] CSRF-tyyppinen hyökkäys voidaan estää tekemällä sopivien HTTP-pyyntöjen lähettäminen mahdottomaksi. Tälläinen suojamekanismi voi olla vaikka käyttäjäkohtainen ja kertakäyttöinen poletti, joka on HTTP-pyyntöön sisällytettävä merkkisarja, jota on mahdoton arvata. Toinen tapa on käyttää toissijaista sessioevästettä HTTP-otsikossa, jota hyökkääjä ei voi arvata. Yksi suojausmekanismi on tehdä sessioevästeistä lyhytikäisiä ja kertakäyttöisiä, tämä ei estä hyökkäystä, mutta tekee hyökkäyksestä ajallisesti rajoitetun. Oxana Andreeva ym. löysivät tutkimuksessaan [6] yhdeksän kappaletta CSRF-tyyppisiä haavoittuvuuksia, ja näistä puolet löytyivät SCADA-järjestelmistä.

2.1.5 Muut haavoittuvuudet

Oxana Andreevan ym. tekemässä tutkimuksessa saatiin selville myös pienempiä määriä muita haavoittuvuuksia. Muutamat SCADA-järjestelmät olivat esimerkiksi haavoittuvia SQL-injektioille ja syötteen validointi oli puutteellista kahdeksassa tapauksessa, joita esiintyi HMI-, RTOS-, SCADA-sovelluksissa sekä OPC-servereillä. Lisäksi kolmeen SCADA-järjestelmään voitiin ladata tiedostoja, joiden koodia voitiin suorittaa laiteympäristössä. Tämän tyyppisistä haavoittuvuuksista voi seurata mitä tahansa. Automaatiojärjestelmissä ja -komponenteissa esiintyy myös haavoittuvuuksia, jotka liittyvät arkaluonteisen tiedon salaamattomaan varastointiin ja lähetykseen. Oxana Andreevan ym. tekemässä tutkimuksessa datalähetyksen kryptaukseen liittyvä haavoittuvuus löytyi kuudesta eri automaatiokomponentista. Yksi syy tämän haavoittuvuuden esiintymiselle oli SSL-salauksen tuen puuttuminen automaatiokomponenteista. Eräissä tapauksissa salasanat vaan tallennettiin selkokielellä ilman mitään salausta. Yhtenä haavoittuvuustyyppinä tutkimuksessa mainitaan autentikoinnin ohitus, joita löytyi 8 kappaletta. Tämän tyyppisiä haavoittuvuuksia löytyi esimerkiksi HMI-käyttöliittymistä, tietoverkkolaitteista ja RTU-laitteista. Tällaisen hyökkäyksen avulla hyökkääjä pystyy kaappaamaan tai muokkaamaan sisäänkirjautumistietoja, injektoimaan koodia tai tekemään oikeastaan mitä tahansa asioita, kuten autentikoidut käyttäjätkin. [6]

2.2 Haavoittuvuudet eri automaatiokomponenteissa

Oxana Andreevan ym. tekemässä tutkimuksessa eniten haavoittuvuuksia löytyi Siemensin ja Schneider Electric automaatiokomponenteista ja komponenttityypeittäin HMI-käyttöliittymistä, SCADA-järjestelmistä ja "sähkölaitteista", joihin luetaan sähköverkon suoja- ja erotuslaitteet, kaasunilmaisimet, pumput ja tehoanalysaattorit. Kuvassa 2.1 on esitelty tutkimuksessa löydettyjen haavoittuvuuksien kappalemäärät eri automaatiokomponenteissa. [6]



Kuva 2.1: Haavoittuvuudet eri automaatiokomponenteissa [6]

2.2.1 Järjestelmätaso

Koko automaatiojärjestelmä voidaan yrittää tehdä haavoittuviksi harhautuksella, jossa henkilöstö yritetään saada paniikkiin harmittomalla valehyökkäyksellä. Tämän jälkeen henkilöstö ryhtyy ajamaan automaatiojärjestelmää ja tuotantoa alas varotoimenpiteenä. Pääkyberhyökkäys on yleensä helpompaa toteuttaa murrostilanteiden aikana, kuten automaatiojärjestelmän seisokin aikana. Tietoturvan seurantakin voi toimia heikommin näiden murrostilanteiden aikana. [3]

2.2.2 Väylälaitteet

Teollisuusautomaatiojärjestelmissä on alettu käyttämään yhä useammin myös yleisiä IP-pohjaisia verkkoteknologioita, sekä sellaisia väyläprotokollia, kuten esimerkiksi Profinet ja Modbus TCP, jotka hyödyntävät IP-pohjaisia verkkoteknologioita. IP-pohjaisten väyläprotokollien käyttö kenttäväylissä tuo mukanaan niiden edut, mutta myös niiden ongelmat, joista suurin on laitteiden mahdollinen näkyvyys automaatioverkon ulkopuolelle. Tämä on ongelma, koska automaatioverkkojen luotettavuus on elintärkeää automaatiojärjestelmien toimivuudelle ja turvallisuudelle. Automaatiojärjestelmissä on perinteisesti käytetty tiedonsiirtoväyliä, jotka ovat suhteellisen tietoturvallisia, koska niiden tietoliikenne ei reitity väylän ulkopuolelle. [11] Monet teollisuusautomaatiojärjestelmien käyttämät väyläprotokollat eivät käytä autentikointimenetelmiä pakettien alkuperän tunnistamiseksi. Tämä haavoittuvuus avaa hyökkääjille mahdollisuuden kaapata, muokata ja välittää datapaketteja, jotka sisältävät esimerkiksi anturien mittaamia arvoja. [39] IP-pohjaisia kenttäväyliä käyttävistä automaatiolaitteista löytyy samoja haavoittuvuustyyppejä kuin muistakin laitteista. Vuonna 2013 julkaistussa artikkelissa [39], joka kantaa nimeä kyberhyökkäykset teollisuusautomaatiojärjestelmään, Thomas H. Morris ja Wei Gao löysivät 17. erilaista tapaa hyökätä Modbus TCP -protokollalla toimivaan SCADA-järjestelmään. Kirjoittajat pystyivät luokittelemaan hyökkäykset neljään eri ryhmään, joita olivat: tiedusteluhyökkäykset, mittaus- ja vastausinjektiot, komentoinjektiot ja palvelunestohyökkäykset. Vaikka artikkelissa olikin testattu vain yhtä väyläprotokollaa, niin kirjoittajat uskovat, että saman tyyppiset hyökkäykset voidaan todennäköisesti suorittaa myös muita väyläprotokollia käyttävissä automaatiojärjestelmissä ja -verkoissa.

Tiedusteluhyökkäyksellä voidaan kerätä tietoja automaatiojärjestelmästä, kartoittaa sen verkkoarkkitehtuuri ja tunnistaa verkossa kiinni olevien laitteiden omi-

naisuudet, kuten: tekniset tiedot, tuetut verkkoprotokollat, verkko-osoitteet ja muistiosoitteet. Tiedusteluhyökkäyksessä voidaan käyttää hyväksi seuraavia menetelmiä: Osoiteskannausta, jolla saadaan selvitettyä kaikkien verkossa olevien laitteiden osoitteet. Funktiokoodiskannausta, jolla saadaan selville, mitä eri funktioita Modbus-verkon laitteet tukevat. Laitteen tunnistushyökkäystä, jolla selvitetään laitteen tekniset tiedot, kuten valmistajan nimi, laitteen sarjanumero ja revisio. Erilaisilla funktiokyselyillä hyökkääjä pystyy selvittämään esimerkiksi laitteen sen hetkisen tilan. Nykyään laitevalmistajat saattavat kirjoittaa ylimääräisiin kenttiin myös oman verkkosivustonsa osoitteen ja muuta tietoa, joista voi olla apua hyökkäyksessä. Pisteskannauksella hyökkääjä voi taas kartoittaa laitteen muistiosoitteet. [39]

Teollisuusautomaatiojärjestelmissä käytetään yleisesti pollaustekniikkaa, kun halutaan monitoroida jotain prosessia ja sen tilatietoja. Pollauksella tarkoitetaan sitä, että asiakas, joka voi olla vaikka monitorointisovellus, lähettää tilakyselyn automaatiopalvelimelle. Tämä kysely koskee jotakin prosessin tilatietoa, joka löytyy jostakin automaatiopalvelimen muistiosoitteesta. Tämän jälkeen automaatiopalvelin vastaa kyselyyn vastauspaketilla. Näitä tilatietoja voidaan lukea eri käyttöliittymistä, niitä varastoidaan historiatiedoiksi eri tietokantoihin, ja niillä voidaan ohjata toisia prosesseja ja laitteita. Näiden vastauspakettien alkuperään ei kuitenkaan autentikoida usein millään tavalla, ja tämä antaakin hyökkääjälle vapaat kädet kaapata, muuttaa ja uudelleenlähettää näitä paketteja. Väyläprotokollat hyväksyvätkin usein ensimmäisen vastauspaketin ja hylkäävät muut vastaukset virheellisinä. Vastauspakettien käsitteleminen ja niiden oikein ajoitettu syöttäminen automaatioverkkoon ovat NMRI- ja CMRI-tyyppisissä vastausinjektiohyökkäyksissä käytettyjä toimintoja. Ennen vastausinjektiohyökkäystä hyökkääjä voi selvittää tiedusteluhyökkäyksellä järjestelmän osoite- ja muistiosoitetiedot. CMRI ja NMRI-tyyppiset hyökkäykset eroavat siinä, että kompleksit vastausinjektiohyökkäykset (CMRI) ovat kehittyneempiä kuin naiivit vastausinjektiohyökkäykset (NMRI). Tämä tarkoittaa sitä, että NMRI-hyökkäyksessä ei tiedetä tarkkoja tietoja itse prosessista, vaan lähetetään vastauspaketeissa nollia, suuria tai negatiivisia lukuja ohjauslaitteille, jolloin ne menevät sekaisin. CMRI-tyyppisessä hyökkäyksessä itse prosessista tiedetään enemmän, silloin vastauspaketin mukana voidaan lähettää esimerkiksi jonkun säiliön pinnankorkeustietoa muutettuna. Vastauspaketissa voidaan esimerkiksi lähettää, että säiliön täyttöaste on 100 %, vaikka todellisuudessa se onkin vain 20 %. Täyttöpumput eivät CMRI-hyökkäyksen vuoksi käynnisty ja säiliö pumpataan ennen pitkää tyhjäksi. Vastausinjektiohyökkäykset voivat olla peräisin automaatiolaitteista, ku-

ten PLC- ja RTU-yksiköistä tai muista verkkoon kytketyistä laitteista, joiden kautta väyläkommunikointia suoritetaan. [39]

Komentoinjektiohyökkäykset voidaan suorittaa monella eri tavalla, niissä voidaan käyttää apuna tikapuulogiikkaa, C-kieltä tai laitteen muistirekistereitä. Komentoinjektiohyökkäykset voidaan jakaa kolmeen eri ryhmään, joista ensimmäinen on tilainjektiohyökkäys (MSCI), jolla voidaan muuttaa esimerkiksi laitteen toiminta automaattisesta manuaaliseksi. Tämä voidaan suorittaa Modbus-protokollaa käytettäessä write coil- tai write register-käskyillä. Toisena ryhmänä ovat parametri-injektiohyökkäykset (MPCI), joissa laitteen asetusarvoja vääristetään. Parametri-injektiohyökkäyksellä voidaan vaikka muuttaa jonkin säiliön pinnakorkeuden hälytysrajat niin suuriksi, että ne menettävät merkityksensä. Viimeisenä ryhmänä ovat funktiokoodi-injektiohyökkäykset (MFCI), joissa Modbus-väylään liitettyjä laitteita sekoitetaan lähettämällä väylään erilaisia käskyjä, kuten force listen only mode -käsky, jolloin laitteet menevät kuuntelutilaan. Väylään voidaan lähettää myös Restart Communication-käsky, jolloin laitteet suorittavat pakotetun uudelleenkäynnistyksen ja yhteys katkeaa väliaikaisesti. [39]

Palvelunestohyökkäykset teollisuusautomaatiojärjestelmässä voivat koskea yhtä venttiiliä tai koko automaatiojärjestelmän kommunikointia. Palvelunestohyökkäys voidaan suorittaa sekä reitittyvää Modbus TCP-protokollaa käyttäville väylälaitteille että reitittymätöntä Modbus RTU- ja Modbus ASCII-protokollaa käyttäville väylälaitteille. Yksi keino suorittaa palvelunestohyökkäys Modbus-verkossa on sellainen, että verkkoon lähetetään paljon epäkelpoja Modbus-paketteja, joissa on virheellinen CRC-tarkistussumma. Modbus-laitteet joutuvat laskemaan jokaisen paketin tarkastussumman erikseen, jonka jälkeen ne ylikuormittuvat, eivätkä lopuksi kykene lainkaan enää kommunikoimaan oikeiden laitteiden kanssa. Palvelunestohyökkäyksen voi tehdä myös langattomiin Modbus-järjestelmiin tukkimalla radiokanava jatkuvilla lähetyksillä. [39]

3 Parhaat kyberturvallisuuskäytännöt

Teollisuuslaitosten ja automaatiojärjestelmien suojaamiseen on olemassa paljon erilaisia kyberturvallisuuskäytäntöjä ja tietoturvatyökaluja. Automaatioverkoissa voidaan käyttää usein myös perinteisten tietoverkkojen suojaamiseen kehitettyjä työkaluja, joko suoraan tai sitten hieman soveltaen. Ensimmäinen näistä hyvistä kyberturvallisuuskäytännöistä on kyberturvallisuussuunnitelman laatiminen, jossa määritellään toimintatavat, miten ihmiset, laitteet ja verkot toimivat keskenään siten, että yritykselle aiheutuisi mahdollisimman vähän ongelmia kyberturvallisuuden osa-alueella. Toinen hyvä käytäntö on automaatioverkkoarkkitehtuurin suunnittelu siten, että se antaa verkolle mahdollisimman hyvän suojan ulko- ja sisäpuolisilta väärinkäyttötapauksilta. Näiden väärinkäyttötapausten havainnointiin ja estämiseen on olemassa nykyään lukuisia erilaisia monitorointijärjestelmiä, tunkeutumisten havainnointijärjestelmiä (IDS) ja tunkeutumisten estojärjestelmiä (IPS).

3.1 Kyberturvallisuussuunnitelma

Kyberturvallisuussuunnitelman laatiminen on yksi yrityksen kyberturvallisuusstrategian kulmakivistä. Kyberturvallisuussuunnitelma voidaan tehdä erikseen yrityksen mille tasolla tahansa. Se olisi kuitenkin hyvä ulottaa kattamaan lopulta kaikki käyttäjäryhmät, verkot ja laitteet aina konsernitasolta tehdastasolle saakka. Kyberturvallisuussuunnitelmaan kuuluvat riskien arvioiminen, riskien pienentäminen ja suunnitelma siitä, että miten toimitaan ja toivutaan tilanteista, joissa kyberuhka on muuttunut todeksi. [15]

3.1.1 Kyberriskien arviointi

Kyberriskianalyysia käytetään arviointityökaluna silloin, kun halutaan määritellä onko yrityksen omaisuus suojattu kyberuhilta vai ei. Kyberriskianalyysilla voidaan selvittää myös yrityksen yleinen kyberturvataso. Kyberriskien arviointi voi olla määrällinen tai laadullinen prosessi tämän analyysin suorittamiseksi. Yleisesti ottaen kyberriskien arviointi on matemaattinen tapa arvioida todennäköisyyttä sille, että voidaanko järjestelmää vastaan hyökätä yleisesti tiedossa olevien kyberhyökkäys-

menetelmien avulla. Riskinarviointeihin liittyy usein mittareita, malleja ja kaavioita. Ajatuksena on se, että analyytikko pystyy suorittamaan arvion siitä, että pystytäänkö teollisuusautomaatiojärjestelmään yhdistetyillä suojamekanismeilla suojautumaan sellaisia kyberhyökkäystyyppejä vastaan, jotka voivat olla kyberuhkia juuri kyseiselle automaatiojärjestelmälle. Jokaisen hyökkäystyypin esiintymiselle on määritelty oma todennäköisyyskerroin, jolloin arvio koko teollisuusautomaatiojärjestelmän kyberturvatasosta muodostuu kaikkien sitä uhkaavien hyökkäystyyppien esiintymistodennäköisyyskertoimien tulosta. [11]

Kyberriskien arvioimiseen ja hallintaan on tehty erilaisia GRC-järjestelmiä ja riskienarviointityökaluja. GRC:llä tarkoitetaan integroitua ja kokonaisvaltaista lähestymistapaa organisaation laajuiseen hallintoon, riskienhallintaan ja vaatimustenmukaisuuden varmistamiseen [45]. GRC-järjestelmällä voidaan hallita, dokumentoida ja raportoida näiden osa-alueiden tapahtumia. Yksi kattavimmista riskienarviointityökaluista on Yhdysvaltojen kotimaan turvallisuusviraston ylläpitämä CSET-ohjelmisto. CSET on suunniteltu erityisesti automaatiojärjestelmien kyberriskiarviointeihin ja sillä pystytään muodostamaan arvio yrityksen kyberturvallisuuden tasosta. CSET-ohjelmistolla tehdyssä kyberriskianalyysissä yrityksen edustajat vastaavat ohjelmiston esittämiin kysymyksiin oman yrityksensä tietoturvallisuuteen liittyvistä asioista. CSET-ohjelmisto käy perusteellisesti läpi useita satoja kysymyksiä, joilla on merkitys yrityksen kyberturvallisuuteen. Kysymykset liittyvät kyberturvallisuuden eri osa-alueisiin, joita ovat esimerkiksi: [22]

1. Pääsynhallinta
2. Tilien hallinta
3. Auditointi ja vastuunjako
4. Kommunikaation suojaaminen
5. Konfiguraatioiden hallinta
6. Jatkuvuus
7. Tapaturman rajaaminen
8. Informaation suojaaminen
9. Monitorointi ja haittaohjelmat
10. Organisationaalinen
11. Henkilökohtainen
12. Fyysinen turvallisuus
13. Suunnitelmat

14. Politiikka
15. Proseduurit
16. Kannettavat, mobiilit ja langattomat laitteet
17. Toimintatavat
18. Etäyhteydet
19. Riskien hallinta ja arviointi
20. Järjestelmä ja palvelujen saatavuus
21. Järjestelmän eheys
22. Järjestelmän suojaaminen
23. Koulutus

Lisäksi CSET:in kyberriskianalyysissa listataan ja mallinnetaan yrityksen tietoverkko, automaatioverkko ja niihin liittyvät komponentit kehittyneellä mallinnustyökalulla. CSET-ohjelmisto tekee varoituksen, jos mallinnustyökalulla on mallinnettu jokin riskialtis kytkentä tietoverkkoon. Tällainen riskialtis kytkentä voi olla esimerkiksi palomuurisuojauksen puute internet-yhteydessä. Kyberriskien arviointiprosessi ajaa ihmiset ajattelemaan automaatiojärjestelmää tietoturvallisuuden näkökulmasta. Tämän arviointiprosessin vuoksi tietoverkoista alkaa paljastua tietoturvaongelmia, kuten virheellisiä palomuurisääntöjä ja tarpeettomia palveluita. Kyberriskien arviointiprosessi on paljon nopeampi ja halvempi suorittaa, kuin järjestelmän penetraatiotestaus. [11] Siksi onkin järkevämpää suorittaa penetraatiotestaus tarvittaessa vasta kyberriskien arviointiprosessin jälkeen, koska suuri osa tunnetuista heikkouksista karsiutuu pois jo kyberriskien arviointiprosessin yhteydessä, kun järjestelmälle suoritetaan asiaan kuuluva haavoittuvuusanalyysi.

Haavoittuvuusanalyysissa järjestelmästä kerätään aluksi tietoa ja näitä tietoja sitten verrataan dokumentoituihin tietoihin, joita löytyy esimerkiksi CVE- ja CVSS-tietokannoista. Tämän jälkeen tehdään johtopäätökset siitä, että muodostavatko kyseiset haavoittuvuudet ja heikkoudet uhan kyseiselle järjestelmälle. Samalla on hyvä tarkastaa myös, että onko näihin tunnettuihin haavoituksiin ilmestynyt uusia tietoturvapäivityksiä. [8]

Penetraatiotestauksella pyritään jäljittelemään hyökkääjän toimintaa. Tehdasautomaatiojärjestelmästä pyritään löytämään haavoittuvuuksia, joiden avulla saadaan avattua yhteys kyseiseen automaatiojärjestelmään myös tehtaan ulkopuolelta. Monet penetraatiotestaajien ja hakkerien käyttämät tietoturvatyökalut ja tekniikat ovat hyödyllisiä, kun halutaan yksilöidä ja arvioida eri haavoittuvuuksia. [8]

3.1.2 Kyberriskien pienentäminen

Kyberriskien pienentäminen on olennainen osa kyberturvallisuussuunnitelmaa ja kyberriskien hallintaa. Kyberriskiä voidaan pienentää pienentämällä kyberhyökkäyksen tapahtumistodennäköisyyttä ja sen seurauksia. On siis pyrittävä vaikuttamaan siihen, että kyberhyökkäys tapahtuisi mahdollisimman harvoin, ja kun se tapahtuu, niin sen seuraukset olisivat mahdollisimman pienet. Ensisijaisesti olisi pyrittävä vaikuttamaan kyberriskin esiintymistodennäköisyyteen ja vasta sitten seurauksien pienentämiseen. Seurauksia voidaan pienentää laatimalla suunnitelma siitä, miten hyökkäyksen aikana toimitaan ja miten siihen vastataan. Jos tuotantokoneita alkaa sammua tai vikaantua itsestään, niin ihmetyksen määrä voi olla suuri, niin kuin se on perinteisten vikatilanteidenkin aikana. Olisikin hyvä, että kohtuullisessa ajassa voitaisiin tarkastella myös tietoverkon tilaa. Parhaassa tapauksessa tietoverkosta voitaisiin nähdä nopeasti, että tilanne siellä ei ole normaali, ja hyökkäykseen voitaisiin vastata viipymättä.

Hyökkäykseen vastaaminen on varautumiseen ja resilienssiin liittyvä toimenpide, jota ei ole vielä täysimääräisesti hyödynnetty monessakaan yrityksessä. Tehokas toimintasuunnitelma kyberhyökkäysten varalle pienentää vahinkoja, palautumisaikaa ja kustannuksia. Tehtaiden tulisikin varautua toimenpiteisiin, joita tehdään silloin, kun haittaohjelma on päässyt leviämään teollisuusautomaatiojärjestelmään. Tällaisia keinoja voi olla automaatiojärjestelmän saartaminen ja yhteyksien katkaiseminen muihin tietoverkkoihin. Myös tehtaan manuaalisia ohjauksia olisi syytä testata aika ajoin, koska yhteydet ohjausjärjestelmään voivat katketa hyökkäyksen seurauksena, milloin on mahdollista, että mikään ohjauslaite ei enää reagoi käskyihin. [57]

Ernst & Youngin vuoden 2017 tietoturvallisuutta käsittelevästä tutkimuksesta [54] selvisi, että 49 % kyselyyn vastanneista yritysjohtajista olisi valmis kasvattamaan rahallisia panostuksia tietoturvatietämyksen lisäämiseen ja harjoitteluun. 46 % yritysjohtajista olisi valmis kasvattamaan rahallisia panostuksia tietoturvakeskusten perustamiseen ja toimintaan seuraavan vuoden aikana, joka oli tutkimuksessa toisella sijalla kohdassa, jossa kysyttiin mihin yritysjohtajat aikovat suunnata rahallisia resursseja ensi vuonna. [54]

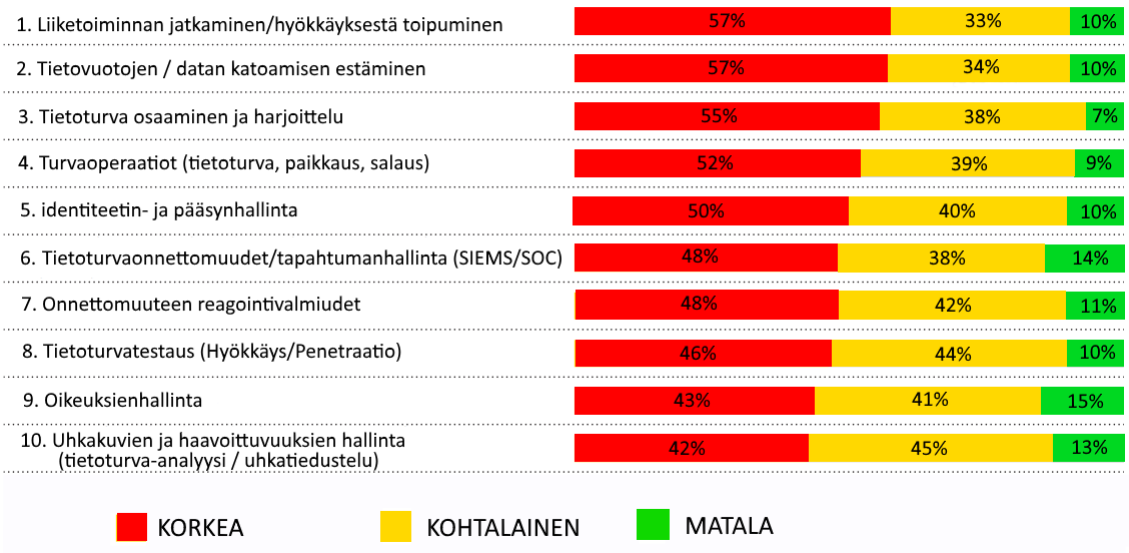
Kaikkien edellä mainittujen toimenpiteiden jälkeen jäänyttä kyberriskiä, ja sen aiheuttamia kustannuksia voidaan yrittää pienentää vielä vakuutuksella. Yritykset voivat nykyään ottaa kybervakuutuksen siltä varalta, että jokin vahinko pääsee tapahtumaan. Tämän tulisi olla tietenkin se viimeinen keino, eikä tällä tulisi sivuuttaa

muita menetelmiä, joilla kyberriskiä saadaan pienennettyä.

