

Opinnäytetyö (AMK)

Tietojenkäsittely

2021

Tarmo Hiltunen

KORKEAN TURVATASON KONESALIN AUTOMAATION MODERNISOINTI

Tarmo Hiltunen

KORKEAN TURVATASON KONESALIN AUTOMAATION MODERNISOINTI

Tämän opinnäytetyön tavoitteena oli selvittää EasyIO FS-20 -kontrollerin soveltuvuus korkean turvatason konesalin automaatiojärjestelmän korvaajaksi. Koska konesalien automaatiojärjestelmät voivat olla vuosikymmeniä vanhoja ja siksi haavoittuvaisia, tarvitaan nykyaikaisempaa automaatiojärjestelmää parantamaan konesalin tehokkuutta käyttämällä uusia teknologioita hyväksi. Rakennuksen automaatiojärjestelmän liittäminen osaksi esineiden internetiä tuo uusia mahdollisuuksia ohjata automaatiojärjestelmään kytkettyjä laitteita, mutta se tuo mukanaan haasteita turvallisuuden näkökulmasta.

Opinnäytetyössä tutustuttiin EasyIO FS-20 -kontrolleriin ja sen sisäisiä ominaisuuksia otettiin käyttöön. Näitä ominaisuuksia testattiin sisäisesti kuin ulkoisesti ja varmistettiin, onko EasyIO FS-20 -kontrolleri sopiva korkean turvatason konesalin automaatiojärjestelmäksi. Tämän lisäksi tavoitteena oli selvittää, miten FS-20 -kontrollerille liitetyn lämpötila-anturin tietoja saataisiin siirrettyä ulos kontrollerista palvelimelle jatkokäsittelyä varten.

Opinnäytetyön tuloksena saatiin toimiva ja turvallinen automaatiojärjestelmä korkean turvatason konesalille. EasyIO FS-20 -kontrolleri soveltuu tarkoitukseensa hyvin ja nykyaikaiset teknologiat oli toteutettu hyvin kontrollerille.

ASIASANAT:

Esineiden internet, automaatio, konesali, MQTT, EasyIO FS-20

Tarmo Hiltunen

MODERNIZATION OF THE AUTOMATION OF THE HIGH SECURITY DATA CENTER

The aim of this thesis was to investigate the suitability of the EasyIO FS-20 controller as a replacement for a high security data center automation system. Because data center automation systems can be decades old and therefore vulnerable, a more modern automation system was needed to improve the data center efficiency by leveraging new technologies. Integrating a building's automation system into the Internet of Things brings new opportunities to control devices connected to the automation system, but it also brings challenges from a security perspective.

The thesis focused on becoming acquainted with the EasyIO FS-20 controller in its entirety and implementing the internal features of the controller. These features were tested internally as well as externally to verify that the EasyIO FS-20 controller is suitable for a high security data center automation system. In addition to this, the aim was to find out how the data of the temperature sensor connected to the FS-20 controller could be transferred from the controller to the server for further processing.

The result of the thesis was a functional and safe automation system for a high security data center. The EasyIO FS-20 controller is well suited of its purpose and modern technologies were well implemented for the controller.

KEYWORDS:

Internet of Things, automation, data center, MQTT, EasyIO FS-20

SISÄLTÖ

KÄYTETYT LYHENTEET	6
1 JOHDANTO	7
2 KONESALI	8
2.1 Konesalin eri tyypit	8
2.2 Konesalin turvallisuus	8
2.2.1 Konesalin fyysinen turvallisuus	9
2.2.2 Konesalin ohjelmistojen turvallisuus	9
2.3 Konesalin energiankulutus	10
3 HVAC-OHJAUSJÄRJESTELMÄ	12
4 IOT-LAITTEET	13
4.1 IoT-laitteiden turvallisuus	14
4.2 MQTT-protokollaa tukevat IoT-laitteet	14
5 EASYIO FS-20 -KONTROLLERI	16
5.1 CPT-Tools	17
5.1.1 Sedona	18
5.1.2 Vuokaavio	19
5.1.3 Grafiikat	19
5.1.4 Käyttäjähallinta	20
5.2 Palvelut	21
5.3 MQTT-ohjauspaneeli	23
6 LOPPUPÄÄTELMÄT	26
LÄHTEET	27