3.1.3 Kyberhyökkäyksestä toipuminen

Kyberhyökkäys pääsee tapahtumaan, jos kyberriskien arvioinnissa ei ole arvioitu kyseistä haavoittuvuutta, tai jos tämän haavoittuvuuden pienentämiseen tarkoitetut turvamekanismit ovat pettäneet. Kun kyberhyökkäys pääsee sitten lopulta tapahtumaan, kaikista ennalta tehdyistä varotoimenpiteistä ja varautumisesta huolimatta, niin yrityksellä on hyvä olla suunnitelma myös toipumisen varalta.

Kyberhyökkäyksestä toipumisessa yrityksen kaikki eri osastot, kuten ICT-, automaatio-, tuotanto-, ylläpito-, korjaus- ja turvallisuusosastot, ovat kaikki tärkeässä roolissa, koska tuotantojärjestelmien ylösajoa ei yleensä voida toteuttaa pelkästään ICT- ja tietoturvatiimin avulla. Ilman riittävää tietämystä tuotannon eri järjestelmien ja toimintamallien yksityiskohdista ja sovituista toimintatavoista, tuotantoon voikin aiheutua uusia häiriöitä, ja näin tilanne voi eskaloitua hätäisten toimien seurauksena. [3]



Kuva 3.1: Tietoturvan eri osa-alueiden prioriteetit v. 2016 [54]

Kuvassa 3.1 on esitetty kymmenen tärkeintä kehityskohdetta, jotka yritysjohtajat mainitsivat Ernst & Youngin vuoden 2016-2017 tietoturvatutkimuksessa [54]. Tutkimuksesta kävi ilmi, että globaalisti toimivat yritykset ovat entistä vakuuttuneempia

siitä, että ne pystyvät ennustamaan ja torjumaan kehittyneitä kyberhyökkäyksiä. Ongelmia sen sijaan aiheuttaa hyökkäyksistä toipuminen, jonka vaatimiin toimenpiteisiin ei ole investoitu tarpeeksi, tai jota varten ei ole edes tehty suunnitelmaa. Tutkimuksesta selvisi myös, että 57% yritysjohtajista asetti hyökkäyksestä toipumisen ja liiketoiminnan jatkon varmistamisen tärkeimmäksi kehityskohteiksi seuraavalle vuoden. Tutkimuksessa jaetulla kärkisijalla oli myös tietovuotojen ja tiedon hukkaamisen estäminen. [54]

3.2 Automaatioverkkoarkkitehtuurin tietoturvasuunnittelu

Automaatioverkkoarkkitehtuurin tietoturvasuunnittelun lähtökohtana on se, että automaatiojärjestelmää ei saa havaita millään skannauksella tehtaan ulkopuolelta, eikä siihen saa pystyä ottamaan suoraan yhteyttä mistään laitteesta, ei edes tehtaan omasta verkosta, jollei tälle ole annettu siihen erikseen lupaa. Hyvä tietoturvasuunnittelu pitää sisällään myös tietoturvallisten automaatiokomponenttien valinnat, sekä niiden toimittajien tietoturvaosaamisen kartoittamisen.

3.2.1 Automaatiojärjestelmän erottaminen muista tietoverkoista

Teollisuusautomaatiojärjestelmässä kiinni olevien laitteiden ei tulisi koskaan antaa muodostaa yhteyttä suoraan yrityksen toimisto- tai internet-verkossa olevan tietokoneen tai laitteen kanssa. Vaikka jossakin teollisuusautomaatiojärjestelmässä ei välttämättä olisikaan suoraan Internet-yhteyttä, niin epäsuorayhteys on edelleen olemassa, jos automaatiojärjestelmät ovat yhteydessä sellaiseen verkon osaan, jolla on olemassa Internet-yhteys. Organisaatiot eivät välttämättä aina ymmärrä, että tällainen uhkaava yhteys on olemassa, mutta sinnikäs hyökkääjä saattaa silti löytää sen ja aiheuttaa fyysistä tuhoa sen avulla. Siksi olisikin hyvä, jos eri organisaatiot tekisivät perusteellisia arviointeja tietoverkoistaan, mukaan lukien toimistotietoverkot, että mitä haavoittuvuuksia ja heikkouksia niissä saattaa olla. Teollisuusautomaatiojärjestelmässä olevien laitteiden ja muiden tietoverkkojen väliset tarpeettomat kanavat on poistettava, että tietojärjestelmän haavoittuvuudet saadaan minimoitua. Yksi hyvä menetelmä on selvittää ja listata kaikki yrityksen tietoverkkoihin liitetyt verkkokomponentit. Näin saadaan kartoitettua myös oleelliset reitit tietoverkoissa. [57]

3.2.2 Automaatiojärjestelmän ulkoreunan suojaaminen

Automaatiojärjestelmän ulkoreunan suojaamiseen voidaan käyttää erilaisia menetelmiä, kuten palomuurisuojausta, VPN-yhteyksiä, auktorisointia, virustentorjuntaohjelmia ja erilaisia autentikointimenetelmiä. Automaatiojärjestelmän ulkoreunan puutteellisen suojauksen voi pahimmassa tapauksessa havaita kuka tahansa verkonkäyttäjä, koska internetissä on saatavilla hakukoneita, jotka ovat erityisesti suunniteltu löytämään automaatiojärjestelmiä ja -laitteita.

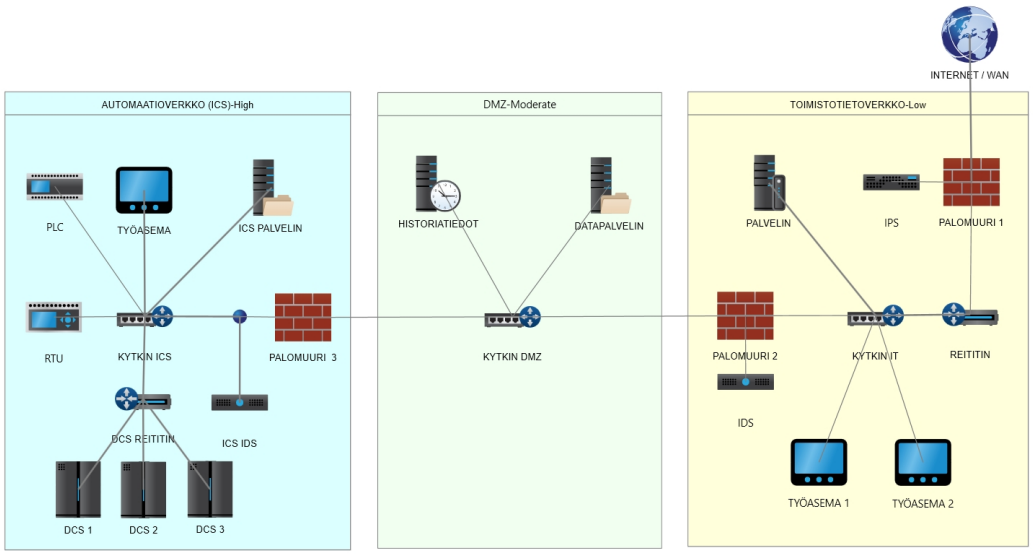
Vuonna 2009 markkinoille tulleella Shodan-hakukoneella voidaan etsiä internetistä erilaisia automaatiolaitteita, jotka voidaan havaita otsikkokenttien informaatiosta. Monet laitevalmistajat tekevät automaatiokomponenttien löytämisen todella helpoksi, kun he lisäävät otsikkokenttiin laitteen versio- ja nimitiedot. Shodanilla voidaan tehdä hakuja, joilla otsikkokentistä etsitään jonkun tietyn protokollan haavoittuvuuksien sormenjälkitietoa. Esimerkiksi Siemensin Simatic S7-300 sarjan automaatiolaitteet löytyvät, kun kyselyssä on merkkijono "HTTP/1.0 302 Location: /Portal0000.htm". Tämän jälkeen Shodan ilmoittaa hakutulosten IP-osoitteet ja arvion niiden maantieteellisestä sijainnista. [24] Timo Kiravuo, Seppo Tiilikainen, Mikko Särelä ja Jukka Manner tekivät vuonna 2013 tutkimuksen, jossa he löysivät Shodan-hakukoneella lähes viiden tuhannen automaatiolaitteen IP-osoitteet Suomesta. Tästä vuonna 2015 julkaistusta tutkimuksesta [24] selviää, että Suomesta ja Ruotsista löytyi väkilukuun suhteutettuna kaikkein eniten avoimia IP-osoitteita, jotka kuuluvat erilaisille automaatiolaitteille. Suurin osa löydetyistä laitteista kuului kuitenkin kiinteistöautomaatiojärjestelmiin ja vain pieni osa, noin yksi kymmenestä, kuului teollisuusautomaatiojärjestelmiin.

3.2.3 Automaatiojärjestelmän segmentointi

Automaatiotietoverkkojen ja teollisuuslaitosten muiden tietoverkkojen segmentoinnin päätavoitteena on minimoida pääsy sellaisiin arkaluonteisiin verkon osiin, tietoihin ja järjestelmiin, joihin pääsy ei ole aivan välttämätöntä. Segmentoinnin yhteydessä täytyy kuitenkin varmistua siitä, että automaatiojärjestelmä ja muut tietoverkot voivat toimia tehokkaasti. Eli segmentointi ei saa aiheuttaa järjestelmään tietokatkoksia tai automaatiotason laskua. Nämä molemmat tavoitteet voidaan saavuttaa käyttämällä erilaisia segmentointitekniikoita hyväksi, ja oikea tekniikka valitaankin lopulta verkkoarkkitehtuurin mukaan. Yleisesti käytetyin laite automaatio- ja toimistotietoverkkojen segmentointiin on palomuuri, ja segmentointi voidaan teh-

dä kahteen tai useampaan eri vyöhykkeeseen.

Kahden vyöhykkeen ratkaisut ovat marginaalisesti hyväksyttäviä, mutta niitä tulisi käyttää äärimmäisen varovasti. Turvallisimmat, hallittavimmat ja skaalautuvat automaatio- ja toimistotietoverkkoarkkitehtuurit perustuvat tyypillisesti segmentointiin, jossa on vähintään kolme vyöhykettä, joista ainakin yksi vyöhyke on DMZ eli demilitarisoitu vyöhyke. [50] Kuvassa 3.2 on esitetty verkkoarkkitehtuuri, jossa automaatio- ja toimistotietoverkko ovat erotettu DMZ-vyöhykkeellä, joka on eristetty kahden palomuurin ratkaisua käyttäen.



Kuva 3.2: CSET-ohjelmalla suunniteltu DMZ-vyöhyke

DMZ-vyöhyke on sisäverkko, jonka ei kuuluisi näkyä avoimesti toimistotietoverkkoon, vaan pääsy DMZ-vyöhykkeelle pitäisi kulkea palomuurin kautta ja yhteyden pitäisi päättyä DMZ-vyöhykkeen palvelimille. DMZ-vyöhykkeen palvelimet tarjoavat sitten näitä automaatioverkon historia- ja tapahtumatietoja toimistotietoverkolle. DMZ-vyöhykkeen palvelimet luovat siis omat erotetut ja eristetyt yhteydet automaatioverkkoon. Palomuuri, joka erottaa automaatio- ja toimistotietoverkot toisistaan, tulee konfiguroida siten, että se sallii eristetyn liikenteen automaatioverkkoon vain DMZ-vyöhykkeen palvelinten kautta. [40]

3.2.4 Automaatiojärjestelmän tietoturvan parantaminen

Yritykset voivat vähentää järjestelmiensä hyökkäyspintaa käyttämällä viimeisimpiä versioita käytetyistä ohjelmistoista ja asentamalla tietoturvapäivitykset, kun ne tulevat saataville. Lisäksi on hyvä poistaa ohjelmistot, joita kukaan ei enää organisaatiossa tarvitse. Yritykset voivat edelleen vähentää riskejä käyttämällä haavoittuvuusskanneria, jolla voidaan tunnistaa päivittämättömät sovellukset. Tämän lisäksi voidaan käyttää virustentorjuntaa, joka estää osaltaan myös hyökkäykset päivittämättömiin sovelluksiin. [17]

Suomen puolustusministeriön kansallinen turvallisuusauditointikriteeristö KATAKRI [44] on tietoturvallisuuden auditointityökalu, joka on suunnattu viranomaisille tai viranomaisten lukuun toimiville turvallisuustarkastajille. KATAKRI:ssa on esitetty asioita, joita voidaan soveltaa myös automaatiojärjestelmien tietoturvan parantamiseen. Esimerkkejä tällaisista asioista ovat KATAKRI:n kolmannessatoista teknisessä tietoturvallisuusosiossa listatut kohdat, joita voidaan vaatia myös automaatiojärjestelmien ohjelmistokehittäjiltä:

1. Ohjelmistokehittäjien tietoturvatietouden varmistaminen.
2. Ohjelmistokehityksen aikana on suoritettava tietoturvauhka-analyysi ja havaitut riskit täytyy hyväksyttää.
3. Ulkoiset rajapinnat testataan viallisilla syötteillä sekä suurilla syötemäärillä.
4. Riippuen ohjelmointiympäristöstä, ongelmia aiheuttavien funktioiden ja rajapintojen käyttöön määritellään politiikka, ja sitä aletaan valvoa.
5. Arkkitehtuuri ja lähdekoodi katselmoidaan.
6. Ohjelmakoodi tarkastetaan automatisoidulla staattisella analyysillä.
7. Ohjelmakoodin versionhallinnan ja kehitystyökalujen eheyden varmistaminen.

3.2.5 Automaatiojärjestelmiin kohdistuvat sopimukset

Teollisuusyritykset tekevät tavallisesti automaatiojärjestelmien toimitus- ja asennussopimuksia eri alihankkijoiden ja laitetoimittajien kanssa. Tämä voi tarkoittaa sitä, että yrityksen omilla automaatioasiantuntijoilla ei ehkä ole tarvittavaa teknistä tietämystä juuri kyseisen automaatiojärjestelmän käyttämistä tiedonsiirto- ja ohjausteknologioista. Tämä tuo mukanaan lukuisia turvallisuushaasteita koko automaatiojärjestelmän elinkaaren aikana. Ensimmäinen haaste on se, että jollei järjestelmän

tekniikkaa ja konfiguraatioita ole ymmärretty tarpeeksi hyvin, niin automaatiohenkilöstö ei pysty monitoroimaan järjestelmää hyökkäyksien ja tunkeutumisyrityksien varalta. Toisena haasteena on se, että yrityksellä voi olla rajallinen kyky suoriutua varautumis- ja palautustoimintojen suunnittelusta, jollei automaatiojärjestelmätoimittajat ole mukana kertomassa sitä, miten heidän laitteiden kanssa tulee menetellä. Viimeisenä haasteena on vielä tietoturvapäivitykset ja niiden asentaminen. Jos laitetoimittaja tulee tekemään nämä tietoturvapäivitykset, niin tästä voi aiheutua viivettä ja järjestelmä voi olla pitempiä aikoja haavoittuvassa tilassa. [20] Ohjelmistoja hankittaessa on myös suositeltavaa edellyttää toimittajaa toimittamaan sellaisen dokumentaation, josta selviää käytetyt verkkoportit sekä ohjelmistokomponentit, kuten ohjelmiston käyttämät kirjastot. [44]

Automaatiolaitetoimittajien kanssa olisikin hyvä sopia ainakin näistä, edellisessä kappaleessa esitetyistä asioista, jos mietitään sopimuksia kyberturvallisuuden näkökulmasta. Järjestelmäkoulutus on tietenkin jo nyt vakiokäytäntö, mutta miten hyvin koulutuksissa käsitellään eri tiedonsiirtoteknologioita ja niiden tietoturvaa? Miten pitää toimia hyökkäyksen aikana, jos epäillään vaikka haittaohjelman päässeen leviämään automaatiojärjestelmään? Miten järjestelmää voidaan monitoroida haittaohjelmien tai tunkeutumisien varalta? Voidaanko järjestelmä erottaa hätätilanteessa turvallisesti muista tehtaan automaatioverkoista, ja olettaa, että se jatkaa toimintaasa normaalisti? Mikä on se aika, jonka sisällä automaatiolaitetoimittajan on tehtävä kriittiset tietoturvapäivitykset, siitä hetkestä lukien, kun ne ovat julkaistu valmistajan toimesta?

Suomen valtiovarainministeriön teknisen ICT-ympäristön tietoturvataso-ohjeen (VAHTI 3/2012 [53]) mukaan, seuraavat tietoturvallisuutta koskevat osa-alueet tulee nostaa esille, ja ne pitää liittää myös hankinta-asiakirjoihin vaatimuksiksi, kun tehdään sopimuksia ICT-alihankkijoiden ja -tavarantoimittajien kanssa:

1. Hankittavalta palvelulta tai tuotteelta edellytettävät tietoturvatasovaatimukset, jotka tulee tarvittaessa sovittaa sopimaan paremmin hankittavaan kohteeseen. Vaatimukset tulee kohdistaa vain hankittavaan kohteeseen, ei toimittajaan.
2. Hankittavalta palvelulta tai tuotteelta edellytettävät ICT-varautumisen vaatimukset, jotka tulee tarvittaessa sovittaa sopimaan paremmin hankittavaan kohteeseen.

3. Yleiset palvelulta edellytettävät tietoturvallisuuteen liittyvät vaatimukset, jotka pitää olla mukana sopimuksessa siten, että molemmat osapuolet ovat ymmärtäneet ja hyväksyneet ne. Näistä vaatimuksista sopiminen voi tulla kalliiksi, jos ne sovitaan vasta jälkikäteen.
4. Palvelun toimintaan liittyvät ns. substanssitietoturvavaatimukset, joita ei voi yleisesti luetella. Substanssitietoturvavaatimukset pitää tarkastaa ja tuottaa hankintoihin aina erikseen.
5. Vaatimukset niistä tietoturvallisuuden osa-alueista, jotka pitää olla valmiina ja hyväksyttyinä, ennen kuin tämä palvelu tai tuote voidaan hyväksyä tuotantokäyttöön ja tietoturvan hallintajärjestelmän piiriin.

3.3 Automaatioverkkoliikenteen monitorointi

Nykyään tietoverkot ovat yhä suurempia ja monimutkaisempia, ja niissä liikkuvan datan määrä on suurempi kuin koskaan aiemmin. Samaa vauhtia tietoverkkojen datamäärien kasvun kanssa ovat kasvaneet myös tietoverkkojen kyberhyökkäykset, jotka ovat nykyään myös yhä kehittyneempiä. Tämän vuoksi tietoverkkojen valvontaa on pystyttävä parantamaan, ja verkkoja on kyettävä hallitsemaan ja myös suojaamaan näiltä kyberuhkilta. Verkonvalvontaa voidaan parantaa monitoroimalla verkkoliikennettä aina pakettitasolle saakka. Mikään muu tapa ei tarjoa yhtä hyvää syvyyttä ja rakeisuutta kuin pakettitasolle ulotettu monitorointi. Kaksi yleisintä menetelmää tietoverkon pakettitason monitoroinnin kytkemiseen ovat SPAN- ja TAP-tekniikat. [19]

3.3.1 TAP-laitteet

Verkkoliikenteen monitoroinnissa voidaan käyttää yksinkertaista TAP-laitetta, joka voidaan kytkeä helposti osaksi tietoverkon kaapelointi-infrastruktuuria. TAP-laite sijoitetaan kahden verkkolaitteen väliin. Tämän jälkeen kaikki data verkkolaitteiden A ja B välillä kulkee TAP-laitteen lävitse. Sisäisen jakajan avulla TAP-laite kopioi kaikki paketit ylimääräisiin valvontaportteihin, kun alkuperäiset tiedot jatkavat esteettömästi TAP-laitteen lävitse. TAP-laite ei kuitenkaan näy itse verkkoon mitenkään, eikä muille verkkolaitteille tarvitse tehdä mitään lisäkonfigurointeja. TAP-laitteita on olemassa aktiivisia ja passiivisia malleja. Passiivisissa TAP-laitteissa on kaksi valvontaporttia, jolloin lähtevät datapaketit kummastakin laitteesta A ja B lähetetään erillisiin valvontaportteihin TxA ja TxB. Passiivista TAP-laitetta ei tarvitse

liittää ulkopuoliseen virtalähteeseen ja se on tämän vuoksi erittäin kestävä. Passiivinen TAP-laite ei myöskään välitä käytetäänkö IPv4- vai IPv6-protokollaa ja virheetkin menevät sen lävitse ilman esteitä. [19]

Aktiivisessa TAP-laitteessa on yleensä vain yksi valvontaportti, johon molemmista laitteista A ja B lähetetyt datapaketit käännetään. Tätä liikennettä on helppo monitoroida, kun se voidaan suorittaa vain yhdestä valvontaportista kahden sijaan. Aktiivinen TAP-laite voi myös estää virheellisten pakettien eteenpäin lähetyksen. Tämä on mahdollista, koska laitteeseen on upotettu mikropiiri, jolla pakettien suodatus voidaan suorittaa. Aktiivinen TAP-laite tarvitsee mikropiirinsä vuoksi myös virtalähteen toimiakseen. Lisätyn tekniikan vuoksi, aktiiviset TAP-laitteet ovat vähän vikaherkempiä kuin passiiviset TAP-laitteet. TAP-laitteita on olemassa sekä galvaanisilla yhteyksillä että kuituoptiikalla toteutetuille tietoverkoille. Jos kyse on kuituoptiikasta, niin TAP-laitteella kopioidaan vain valoa, eli ratkaisu on täysin passiivinen. TAP-laitteet voidaan luokitella data-diodeiksi, ja ne soveltuvatkin yksinkertaisuutensa ansiosta hyvin kriittisimpiinkin toimintaympäristöihin, kuten puolustussektorille ja ydinvoimaloihin. [19] [60]

3.3.2 SPAN-portit

SPAN-portti, jota joskus kutsutaan myös peiliportiksi, on ohjelmistolla toteutettu verkkoportti, joka sijaitsee kytkimessä, palomuurissa tai reitittimessä. SPAN-porttiin voidaan lähettää vain tietyt datapaketit, jotka valitaan ohjelmiston asetuksien perusteella. Ohjelmiston avulla pääkäyttäjä voi helposti määrittää tai muuttaa, mitä datapaketteja SPAN-porttiin lähetetään. SPAN-portit voivat kuitenkin vaikuttaa negatiivisesti isäntälaitteen suorituskykyyn ja verkkoliikenteeseen luotettavuuteen. Väärin konfiguroidut SPAN-portit ruuhkautuvat, ja silloin niissä voi esiintyy myös pakettihäviöitä. [19]

SPAN-portteja on olemassa eri tyyppisiä, joista yleisimmät ovat paikallinen SPAN ja etäkäyttöinen RSPAN. Paikallisessa SPAN-portissa lähde- ja kohdeportit sijaitsevat samassa laitteessa. Etäkäyttöisissä RSPAN-porteissa lähdeportit sijaitsevat eri kytkimissä kohdeportin kanssa, jolloin pakettien välittämiseen tarvitaan erityistä VLAN-yhteyttä kytkimien välille. Kaikki kytkimet eivät tue RSPAN:in käyttöä. [10]

3.3.3 NPB-järjestelmät

NPB-järjestelmällä, eli tietoverkon datapakettien välittäjällä, voidaan kerätä datapaketteja useammasta pisteestä, kuten edellä mainituista pisteistä, eli TAP-laitteista ja SPAN-porteista, ja yhdistää nämä pienemmät tietovirrat suuremmaksi kokonaisuudeksi ja lähettää ne sitten oikeaan kohteeseen. Datapakettien yhdistämisen tarkoituksena on se, että koko verkkoliikenne voidaan monitoroida kerralla samasta pisteestä. Kerätty data voidaan lähettää erilaisille verkkomonitorointisovelluksille, kuten palomuureille ja IPS- tai IDS-järjestelmille. Nykyaikaisella NPB-järjestelmällä voidaan myös käsitellä datapaketteja, kuten suodattaa niitä ja poistaa duplikaatteja turvallisesti. Lisäksi NPB-järjestelmällä voidaan purkaa SSL-salauksia ja maskata sensitiivistä dataa. Maskauksella tarkoitetaan tietojen salaamista tai muuntamista pois selkokielisestä muodosta. [21]

3.3.4 Monitorointiohjelmat

Verkkoliikenteen monitoroimiseen on kehitetty paljon erilaisia monitorointiohjelmistoja, joista osaa voidaan käyttää myös tunkeutumisen havaitsemiseen ja estoon, ja jotkin näistä ohjelmistoista ovat taas integroitu palomuuriin. Tarjolla on sekä maksullisia että avoimeen lähdekoodiin perustuvia ilmaisohjelmistoja. Erilaisia pakettitason monitorointityökaluja sisältävät ainakin: Wireshark-, tcpdump-, Snort-, pfSense- ja Bro NSM-ohjelmistot.