KUVAT

Kuva 1. Turvallisuus kerroksittain (Shailaja 2020).	9
Kuva 2. Tyypillisen konesalin energiakulutus (Evans 2018).	10
Kuva 3. Internetiin kytketyt IoT-laitteet (Lueth 2018).	13

Kuva 4. MQTT-protokollan toimintaperiaate (Yuan 2020).	15
Kuva 5. EasyIO FS-20, johon kytketty PT1000 lämpötila-anturi.	16
Kuva 6. CPT Tools -työkalun kirjautumisosio	17
Kuva 7. Sedona-pakettihallintajärjestelmä	18
Kuva 8. Lämpötila-anturi kytkettynä vuokaavioon.	19
Kuva 9. Lämpötila-anturille tehty grafiikka.	20
Kuva 10. Käyttäjäoikeuksien hallinta.	20
Kuva 11. Kontrollerin ohjauspaneeli palveluille.	21
Kuva 12. Nmap -työkalulla tehty porttiskannaus.	22
Kuva 13. Nmap -työkalulla löydetty haavoittuvuus SMB portissa.	22
Kuva 14. Aiheiden hallinta -toiminnallisuus, jossa määriteltä aiheet.	23
Kuva 15. Viestienhallinta -toiminnallisuus, jossa määriteltä viestit aiheiden sisään.	24
Kuva 16. Yhteyden muodostaminen broker-palvelimelle.	24
Kuva 17. Lämpötila-anturin tietojen lähetys MQTT-brokerille	25

TAULUKOT

Taulukko 1. Konesalien energiankulutus (Geng 2014).	10
---	----

KÄYTETYT LYHENTEET

BACnet	Rakennusautomaation tiedonsiirtoprotokolla (Building Automation and Control Networks)
BAS	Rakennusautomaatiojärjestelmä (Building Automation System)
BEMS	Rakennuksen energianhallintajärjestelmä (Building Energy Management System)
GDPR	Yleinen tietosuoja-asetus (General Data Protection Regulation)
HTML	Hypertekstin merkintäkieli (HyperText Markup Language)
HVAC	LVI, Lämmitys, vesi ja ilmastointi (Heating, Ventilation and Air Conditioning)
IoT	Esineiden internet (Internet of things)
MQTT	Telemetrian siirtoprotokolla (Message Queuing Telemetry Transport)
M2M	Laitteiden välinen viestintä (Machine to Machine)
SIEM	Turvallisuustietojen ja -tapahtumien hallinta (Security Information and Event Management)
SMB	Hajautettu levyjärjestelmä (Server Message Block)

1 JOHDANTO

Opinnäytetyön aiheena on korkean turvatason konesalin automaatio ja sen modernisointi. Työssä tarkastellaan EasyIO-kontrolleria ja sen soveltuvuutta konesalin automaatiojärjestelmäksi, luotettavuus ja turvallisuus huomioon ottaen. Tämän opinnäytetyön toimeksianto on päivittää 80-luvun korjauskelvottomaksi rikkoutunut automaatiojärjestelmä. Opinnäytetyö on rajattu konesalin jäähdytys- ja lämmitysjärjestelmän (HVAC) automaattiseen ohjaamiseen.

Konesalit kehittyvät jatkuvasti tehokkaammaksi ja niiden tarve on kasvanut digitalisaation myötä. Konesalin tarkoituksena on mahdollistaa tietoliikenneyhteydet ja olla tietovarastona, jossa saattaa olla kriittisiä tietoa, kuten yleisen tietosuoja-asetuksen (GDPR) mukaista tietoa tai sellaista tietoa, mitä tarvitaan esimerkiksi julkisen sektorin palveluissa. Tästä syystä konesalit ovat tärkeässä asemassa digitalisaatiossa.

Opinnäytetyön teoriaosuudessa esitellään konesalien merkitys yhteiskunnalle, mistä konesalin turvallisuus koostuu ja erilaisia keinoja jäähdyttää konesalin jäähdytettäviä komponentteja. Tämän jälkeen esitellään teoriaa rakennuksen automaatiojärjestelmästä ja jäähdytysjärjestelmästä. Lopuksi käydään läpi esineiden internetin vaikutuksesta nyky-yhteiskuntaan ja esitellään, millainen EasyIO FS-20 -kontrolleri on, minkälaisia ominaisuuksia se sisältää, ja testataan niitä penetraatiotestein.

2 KONESALI

Konesalit ovat kaikissa elämän osa-alueilla mukana ja mahdollistavat tarpeet liittyen ruokaan, vaatetukseen, majoitukseen, logistiikkaan, terveydenhuoltoon ja sosiaalisiin aktiviteetteihin, jotka kattavat yksilöiden väliset suhteet yhteiskunnassa (Geng 2014).

Konesali koostuu reitittimisestä, kytkimisestä, palomuuereista, tietojärjestelmistä, palvelimista ja tietoliikenteen kuormituksen tasaussovelluksista. Nämä muodostavat verkkoinfrastruktuurin, tietovarastoinfrastruktuurin ja laskentaresurssit. (Cisco Systems 2021)

2.1 Konesalin eri tyypit

Konesaleja on kolmea erilaista tyyppiä. Konesalin luokittelu riippuu omistajien määrästä, konesalissa käytettävistä teknologioista ja energiatehokkuudesta (Cisco Systems 2021).

Yritystason konesaleja rakentavat ja hallinnoivat yritykset, joiden konesalit ovat optimoitu loppukäyttäjää varten (Cisco Systems 2021).

Hallinnoitavat palvelukonesalit ovat kolmansien osapuolien käytettävissä. Yritykset voivat vuokrata konesalin laitteistoa ja infrastruktuuria, eli kapasiteettia omiin tarpeisiinsa. (Cisco Systems 2021)

Colocation-konesali on palvelu, jossa kolmannet osapuolet vuokraavat konesalin omistajalta tilaa omille laitteistoille. Konesalin omistaja vuokraa laitteiston omistajille infrastruktuurit, kuten rakennuksen, jäähdytyksen, kaistan ja tietoturvan. (Cisco Systems 2021)

2.2 Konesalin turvallisuus

Konesalit ovat monimutkaisia kokonaisuuksia. Jotta niitä voidaan turvata erilaisilta uhilta, turvakomponentteja on tarkasteltava erikseen, mutta samalla niiden on noudatettava yhtä kokonaisvaltaista turvallisuuspolitiikkaa. Konesalin turvallisuus on jaettu kahden osaan, fyysiseen ja ohjelmistojen turvallisuuteen. (Forcepoint 2021)

2.2.1 Konesalin fyysinen turvallisuus

Konesalin fyysinen turvallisuus alkaa sijainnin valinnalla. Sijainnin valintaan vaikuttavat geologiset aktiviteetit, kuten tulvan ja maanjäristyksen riski. (Shailaja 2020) Tulipalo on todennäköisin riski ja sen seuraukset ovat tuhoisat konesalille. Tulipalo voi tuhota konesalissa olevat tiedot täysin ja tuhota koko konesali-infrastruktuurin. (Carroll 2021)

Optimaalisin ja strategisin tapa suojata konesali on hallita sen fyysistä turvallisuutta kerroksittain (Kuva 1). Kerrokset tarjoavat jäsennellyn fyysisen turvallisuuden, ulommat tasot ovat fyysisiä ja sisemmät kerrokset estävät tietomurrot. (Shailaja 2020)



Kuva 1. Turvallisuus kerroksittain (Shailaja 2020).