Tunnetuin näistä avoimen lähdekoodin monitorointi- ja analysointiohjelmisto on Wireshark, joka toimii esimerkiksi: Windows-, Linux- ja OS X-käyttöjärjestelmissä. Wiresharkissa on graafinen käyttöliittymä, jonka käyttäminen on havainnollisempaa kuin esimerkiksi komentoriviltä käytettävän tcpdump-ohjelmiston käyttäminen. Wireshark tukee yli tuhatta eri protokollaa, ja avoimen lähdekoodin ohjelmistona Wiresharkin lähdekoodi on myös vapaasti muokattavissa, ja siihen voidaan lisätä uusia protokollia, vaikka jokaisella päivityskerralla. Wireshark tukee myös harvinaisempia protokollia, kuten automaatiojärjestelmissä käytettyjä Modbus-, Profinet- ja DNP3-protokollia. Wireshark-yhteisö on poikkeuksellisen aktiivinen kehittämään ja päivittämään ohjelmistoa. [47]

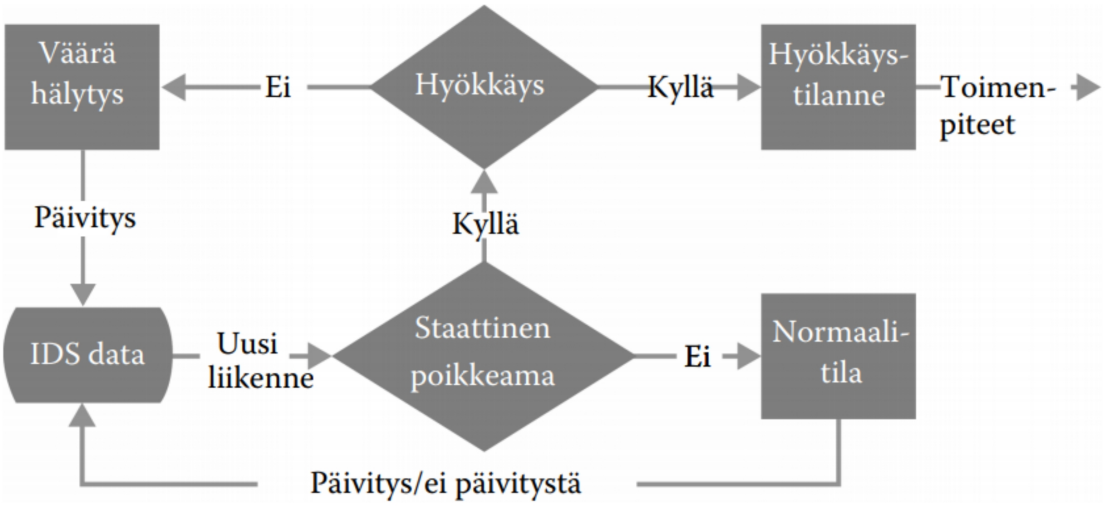
3.4 Tunkeutumisen havaitsemismenetelmät ja -järjestelmät

Tunkeutumisen havaitsemismenetelmillä, sekä niitä hyväksikäyttävillä tunkeutumisen havaitsemis- ja estojärjestelmillä (IDS/IPS), pyritään havaitsemaan ja estämään tietoverkon ja sen laitteiden luvaton käyttö, sekä mahdollisten muiden tietoturvaongelmien, kuten haittaohjelmien ja virusten leviäminen. Näiden kyberhyökkäyksien havainnointiin verkkoliikenteestä on olemassa kaksi päämenetelmää, jotka ovat tunkeutumisen havaitseminen poikkeaman eli anomalian perusteella ja tunkeutumisen havaitsemien tunnistetiedon eli niin sanotun sormenjälkitiedon perusteella. Näitä molempia havaitsemismenetelmiä voidaan soveltaa käytettäväksi myös sellaisissa tunkeutumisen havaitsemis- ja estojärjestelmissä, joita käytetään automaatioverkon kanssa, vaikka automaatioverkon protokollat ja itse hyökkäyksetkin eroavat hieman niistä, joita tavataan toimistotietoverkon puolelta. Oikein konfiguroituina tunkeutumisen havaitsemisjärjestelmät voivat parantaa merkittävästi yrityksen kykyä havaita hyökkäyksiä verkkoliikenteestä, joka taas parantaa osaltaan yrityksen tietoturvaa [50].

3.4.1 Havaitseminen poikkeaman perusteella

Tunkeutumisen havaitseminen poikkeaman perusteella tapahtuu siten, että aluksi pyritään selvittämään ja luomaan malli verkon toiminnasta sen ollessa normaalitilassa. Tämän jälkeen uutta verkkoliikennettä verrataan tähän selvitettyyn normaaliin verkkoliikenteeseen ja sen rajoihin. Mahdolliset poikkeamat normaaliksi oletetusta liikenteestä osoittavat tunkeutumisen tai epäilyttävän toiminnan. Tämä periaate perustuu oletukseen, että epänormaali liikenne poikkeaa normaalista liikenteestä, ja että se on myös harvinaisempaa. Jos tämä oletus täyttyy, niin yleensä tällä tekniikalla pystytään tunnistamaan myös nollapäivähyökkäykset, koska myös ne poikkeavat yleensä odotetusta normista. Kuten missä tahansa järjestelmässä, tämä on kuitenkin todellisen elämän approksimaatiota, jota edustaa rajallinen määrä säädeltäviä muuttujia, joten malli ei ole koskaan täydellinen. Menetelmän käyttö voikin johtaa vääriin tulkintoihin poikkeaman havaitsemisessa. Oikeutettu liikenne voidaan tulkita hyökkäykseksi ja hyökkäykset, jotka ovat naamioitunut lailliseksi liikenteeksi, eivät aiheuta hälytystä. Kuvassa 3.4 on esitetty lohkokaavio hyökkäyksen havaitsemisesta poikkeaman perusteella. [43]

Automaatioverkon normaalitilan opettamiseen voidaan käyttää esimerkiksi eri verkkoprotokollien, kuten: TCP-, UDP-, ICMP-yhteyksien määrää, yhteyksien kes-



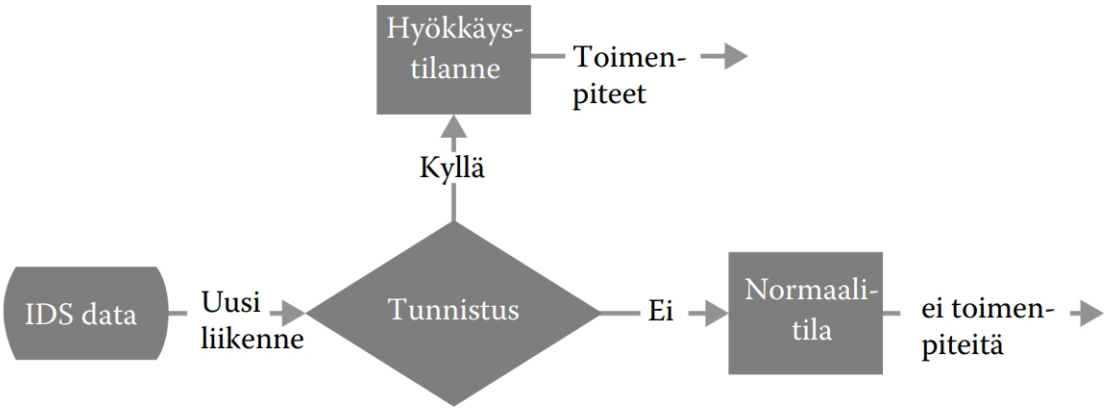
Kuva 3.3: Lohkokaavio, hyökkäyksen havaitseminen poikkeamasta. [43]

toaikaa, lähetettyjen ja vastaanotettujen pakettien määrää ja kokoa sekä verkon fragmentteja, kuten Mantere, Sailio ja Noponen kirjoittavat artikkelissaan [31], jossa he esittelevät passiivisen anomaliapohjaisen IDS-järjestelmän. Tämä järjestelmä käyttää hyväkseen valmista Bro NSM-monitorointityökalua, johon on yhdistetty kirjoittajien kehittämä SOM-koneoppimisalgoritmi, jolla voidaan havainnoida poikkeamia teollisuusautomaatioverkoista.

Poikkeustiloja voidaan yrittää havaita automaatioverkkojen lisäksi myös tehtaan prosessitiloista. Tässäkin tapauksesta fyysisestä prosessista luodaan ensin malli, ja tämä malli normaalitilasta tallennetaan havainnointijärjestelmään. Tämän jälkeen prosessin tilaa verrataan normaalitilaan ja poikkeamista voidaan generoida hälytyksiä, kuten Ghaeini, Antonioli, Brasser, Sadeghi ja Tippenhauer kertovat artikkelissaan [18]. Artikkelissa kerrotaan, miten hyökkäys voidaan havaita säiliön pinnankorkeusmittauksen, pumpun ja venttiilien tilatietojen perusteella. Artikkelissa esitetty menetelmä soveltuukin parhaiten juuri yksinkertaisten prosessien seurantaan, ja näin "syvältä" prosessista tehty hyökkäyksentunnistus voisikin todellisuudessa olla vain todella merkittävän prosessin tietoturvatyökalu.

3.4.2 Havaitseminen tunnistetiedon perusteella

Tunkeutumiset ja muut väärinkäyttötapaukset voidaan havaita ja tunnistaa, verkkoliikenteen poikkeamien lisäksi, myös tunnistetietojen perusteella, jolloin tunnetut hyökkäysmallit ja -kaavat toimivat tunnistetietoina, joista hyökkäys tunnistetaan. Tapa on vastakohta poikkeaman perusteella tehdylle tunnistukselle, koska siinä tietoliikenne, joka ei ole asetettujen rajojen sisällä, tulkitaan väärinkäytöksi. Tunnistetiedon perusteella tapahtuva havaitseminen on osoittautunut erittäin tehokkaaksi menetelmäksi tunnettujen hyökkäystyyppien havaitsemiseksi ja sillä pystytään luomaan yksityiskohtaiset hälytykset, joissa juurisyykin on jo mukana. Tällä havaitsemismenetelmä ei kuitenkaan pystytä tunnistamaan kaikkia uusia hyökkäyksiä, ja tunnistusmallien kehittäminen onkin vaikea ja aikaa vaativa prosessi. Tunnistus ei tälläkään havaitsemismenetelmällä ole täydellinen. Tunnistusmallit kehitetään yleensä historiallisesti tunnetuista hyökkäyksistä, mikä aiheuttaa menetelmälle päivitystarpeen. Kuvassa 3.5 on esitetty lohkokaavio hyökkäyksen havaitsemisesta tunnistetiedon perusteella. [43]



Kuva 3.4: Lohkokaavio, hyökkäyksen havaitseminen tunnistetiedoista. [43]

3.4.3 Tunkeutumisen havaitsemis- ja estojärjestelmät

IDS-järjestelmät ovat verkkoliikenteen näkökulmasta passiivisia järjestelmiä, joista on olemassa kaksi päätyyppiä, jotka ovat verkkopohjainen NIDS-järjestelmä ja isäntäpohjainen HIDS-järjestelmä. Nykyisin teollisuusautomaatiojärjestelmien suo-

jaamiseen käytetään useimmiten NIDS-järjestelmää, joka on sijoitettu palomuurin yhteyteen, automaatio- ja toimistotietoverkon välillä. NIDS-järjestelmällä valvotaan siis kokonaista verkkosegmenttiä, kun taas HIDS-järjestelmällä valvotaan yhtä verkossa olevaa tietokonetta tai laitetta. HIDS-järjestelmää käytetään useimmiten sellaisissa työasemissa, joihin on asennettu yleiskäyttöisiä sovelluksia ja käyttöjärjestelmiä, kuten HMI-, SCADA- ja engineering-työasemissa. [50]

Tunkeutumisen estoon tarkoitettu IPS-järjestelmä on periaatteessa aktiivinen IDS-järjestelmä, johon on lisätty ominaisuuksia, joilla voidaan estää hyökkäykseen. Tällainen aktiivinen estotoimenpide voi olla vaikka tietystä verkko-osoitteesta tulevien datapakettien blokkaaminen, ja kyseisen verkko-osoitteen lisääminen mustalle listalle. Tosin IDS- ja IPS-järjestelmissäkin olisi hyvä käyttää mustalistauksen sijasta valkolistausta, jolla tarkoitetaan sallittujen osoitteiden lisäämistä listalle, jotka saavat viestiä tietoverkossa. Tunnetuin IDS/IPS-järjestelmä on avoimeen lähdekoodiin perustuva Snort, joka voidaan asentaa esimerkiksi yrityksen palomuurin yhteyteen. Snort on tunnistaa tunkeutumiset tunnistetietojen perusteella ja se on verkkoonkytkettävä NIDS/NIPS-järjestelmä. Snortiin voidaan luoda erilaisia sääntöjä, joilla pystytään havainnoimaan tunkeutumisia esimerkiksi erilaisista automaatioväylistä, kuten esimerkiksi Profinet- [14], Modbus- [59] ja DNP3-väylistä [25].

Modbus TCP-protokollaa käyttävään automaatioverkkoon kytkettyyn Snortiin voidaan tehdä esimerkiksi säännöt luvattomista PLC-ohjaimen luku- ja kirjoituspyynnöistä. Kun Snort havaitsee tällaisen vihamielisen Modbus-asiakkaan, joka tekee luvattoman pyynnön PLC-ohjaimelle tai SCADA-järjestelmään, niin se pystyy generoimaan tapauksesta hälytyksen ja blokkaamaan kyseisen lähettäjän pyynnöt. Tällaiset pyynnöt voivat olla osa automaatioverkkoon kohdistuvaa vihamielistä tiedustelua, jotka voivat taas olla ensimmäinen merkki tulevasta suuremmasta hyökkäyksestä teollisuuslaitosta vastaan. [59]

Tietoliikenne on automaatioverkossa pääosin staattista. Tämä tarkoittaa sitä, että automaatioverkko ja sen säännöllinen viestintä eivät muutu kovinkaan usein, jos esimerkiksi PLC-ohjaimella ohjataan vakaata prosessia, niin viestintäparametreja ei tarvitse muuttaa kuin poikkeustapauksissa. Snortilla voidaan tarkastaa lähes kaikki Modbus-parametrit. Modbus-liikenteen yksinkertaisuuden ja vakaan luonteen vuoksi vain pieni osa näistä Modbus-parametreista joudutaan muuttamaan Snort-säännöiksi, että lähes kaikki poikkeamat saadaan tunnistettua. Parametreina voidaan käyttää esimerkiksi: [12]

- Verkko- ja kuljetuskerroksen (TCP/IP)
  - Lähdeosoite
  - Kohdeosoite
  - Protokolla
  - Portti
- Sovelluskerroksen (Modbus)
  - Modbus-otsikko
  - Funktiokoodi ja -alikoodi
  - Data

Snort pystytään käyttöönottamaan esimerkiksi pfSense-palomuuriohjelmistossa, kun mukaan lisätään Wireshark-monitorointityökalu, niin järjestelmästä voidaan rakentaa täydellinen avoimen lähdekoodin verkkoliikenteen monitorointi- ja IDPS-järjestelmä.

Teollisuusautomaatioverkoista voidaan havaita poikkeustilanteita myös passiivisella tunkeutumisen havaitsemisjärjestelmällä, jolla tarkoitetaan järjestelmää, joka on kytketty kuuntelemaan verkkoa passiivisesti. Se ei kykene tekemään verkkoon mitään kyselyitä, kuten skannauksia tai muita aktiivisia kartoituksia. Sillä voidaan kuitenkin tarkastella verkossa liikkuvien datapakettien osoitteita, ominaisuuksia ja käytettyjä protokollia, kuten muillakin tunkeutumisen havaitsemisjärjestelmillä. Passiivinen tunkeutumisen havaitsemisjärjestelmä ei myöskään näy automaatioverkkoon mitenkään, eli sillä ei ole näkyviä IP- tai MAC-osoitteita. Se on myös erotettu automaatioverkosta passiivisten TAP-laitteiden tapaan. Passiivinen tunkeutumisen havaitsemisjärjestelmä voikin olla tehokas ja vakaa työkalu automaatiojärjestelmän verkkoliikenteen seurantaan.

3.4.4 Tietoturvakeskukset ja SIEM-järjestelmät

Tietoturvakeskus (SOC) on yrityksen IT-organisaation osa tai IT-palvelu, jonka tehtävänä on seurata yrityksen IT-omaisuuteen liittyviä tietoturvatapahtumia. Tietoturvakeskus vastaanottaa tapahtumainformaatiota ja lokitiedostoja, ja rakentaa näiden pohjalta automaattisia hälytystoimintoja oletetuista uhkista. Kun hälytys käynnistyy, niin SOC-henkilöstö määrittelee sen, että onko jokin automaattihälytys käynnistynyt vahingossa vai onko todellakin kyse kyberhyökkäystilanteesta. [9]

Tietoturvakeskuksen vastuulla voivat olla esimerkiksi [33]:

- SIEM-järjestelmän seuranta ja korrelaatio.
- Virustentorjunnan lokitietojen seuranta ja määrittely.
- IDS- ja IPS-järjestelmien lokitietojen seuranta ja määrittely.
- DLP-järjestelmien lokitietojen seuranta ja määrittely.
- Keskitetyt lokialustat (syslog jne.).
- Sähköpostiyhdyskäytävien suodatus.
- Web-yhdyskäytävien suodatus.
- Kyberuhkien seuranta ja kyberälykkyys.
- Palomuurien valvonta ja hallinta.
- Sovelluksien valkolistaus ja tiedostojen eheyden seuranta.
- Haavoittuvuuksien arviointi ja seuranta.

SIEM-järjestelmät mahdollistavat palomuurien, IPS- ja IDS-järjestelmien tuottamien tietoturvatietojen keskitetyn keräämisen ja analysoinnin. SIEM-järjestelmällä voidaan saada selville kokonaisvaltainen kuva yrityksen kyberturvallisuustilanteesta, joka olisi muuten hankalaa saada selville, koska yrityksillä on nykyään usein käytössä niin paljon erilaisia tietoturvatyökaluja, ja näiden työkalujen tuottamat tiedot ovat levällään eri puolilla. SIEM-järjestelmällä voidaan havaita kehittyneitä kyberuhkia ja reagoida nopeasti onnettomuustilanteisiin. Sillä voidaan myös käsitellä ja yhdistää erilaisia tietoformaatteja, joista taas voidaan havaita ja analysoida poikkeamia joko reaaliaikaisesti tai historiallisesti. Useimmat yritykset siirtävät SIEM-järjestelmän ja sen valvonnan tietoturvakeskuksen vastuulle. [55]

4 IIoT-arkkitehtuuriratkaisu ja sen kyberturvallisuus

Tässä luvussa kerrotaan tilaajayritykselle suunnitellusta IIoT-arkkitehtuuriratkaisusta, jonka avulla on tarkoitus yksinkertaistaa ja selkeyttää yrityksen IoT-tekniikoiden ja -tiedonsiirtoteknologioiden kirjoa, ja samalla parantaa yrityksen ja siihen kuuluvien teollisuuslaitosten kyberturvallisuutta. Luvussa kerrotaan yksityiskohtaisesti tähän IIoT-arkkitehtuuriin käytettyjen tekniikoiden, protokollien ja standardien toimintaperiaatteista ja tietoturvaratkaisuista. Esitetyn IIoT-arkkitehtuurin on tarkoitus olla tulevaisuudessa ensisijainen vaihtoehto, kun tilaajayritys tai sen alihankkijat haluavat siirtää tietoa ulos tehtaiden automaatioverkkoihin kytketyistä laitteista. Tässä luvussa kerrotaan myös esitetyn IIoT-arkkitehtuuriratkaisun pohjalta tehdyn PoC-projektin käytännön toteutuksesta ja tuloksista.

4.1 IIoT-arkkitehtuurin valinta

IIoT-järjestelmien ja -palveluiden, eli teollisen internetin, rakentamiseen on nykyään tarjolla paljon erilaisia tiedonsiirtoteknologioita, verkonhallintasovelluksia ja pilvipalveluita. Tiedonsiirtoteknologioiden kirjo tulee tulevina vuosina jopa lisääntymään merkittävästi, kun markkinoille tulee uusia teknologioita, kuten 5G NR-teknologiat. Niiden mukana tulevat tiedonsiirtoteknologiat, joista löytyy vaihtoehtoja eri tiedonsiirtonopeuksille, kantamille ja taajuusalueille, kuten alle 1 GHz:in ja alle 6 GHz:in taajuusalueille, sekä korkeammille kymmenien gigahertsien taajuusalueille asti, joita kutsutaan myös millimetrialueiksi. Tarjolla on myös muutamia erilaisia LPWAN-tiedonsiirtoteknologioita, kuten: SigFox, NB-IoT ja LoRaWAN, jotka ovat optimoitu pienelle virrankulutukselle, pienille datamäärille ja suurelle kantamalle. Nämä LPWAN-tiedonsiirtoteknologiat sopivatkin erityisen hyvin laajoille tehdasalueille, joissa ohjattavien laitteiden lukumäärä on suuri tai ne sijaitsevat hankalissa paikoissa, kuten: liikkuvissa koneissa, piipuissa, mastoissa, katoilla, kaivoissa tai rakenteiden sisällä, ja näissä tapauksissa on usein järkevää käyttää paristoa sensorinoodin virranlähteenä.

Teollisuuslaitoksissa on tietysti myös paljon olemassa olevia antureita ja datankeräystä, joita käytetään hyväksi prosessinohjauksessa. Tällaisissa paikoissa ei ole

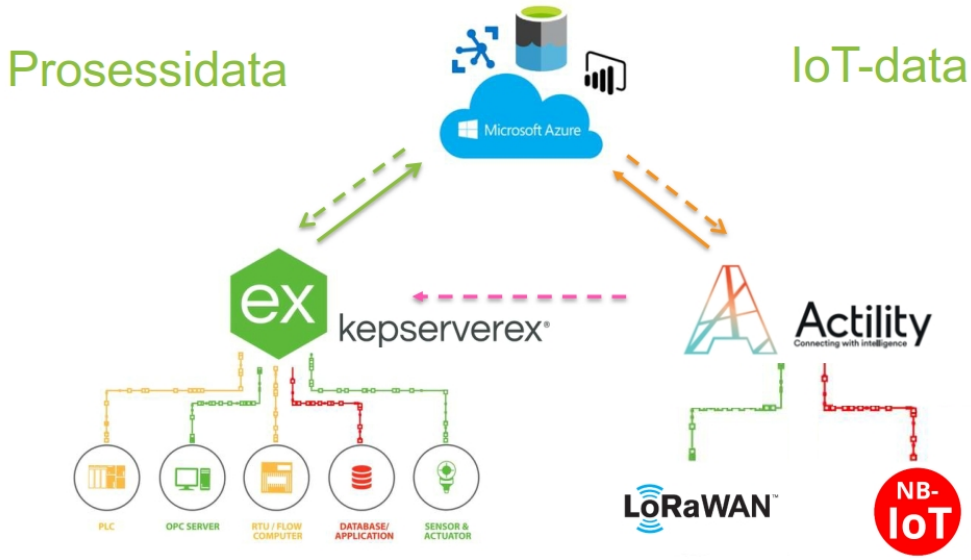
järkevää alkaa kahdentaa antureita uudella tekniikalla, vaan tiedot voidaan välittää eteenpäin näistä olemassa olevista väylistä ja verkoista, joissa tämä prosessidata jo liikkuu. Suuressa tehtaassa voi olla paljon erityyppisiä ja eritasoisia verkkoja, ja niissä voidaan liikutella tietoa eri standardien tekniikoilla ja protokollilla, kuten: Modbus TCP-, Profinet- ja EtherNet/IP-protokollilla. Monesti näiden TCP/IP-protokollaa käyttävien teollisuus-Ethernet-verkkojen alla on vielä vanhempia sarja- ja kenttäväyliä käyttäviä RTU- ja PLC-laitteita, jotka käyttävät esimerkiksi: Modbus RTU, Profibus, CAN, RS-485 tai RS-232-väyliä. Näistä automaatiolaitteista ja -väylistä kerättyjä tietoja voidaan lähettää pilvipalveluihin useilla erilaisilla yhdyskäytävillä, OPC-liittymillä, väliohjelmistoilla ja reunapalvelimilla. Yhdyskäytävät käyttävät automaatioverkon puolella yleisiä automaatioväyläprotokollia, kuten: Profibus-, CAN- tai Modbus-protokollaa, ja pilven puolella REST-rajapintaa, MQTT- tai AMQP-protokollaa. OPC-liittymissä ja väliohjelmistoissa protokolla vaihtoehtoja on vieläkin enemmän kuin yhdyskäytävissä, ja niissä saattaakin olla ajurit lähes kaikkiin tunnettuihin automaatioväyliin, joista dataa pystytään keräämään useilla väylillä rinnakkain.

Eri tiedonsiirtoteknologioille on olemassa erilaisia väliohjelmistoja, verkkoalustoja, joihin verkon eri tukiasemat ja päätelaitteet voidaan liittää. LoRaWAN-tiedonsiirtoverkolle on olemassa esimerkiksi avoimen lähdekoodin verkkoalustoja, kuten The Things Network, joka on erityisen suosittu kotiautomaation laiterakentajien keskuudessa. Tarjolla on myös ammattimaisempaan käyttöön tarkoitetut Loriot.io ja Actility Thingpark. Verkkoalustoja käytetään yleensä palveluna, mutta ne voidaan tapauksesta riippuen asentaa myös asiakkaan omalle palvelimelle. Tiedot lähetetään verkkoalustoista REST-rajapinnan tai MQTT-protokollan kautta eteenpäin, ja tiedon loppuvarastona toimii usein jokin isompi IoT-pilvipalvelu tai -tietokanta. Amazonin AWS-, IBM Cloud- tai Microsoftin Azure-pilvipalveluita käytetään loppuvarastoina, koska niissä on edistyneemmät laskenta-, analysointi-, visu-alisointi- ja raportointityökalut kuin väliohjelmistoissa ja verkkoalustoissa.

IoT-viestirajapintoja ja protokollia voidaan käyttää laitteiden keskinäiseen tai laiteiden ja ihmisten väliseen viestintään, niin sensoreissa, mobiililaitteissa, mikrokontrollereissa, pöytätietokoneissa, palvelimissa kuin pilvipalveluissakin. Viestiprotokollien pitää toimia hyvin yhteen hajautetuissa LAN- ja WAN-verkoissa käytettyjen erilaisten langallisten ja langattomien tiedonsiirtotekniikoiden, kuten: Ethernetin, WiFi-, RFID-, NFC-, Zigbee-, Bluetooth-, GSM-, GPRS-, GPS-, 3G- ja 4G-tiedonsiirtotekniikoiden kanssa. Viestirajapintoja ja -protokollia on tarjolla useita

vaihtoehtoja, kuten esimerkiksi: DDS-, AMQP-, MQTT-, JMS-, REST-, CoAP-, XMPP-, OPC- ja OPC UA-protokollat. [16] [41]

Tilaajayrityksen PoC-projektiin suunnitellun IIoT-arkkitehtuuriratkaisun pääsuunnittelukriteereitä olivat, vahvan tietoturvan lisäksi, järjestelmän yksinkertaisuus ja selkeys, jolla tarkoitetaan erilaisten IIoT-teknologioiden: tiedonsiirtoverkkojen, komponenttien, sovellusten ja protokollien määrän minimointia. Tämä on erityisen tärkeää, kun sama IIoT-arkkitehtuuri on tarkoitus monistaa useille tehtaille. Olisi resurssitehokkuuden ja teollisuuslaitosten kyberturvallisuuden kannalta katastrofaalista, jos jokainen yksikkö käyttäisi omaa räätälöityä IIoT-teknologiapalettia ja -tietoturvaratkaisuja, koska valinnanvaraa eri teknologioissa riittää. Onkin mahdollista, että ilman alusta alkaen tehtävää IIoT-teknologioiden harmonisointia, yritys joutuisi ennen pitkää siivoamaan eri teknologioita pois tehtailta, koska niiden ylläpito kävisi liian raskaaksi. Voi olla, että jotkut teollisuusyrityksen joutuvat tekemään tulevaisuudessa tällaisen teknologioiden siivous- ja harmonisointiprojektin, kun järjestelmästä on paljastunut ensin jokin vakava haavoittuvuus, tai on päässyt käymään jopa niin, että ensimmäinen isompi kyberhyökkäys on sattunut. Tämä tulisi yritykselle huomattavasti kalliimmaksi kuin teknologioiden harmonisointi nyt saman tien, kun IIoT-teknologiat ovat vasta alkamassa yleistyä tehtailla. Kyberriskien arviointi on myös helpompi suorittaa, kun käytetyt teknologiat ovat minimoitu ja harmonisoitu konsernitasolla.



Kuva 4.1: IIoT-arkkitehtuuriratkaisu

Tilaajayrityksen IIoT-arkkitehtuuriratkaisussa päädyttiin käyttämään Microsoftin Azure-pilvipalvelua ja sen Data Lake-tietovarastoa kaiken tuotettavan tiedon päätietovarastona, johon jokaiselta anturilta ja toimilaitteelta tulevat tiedot lopulta tallennetaan. Tiedonsiirtoputkia valittiin IIoT-arkkitehtuuriratkaisuun aluksi kaksi kappaletta, joista toinen on prosessidatalle ja toinen IoT-datalle, kuten kuvasta 4.1 käy ilmi. Tiedonsiirtoputkien määrää yritetään IIoT-arkkitehtuurissa myös minimoida, mutta tuleville 5G-tiedonsiirtoteknologioille jätettiin arkkitehtuuriratkaisuun varaus. Kuvassa 4.1 esitetyn yksinkertaistetun arkkitehtuurimallin mukaan, prosessidata kulkee KEPServerEX-palvelimen kautta Azureen, kun taas IoT-data kulkee Azure-pilveen Actilityn Thingpark LPWAN-verkkoalustan kautta, joka kerää datan LoRaWAN- sekä NB-IoT-verkkoihin kytketyistä sensorinoodeista. Prosessidata edustaa arkkitehtuurissa sitä dataa, jota tehdas tuottaa jo olemassa olevilla automaatiojärjestelmillä. Tehtaiden teollisuusautomaatioverkoissa käytettävien automaatioprotokollien kirjo on valtava, mutta keskitetyn OPC-liittymän ja -palvelimen avulla, tiedot saadaan kerättyä kaikista eri protokollia käyttävistä järjestelmistä tietoturvallisesti. Tämä tapahtuu ilman, että alihankkijat joutuvat asentamaan tehtaille omia 3G/4G-reitittimiä, jotka luovat merkittävän tietoturvariskin. OPC-liittymän tiedonsiirtokyky on myös valtava, sillä voidaan reitittää ja siirtää tiedot tuhansista antureista samaan aikaan. IoT-datalla tarkoitetaan sellaista dataa, joka tuotetaan tulevaisuudessa langattomia verkkoja käyttävillä IoT-laitteilla, jotka halutaan pitää erillään automaatioverkosta, tai jotka ovat hankalia tai mahdottomia liittää siihen.

4.2 IIoT-sovellukset

Tässä alaluvussa keskitytään kertomaan IIoT-sovelluksista, jotka valittiin tilaajayrityksen IIoT-arkkitehtuuriratkaisuun. IoT-sovellukset käsittävät Microsoftin Azure-pilvipalvelun, KEPServerEX-palvelimen ja Actilityn Thingpark LPWAN-verkkoalustan, jotka kaikki pystyvät tarvittaessa kommunikoimaan toistensa kanssa, eli ottamaan dataa vastaan ja lähettämään sitä eteenpäin. Useimmissa tapauksissa datavirta kuitenkin kulkee teollisuuslaitosten lattiatason antureista kohti pilveä, jossa data sitten muokataan lopulliseen muotoonsa – sellaiseen muotoon, josta datan sisältämä sanoma välittyy selkeimmin käyttäjälle.

4.2.1 Thingpark LPWAN-verkkoalusta

Actilityn Thingpark toimii LPWAN-tiedonsiirtoverkkojen verkkoalustana ja koko LPWAN-verkon keskussolmuna. Thingparkia voidaan käyttää LoRaWAN- LTE-M- ja NB-IoT-laitteiden yhdistämiseen, ja niiden tuottaman datan eteenpäin lähettämiseen. Thingparkin eri tuotteita ja moduuleita ovat: ThingPark Wireless, ThingPark OS, ThingPark X, ThingPark Exchange ja ThingPark Market, joka on IoT-laitekauppa ja IoT-palveluiden hankintakanava. Actility tarjoaa Thingpark:ista myös Enterprise versiota, joka on tarkoitettu yrityksille yksityisien LPWAN-verkkojen rakentamista varten. Thingparkin tuotteet ja moduulit voidaan ottaa käyttöön yhdessä tai erikseen, ja niistä asiakas voi rakentaa itselleen parhaan mahdollisen kokonaisuuden omiin IIoT-tarpeisiinsa. Thingparkilla on yli 50 maanlaajuista operaattoria. [1]

Thingpark Wireless on ydinverkonhallintajärjestelmä ja toimintojen tukijärjestelmä (OSS) LPWAN-tukiasemille ja -laitteille. Se on suunniteltu pääasiassa kansallisille ja kansainvälisille verkko-operaattoreille, jotka pystyvät tarjoamaan LPWAN-verkkoa pienemmille toimijoille. Järjestelmään voidaan liittää erikokoisia tukiasemia, kuten makro-, nano- ja pikosolutukiasemia, joilla operaatorit voivat tarjota julkisia ja yksityisiä verkkoja. Thingpark Wireless koostuu Thingpark Wireless ydinverkosta ja OSS-järjestelmästä. Thingpark Wireless ydinverkon päätehtävä on LPWAN-päätelaitteilta tulevien ja lähtevien viestien edestakainen kuljettaminen tukiasemien (LRR) ja IoT-verkkokontrollerin (LRC) välillä. LRC on verkkopalvelimella sijaitseva taustajärjestelmä, jolla ohjataan virtualisoitua linkkikerrosta, jolla taas koordinoidaan lähetettäviä viestikehyksiä ja MAC-komentoja tukiasemien ja Thingpark OS-järjestelmän välillä. Sillä ohjataan myös viestien reititystä ja dynaamista tukiaseman valintaa silloin, kun järjestelmä on ruuhkautunut. Verkkokontrolleri suorittaa myös duplikaattien poistamisen, laitteiden autentikoinnin ja mukautuvan tiedonsiirtonopeuden ohjauksen (ADR). LRR ja LRC käyttävät omassa keskinäisessä kommunikoinnissaan IEC104-protokollaa. Thingpark OSS on toimintojen tukijärjestelmä, ja sillä voidaan hallita sekä laitteita että tukiasemia. Laitteiden hallintajärjestelmässä on työkalut, joilla loppukäyttäjä voi lisätä uusia laitteita järjestelmään. Se tarjoaa tietoa laitteiden GPS-sijainnista ja yksityiskohtaisia tilastotietoja, kuten uplink- ja downlink-viestien määrät sekä raportin laitteiden toimintakunnosta ja hälytyksistä. Tällä työkalulla voidaan määritellä myös laitteiden yhdistämiseen liittyvät: verkkopalveluntarjoajat, sovelluspalvelimien verkko-osoitteet, reititysprofiilit, sekä kuittausviestien ja dowlink-yhteyksien määrät. Verkonhallintajärjestelmä ja sen työkalut ovat tarkoitettu käyttäjille, kuten verkko-operaattoreille ja yksityis-

ten verkkojen hallitsijoille, jotka ottavat käyttöön omia tukiasemia ja operoivat niitä. Verkonhallintajärjestelmän työkaluilla voidaan seurata tukiasemien tilatietoja, kuten hälytyksiä, lämpötiloja, CPU-, RAM- ja levynkäyttöä, sekä RF-solun tilatietoja, kuten toimintajaksoja, SF-, RSSI- ja SNR-kertoimia. Lisäksi työkalulla voidaan tarkastella runkoverkkoyhteyden tilatietoja, kuten statusta ja pakettien lähetysmääriä. Verkonhallintatyökalua voidaan käyttää sekä julkisten verkkojen hallinnointiin että alueellisten ja kampusverkkojen hallintaan. Sen avulla verkon omistajat voivat myös luoda nopeasti ja tehokkaasti uusia verkkoja. Actility tarjoaa Thingpark Wirelessiä ensisijaisesti SaaS-palveluna, mutta se voidaan ottaa kokonaisuudessaan käyttöön myös asiakkaan omistamilla palvelimilla. [1]

ThingPark OS:llä voidaan hallita LPWAN-verkkoa erilaisista liiketoimintarooleista, kuten operaattori, toimittaja ja tilaaja. ThingPark OS sisältää myös edellä mainitun toimintojen tukijärjestelmän (OSS), jolla voidaan hallita laitteita. ThingPark OS tarjoaa mahdollisuuden kehittyneeseen verkonhallintaan, jossa operaattorilla voi olla useita yhteydentarjoajia. ThingPark OS-työkaluilla voidaan suorittaa myös verkkoliikenteen analysointia, seurantaa ja laskutusta. [1]

ThingPark X-moduuli tarjoaa toimintoja, kuten: datanhallintaa, datan varastointia, algoritmeja ja ennakoivaa analytiikkaa, joilla voidaan helpottaa sovelluksien kehittämistä. Thingpark Wireless voidaan yhdistää ThingPark X:llä pilvipalveluihin, kuten IBM Bluemix-, Amazon Web Services-, Microsoft Azure-, Bosch IoT-, ThingWorx-, GE Predix- tai Daliworks-pilvipalveluihin. Yhdistämiseen voidaan käyttää eri viestiprotokollia, kuten REST-, AMQP- ja MQTT-protokollia. [1]

Actility tarjoaa Thingpark Enterprise ratkaisua yrityksille, jotka haluavat rakentaa verkon yksityiskäyttöön. Thingpark Enterprise tarjoaa Thingpark Wireless ratkaisua suppeamman palveluvalikoiman, mutta toiminnallisuudet ovat pääratkaisuiltaan samoja. Palvelun tietoturva on korkealla tasolla, ja sitä voidaan käyttää turvallisesti teollisuuslaitoksissa ja valtiollisissa palveluissa. Thingpark Enterprise voidaan ottaa käyttöön asiakkaan pilveen tai asiakkaan paikalliselle palvelimelle asennettuna versiona, jolloin käyttöjärjestelmänä tulee olla CentOS 7.3. [1]

Myös erilaiset hybridiratkaisut julkisen Thingpark Wirelessin ja yksityisen Enterprisen välillä ovat mahdollisia. Actility on tuonut hiljattain markkinoille myös ThingPark Exchange-hubin, joka mahdollistaa LoRaWAN-pakettien kansainvälisen roamingin eri verkkojen välille. Tämä taas lisää LoRaWAN-teknologian käyttömahdollisuuksia kansainvälisissä sovelluksissa. [1]

4.2.2 KEPServerEX-palvelin

KEPServerEX on teollisuuden käyttöön suunniteltu IIoT-alusta ja väliohjelmisto, joka hyödyntää ICS-, IT- ja IoT-viestiprotokollia, joilla se pystyy välittämään yksittäiset tilatiedot automaatiojärjestelmistä yrityssovelluksiin. Se tarjoaa tuen yli 150 automaatioväyläprotokollalle, ja se jakelee datan REST-, MQTT- OPC UA- ja ThingWorx-rajapintojen kautta eteenpäin. [41]

Kun KEPServerEX-palvelimella aletaan määrittää uutta tiedonsiirtoputkea, niin silloin joudutaan tekemisiin muutaman avainkomponentin kanssa, kuten: kanava, laite, tägi ja IoT-gateway, jotka kaikki joudutaan konfiguroimaan erikseen palvelimen asetuksissa. Ensimmäisenä konfiguroidaan kanava, joka pitää olla asennettuna ennen kuin laitteita voidaan alkaa lisäämään palvelimelle. Kanava edustaa tiedonsiirtoputkea KEPServerEX-palvelimen ja automaatiolaitteen välillä, jota voidaan käyttää sarjaportin tai Ethernet-liitännän kautta. Yhteen kanavaan voidaan asentaa vain yksi automaatioprotokolla kerrallaan, jolloin tähän kanavaan voidaan liittää kaikki samaa protokollaa käyttävät automaatiolaitteet. Kanavia voi kuitenkin olla useita, jolloin yhdellä palvelimella voidaan olla yhteydessä useampaan automaatiojärjestelmään samanaikaisesti. Kanavan perustamisen jälkeen, kanavalle voidaan lisätä automaatiolaitteita joko manuaalisesti tai automaattisesti, jolloin palvelin suorittaa laitteiden kartoituksen automaattisesti valitulla kanavalla, jolloin se löytää esimerkiksi kaikki samaa protokollaa käyttävät PLC- ja RTU-laitteet. Jotta laitteen lisääminen onnistuu, niin palvelin tarvitsee laitteen verkko-osoitteen, kuljetuskerroksella käytetyn protokollan ja porttinumeron, jotka voidaan syöttää myös manuaalisesti. Palvelimelle voidaan määrittää lisäksi laitekohtaisia yhteyden laatuun ja kommunikointiin liittyviä parametreja, kuten erilaisia viiveitä, yhteyden katkaisu ehtoja, luettavien lohkojen kokoja ja laiteryhmiä. Kun mennään syvemmälle laitteen sisällä, niin sieltä löytyvät laitteen muistiosoitteet, joissa varsinaista prosessitietoa säilytetään. Yksi tällainen muistiosoite on palvelimen kielellä tägi, joka voidaan konfiguroida joko staattisesti käyttäjän toimesta tai sitten dynaamisesti, jolloin tägin tiedot tulevat palvelimelle automaattisesti OPC-asiakkaalta, joka on luonut tägin. Jos tägi luodaan staattisesti, niin sille määritellään nimi, muistipaikan osoite, kuvaus, lukuoikeudet, pollausintervalli, skaalaus ja datatyyppi. Erilaisia datatyyppejä on tarjolla yli kymmenen, kuten: BCD, Boolean, Byte, Char, Double, DWord, Float, LBCD, LLong, Long, QWord, Short, String tai Word. Nyt kun tägit ovat luotu, niin ne voidaan lähettää IoT-gateway:llä eteenpäin, joka on KEPServerEX-palvelimen lisämoduuli, jolla dataa voidaan siirtää toisen palvelimen kanssa. Dataa

voidaan lähettää MQTT-agentilla, REST-asiakasagentilla tai REST-palvelinagentilla, ja dataformaatteina voidaan käyttää JSON-, XML- tai CSV-formaatteja. KEPServerEX-palvelimessa on myös tapahtumaloki, joka tallentaa erilaiset virhetilanteet, varoitukset, tietoturvahälytykset ja informaation kulussa tapahtuvat häiriöt. Tapahtumalokiin kirjautuvat tapahtumat voidaan määrätä asetuksista. [23]

4.2.3 Azure-pilvipalvelu

Microsoftin Azure on virtaaliverkko ja pilvipalvelu, joka sisältää useita erilaisia palveluita ja sovelluksia, jotka liittyvät tiedon siirtämiseen, varastointiin, analysointiin sekä tietoa käyttävien sovellusten rakentamiseen. Azuressa on käytettävissä esimerkiksi Linux ja Windows-virtuaalikonekapasiteettia, erilaisia tietovarastoja ja tietokantoja, data-analytiikkatyökaluja, tekoälyä, koneoppimisalgoritmeja ja visualisointityökaluja, joiden käytöstä peritään maksu sen mukaan, mitä palveluita kulloinkin käyttää ja miten suurella datamäärällä. Azuressa voidaan datavirtaa hallita minimissään muutamalla sovelluksella, joita ovat: IoT Hub, Stream Analytics, Blob- tai Data Lake-tietovarastot sekä SQL/NoSQL-tietokannat. [35]

IoT Hub toimii Azure-pilvipalveluiden keskitettynä viestikeskuksena, jolla kommunikoidaan erilaisten IoT-sovellusten ja -laitteiden välillä. IoT Hubin ominaisuuksilla voidaan luoda skaalautuvia ja monipuolisia IoT-ratkaisuja, kuten ratkaisuja teollisuuslaitteiden hallintaan tai arvokkaiden hyödykkeiden seurantaan.IoT Hub tukee kaksisuuntaista viestintää sekä laitteesta pilveen että pilvestä laitteeseen. IoT Hubin kanssa voidaan käyttää lukuisia erilaisia tiedonsiirtotyyppejä, kuten pilvestä-laitteeseen tiedonsiirtoa, pyyntö-vastausmallia tai tiedostojen lähettämistä laitteista. Käytössä olevista tiedonsiirtoprotokollista yleisimmät ovat MQTT, AMQP ja HTTPS. IoT Hubin monitorointityökalun avulla voidaan taas tarkastella sovellusten toimivuutta ja IoT-laitteiden tapahtumia, kuten laitteiden asennusta, virhetiloja ja yhteysongelmia. [35]

Azuren virtuaaliverkon ja paikallisen verkon väliseen tietoturvaan voidaan käyttää VPN-tunnelia, mutta sitä voidaan käyttää myös yhtä hyvin kahden virtuaaliverkon yhdistämiseen. Tämä ei kuitenkaan ole hyvä ratkaisu, jos tietoa halutaan siirtää paljon, koska Azuren VPN-yhdyskäytävän tiedonsiirtokapasiteetti on rajallinen. Azuressa on kuitenkin tähän tarkoitukseen kaksi muutakin vaihtoehtoa, jotka ovat ExpressRoute ja Peering. ExpressRoutea käytettäessä virtuaaliverkot ovat yhteydessä toisiinsa Microsoftin MSEE-reunareitittimen kautta. Tällä tavalla asiakas voi käyttää Microsoftin runkoyhteyttä hyväkseen, kun se haluaa kytkeä virtuaalipalvelimia

yhteen. Peering taas tarkoittaa yhdyskäytävän muodostamista kahden verkon välille, jonka jälkeen verkot toimivat ikään kuin ne olisivat samaa verkkoa. Yhteys muodostetaan tällöin Microsoftin runkoyhteyden kautta yksityisiä IP-osoitteita käyttäen. Tällä tavalla yhdistettynä verkkojen latenssi on pieni ja tiedonsiirtonopeus korkealla tasolla, tiedonsiirtoa ei myöskään tarvitse salata enää erikseen. Suoria RDP- tai SSH-yhteyksiä ei myöskään suositella käytettäväksi Azuren kanssa, vaan ne olisivat syytä muodostaa VPN-yhteyden kautta. Azure-virtuaaliverkkojen tietoturvan kulmakiviksi mainitaan: [34] [35]

1. Autentikointi ja roolipohjainen käyttöoikeuksien hallinta.
2. Monitorointi, lokitietojen keräys ja auditointi.
3. Sertifikaattien käyttö ja salattu viestintä.
4. Verkonhallintaportaali.
5. Verkkopakettien suodatus.

Azure-pilvipalveluihin voidaan lisätä useita erilaisia tietoturvaominaisuuksia, joita voivat olla esimerkiksi: tietoturvakeskus, erilaiset palomuurit, DDoS-suojaus, virtuaaliset TAP-portit, IPS/IDS-sovellukset, kyberanalyysipalvelut ja SIEM-integraatio. Nämä voivat olla Microsoftin tai kolmannen osapuolen sovelluksia, jotka ostetaan Azuren verkkokaupasta. Azuren tietoturvakeskuksen avulla määritellään virtuaaliverkon tietoturvapolitiikka. Sillä pystytään myös hallitsemaan ja monitoroimaan Azuressa käytettyjä tietoturvaratkaisuja. Tietoturvakeskuksen alle voidaan liittää esimerkiksi Azuren Key Vault-sovellus, jolla pystytään hallitsemaan ja luomaan erilaisia salasanoja ja sertifikaatteja. Azuren palomuurissa voidaan käyttää tyypillisiä palomuurisääntöjä, kuten suodatusta IP-osoitteen, portin tai protokollan perusteella. Näiden lisäksi palomuuuriin voidaan luoda FQDN-lista ja -tägit, joiden avulla voidaan helpottaa eri domainien oikeuksien jakoa ja ylläpitoa. Azure-palomuurissa voidaan ottaa käyttöön sekä lähtevän liikenteen osoitteenmuunnos (SNAT) että tulevan liikenteen osoitteenmuunnos (DNAT), jolloin virtuaaliverkon sisäiset IP-osoitteet pystytään peittämään. Web-sovelluksien suojaamiseen voidaan käyttää WAF-palomuureja, joilla pystytään suojautumaan tyypillisiltä kyberhyökkäyksiltä, kuten: SQL-injektioilta, XSS-hyökkäyksiltä, porttiskannauksilta, bottihyökkäyksiltä ja HTTP-protokollan väärinkäytöltä. WAF-palomuuri voidaan asettaa kahteen eri tilaan, jolloin se pystyy joko vain havaitsemaan hyökkäykset tai sitten estämään ne kokonaan. Palomuureista saadaan lokitiedostot, jotka voidaan yhdistää Azuren Log Integration -sovelluksella ja analysoida joko Azuren omassa tietoturva-

keskuksessa tai sitten kolmannen osapuolen SIEM-järjestelmän avulla. Azureen on saatavilla Splunk-, QRadar- ja ArcSight-sovittimia, jotka helpottavat integraatiota ja lokitiedostojen siirtämistä näiden SIEM-järjestelmien kanssa. Azureen tulevia ja lähteviä datapaketteja voidaan seurata reaaliajassa Azuren virtuaalisen TAP-portin kautta. TAP-portin kautta voidaan suorittaa myös pakettikaappauksia, jotka voidaan analysoida kolmannen osapuolen analysointityökaluilla. [35]

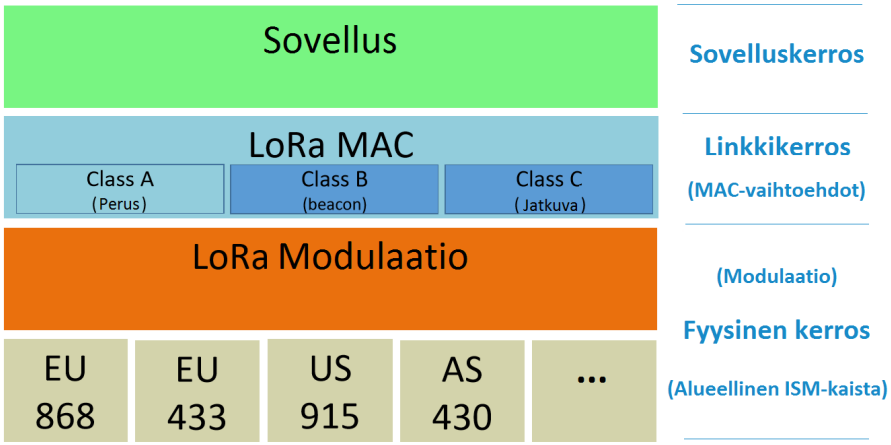
4.3 IIoT-tiedonsiirtoverkot ja -protokollat

Tässä alaluvussa esitellään IIoT-arkkitehtuuriratkaisuun valittujen IIoT-sovellusten käyttämiä tiedonsiirtoprotokollia ja -verkkoja. Valitut IIoT-sovellukset käyttävät tiedonsiirrossa hyväksi REST-rajapintaa, MQTT-, AMQP- IEC104- ja OPC/OPC UA-protokollia sekä LoRaWAN-tiedonsiirtoverkkoa. Kaikkien näiden tekniikoiden ominaisuudet eroavat toisistaan, mutta monet niistä turvautuvat samoihin tietoturvaratkaisuihin, tämä on hyvä asia tietoturvallisuuden näkökulmasta, koska tällöin sen ylläpito on helpompaa. Kun saman tietoturvallisen IIoT-sovelluksen sisällä voidaan käyttää useampaa protokolla vaihtoehtoa, niin protokolla voidaan valita aina tapauskohtaisesti, että mikä tekniikka sitten soveltuukin yritykselle, kolmannelle osapuolelle, sovellukselle tai datalle parhaiten.

4.3.1 LoRaWAN-tiedonsiirtoverkko

LoRaWAN on tähtien-tähtitopologian mukainen tiedonsiirtoverkko, jossa sensorinoodien välittämät tiedot kulkevat LoRaWAN-tukiasemien kautta ydinverkkoon ja keskitetylle verkkopalvelimelle, joko toimii keskussolmuna. Sensorinoodit sijaitsevat aina yhden hypyn päässä LoRaWAN-tukiasemista, jotka ovat taas yhteydessä keskitettyyn verkkopalvelimeen, joko matkapuhelinverkon tai Ethernetin välityksellä. LoRaWAN määrittää verkon tietoliikenneprotokollan ja järjestelmäarkkitehtuurin, jotka määrittävät yhdessä verkkokapasiteetin, palvelun laadun ja tietoturvatason. LoRaWAN:in protokollapinon ansiosta myös sensorinoodien virrankulutus on saatu todella pieneksi, sensorinoodin paristo voikin parhaimmillaan kestää noin 10 vuotta. LoRaWAN-teknologia on joustava kaksisuuntainen tiedonsiirtoteknologia, joka soveltuu monimuotoisiin käyttötapauksiin. [2] [1]

LoRaWAN-päätelaitteet jaetaan kolmeen eri luokkaan: A-, B- ja C-tyyppisiin päätelaitteisiin, niiden linkkikerroksella käyttämänsä MAC-vaihtoehdon mukaan. Lo-



Kuva 4.2: LoRaWAN-protokollapino [49]

RaWAN:in protokollapino on esitetty kuvassa 4.2. A-luokan laitteet ovat yleisimpiä ja niiden virrankulutus on muita luokkia pienempi. A-luokan laitteet ovat kaksisuuntaisia päätelaitteita, joissa jokaista päätelaitteen lähetysikkunaa seuraa kaksi lyhyttä vastaanottoikkunaa. Päätelaitteen aikataulun mukainen lähetyspaikka perustuu sen omiin viestintätarpeisiin pienellä vaihtelulla. Se onkin lähellä ALOHA-tyyppistä MAC-protokollaa. A-luokan LoRaWAN-päätelaitteet ovat tarkoitettu käyttöpaikkoihin, joissa downlink-yhteyttä ei tarvita, tai sitä tarvitaan vain uplink-yhteyksien jälkeen. Ja jos järjestelmällä yritetään lähettää downlink-viestiä muuna aikana, niin se joutuu kuitenkin odottamaan vuoroaan, kunnes päätelaite on lähettänyt seuraavan aikataulun mukaisen uplink-viestin. B-luokan päätelaite on muuten samanlainen kuin A-luokka, mutta sillä on käytössä ylimääräinen vastaanottoikkuna, joka aukeaa aikataulun mukaisesti. Jotta päätelaite pystyy avaamaan vastaanottoikkunan oikeassa aikataulussa, niin se vastaanottaa aikasynkronoidun beacon-viestin tukiasemalta. C-luokan laitteet kuluttavat eniten virtaa, koska niillä on vastaanottoikkuna lähes koko ajan auki, se sulkeutuu ainoastaan lähetyksen ajaksi. C-luokan LoRaWAN-päätelaitteilla onkin pienin latenssi, kun se mitataan palvelimelta sensorinoodille tulevista viesteissä. [49]

LoRa on LoRaWAN:in fyysinen kerros, joka mahdollistaa pitkän kantaman tiedonsiirtoyhteyden. LoRa toimii 433, 868 ja 915 MHz ISM-kaistalla, ja sen kantama on kaupungissa noin 5 km ja maaseudulla jopa 15 km. LoRan kehitti aikoinaan ranskalainen Cycleon, jonka Semtech osti vuonna 2012. LoRan fyysinen kerros ja langaton LoRa-modulaatio perustuvat CSS-modulaatioon, kun taas useat toiset langattomat

järjestelmät käyttävät FSK-modulaatiota, koska se on myös erittäin tehokas modulaatio, jos laitteelle halutaan pieni virrankulutus. CSS-modulaatio ylläpitää samoja virrankulutus ominaisuuksia kuin FSK-modulaatiokin, mutta lisää merkittävästi radion tiedonsiirtokantamaa. Yhdellä tukiasemalla voi kattaa koko pienen kaupungin eli kymmeniä neliökilometrejä. Alueen koko on tietysti riippuvainen ympäristöstä ja esteistä, mutta LoRa:n ja LoRaWAN:in tarjoama linkkibudjetti on suurempi kuin millään muulla standardoidulla tiedonsiirtoteknologialla. Suuri linkkibudjetti tarkoittaa käytännössä sitä, että alueen tukiasematiheys voi taas olla vastaavasti pieni, mikä alentaa kustannuksia. FSK-modulaatio on kuitenkin usein käytössä LoRaWAN-laitteissa LoRa-modulaation vaihtoehtona sellaisissa tapauksissa, joissa tarvitaan paikallisesti suurempaa tiedonsiirtonopeutta, FSK-modulaatiota käytettäessä se on maksimissaan 50kb/s, kun taas LoRa-modulaatiolla tiedonsiirtonopeus on pieni, parhaimmillaankin se on vain noin 11kbit/s 125kHz kaistalla, kuten taulukosta 4.1 käy ilmi. Myös viestin hyötykuorman maksimi koko M (tavua) riippuu tiedonsiirtonopeudesta. [2] [1] [29]

Taulukko 4.1: TX-tiedonsiirtonopeudet

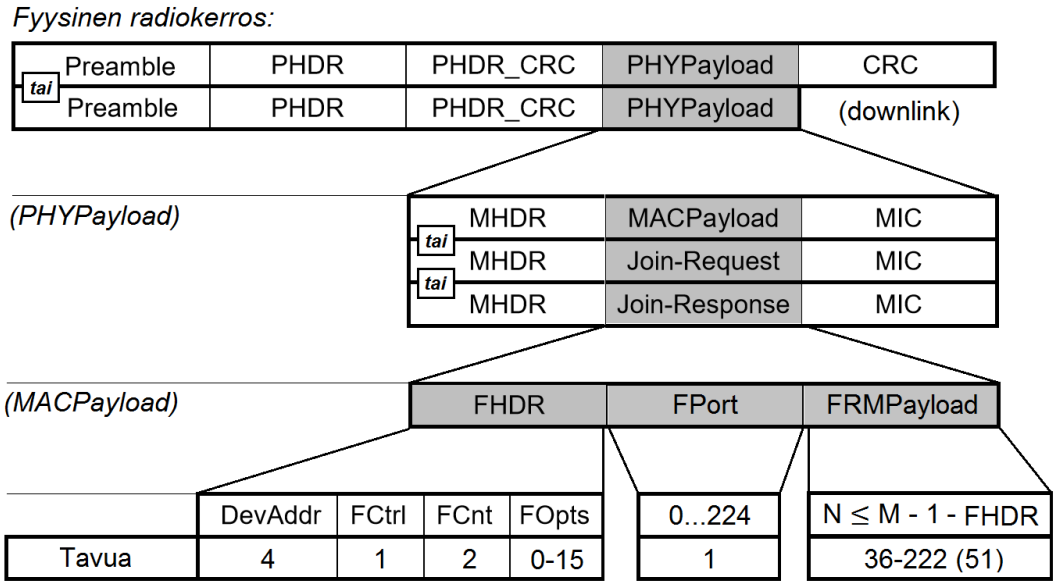
Taso	*Modulaatio*	*Levityskerroin*	*Kaistanleveys*	*Nopeus*	*M*
0	LoRa	SF12	125 kHz	250 bit/s	59
1	LoRa	SF11	125 kHz	440 bit/s	59
2	LoRa	SF10	125 kHz	980 bit/s	59
3	LoRa	SF9	125 kHz	1760 bit/s	123
4	LoRa	SF8	125 kHz	3125 bit/s	230
5	LoRa	SF7	125 kHz	5470 bit/s	230
6	LoRa	SF7	250 kHz	11000 bit/s	230
7	FSK			50000 bit/s	230

CSS-modulaatiossa taajuus kasvaa tai vähenee suhteessa aikaan. Yhtä kaistan poikki fmin-fmax nousevaa taajuuspyyhkäisyä kutsutaan up-chirp:iksi ja yhtä fmax-fmin laskevaa taajuuspyyhkäisyä down-chirpiksi. Levityskerroin (SF) kuvaa tällaiseen taajuuspyyhkäisyyn kulunutta aikaa. LoRa toimii levityskertoimilla SF7-SF12. Levityskertoimella SF7 taajuuspyyhkäisyyn kulunut aika on lyhin ja SF12:sta aika on pisin. SF-kertoimen nousu yhdellä pykälällä, kaksinkertaistaa sen ajan, jossa tietty datamäärä voidaan lähettää. Samalla kaistanleveydellä pidempi lähetysai-

ka tarkoittaa suoraan pienempää tiedonsiirtonopeutta. Teoreettinen tiedonsiirtonopeus Rb (bit/s) voidaan laskea kaavalla 4.1, jossa kaistanleveys (BW) ilmoitetaan hertseinä. [48] [13]

$$R_b = SF * \frac{1}{[\frac{2^{SF}}{BW}]} bit/s \tag{4.1}$$

LoRaWAN-verkossa lähetettävien uplink- ja downlink-viestien formaatit ovat esitelty kuvassa 4.3. LoRaWAN-viestien kokoonpano alkaa rakentua payloadista (FRMPayload) eli hyötykuormasta, joka voi olla tiedonsiirtonopeudesta ja FOpts-asetuksista johtuen 36-222 tavun kokoinen. Yleensä käytetään kuitenkin maksimissaan 51-tavun kokoista (N) payloadia. [49] [29]



Kuva 4.3: LoRaWAN-viestien formaatti

MACPayload koostuu FRMPayloadin lisäksi yhden tavun kokoisesta FPortista eli porttinumerosta ja kehyksen otsikosta (FHDR). FPort asettuu tavallisesti välille 1-223, jos kyseessä on tavallinen viesti. Jos FPort on nolla, niin se tarkoittaa, että kyseessä on MAC-ohjauskomento. Jos FPort on 224, niin kyseessä on LoRaWAN-linkkikerroksen testiprotokolla. FHDR koostuu DevAddr-osoitteen lisäksi kahdesta kehyslaskurista (FCnt), kehysasetuksista (FCtrl) ja FOpts:ista, joka sisältää 0-15 ta-

vua MAC-komentoja. FCtrl-tavu sisältää kuittauksien (ACK) käytön ja FPending-bitin, jolla palvelin kertoo laitteelle, koska viestin lähetys loppuu. [49]

PHYPayload koostuu tavun kokoisesta MAC-otsikosta (MHDR), jonka sisältämä kolmen bitin kokoinen MType-osa määrää viestin tyypin, joka voi olla: MACPayload, JOIN-pyyntö, JOIN-vastaus, datanlähetys uplink:iin tai downlink:iin. Datanlähetys voi olla joko vahvistettua tai vahvistamatonta. Koko PHYPayloadin eheys varmistetaan sen viimeisenä osana olevalla MIC-tarkistussummalla. [49]

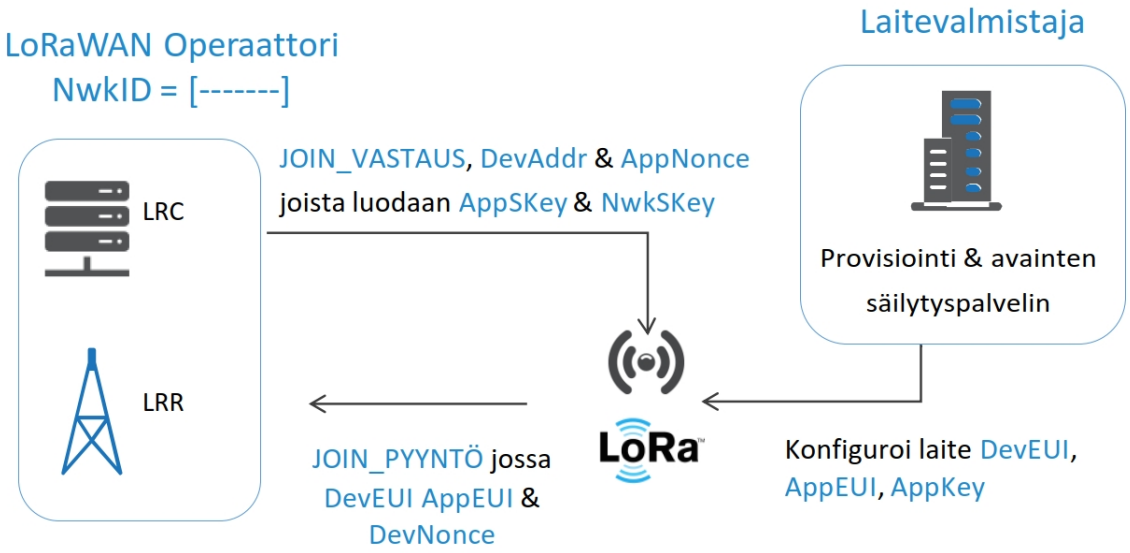
Uplink- ja downlink- viestien otsikkojen kokoonpano on fyysisellä radiokerroksella CRC:tä lukuun ottamatta sama. CRC lähetetään vain uplink-viesteissä ja sillä suojataan koko uplink-viestin eheys. LoRa-radiolähetin lisää PHYPayloadiin automaatisesti PHDR-otsikon, PHDR CRC-tarkastuksen ja koko viestin CRC-tarkastuksen. [49]

Kaikilla LoRaWAN-laitteilla on globaalisti uniikki EUI-64 tyyppinen DevEUI-osoite, jonka laitevalmistajat joutuvat hankkimaan IEEE:ltä. LoRaWAN-laitteilla on käytössä kaksi eri menetelmää, joilla ne voidaan autentikoida ja aktivoida osaksi verkkoa, nämä aktivointimenetelmät ovat OTAA ja ABP. Kummassakin aktivointimenetelmässä käytetään yksilöllisiä 128-bittisiä AES-salausavaimia, joihin LoRaWAN-verkon tietoturva perustuu. LoRa Alliancen ylläpitämän LoRaWAN 1.0.2 spesifikaation [49] mukaan aktivointiproseduurin aikana LoRaWAN-päätelaitteeseen tallennetaan seuraavat tiedot:

1.	Network Session Key	(NwkSkey)	128-bittinen AES-salausavain
2.	Application Session Key	(AppSkey)	128-bittinen AES-salausavain
3.	Application EUI	(AppEUI)	64-bittinen EUI-osoite
4.	Device Address	(DevAddr)	32-bittinen laiteosoite

Viestien autentikointi suoritetaan OTAA-aktivoinnissa NwkSkey-salausavaimella, joka jaetaan päätelaitteen ja verkkopalvelimen välillä. Eheyden tarkistus suoritetaan RFC4493 standardin mukaisella MIC-testillä. AppSkey-salausavaimella salataan viestien tietosisältö laitteen ja sovelluspalvelimen välillä. AppSkey-salausavain voidaan jakaa myös verkkopalvelimelle, jolloin viestin tietosisältö saadaan luettavaan muotoon myös siellä. AppEUI-osoite taas indentifioi verkkopalvelimen osoitteen, johon päätelaite ollaan liittämässä, ja päätelaite voidaan liittää vain yhdelle verkkopalvelimelle. 32-bittinen DevAddr-osoite koostuu Network ID-osasta (NwkID) ja Network Address-osasta (NwkAddr). NwkID-osa identifioi LoRaWAN-verkot toisistaan, koska samalla alueella voi olla useita päällekkäisiä verkkoja. DevAddr-

osoitteen seitsemän eniten merkitsevää bittiä, eli bitit paikoilla [31..25], osoittavat NwkID-osan ja loput 25 bittiä, eli bitit paikoilla [24..0], voi verkonhallitsija valita itse vapaasti. DevAddr-osoitteessa on myös prefix-osa, joka yksilöi laitteen omistavan organisaation. Actilityn verkossa prefix-osa on 0x04 tai 0x05. [51] [49]



Kuva 4.4: OTAA-aktivointimenetelmä [1]

Kun JOIN-pyyntö lähetetään, kuvassa 4.4 näkyvää dynaamista OTAA-aktivointimenetelmää käytettäessä, niin päätelaite identifioidaan DevEUI-osoitteen perusteella ja verkkopalvelin AppEUI-osoitteen perusteella. OTAA-aktivoinnissa käytetään uniikkia Application Key (AppKey) nimistä salausavainta, joka jaetaan verkkopalvelimen ja laitteen kesken. JOIN-pyyntö allekirjoitetaan AppKey-salausavaimella, ja pyynnön mukana verkkopalvelimelle lähetetään DevEUI- ja AppEUI/(JoinEUI)-osoitteet sekä kaksi tavuinen DevNonce-satunnaisavain. Näiden kaikkien tietojen perusteella lasketaan JOIN-pyynnölle neljä tavuinen MIC-tarkistussumma kaavan 4.2 mukaan. [36] [49]

$$cmac = aes128cmac(AppKey, MHDR|AppEUI|DevEUI|DevNonce)$$
$$MIC = cmac[0..3] \quad (4.2)$$

Verkkopalvelin autentikoi JOIN-pyynnön, ja lähettää tämän jälkeen JOIN-vastauksen, jos päätelaitteella on oikeus verkkoon. Jos oikeutta ei ole, niin verkkopalve-

lin ei tee mitään. Verkkopalvelin pitää lisäksi tietyn määrän jokaisen laitteen lähettämiä DevNonce satunnaislukuja muistissaan, että se pystyy estämään JOIN-pyynnöt laitteelta, joka lähettää uuden JOIN-pyynnön samalla tai hiljattain käytetyllä DevNonce-satunnaisluvulla. Tällä halutaan estää Replay-hyökkäykset, joissa lähetetään uudelleen aiemmin nauhoitettu JOIN-viesti. [49] Jotkut operaattorit käyttävät myös proseduuria, jolla he sulkevat kokonaan pois verkosta sellaiset laitteet, jotka ovat lähettäneet saman DevNonce-satunnaisluvun uudelleen. Stefano Tomasin, Simone Zulian ja Lorenzo Vangelista esittelevät artikkelissaan [52] DoS-haavoittuvuuden, jossa Join-pyyntöjen tulvalla ja DevNonce-satunnaisluvun muuntamisella saadaan verkkopalvelin pudottamaan LoRaWAN-laite pois verkosta.

Verkkopalvelin tarkastaa JOIN-pyynnön eheyden, ja jos se on kunnossa, niin se luo kolme tavuisen AppNonce-satunnaisluvun sekä NwkSkey- ja AppSkey-salausavaimet, jotka lasketaan JOIN-pyynnössä lähetettyjen tietojen perusteella kaavojen 4.3 ja 4.4 mukaan. [49]

$$NwkSKey = aes128encrypt(AppKey, 0x01| \\ AppNonce|NetID|DevNonce|pad16) \tag{4.3}$$

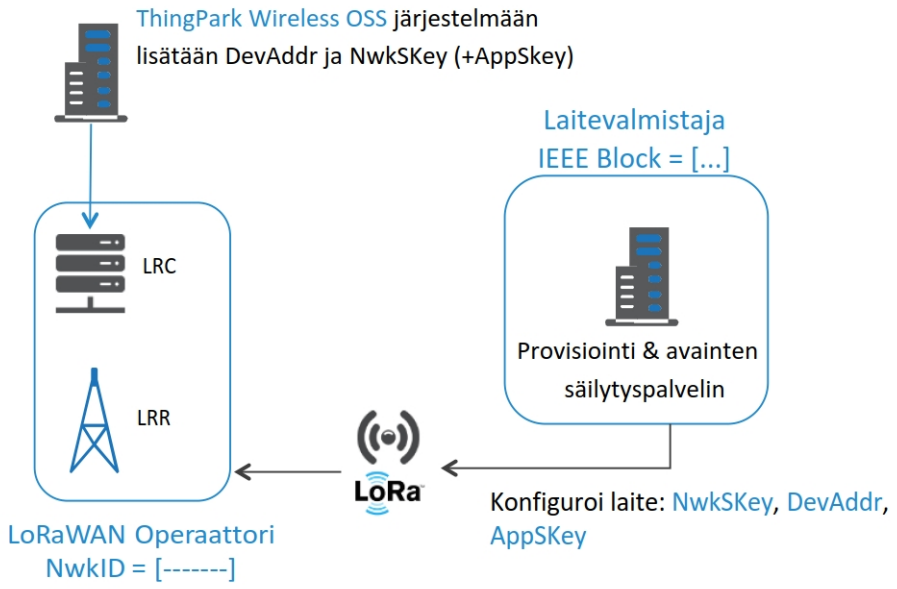
$$AppSKey = aes128encrypt(AppKey, 0x02| \\ AppNonce|NetID|DevNonce|pad16) \tag{4.4}$$

$$cmac = aes128cmac(AppKey, MHDR|AppNonce| \\ NetID|DevAddr|DLSettings|RxDelay|CFList) \\ MIC = cmac[0..3] \tag{4.5}$$

$$aes128decrypt(AppKey, AppNonce|NetID| \\ DevAddr|DLSettings|RxDelay|CFList|MIC) \tag{4.6}$$

Tämän jälkeen verkkopalvelin alkaa rakentamaan JOIN-vastausta, joka sisältää: AppNonce-satunnaisluvun, NetID:een, laitteen DevAddr-osoitteen, DL-asetukset, RF-viiveet (RxDelay) ja kanavalistan (CFList). JOIN-vastauksen eheyden turvaamiseksi sille lasketaan MIC-tarkistussumma kaavan 4.5 mukaan. Lopuksi verkkopalvelin salaa koko Join-vastauksen AppKey-salasanalla kaavan 4.6 mukaan. Kaavasta voidaan huomata, että verkkopalvelin itseasiassa salaa viestin käyttämällä AES-

dekryptausta. LoRaWAN-päätelaite pystyy näin ollen purkamaan JOIN-vastauksen käyttämällä AES-salausta ja AppKey-salausavainta. Tämän jälkeen päätelaite pystyy laskemaan AppNonce-salausavaimen perusteella nämä uudet AppSkey- ja NwkSkey-salausavaimet. Näin päätelaite on saatu aktivoitua osaksi verkkoa OTAA-aktivointimenetelmällä. [49] Kaavasta 4.5 nähtävässä JOIN-vastauksessa on myös DL-asetukset, joista laite saa tiedot downlink-konfiguraatioon. DL-asetuksien seitsemäs OptNeg- bitti kertoo, mitä LoRaWAN-spesifikaatiota verkkopalvelin käyttää. Jos bitti on 0, niin käytetään LoRaWAN 1.0.2-spesifikaatiota, jos bitti on 1, niin käytetään LoRaWAN 1.1 tai siitä uudempaa spesifikaatiota. [28]



Kuva 4.5: ABP-aktivointimenetelmä [1]

Kuvassa 4.5 näkyvää ABP-aktivointimenetelmää käytettäessä päätelaite indentifioidaan DevAddr-osoitteen perusteella. Toinen ero OTAA-aktivointimenetelmään verrattuna ovat AppSkey- ja NwkSkey-salausavaimet, jotka molemmat luodaan itse, eikä AppKey-salausavainta käytetä ollenkaan. ABP-aktivointimenetelmä voikin vaikuttaa aluksi OTAA-aktivointimenetelmää helpommalta vaihtoehdolta, koska JOIN-proseduuri on korvattu kovakoodatuilla salasanoilla. Tietoturvan kannalta kovakoodattujen salasanojen jakelu ja säilyttäminen aiheuttaa kuitenkin haasteita, kuten alaluvussa 2.1.2 käytiin läpi. Dynaamisen OTAA-aktivointimenetelmän käyttö onkin usein tieturvan, joustavuuden ja skaalautuvuuden kannalta perusteltu ratkaisu. [51] [49]

4.3.2 MQTT-protokolla

MQTT-protokolla on avoimen lähdekoodin viestiprotokolla, joka perustuu julkaisija-tilaajamalliin, jossa julkaisija (publisher) julkaisee tiedon välittäjälle (broker), josta tilaaja (subscriber) on tilannut tiedon. MQTT-protokolla on yksinkertainen ja kevyt, mutta sillä on alhainen tiedonsiirtonopeus ja korkea latenssi. Nämä ominaisuudet tekevät siitä ihanteellisen käytettäväksi rajoitetuissa ympäristöissä, joissa verkon käyttö on esimerkiksi kallista, tiedonsiirtonopeus on pieni tai tiedonsiirto on epäluotettavaa. Se soveltuu käytettäväksi myös sulautetuissa laitteissa, joilla on rajoitettu prosessointi- ja muistikapasiteetti. Kuljetuskerroksella MQTT-protokolla käyttää luotettavaa TCP-protokollaa. MQTT-protokolla ei välitä hyötykuorman sisällön muodosta, eikä sille ole määritelty ulkoasua tai sitä, miten tiedot tulee esittää. MQTT tarjoaa asiakkaan ja palvelimen väliselle tiedonsiirrolle kolme QoS-laatutasoa:

QoS 0 Viesti välitetään enintään yhden kerran. Tällöin on mahdollista, että viesti ei välity lainkaan, koska sen jakelussa ei käytetä kuittauksia. Viestiä ei tallenneta ja se voi kadota, jos asiakkaan yhteys katkeaa tai välityspalvelin kaatuu. Lähetysnopeudessa tapa on nopein.

QoS 1 Viesti välitetään ainakin yhden kerran. PUBLISH-viesti lähetetään ja tallennetaan lähettäjälle siksi aikaa, kunnes PUBACK-kuittaus on saapunut välittäjältä. Jos kuittausta ei tule, niin lähettäjä voi joutua välittämään viestin useita kertoja. Duplikaattiviestejä voi syntyä.

QoS 2 Viesti välitetään tasan yhden kerran. Lähettäjä lähettää PUBLISH-viestin, jonka välittäjä kuittaa PUBREC-viestillä vastaanotetuksi ja julkaistuksi. Lähettäjä kuittaa PUBREC-viestin PUBREL-viestillä. PUBREL-viestin lähetyksen jälkeen lähettäjä ei enää lähetä PUBLISH-viestiä uudelleen ja välittäjä poistaa alkuperäisen viestin ja lähettää PUBCOMP-viestin takaisin lähettäjälle. Tämän jälkeen myös lähettäjä poistaa viestn. Edellistä viestiä (sis. ID ja DUP-flag) lähetetään jokaisessa kättelyvaiheessa uudestaan niin monta kertaa, että viesti on kuitattu. Myös viestin ID tarkastetaan. Duplikaattiviestejä ei synny, mutta lähetysnopeudessa tapa on hitain.

MQTT-protokollalla voidaan liittää internettiin useita erilaisia IoT-alustoja, sekä sitä voidaan käyttää viestiprotokollana myös antureiden, toimilaitteiden ja palvelimien välillä, mikä tekee siitä monikäyttöisen ja tärkeän viestiprotokollan IoT-

järjestelmien rakentamisessa. Viestien salauksessa käytetään SSL/TLS-salausprotokollaa, ja käyttäjien autentikointiin voidaan käyttää MQTT3.1 versiossa käyttäjänimeä ja salasanaa, jotka lähetetään viestien mukana. [26] [16] [27]

4.3.3 AMQP-protokolla

AMQP-protokolla on avoimen standardin viestijonoprotokolla, jota käytetään sovelluskerroksen viestipalveluiden, kuten: jonotuksen, reitityksen, tietoturvan ja luotettavuuden tuottamiseen. AMQP-protokollaa voidaankin pitää viesteihin erikoistuneena väliohjelmistona, ja sen avulla asiakkaat voivat saavuttaa vakaan ja luotettavan viestien välityksellä, vaikka asiakkaat olisivatkin ohjelmoitu eri ohjelmointikielillä. AMQP-protokolla toteuttaa lisäksi erilaisia viestinvaihtoarkkitehtuureita, kuten tallenna-välitämallia, julkaisija-tilaajamallia, viestien jakamista, viestien jonotusta, kontekstipohjaista reititystä ja piste-piste reititystä. AMQP-protokollalla on käytössä samat QoS-laatutasot kuin MQTT-protokollalla. Tietoturvaan käytetään pääasiassa SSL/TLS-salausprotokollaa, mutta näiden lisäksi voidaan käyttää myös SASL-menetelmää. [26] [4]

4.3.4 REST-rajapinta

REST on HTTP-protokollaa ja -metodeja hyväksikäyttävä viestirajapinta, joka perustuu yksinkertaiseen pyyntö-vastausmalliin, jossa REST-asiakkaat tekevät HTTP-pyyntöjä REST-palvelimille. Palvelimet käsittelevät HTTP-pyynnöt ja palauttavat vastaukset asiakkaalle internetin yli. REST ei tarjoa asynkronista ja löyhästi kytkettyä julkaisija-tilaajamallista tiedonsiirtoa kuten MQTT, vaan siinä asiakas ja palvelin ovat suoraan yhteydessä toisiinsa. REST on yhteensopiva useimpien alustojen ja laitteiden kanssa, koska niiden ei tarvitse kuin kyetä kommunikoimaan HTTP-protokollan avulla. REST-rajapinnan viestien välityksen ja palvelun laadun takaa kuljetuskerroksella käytetty luotettava TCP-protokolla. REST-rajapinnan ja HTTP-protokollan kanssa voidaan kuljetuskerroksella käyttää myös epäluotettavaa UDP-protokollaa, mutta se ei ole niin yleistä kuin TCP-protokollan käyttö. REST:in tietoturvasta ja viestien salauksesta vastaa AMQP- ja MQTT-protokollien tapaan HTTPS-yhteydessä käytetty SSL-salausprotokolla tai vaihtoehtoisesti uudempi TLS-salausprotokolla, jotka molemmat tarjoavat HTTP-asiakkaalle ja -palvelimelle epäsymmetrisen salauksen avaintenvaihdossa ja symmetrisen salauksen tiedonsiirron aikana. [16]

4.3.5 OPC/OPC UA-protokolla

OPC-protokolla tai -liittymä on avoimen tiedonsiirron standardi, joka määriteltiin alun perin vuonna 1995 Microsoftin ja useiden eri automaatiotoimijoiden kesken. Aluksi OPC-standardi rajoittui vain Windows-käyttöjärjestelmään, ja se pohjautuukin Microsoftin tekniikoihin, kuten OLE ja DCOM-teknologioihin. OPC lyhenne syntyi sanoista OLE, eli objektin linkittäminen ja upottaminen, sekä prosessinhallinta. OPC on itse asiassa teollisuusautomaatiojärjestelmien yhteentoimivuusstandardi, jolla taataan tietoturvallinen ja luotettava tiedonvaihto eri valmistajien laitteiden kesken. OPC-Foundation vastaa standardin kehittämisestä ja ylläpidosta. OPC on asiakas–palvelinmalliin perustuva viestiprotokolla, jossa on käytössä kaksi eri tiedonhakumenetelmää. On pollaava tiedonhaku, jossa asiakas pyytää tietoja palvelimelta, ja on tapahtumapohjainen tiedonhaku, jossa palvelin toimittaa tiedot asiakkaalle muutostilanteissa. OPC-standardi on sarja spesifikaatioita, joilla määritellään esimerkiksi asiakkaan ja palvelimen sekä palvelimen ja palvelimen väliset rajapinnat, kuten pääsyn reaaliaikaisiin tietoihin, historiatietoihin, hälytystietoihin ja muihin tapahtumiin. OPC Classic sisältää seuraavat protokollat: Data Access (DA), Alarms and Events (AE), Historical Data Access (HDA), XML Data Access (XML DA) ja Data eXchange (DX). [41] [42]

OPC Classic protokollien lisäksi OPC Foundation kehitti uuden OPC UA (Unified Architechture) standardin, koska uudet palvelusuuntautuneet arkkitehtuurit alkoivat yleistyä teollisessa valmistuksessa, ja niiden myötä alkoi nousta esille myös uusia haasteita tietoturvan ja datamallinnuksen osa-alueilla. OPC UA on mallipohjainen ja alustariippumaton viestiprotokolla, joka rakentuu TCP/IP-protokollien päälle. OPC UA standardia voidaan käyttää useilla eri alustoilla, kuten Windowsilla, Linuxilla, Androidilla ja Applen OSX:llä. Se ei myöskään pohjaudu OLE- tai DCOM-tekniikoihin, ja tämän vuoksi OPC-Foundation sanookin OPC lyhenteen tulevan nykyisin sanoista "Open Platform Communications". OPC UA:lla voidaan käyttää myös struktuureja ja tietomalleja, jotka mahdollistavat esimerkiksi sen, että tägejä voidaan ryhmitellä ja niille pystytään luomaan kontekstia. [41] [42]

OPC UA-protokollan tietoturvamalli pohjautuu avoimen lähdekoodin OpenSSL-kirjastoon ja X.509 sertifikaattien käyttöön. OPC UA-protokolla on suunniteltu vastaamaan monien erilaisten järjestelmien vaatimuksiin tietoturvan ja hallinnon osa-alueilla. OPC UA-protokollaa käytettäessä jokaisen sovelluksen asennuksen yhteydessä tulee määritellä sovellukselle yksilöllinen sertifikaatti, joka yksilöi sovelluksen tai laitteen, joka sitä käyttää. Sertifikaateilla luodaan salattuja viestintäkanavia,

joiden liikennettä kolmannet osapuolet eivät voi tarkastella tai manipuloida. Sertifikaateilla tunnistetaan verkon eri pisteet toisistaan. OPC UA-protokollan tietoturvamalli tarjoaa neljä eri tasoa autentikointiin ja kaksi tapaa sertifikaattien hallintaan. Ensimmäisellä autentikointitasolla ei autentikointi ole ollenkaan käytössä, ja asiakas ja palvelin antavat minkä tahansa laitteen kommunikoida kanssaan, mikä tarkoittaa sitä, että kaikki voimassa olevat sertifikaatit hyväksytään ja todetaan luotettaviksi. Tällä menetelmällä sertifikaatin vastaanottajalla ei ole mitään keinoa tietää, onko lähettäjä sertifikaatin oikeutettu haltija. Toisella autentikointitasolla palvelin sallii minkä tahansa asiakkaan muodostaa yhteyden kanssaan, ja käyttäjän autentikointi tapahtuu lähettämällä käyttäjätunnukset eli käyttäjänimi ja salasana. Asiakkaat joudutaan kuitenkin konfiguroimaan siten, että ne luottavat palvelimeen. Se tapahtuu laittamalla palvelimen sertifikaatti tai palvelimen tunnistaneen sertifikaattiviranomaisen (CA) tiedot asiakkaan hyväksyttyjen sertifikaattien listalle. Kolmannella autentikointitasolla asiakas voi muodostaa yhteyden minkä tahansa palvelimen kanssa, mutta palvelin sallii vain luotettujen asiakkaiden muodostaa yhteyden kanssaan. Asiakkaille ei tarvitse tässä tapauksessa tehdä muuta konfiguraatiota kuin ilmoittaa palvelimen URL-osoite. Palvelin luottaa kuitenkin vain sellaisiin asiakkaisiin joiden sertifikaatti tai sertifikaattiviranomaisen tiedot ovat niiden listalla. Neljäs autentikointitaso on yhdistelmä tasoista kaksi ja kolme, jolla sekä palvelin että asiakas joudutaan konfiguroimaan siten, että ne molemmat tarkastavat toistensa sertifikaatit tai tunnistuksen tehneen sertifikaattiviranomaisen tiedot. Neljäs autentikointitaso tarjoaa parhaan tietoturvan, ja se onkin ohjelmistoissa yleensä aina oletusasetuksena päällä. Sertifikaatteja voidaan puolestaan hallita ja tallentaa joko suoraan hakemistoihin tai sitten Windowsin sertifikaattisäilöön, jolloin ne ovat käytettävissä käyttäjäprofiilin mukaan joko kaikilla tietokoneen käyttäjillä tai pelkästään tietyn käyttäjän tilillä. [7]

4.3.6 IEC104-protokolla

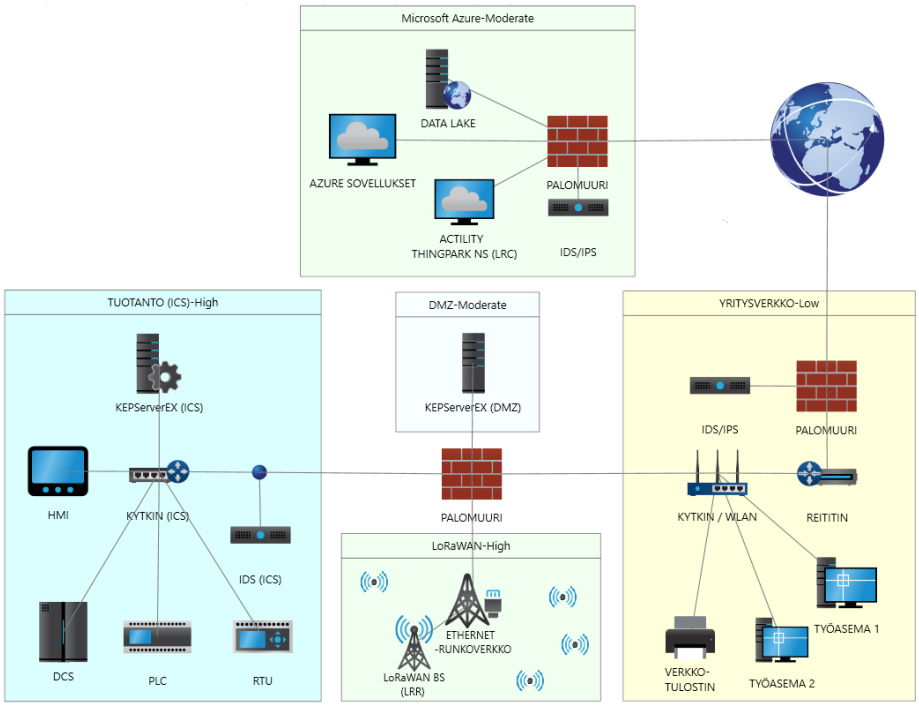
IEC 60870-5-104-protokolla (IEC104) on osa IEC 60870-5 Telecontrol Equipment and Systems -standardiperhettä, joka tarjoaa menetelmät televiestien lähettämiseen kahden automaatiojärjestelmän välillä. Alunperin protokolla suunniteltiin sähköverkonvalvontajärjestelmien väliseen televiestintään, mutta nykyisin sitä käytetään usein myös SCADA-järjestelmissä RTU-laitteiden ja PC-sovellusten välillä. IEC104-protokollan viestintä perustuu asiakas-palvelinmalliin, ja sen verkkotopologiana käytetään yleisimmin point-to-point tai multiple point-to-point-topologioita. Käytän-

nössä IEC104-protokolla mahdollistaa IEC 60870-5-101-protokollan (IEC101) mukaisen viestinnän tavallisen TCP/IP-yhteyden kautta. Sovelluskerroksen IEC101-protokollalla on kaksi erilaista lähetysproseduuria, jotka ovat balansoitu ja balansoimaton lähetys. Balansoimattomassa lähetysproseduurissa master-keskus voi pollata sekvensoiduilla REQUEST/RESPOND-viesteillä tietoja slave-keskukselta. Master-keskus voi myös lähettää SEND/CONFIRM-viestejä slave-keskukselle, joilla se voi muuttaa tämän asetusarvoja tai ohjata sitä. Balansoidussa lähetysproseduurissa kaikki keskukset voivat käynnistää lähetyksen SEND/CONFIRM-viesteillä, tällöin keskukset voivat toimia sekä master- että slave-keskuksina samanaikaisesti. Balansoiduissa ja balansoimattomissa lähetyksissä on myös mahdollista käyttää broadcast-tyyppisiä SEND/NO REPLY-viestejä, jolloin ohjausviestit välittyvät useille slave-keskuksille samanaikaisesti. IEC104-protokollaan ei ole määritelty mitään tietoturvaominaisuuksia, kuten käyttäjien autentikointia tai viestien salausta. IEC104-protokolla onkin monen muun SCADA-tiedonsiirtoprotokollan tavoin haavoittuvainen lukuisille kyberhyökkäystyypeille, jos sitä käytään muualla kuin tehtaiden sisäverkoissa. Tehtaan ulkopuolelle sitä ei tulisikaan käyttää ilman asianmukaista salausmenetelmää. IEC104-protokollan salausmenetelmäksi soveltuu esimerkiksi VPN-tunneli. [32]

4.4 Tietoturva

Tässä alaluvussa kerrotaan esitettyyn IIoT-arkkitehtuuriratkaisuun käytetyistä tietoturvamenetelmistä ja tietoturvauhkista, joita ratkaisulla pystytään välttämään. Kuvassa 4.6 on esitelty IIoT-arkkitehtuuriratkaisun pohjalta suunniteltu yksinkertaistettu verkkodiagrammi, jota voidaan käyttää hyväksi, kun halutaan arvioidaan järjestelmän kyberturvallisuutta. Verkkodiagrammi on suunniteltu CSET-kyberarviointityökalulla, joka esiteltiin alaluvussa 3.1.1. Verkkodiagrammissa on nähtävissä kaikki IIoT-arkkitehtuurissa käytetyt pääkomponentit, kuten: verkon osat ja vyöhykkeet, palomuurit, tukiasemat, IDS/IPS-järjestelmät ja IIoT-sovellukset. Tiedonsiirto automaatiojärjestelmistä pilvipalveluun jakautuu IIoT-arkkitehtuuriratkaisussa kahteen eri tiedonsiirtoreittiin, joiden molempien tietoturvamenetelmät poikkeavat osittain toisistaan. Monessa kohdassa tiedonsiirtoreitillä on taas useita tietoturvakerroksia päällekäin, joka parantaa järjestelmän kykyä torjua erilaisia kyberhyökkäyksiä. Kuvasta 4.6 voidaan nähdä, että prosessi- ja IoT-datan siirtämiseen tarvitaan useita hyppyjä järjestelmästä toiseen ennen kuin data on saatu siirret-

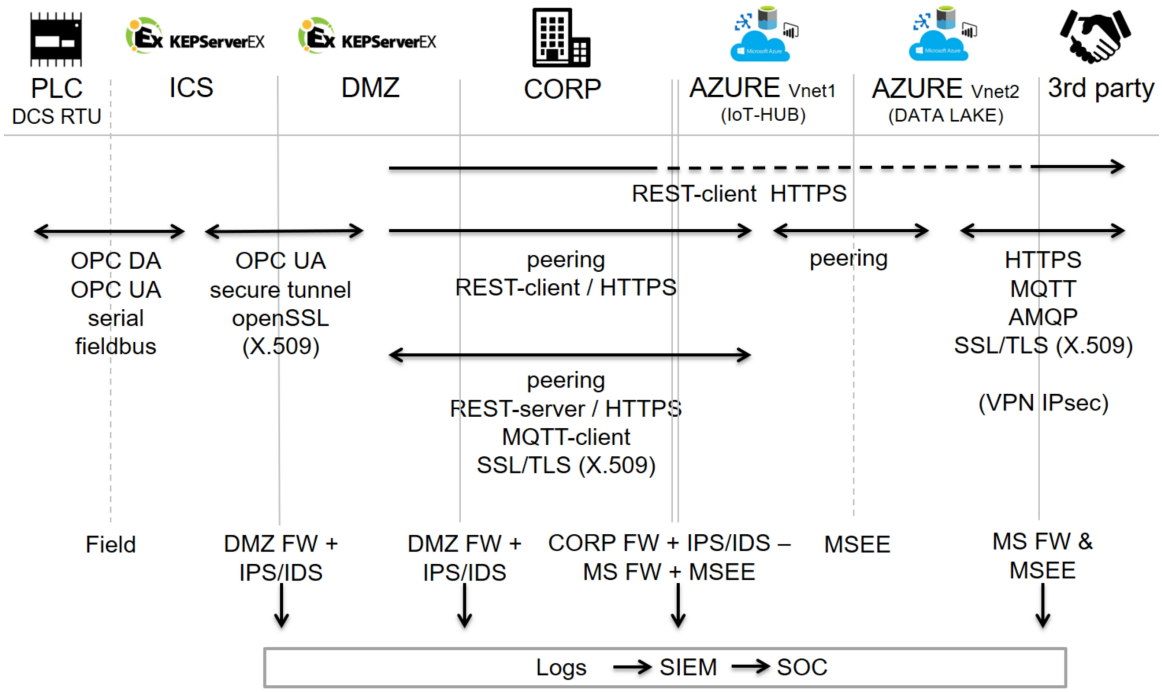
tyä anturilta pilveen. Data kulkeen matkallaan myös useiden verkkoalueiden läpi, joita ovat: automaatioverkon alue (ICS), LoRaWAN-verkon alue, DMZ-alue, laajemman yritysverkon alue, Internet-alue ja Azuren virtuaaliverkon alua. Kaikille näille verkkoalueille on asetettu erilaiset kyberturvatasot. Automaatioverkon alueella on käytössä korkein kyberturvataso, koska siellä data ja ohjauskäskyt linkittyvät fyysisen maailman kanssa järeiden tuotantolaitteiden kautta. Tämä sisältää luonnollisesti myös korkeamman kyberriskin, koska alueella työskentelee ihmisiä, joiden työturvallisuus tulee olla etusijalla kaikessa yritystoiminnassa. Automaatioverkkoa suojataan omalla DMZ-alueella, jolla estetään suora yhteydenpito ulkopuolelta automaatioverkon laitteiden kanssa. Myös LoRaWAN-verkon alue määritellään diagrammissa korkealle kyberturvatasolle, koska LoRaWAN-sensorinoodit voivat olla yhteydessä tuotantokoneisiin tai jopa osa niitä. DMZ-alue on arvioitu CSET-ohjelmistossa kohtalaisen kyberturvatason alueeksi, koska se sijaitsee korkean tason automaatioverkon ja matalan tason yritysverkon välissä. Azure-virtuaaliverkon kyberturvataso pitää arvioida ainakin kohtalaiseksi, koska sieltä voi olla yhteyksia useampiin tehtaiden paikallisverkkoihin, ja näin yhteyksien määrä alkaa kasvattamaan kyberriskiä.



Kuva 4.6: IIoT-verkkodiagrammi

4.4.1 Prosessidatan siirtoyhteys

Prosessidatan siirtäminen pilveen alkaa automaatiojärjestelmään liitetystä anturista, kun se muuntaa jonkin mitattavan fyysisen suureen virta- tai jänniteviestin muodossa olevaksi dataksi, jonka sitten tehtaan automaatioverkossa sijaitsevat PLC-logiikat, DCS-järjestelmät tai RTU-yksiköt pystyvät lukemaan. Nykyisin anturit lähettävät datan eteenpäin usein myös sarjaväylätekniikalla tai TCP/IP-yhteensopivilla kenttäväylillä, jolloin PLC-taso jää yhä useammin välistä pois kokonaan. Anturilta lähtiessään data kulkee yleensä salaamattomana, mutta kun anturikaapelit sijaitsevat fyysisesti tehdasalueella, niin kyberuhka datan manipuloinnista on aika pieni.



Kuva 4.7: Prosessidatan siirtoyhteyden tietoturva

Ensimmäisessä täysin digitaalisessa tiedonsiirtovaiheessa data luetaan PLC-logiikasta KEPServerEX(ICS)-palvelimelle, ja lukeminen tapahtuu logiikasta riippuen joko OPC DA- tai OPC UA-protokollalla, sarjaliikenteellä tai kenttäväylällä, kuten kuvasta 4.7 käy ilmi. Data kulkee tässäkin vaiheessa usein vielä salaamattomana tehtaan automaatioverkon alueella. Kun PLC-logiikat aikanaan uudistuvat, niin ne voidaan konfiguroida käyttämään X.509-sertifikaatteja ja salattua OPC UA-viestintää. Kun kaikki viestintä salataan, niin tämä estää selkotekstimuodossa olevien salasanojen ja käyttäjätunnusten leviämisen tehtaan automaatioverkossa.

Toisessa tiedonsiirtovaiheessa ICS-alueella sijaitsevan KEPServerEX(ICS)-palvelimen ja DMZ-alueella sijaitsevan KEPServerEX(DMZ)-palvelimen välille muodostetaan salattu OPC UA-tunneli, jossa KEPServerEX(DMZ) toimii OPC UA asiakkaana ja KEPServerEX(ICS) OPC UA palvelimena. Tunnelia varten alueiden väliseen DMZ-palomuuriin joudutaan avaamaan portti. Tunnelia konfiguroitaessa KEPServerEX (DMZ)-palvelimelle annetaan KEPServerEX(ICS)-palvelimen URL muodossa *opc.tcp://<palvelimenIP>:<porttinumero>*, sekä valitaan yhteydelle salauspolitiikka vaihtoehdoista: *None*, *Basic128Rsa15* tai *Basic256* ja viestimoodi vaihtoehdoista: *None*, *Sign* tai *Sign and Encrypt*. Salattu OPC UA-viestintäkanava tulisi muodostaa käyttämällä *Basic256* salauspolitiikkaa ja *Sign and Encrypt* viestimoodia, koska ne tarjoavat vaihtoehdoista korkeimman tietoturvatason. KEPServerEX(ICS)-palvelin voidaan konfiguroidaan OPC UA palvelimeksi, kun sille annetaan asetuksissa URL-päätepiste muodossa *opc.tcp://<IP/hostname>:<porttinumero>*, jonka jälkeen palvelimelle asetetaan salauspolitiikka vaihtoehdoista: *None* , *Basic128Rsa15* tai *Basic256*. Viestimoodi valitaan vaihtoehdoista: *Sign*, *Sign and Encrypt* tai *Sign; Sign and Encrypt*. Palvelimelle voidaan salauspolitiikaksi valita molemmat *Basic128Rsa15* ja *Basic256*, ja näille viestimoodeiksi *Sign; Sign and Encrypt*, jolloin sekä asiakas että palvelin autentikoidaan sekä viestintä salataan. Tämän jälkeen X.509-sertifikaatit vaihdetaan asiakkaan ja palvelimen välillä, tämä tapahtuu helpoilla *Export-* ja *Import*-komennoilla, joilla ne saadaan lisättyä luotettujen palvelinten tai asiakkaiden listalle. Eri kyberturvatason alueilla sijaitsevien palvelimien ja asiakkaiden välinen viestintä tulee aina salata mahdollisuuksien mukaan, vaikka ne olisivatkin fyysisesti yrityksen sisäverkossa. Alueiden välisen palomuurin yli kulkevaa viestintää olisi myös hyvä seurata jollain IDS-järjestelmällä, jotta pystytään varmistumaan siitä, että järjestelmän tietoturva toimii myös syvyyssuunnassa. KEPServerEX-palvelimelle pystytään luomaan käyttäjille henkilökohtaiset käyttäjäprofiilit, joilla käyttäjiä mahdollisuuksia voidaan kontrolloida, ja poistaa heiltä turhat käyttöoikeudet. Käyttäjien pääsynhallinta on myös yksi CSET-ohjelmistolla tehtävän kyberriskianalyysin pääkohdista.

Kolmannessa tiedonsiirtovaiheessa dataa lähetetään ja vastaanotetaan DMZ-alueen KEPServerEX-palvelimen ja Microsoftin Azure-pilvipalvelun välillä. Tätä varten KEPServerEX(DMZ)-palvelimelle joudutaan asentamaan IoT-Gateway-lisämoduuli, jonka avulla pystytään luomaan MQTT-protokollaa käyttävä MQTT-agentti, REST-asiakasagentti tai REST-palvelinagentti, jotka pystyvät kommunikoimaan Azuren IoT-Hubin kanssa. Dataa voidaan lähettää JSON, XML, CSV tai täysin mukaute-

tussa formaatissa. REST-asiakasagentilla voidaan lähettää dataa turvallisesti HTTPS-yhteyden kautta myös suoraan kolmannen osapuolen pilveen, jos kaikkea dataa ei haluta viedä yrityksen omaan Azure-pilveen.

MQTT-agentin tietoturva perustuu MQTT-protokollan tukemaan perusautentikointiin ja SSL-salaukseen, joka onkin syytä ottaa käyttöön kolmannen osapuolen MQTT-välittäjän ja IoT-Gateway:n MQTT-agentin välillä. Ja koska MQTT-agentin tehtävänä on lähettää ja vastaanottaa dataa ulkopuolisen MQTT-välittäjän kanssa, on tällöin tärkeää, että myös MQTT-välittäjän tietoturvasta huolehditaan ja kaikki tietoturvapäivitykset tehdään toimittajan ohjeiden mukaisesti. Jotkut MQTT-välittäjät voivat olla konfiguroituja hyväksymään sekä SSL-salatut että -salaamattomat yhteydet samanaikaisesti. Onkin tärkeää varmistaa, että salaus on käytössä, koska muuten kaikki viestintä lähetetään selkotekstinä. MQTT-agentin ja -välittäjän välinen autentikointi voidaan tehdä molempiin suuntiin sertifikaateilla, jolloin autentikoinnissa käytetään TLS-salausta, josta tulisi käyttää aina uusinta versiota, tällä hetkellä on käytössä versio 1.2. Sertifikaatti ladataan *Import*-komennolla KEPServerEX-palvelimen asetuksissa. Välittäjä voi autentikoida asiakkaan myös perusautentikointia käyttämällä, mutta TLS-salauksen ja X.509 sertifikaattien käyttö on kuitenkin suositeltavaa. Datalle voidaan MQTT-välittäjäohjelmistosta riippuen merkitä myös aihekohtaiset luku- ja kirjoitusoikeudet. Kirjoitusoikeutta ei pitäisi kuitenkaan jakaa kuin tarpeesta ja ainoastaan autentikoiduille MQTT-asiakkaille. Koska muuten on mahdollista, että joku MQTT-asiakas pääsee injektoimaan tai manipuloimaan aihetta, jonka MQTT-agentti on tilannut. Perusautentikoinnilla on myös mahdollista rajata eri toimijoiden lukuoikeutta. Muita keinoja MQTT-tietoliikenteen turvaamiseksi ovat VPN-putken tai yksityisen LAN-verkon käyttö, mutta silloinkin perusautentikointia ja SSL-salausta on syytä käyttää. IoT-Gateway:n MQTT-agenttia ei ole myöskään hyvä asettaa tilaamaan aihetta, joka sijaitsee avoimella ja suojaamattomalla MQTT-välittäjällä. [23]

IoT-Gateway:n REST-asiakasagentin tietoturva pohjautuu taas pääasiassa siihen, miten siihen yhteydessä olevan kolmannen osapuolen REST-palvelin on konfiguroitu, ja mitä tietoturvamenetelmiä se käyttää. REST-asiakasagentti pystyy ainoastaan yksisuuntaisesti julkaisemaan viestejä, ja sillä on ainoastaan lukuoikeus tägeihin, eikä lainkaan kirjoitusoikeutta. REST-asiakasagentti tukee sekä salattuja että salaamattomia yhteyksiä REST-palvelimen kanssa. HTTPS-yhteyden käyttäminen on suositeltavaa, koska HTTP-yhteydellä perusautentikoinnissa käytetyt käyttäjänimet ja salasanat kulkevat selkotekstinä. On myös suositeltavaa, että kolman-

nen osapuolen REST-palvelin konfiguroidaan ottamaan vastaan ainoastaan HTTPS POST-pyyntöjä autentikoiduilta käyttäjiltä. Kun käyttäjätunnisteet ovat ensin asetettu REST-palvelimelle, ne voidaan sen jälkeen asettaa myös REST-asiakasagentille. VPN-putken tai yksityisen paikallisverkon käyttö vähentää myös datan ja järjestelmän haavoittuvuutta. [23]

REST-palvelinagentin tietoturvamenetelmät konfiguroidaan IoT-gateway:ssä, jonne asetetaan perusautentikointi ja konfiguroidaan REST-palvelinagentti käyttämään HTTPS-yhteyttä, joka onkin päällä aina oletusasetuksena. IoT-gateway:llä pystytään luomaan oletusasetuksen mukaiset X.509-sertifikaatit, vaikka REST-palvelinagentti pystyykin käyttämään myös CA:n luomia sertifikaatteja. Oletusasetuksena myös anonyymi kirjautuminen on poistettu käytöstä, ja REST-asiakkaan ja -palvelimen perusautentikointiin vaaditaan käyttäjänimi ja salasana, jotka konfiguroidaan KEPServerEX(DMZ)-palvelimen asetuksissa. Asetuksissa voidaan antaa eri käyttäjille tapauskohtaisesti erilaiset tagien luku- ja kirjoitusoikeudet. REST-palvelinagentin käyttämissä tageissä onkin oletusasetuksena ainoastaan lukuoikeus, vaikka käyttäjäprofiilin asetuksiin olisikin tallennettu muuta. Kirjoitusoikeutta ei tulisi antaa tarpeettomasti, koska muuten on vaarana se, että tägeihin tulee kirjoitettua jotain sinne kuulumatonta. [23]

IoT-Gateway:n agentit yhdistetään Azuren IoT-hubin kanssa peering-siirtoyhteyden avulla, ja yhteyden salaamiseen käytetään joka SSL- tai TLS-salausta agentista riippuen. Samalle virtuaalikoneelle KEPServerEX(DMZ)-palvelimen kanssa joudutaan asentamaan Microsoftin Device Explorer -työkalu, jolla salattu yhteys saadaan luotua. Aluksi kopioidaan IoT-Hubista Device Exploreriin *IoT Hub Connection String*, joka sisältää seuraavat IoT-Hubin tiedot: *URL*, *Shared Access Key Name* ja *Shared Access Key*. Tämän jälkeen valitaan Device Explorerista salausmenetelmäksi X.509-sertifikaatit. Agentin sertifikaattia ei tarvitse vaihtaa IoT-hubin kanssa, vaan riittää, että sertifikaatin yhteydessä oleva "sormenjälki" kopioidaan Device Explorer -työkalulla luodun laitteen asetuksiin. KEPServerEX(DMZ)-palvelimen asetuksiin taas kirjoitetaan konfiguroinnin yhteydessä Azuren IoT-Hubin tiedot: URL muodossa *ssl://<Azure IoT Hub nimi>:<portti>*, käyttäjätunnukset, salasanat, laite ID ja mahdolliset aiheet.

Neljännessä tiedonsiirtovaiheessa dataa vaihdetaan Azure-virtuaaliverkkojen välillä, jolloin data siirretään tapauskohtaisesti joko peering-yhdyskäytävällä Microsoftin runkoyhteyden kautta tai ExpressRoutea käyttämällä, jolloin virtuaaliverkot yhdistetään Microsoftin MSEE-reunareitittimen kautta. Microsoft tarjoaa tällöin oman

salauksensa virtuaaliverkkojen välisiin yhteyksiin. Azuren virtuaaliverkosta voidaan siirtää dataa helposti myös alihankkijoiden virtuaaliverkkoihin tai toimipisteisiin, tällöin on kuitenkin syytä ottaa VPN-yhteys ja SSL/TLS-salaus käyttöön. Myös tietoliikennettä kolmannen osapuolen järjestelmiin on hyvä seurata esimerkiksi SIEM-järjestelmällä. Lisäksi on syytä poistaa kaikki turhat oikeudet alihankkijoilta, jotta he eivät esimerkiksi pääse vahingossa ylikirjoittamaan tägejä tai muuttamaan asetuksia. Tiedonsiirtoyhteys alihankkijan suuntaan on hyvä pitää aina yksisuuntaisena, jos se on vaan mahdollista. Azure-virtuaaliverkkoon voidaan tehdä tarvittaessa myös oma DMZ-alue, jonka kautta tiedonsiirrot suoritetaan.

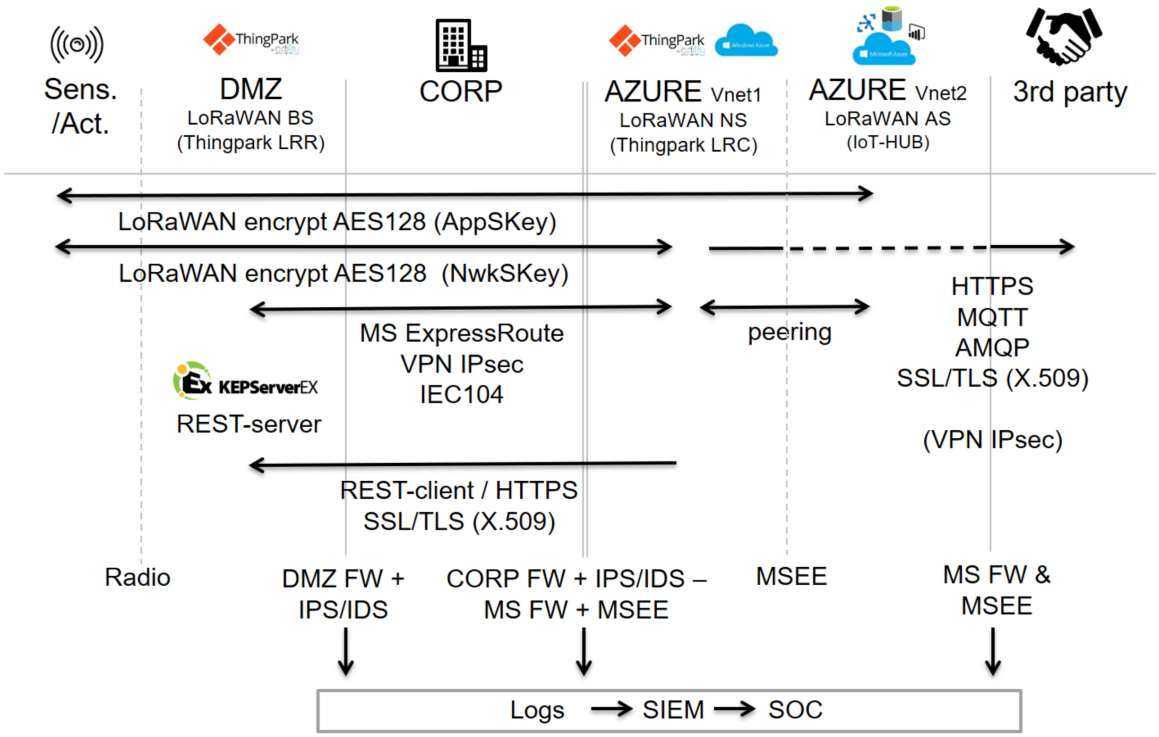
DMZ- ja CORP-palomuurien on tarkoituksena estää suora liikenne yritysverkon ulkopuolelta ICS-alueelle. Tätä toimintoa varten palomuurien asetuksiin konfiguroidaan tiukat palomuurisäännöt valkolistausmenetelmää hyväksikäyttäen. Palomuureihin integroiduilla IPS/IDS-toiminnallisuuksilla voidaan suorittaa väärinkäytösten ja poikkeamien havainnointia. Lisäksi näistä järjestelmistä pystytään keräämään lokitietoja, jotka kootaan SIEM-järjestelmään. Yrityksen tietoturvakeskus seuraa taas SIEM-järjestelmää, ja konfiguroi sinne tarvittaessa uusia parametreja. Azure-pilvipalvelua ja siihen asennettuja tietoturvasovelluksia, kuten virtuaalisia palomuureja ja IPS/IDS-sovelluksia, pystytään myös seuraamaan yrityksen tietoturvakeskuksesta. Tätä varten täytyy suorittaa Azuren ja SIEM-järjestelmän integraatio, jonka jälkeen lokitiedostot saadaan kuljetettua järjestelmästä toiseen.

4.4.2 IoT-datan siirtoyhteys

IoT-datan siirtäminen pilveen alkaa LoRaWAN-verkkoon liitettävästä sensorinoodista, johon on valittu aktivointimenetelmäksi joko ABP- tai OTAA-aktivointi. Aktivoinnilla laite autentikoidaan ja liitetään osaksi verkkoa. Aktivointimenetelmästä riippuen sensorinoodiin ja LoRaWAN-verkkopalvelimelle konfiguroidaan tarvittavat salausavaimet ja EUI-osoitteet. Sensorinoodien konfigurointi suoritetaan yleensä USB-kaapelilla, Bluetooth- tai WiFi-verkon välityksellä.

Ensimmäisessä tiedonsiirtovaiheessa LoRa-radioviesti kulkee, kuvan 4.8 mukaan, sensorinoodilta LoRaWAN-tukiasemalle. LoRa-viesti on tällöin salattu sekä AppSKey-salausavaimella että NwkSKey-salausavaimella, jotka molemmat ovat tyypiltään AES128-salausavaimia. NwkSKey-salaus jatkuu aina LoRaWAN-verkkopalvelimelle saakka ja AppSKey-salaus aina LoRaWAN-sovelluspalvelimelle saakka, jotka molemmat ovat virtuaalipalvelimia ja sijaitsevat Azure-pilvipalvelussa. Periaatteessa AppSKey-salaus on mahdollista ulottaa vaikka kolmannen osapuolen järjestelmiin

saakka, jolloin se kulkisi salattuna koko järjestelmän läpi.



Kuva 4.8: IoT-datan siirtoyhteyden tietoturva

Toisessa tiedonsiirtovaiheessa LoRa-radioviesti muuntuu DMZ-alueella sijaitsevalla LoRaWAN-tukiasemalla IEC104-protokollan mukaiseksi viestiksi, ja viesti jatkaa kulkuaan DMZ- ja CORP-palomuurin läpi kohti Azure-pilvipalveluun asennettua LoRaWAN-verkkopalvelinta eli Actilityn Thinpark Enterprise-verkkoalustaa. LoRaWAN-tukiaseman ja Thingpark-verkkoalustan välisessä IEC104-viestinnässä käytetään Microsoftin ExpressRoute-yhteyttä ja VPN IPsec-tunnelia, joilla pystytään varmistamaan tiedonsiirron salaus ja autentikointi. LoRaWAN-tukiasemaan joudutaan myös asentamaan Actilityn toimittama lisenssi, että tukiasema ja Thingpark-verkkoalusta saadaan toimimaan keskenään. Tässä tiedonsiirtovaiheessa viestintä on salattu useammassa kerroksessa, kuten kuvasta 4.8 voidaan havaita.

Kolmannessa tiedonsiirtovaiheessa dataa välitetään Azuren virtuaaliverkkoihin asennettujen Thingpark-verkkoalustan ja Microsoftin IoT Hubin välillä, jolloin data siirretään tapauskohtaisesti joko peering-yhdyskäytävällä Microsoftin runkoyhteyden kautta tai ExpressRoutea käyttämällä, jolloin virtuaaliverkot yhdistetään Microsoftin MSEE-reunareitittimen kautta. Viestiprotokollana käytetään MQTT- tai HTTP-

protokollaa ja salauksessa SSL/TLS-salausta. Thingpark-verkkoalustaan voidaan tehdä myös lähetysryhmiä, jolloin kaikki viestintä monistetaan useammalle vastaanottajalle. Menetelmällä on turvallista lähettää viestejä myös kolmansille osapuolille, kunhan muistetaan käyttää SSL/TLS-salausta.

LoRaWAN-viestit voidaan kierrättää kolmannessa vaiheessa myös takaisin tehtaan DMZ-alueella sijaitsevalle KEPServerEX(DMZ)-palvelimelle, jonka kautta saadaan luotua epäsuora yhteys LoRaWAN-verkosta tehtaan automaatiotietoverkossa sijaitsevalle KEPServerEX(ICS)-palvelimelle. Tätä kautta LoRaWAN-sensorinoodien tiedot saadaan näkymään prosessinäytöillä. LoRaWAN-verkkoa ei tulisi kuitenkaan käyttää toimilaitteiden suoraan ohjaukseen missään sellaisissa kohteissa, jotka voivat aiheuttaa vaaraa henkilöiden tai omaisuuden fyysiselle turvallisuudelle.

Neljännessä tiedonsiirtovaiheessa, kun tietoa siirretään Azure-pilvipalvelusta kolmansille osapuolille, niin tietoturvamenetelmät ovat samat, jotka mainittiin jo alaluvussa 4.4.1. samaa asiaa käsiteltäessä. Myös lokitiedostojen kerääminen palomuureista, IPS- ja IDS-järjestelmistä SIEM-järjestelmään on tärkeää.

4.5 Toimivuuden ja riskien arviointi

Kun IIoT-arkkitehtuuriratkaisua testattiin teollisuusympäristössä, niin kaikki ratkaisussa käytetyt IIoT-teknologiat: pilvipalvelut, verkkoalustat, väliohjelmistot, tiedonsiirtoverkot, viestiprotokollat ja tietoturva saatiin asennettua toimintaan sekä prosessidatan että IoT-datan siirtoyhteyksien osalta. IIoT-arkkitehtuuri on monipuolinen, ja sillä pystytään tekemään erilaisia sovelluksia ja takaisinkytkentöjä. Tässä piilee myös ratkaisun ensimmäinen riskitekijä, koska automaatiolaitteiden, pilvipalveluiden ja langattomia radioyhteyksiä käyttävien tiedonsiirtoverkkojen toimintavarmuus ei joka tilanteessa ole niin hyvällä tasolla kuin perinteisten langallisten automaatioverkkojen toiminta. IIoT-järjestelmällä tehtävät tyyppisovellukset ja -kytkennät tulisikin miettiä ja dokumentoida etukäteen, ennen kuin järjestelmää aletaan markkinoida yrityksen sisällä ja sen alihankkijaverkostossa. Järjestelmän dokumentointi, käyttö- ja turvallisuusohjeiden jakaminen sekä koulutus mitigoivat tehokkaasti vaarallisten kytkentojen riskin.

KEPServerEX(DMZ)-palvelimella pystyttiin lähettämään PLC-dataa Azuren IoT Hubiin MQTT-protokollalla, kun pollausnopeus ja tiedonvälitys valittiin periytymään KEPServerEX(ICS)-palvelimelta. Tämä tarkoittaa sitä, että molemmat palvelimet eivät tässä tapauksessa pollaa suoraan PLC-logiikoita, vaan pollauksen suo-

rittaa ainoastaan automaatioalueella sijaitseva palvelin. DMZ-alueen palvelin tyytyy vaan vastaanottamaan valmiiksi kerättyä PLC-tietoa. Tällä tavalla estetään PLC-logiikoiden tiedonsiirtoa ylikuormittumasta, koska niiden prosessorikapasiteetti on kuitenkin rajallinen. Jos logiikoita pollattaisiin useilla järjestelmillä, niin niiden normaali toiminta voisi häiriintyä. Tämä voisi olla vaarallista, koska PLC-logiikat ohjaavat suoraan tehtaiden toimilaitteita. Tämän seurauksena voisi syntyä tuotantokatkoja tai jopa vaaratilanteita. Kyseessä olisi tällöin automaatiojärjestelmän palvelunestotila. Tämä haavoittuvuus voi käydä toteen tahattoman tai tahallisen toiminnan seurauksena, jos KEPServerEX-palvelimen asetuksia pääsee vaikka muuttamaan joku henkilö, joka ei ymmärrä järjestelmän toimintaa tarpeeksi hyvin. Myös hyökkääjä voisi yrittää käyttää haavoittuvuutta hyväkseen. Tämä haavoittuvuus voidaan mitigoida pääsynhallinnalla, kun otetaan käyttäjäprofiilit ja perusautentikointi käyttöön KEPServerEX-palvelimilla ja salataan liikenne SSL/TLS-salauksella. Vastaavia vaaratilanteita voi aiheutua tägien ylikirjoituksesta, jos luku- ja kirjoitusoikeudet ovat konfiguroitu väärin. Tämän vuoksi KEPServerEX-palvelimien asennukset tulisi suorittaa kovennettuina asennuksina, joissa kaikki turhat palvelut poistetaan KEPServerEX-ohjelmistosta. Myös palvelimen käyttöjärjestelmän asennus on syytä tehdä kovennettuna.

Palvelunestotilanteet voivat lisääntyä tulevaisuudessa myös siirrettävien datamäärien kasvun seurauksena. Kun mietitään esimerkiksi tekoälyllä tehtäviä dataanalyyseja, niin dataa on pystyttävä siirtämään automaatiojärjestelmistä pilveen vieläkin enemmän, että näiden analyysien tekeminen olisi mahdollista. Koska jo nykyään, kun automaatiojärjestelmästä siirretään dataa pilveen sekunnin tai sekunnin kymmenesosan intervallilla, niin esimerkiksi yhtään kehittyneemmän värähtelyanalyysin tekeminen on mahdotonta, koska datan resoluutio on niin huono. Datan lähetysintervalli kuitenkin pienenee ja lähetettävien datapakettien koko kasvaa kaiken aikaa. Kun teollisuuslaitokset, järjestelmät ja laitteet linkittyvät toisiinsa pilvipalveluiden kautta, niin on mahdollista, että joku komponentti tai sovellus toimii odottamattomasti eri kuormitustilanteissa tai päivityksen yhteydessä. Tietoa voi kadota ja lopputuloksena voi syntyä monimutkaisia ja laaja-alaisia tietokatkoja, jotka voivat levitä yrityksen ja sen kumppaneiden eri tietoverkkoihin. Tiedonmenetys pilvipalvelussa ei ole kuitenkaan niin suuri riski kuin tietokatkojen ja palvelunestotilojen leviäminen automaatiotietoverkosta tehtaan toimilaitteisiin.

Tämän vuoksi tietoa on syytä kerätä tulevaisuudessa myös IoT-laitteista, jotka ovat erotettu automaatioverkosta. LoRaWAN-tiedonsiirtoverkko on tähän tarkoi-

tukseen hyvä työkalu. LoRaWAN-sensorinoodilla pystytään keräämään anturitietoa puskuriin ja lähettämään sitä koostettuna eteenpäin pilvipalveluihin. Myös pilvestä saadaan yhteys sensorinoodiin tai toimilaitteeseen, joten LoRaWAN-tiedonsiirto on kaksisuuntaista. Automaatiojärjestelmiin vietävän tiedon kanssa tulisi tässä tapauksessa olla kuitenkin varovainen, koska radiolla lähetettävän IoT-datan siirtämiseen on aina kuitenkin syytä suhtautua pienellä varauksella, että tulevatkohan kaikki datapaketit perille ja millä viiveellä. Mitään sellaisia kytkentöjä ja ohjauksia ei tulisi tehdä, joissa järjestelmä kaatuu heti, jos yksikin datapaketti jää välille. Automaatiojärjestelmään LoRaWAN-verkon avulla lähetettävän datan tulisi olla enemminkin informatiivista kuin ohjaavaa. Ainakaan henkilöturvallisuuteen liittyviä sovelluksia ei LoRaWAN-tiedonsiirron avulla voi tehdä, mutta ei niitä voi tehdä myöskään muilla radiolinkeillä. LoRaWAN-tiedonsiirto soveltuu kuitenkin joidenkin toimilaitteiden suoraan ohjaukseen, kuten vaikka valo-ohjauksien tekemiseen. Jos laitteiden ohjausdata tai muukaan lähetettävä data ei ole niin sensitiivistä, niin tämä pienentää myös tiedonsiirrosta aiheutuvien riskien vaikuttavuutta.

LoRaWAN-sensorinoodien aktivoinnissa käytettyihin salausavaimiin liittyy myös riski niiden paljastumisesta. Jos samat salausavaimet laitetaan kahdelle laitteelle samaan verkkoon, niin laitteiden tiedonsiirto häiriintyy. Salausavaimet on syytä konfiguroida aina uudelleen, jos laitesovelluksessa on vaan tähän mahdollisuus, koska oletuksena laitteeseen tallennetut salausavaimet eivät ole luotettavia. Salausavaimet pystytään luomaan usein myös jollain ulkopuolisella sovelluksella, jos on epäselvyyttä siitä, miten sensorinoodin ohjelmisto luo salausavaimet. Kaikkien sensorinoodien avaimet täytyy kuitenkin listata ja tallentaa jonnekin turvalliseen paikkaan, josta ne eivät päädy vääriin käsiin. HSM-moduuli tai Azuren Key Vault voivat olla ratkaisuja tähän. LoRaWAN-sensorien käytöstä poisto tulee myös suorittaa asianmukaisesti, että salausavaimet eivät paljastu. Kahdelle laitteelle voi myös tulla vahingossa samat salausavaimet, jos uudelle laitteelle konfiguroidaan samat salausavaimet kuin poistettavalle laitteelle ja vanha laite kytketään vahingossa päälle.

IIoT-järjestelmän tietoturvariskit arvioitiin ISO27001-standardin mukaan, ja arvioinnissa käytettiin asiakasyrityksen käyttämää Granite GRC-ohjelmistoa, johon pystyttiin kirjaamaan kaikki havaitut tietoturvariskit yksityiskohtia myöten. Riskit jaettiin kolmeen eri riskialueeseen, joita olivat: ihmiset, prosessit ja teknologiat. Tämän jälkeen yksilöitiin riskin lähde, itse riski, tarkennukset, ISO27001-hallintakeinot, hallintakeinojen tarkennukset, todennäköisyydet ja seuraukset. Kooste tästä riskien arvioinnista on lisätty tutkielman liitteeksi.

5 Yhteenveto

Tässä teollisuusautomaatiojärjestelmien ja teollisen internetin kyberturvallisuutta käsittelevässä tutkielmassa kartoitettiin ensin kirjallisuuskatsauksen menetelmin automaatiojärjestelmien kyberturvallisuuden erityispiirteitä ja kyberturvallisuusratkaisuja. Lähdemateriaaliksi pyrittiin valitsemaan tuoreimpia ja osuvimpia artikkeleja. Johdantoluvussa kerrottiin teollisuuslaitoksia ja -automaatiojärjestelmiä uhkaavista kyberuhista, sekä automaatiotietoverkkojen eroavaisuuksista toimistotietoverkkoihin nähden. Johdantoluvussa kerrottiin myös kirjallisuuskatsauksessa käytetyistä hakupalveluista, -menetelmistä ja -sanoista. Toisessa luvussa vastattiin tutkimuskysymykseen: Mitkä kyberuhat ja haavoittuvuudet liittyvät teollisuuden käyttämiin automaatiojärjestelmiin ja -laitteisiin? Luvussa selvitettiin yleisimmät haavoittuvuustyypit, jotka olivat: puskurinylivuoto, kovakoodatut kirjautumistiedot, XSS- js CSRF-tyyppiset haavoittuvuudet. Lisäksi luvussa selvitettiin haavoittuvimmat automaatiokomponentit, joita olivat HMI-käyttöliittymät, SCADA-järjestelmät ja väylälaitteet yleisesti. Kolmannessa luvussa vastattiin tutkimuskysymykseen: Mitkä ovat parhaat käytännöt teollisuuslaitosten hyvän kyberturvallisuustilanteen takaamiseksi? Tähän kysymykseen voidaan vastata tiivistetysti:

- Laaditaan yritykselle kyberturvallisuussuunnitelma.
- Suunnitellaan teollisuuslaitosten automaatio- ja toimistotietoverkkoarkkitehtuuri tietoturvalliseksi segmentoimalla se eri vyöhykkeisiin.
- Käyttöönotetaan IPS/IDS-järjestelmät myös teollisuuslaitosten automaatiotietoverkoissa, ja ohjataan näissä syntyvät lokitiedostot SIEM-järjestelmään.
- Monitoroidaan tietoverkkoihin kytkettyjen sovellusten tietoliikennettä, sisäänkirjautumisia ja järjestelmämuutoksia.
- Luodaan tietoverkkoon kytketyille palvelimille ja niissä käytettyihin sovelluksiin käyttäjäprofiilit, ja poistetaan henkilöstöltä tarpeettomat oikeudet.

Neljännessä luvussa vastattiin tutkimuskysymykseen: Millä tiedonsiirtotekniikoilla ja tietoturvamenetelmillä saadaan rakennettua optimaalinen IIoT-arkkitehtuuri? Tähän kysymykseen vastattiin tutkimalla erilaisia IIoT-teknologioita ja suunnittelemalla asiakasyritykselle IIoT-arkkitehtuuriratkaisusta, jota PoC-projektin puit-

teissa testattiin oikeassa teollisuusympäristössä. Myös IIoT-arkkitehtuuriratkaisuun käytettyjen teknologioiden ominaisuudet ja tietoturvamenetelmät kuvattiin yksityiskohtaisesti, että niistä pystyttiin luomaan kokonaiskuva ratkaisun kyberriskien arviointia varten, joka suoritettiin Granite GRC-ohjelmistolla.

Jatkotutkimusaiheeksi nousi tämän tutkielman myötä 5G-tiedonsiirtoteknologioiden testaaminen teollisuusympäristössä. Miten 5G-verkkojen kasvanutta tiedonsiirtokapasiteettia voidaan käyttää hyväksi? Miten pilvipalveluiden tiedonsiirtorajapinnat toimivat yhteen 5G-teknologioiden kanssa?

Lähteet

[1] ACTILITY SA. Thingpark IoT network. URL https://www.actility.com/products/, viitattu 1.10.2018.

[2] ADELANTADO, F., VILAJOSANA, X., TUSET-PEIRO, P., MARTINEZ, B., MELIA-SEGUI, J., JA WATTEYNE, T. Understanding the limits of lorawan. *IEEE Communications magazine 55*, 9 (2017), 34–40.

[3] AHONEN, P., JA MUUT. KYBER-TEO - tuloksia 2014-2016, julkisten tulosten kooste. *Teknologian tutkimuskeskus VTT Oy* (2017).

[4] AL-FUQAHA, A., GUIZANI, M., MOHAMMADI, M., ALEDHARI, M., JA AYYASH, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials 17*, 4 (2015), 2347–2376.

[5] ALA-TALA, A., JA MUUT. *Teollisuusautomaation tietoturva*. Suomen Automaatioseura ry, Helsinki, 2010.

[6] ANDREEVA, O., GORDEYCHIK, S., GRITSAI, G., KOCHETOVA, O., POTSELUEVSKAYA, E., SIDOROV, S. I., JA TIMORIN, A. A. Industrial control systems vulnerabilities statistics. *Kaspersky Lab* (2016).

[7] ARMSTRONG, R., JA HUNKAR, P. The OPC UA security model for administrators. *white paper, version 2* (2010).

[8] BAN, N. C. Is penetration testing recommended for industrial control systems? Tekninen raportti, Honeywell, 2013. URL https://www.honeywellprocess.com/library/marketing/presentations/EmailAssets/ICSFullArticle.pdf, viitattu 31.7.2017.

[9] BHATT, S., MANADHATA, P. K., JA ZOMLOT, L. The operational role of security information and event management systems. *IEEE security & Privacy*, 5 (2014), 35–41.

[10] CISCO. Catalyst switched port analyzer (SPAN) configuration example. URL https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html#anc10, viitattu 13.1.2018.

[11] CPNI. Cyber Security Assessments of Industrial Control Systems - a Good Practice Guide. URL https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/CPNI-Guia-SCI.pdf, viitattu 5.6.2017.

[12] DIAZ, J. J. Using SNORT for intrusion detection in MODBUS TCP/IP communications. *SANS Institute* (2011), 24.

[13] EXPLORATORY ENGINEERING. Data Rate and Spreading Factor. URL https://docs.exploratory.engineering/lora/dr_sf/, viitattu 20.10.2018.

[14] FENG, Z., QIN, S., HUO, X., PEI, P., LIANG, Y., JA WANG, L. Snort improvement on profinet rt for industrial control system intrusion detection. Julkaisusarjassa *Computer and Communications (ICCC), 2016 2nd IEEE International Conference on* (2016), IEEE, pp. 942–946.

[15] FERNANDEZ, I. Cybersecurity for industrial automation & control environments: Protection and prevention strategies in the face of the growing threats. *Frost & Sullivan* (2013).

[16] FOSTER, A. Messaging technologies for the industrial internet and the internet of things. *PrismTech Whitepaper* (2015).

[17] FUNK, C., JA GARNAEVA, M. Kaspersky security bulletin 2013. overall statistics for 2013. *Kaspersky Lab* (2013).

[18] GHAEINI, H. R., ANTONIOLI, D., BRASSER, F., SADEGHI, A.-R., JA TIPPENHAUER, N. O. State-aware anomaly detection for industrial control systems.

[19] GIGAMON. To TAP or SPAN? URL https://www.gigamon.com/content/dam/resource-library/english/white-paper/wp-tap-vs-span.pdf, viitattu 5.10.2017.

[20] HAHN, A. Operational technology and information technology in industrial control systems. Kirjassa *Cyber-security of SCADA and Other Industrial Control Systems*. Springer, 2016, pp. 51–68.

[21] HARRIS, J. Network packet brokers: The abcs of network visibility. URL https://www.ixiacom.com/company/blog/network-packet-brokers-abcs-network-visibility, viitattu 27.10.2017.

[22] ICS-CERT. Assessment Program Overview. URL https://ics-cert.us-cert.gov/Assessments, viitattu 28.1.2019.

[23] KEPWARE. KEPServerEX. URL https://www.kepware.com/en-us/products/kepserverex/, viitattu 24.11.2018.

[24] KIRAVUO, T., TIILIKAINEN, S., SÄRELÄ, M., JA MANNER, J. Peeking under the skirts of a nation: finding ics vulnerabilities in the critical digital infrastructure. Julkaisusarjassa *European Conference on Cyber Warfare and Security* (2015), Academic Conferences International Limited, pp. 137–144.

[25] LI, H., LIU, G., JIANG, W., JA DAI, Y. Designing snort rules to detect abnormal dnp3 network data. Julkaisusarjassa *Control, Automation and Information Sciences (ICCAIS), 2015 International Conference on* (2015), IEEE, pp. 343–348.

[26] LIN, J., YU, W., ZHANG, N., YANG, X., ZHANG, H., JA ZHAO, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal 4*, 5 (2017), 1125–1142.

[27] LIRI, E., SINGH, P. K., RABIAH, A. B., KAR, K., MAKHIJANI, K., JA RAMAKRISHNAN, K. Robustness of iot application protocols to network impairments. Julkaisusarjassa *2018 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)* (2018), IEEE, pp. 97–103.

[28] LORA ALLIANCE TECHNICAL COMMITTEE. LoRaWAN 1.1 Specification. *LoRa Alliance* (2017).

[29] LORA ALLIANCE TECHNICAL COMMITTEE. LoRaWAN 1.0.3 Regional Parameters. *LoRa Alliance* (2018).

[30] LUKKA, K. Konstruktiivinen tutkimusote, 2001. URL https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/, viitattu 9.10.2017.

[31] MANTERE, M., SAILIO, M., JA NOPONEN, S. A module for anomaly detection in ics networks. Julkaisusarjassa *Proceedings of the 3rd international conference on High confidence networked systems* (2014), ACM, pp. 49–56.

[32] MATOUŠEK, P. Description and analysis of iec 104 protocol.

[33] MCAFEE WHITE PAPER. Creating and maintaining a soc, the details behind successful security operations centres. 64.

[34] MICROSOFT. Azure Network Security. URL https://azure.microsoft.com/mediahandler/files/resourcefiles/azure-network-security/Azure%20Network%20Security.pdf, viitattu 5.11.2018.

[35] MICROSOFT. Azure overview. URL https://azure.microsoft.com/en-us/overview/, viitattu 5.13.2018.

[36] MILLER, R. Lora security: Building a secure lora solution. *MWR Labs Whitepaper* (2016).

[37] MIT. Review of Buffer Overflow Attacks. URL https://ocw.mit.edu/..../MIT6_858F14_lec2.pdf, viitattu 24.8.2017.

[38] MIT. User Authentication. URL https://ocw.mit.edu/...../MIT6_858F14_lec17.pdf, viitattu 2.10.2017.

[39] MORRIS, T. H., JA GAO, W. Industrial control system cyber attacks. Julkaisusarjassa *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research* (2013), p. 22.

[40] NEITZEL, L., JA HUBA, B. Top ten differences between ics and it cybersecurity. *InTech 61*, 3 (2014), 12–18.

[41] NOVOTEK. Kepware-kommunikointialusta. URL https://www.novotek.com/fi/ratkaisut/kepware-kommunikointialusta/, viitattu 16.9.2018.

[42] OPC FOUNDATION. What is OPC? URL https://opcfoundation.org/, viitattu 17.9.2018.

[43] PATHAN, A.-S. K. *The state of the art in intrusion prevention and detection*. CRC press, 2014.

[44] PUOLUSTUSMINISTERIÖ, S. Katakri 2015 - tietoturvallisuuden auditointityökalu viranomaisille. URL http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf, viitattu 6.1.2018.

[45] RACZ, N., WEIPPL, E., JA SEUFERT, A. A frame of reference for research of integrated governance, risk and compliance (grc). Julkaisusarjassa *IFIP International Conference on Communications and Multimedia Security* (2010), Springer, pp. 106–117.

[46] RAUTIAINEN, A., SIPPOLA, K., JA MÄTTÖ, T. Perspectives on relevance: The relevance test in the constructive research approach. Management accounting research. *Elsevier vol. 34* (2017), 19–29.

[47] SANDERS, C. *Practical packet analysis: Using Wireshark to solve real-world network problems*. No Starch Press, 2017.

[48] SEMTECH. Application Note AN1200.22. *LoRa Modulation Basics*, Rev. 2 (2015).

[49] SORNIN, N., LUIS, M., EIRICH, T., KRAMP, T., JA HERSENT, O. LoRaWAN 1.0.2 Specification. *LoRa Alliance* (2016).

[50] STOUFFER, K., LIGHTMAN, S., PILLITTERI, V., ABRAMS, M., JA HAHN, A. Guide to industrial control systems (ICS) security. *NIST special publication 800-82*, Rev. 2 (2015), 247.

[51] THE THINGSNETWORK. Lorawan address space. URL `https://www.thethingsnetwork.org/docs/lorawan/address-space.html#over-the-air-activation-otaa`, viitattu 29.9.2018.

[52] TOMASIN, S., ZULIAN, S., JA VANGELISTA, L. Security analysis of lorawan join procedure for internet of things networks. Julkaisusarjassa *Wireless Communications and Networking Conference Workshops (WCNCW), 2017 IEEE* (2017), IEEE, pp. 1–6.

[53] VALTIOVARAINMINISTERIÖ. Teknisen ICT-ympäristön tietoturvataso-ohje. URL `https://www.vahtiohje.fi/c/document_library/get_file?uuid=5a273c6e-2935-4bbf-a4c6-f00e0f878db5&groupId=10229`, viitattu 13.11.2017.

[54] VAN KESSEL, P. Path to cyber resilience: Sense, resist, react | 19th global information security survey 2016-17. *Ernst & Young* (2016).

[55] VIELBERTH, M., JA PERNUL, G. A security information and event management pattern. *The Hillside Group* (2018), 12.

[56] VIESTINTAVIRASTO. Cross site scripting -haavoittuvuudet. URL https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2008/03/P_6.html, viitattu 23.8.2017.

[57] WATERISAC. 10 basic cybersecurity measures: Best practices to reduce exploitable weaknesses and attacks. URL https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_Oct2016%5B2%5D.pdf, viitattu 25.7.2017.

[58] WEISS, J. Assuring industrial control system (ICS) cyber security. *Center for Strategic and International Studies* (2008).

[59] WILHOIT, K. Who 's really attacking your ics equipment? *Trend Micro Incorporated, Research Paper* (2013), 10.

[60] YMON. Tap-laitteet. URL http://ymon.fi/tuotteet/verkkoliikenteen-monitorointi/tap-laitteet.html, viitattu 12.10.2017.

A ISO27001-Tietoturvariskit

Kohde:	Riskialue:	Riskin lähde:	Riski:	Tarkennus:	ISO 27001 Hallintakeinot:	Hallintakeinot:	Todennäköisyys:	Seuraus:	Kok.
IoT/IIoT-järjestelmät (Nykytila)	Teknologiat	Tietojärjestelmät	Erilaisten IoT/IIoT-järjestelmien ja -laitteiden määrä uhkaa entisestään kasvaa tehtailla	Tehtaat ja alihankkijat käyttävät erilaisia tiedonsiirtoväyliä, sovelluksia ja laitteita, joilla he siirtävät tietoa omiin tietojärjestel-miinsä. Tämä aiheuttaa vakavan ja hallitsemattoman uhkan tehtaiden kyber-turvallisuudelle. Jotain sattuu ennen pitkää.	5.1.1 Tietoturvapolitiikat	Luodaan yritykselle yksi standardi tietoturvallinen IIoT-arkkitehtuuri, jota kaikki toimijat ensisijaisesti käyttävät.	5	5	25
IIoT-järjestelmät (LoRaWAN)	Prosessit	Tietoturvapolitiikat	LoRaWAN-laitteiden salausavaimien säilytys	Jos salausavaimet kirjoitetaan Excel-listalle jne, niin ne voi joutua vääriin käsiin esim. sähköpostin välityksellä.	5.1.1 Tietoturvapolitiikat 10.1.2 Salausavainten hallinta	HSM-moduuli Azure Key Vault	2	3	6
IIoT-järjestelmät (KEPServerEX)	Prosessit	Tietoliikenteen valvonta	KEPServerEX-palvelimen käyttäjätunnuksien paljastuminen	käyttäjätunnukset ja salasanat kulkevat selkotekstinä ICS- ja DMZ-verkon alueilla	10.1.1 Salauksen käytön periaatteet 13.1.2 Verkkojen turvaaminen	Secure OPC UA-tunneli (SSL-salaus) myös ICS-alueella	1	3	3
IIoT-järjestelmät (KEPServerEX)	Ihmiset	Tunnistautumistiedot	KEPServerEX-palvelimien käyttäjäprofiilit puuttuvat	Väärä asennus tai asetuksien muuttaminen (tägien ylikirjoitus tai pollausnopeuden kasvattaminen) aiheuttaa ongelmia PLC-logiikoilla, jotka ovat yhteydessä tehtaan fyysisiin prosesseihin.	7.2.2 Tietoturvatietoisuus, -opastus ja -koulutus 9.1.1 Pääsynhallintapolitiikka 9.2.2 Pääsyoikeuksien jakaminen 12.1.1 Dokumentoidut toimintaohjeet	Luodaan käyttäjäprofiilit KEPServerEX-palvelimille ja virtuaalipalvelimille. Poistetaan turhat oikeudet	2	5	10
IIoT-järjestelmät (kokonaisuus)	Ihmiset	Toimintaohjeet	IIoT-järjestelmän turvallisuus- ja käyttöohjeet puuttuvat	Mitä kytkentöjä saa tehdä ja mitä ei. Vääränlaiset kytkennät IIoT-sovelluksista automaatioverkkoon aiheuttavat suuren riskin.	7.2.2 Tietoturvatietoisuus, -opastus ja -koulutus 12.1.1 Dokumentoidut toimintaohjeet	Käyttöohjeet järjestelmän käyttäjille	3	5	15
IIoT-järjestelmät (kokonaisuus)	Teknologiat	Tietojärjestelmät	Tietovuoto IIoT-tiedonsiirrossa	Lähetettävän datan paljastuminen salaamattoman tai autentikoimattoman tietoliikenteen vuoksi	10.1.1 Salauksen käytön periaatteet 13.1.2 Verkkojen turvaaminen	Secure OPC UA-tunneli VPN/IPsec -tunneli SSL/TLS-salaus AES128-salaus	1	3	3
IIoT-järjestelmät (kokonaisuus)	Teknologiat	Ohjelmistot	Injektiot, XSS-haavoittuvuus	Ohjelmistoissa ja sovelluksissa on kenttiä, joihin voidaan kirjoittaa vapaasti merkkejä, syötteen validoinnissa voi olla puutteita	14.2.8 Järjestelmän turvallisuustestaus	Ulkoiset rajapinnat testataan viallisilla syötteillä sekä suurilla syötemäärillä.	1	2	2
IIoT-järjestelmät (LoRaWAN)	Teknologiat	Laitteet	LoRaWAN-laitteen salausavaimien paljastuminen	Salausavaimet paljastuvat, kun laite poistetaan käytöstä	10.1.2 Salausavainten hallinta 11.2.7 Laitteiden turvallinen käytöstä poistaminen ja kierrättäminen	Ohjeistus: LoRaWAN-sensoreiden käytöstä poisto	1	2	2
IIoT-järjestelmät (LoRaWAN)	Teknologiat	Laitteet	Kovakoodatut salausavaimet	Salausavaimet ovat kovakoodattu ja ne ovat voineet paljastua jo kuljetus- tai käsittelyvaiheessa	10.1.2 Salausavainten hallinta 18.2.3 Teknisen vaatimustenmukaisuuden katselmoin	Ei käytetä sensoreita, jotka eivät ole turvallisia	1	2	2
IIoT-järjestelmät (MS Azure)	Teknologiat	Pilvipalvelut	Tiedonsiirtoa Azureen ei ole testattu suurilla datamäärillä	Sovelluskomponenttien yhteentoimivuus eri kuormitustilanteissa ja asetuksilla voi aiheuttaa ongelmatilanteita	12.6.1 Teknisten haavoittuvuuksien hallinta 18.2.3 Teknisen vaatimustenmukaisuuden katselmointi	Kuormitustestaus	2	4	8
IIoT-järjestelmät (PLC-logiikat)	Teknologiat	Laitteet	PLC/DCS/RTU-laitteiden tiedonsiirtonopeuden	Tiedonsiirtonopeuksien ja -määrien kasvattaminen IIoT-tiedonsiirrossa aiheuttaa ongelmia muissa	12.1.1 Dokumentoidut toimintaohjeet 18.2.3 Teknisen vaatimustenmukaisuuden katselmointi	PLC/DCS/RTU-laitteiden ominaisuuksien selvittäminen	2	4	8