2.2.2 Konesalin ohjelmistojen turvallisuus

Konesalille oleellimmat uhkat ovat hakkerointi, haittaohjelmat ja vakoiluohjelmat. Tietoturvatietojen ja tapahtumien hallintatyökalulla (SIEM) hallitaan reaaliaikaisia tapahtumia konesalin eri arkkitehtuureissa. Konesalin verkkoturvallisuutta voidaan lisätä tekemällä alueita eri tarkoituksiin kuten testaamiseen, kehitykseen ja tuotantoon. (Forcepoint 2021)

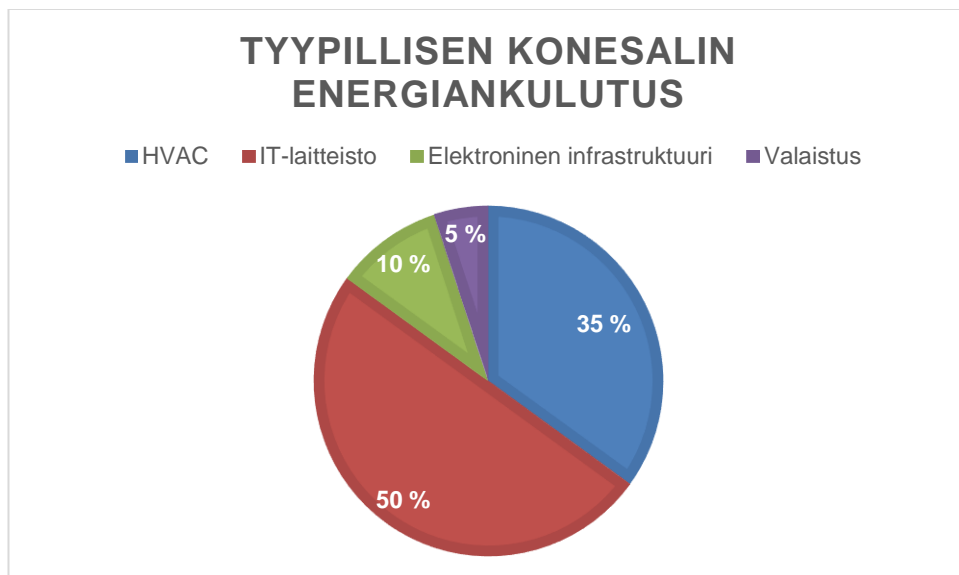
2.3 Konesalin energiankulutus

Konesali kuluttaa sähköä yhdestä kilowatista viiteensataan megawattiin koosta ja tarkoituksesta riippuen (Taulukko 1). Konesalit sisältävät erilaisia järjestelmiä, joita käytetään ICT-laitteiden jäähdyttämiseen. (Geng 2014) Jäähdytysmenetelmistä vapaa jäähdytys on taloudellisin menetelmä, koska silloin hyödynnetään ympäristön viileyttä. Ympäristön viileys on kylmää ulkoilmaa tai maakylmyyttä maalämpökaivoista.

Taulukko 1. Konesalien energiankulutus (Geng 2014).

Laitoksen tyyppi	Laitosten määrä	Palvelimet per laitos	2006 sähkönkulutus (mrd. kWh)
Palvelinkaappi	1 798 000	1-2	3,5
Palvelinhuone	2 120 000	3-36	4,3
Keskitetty konesali	1 820 000	36-300	4,2
Keskitaso konesali	1 643 000	300-800	3,7
Yritystason konesali	3 215 000	800-2000+	8,8

Tyypillisen konesalin energiankulutus (Kuva 2) jakautuu IT-laitteistolle (50 %), HVAC-järjestelmälle (35 %), elektroniselle infrastruktuurille (10 %) ja valaistukselle (5 %). (Evans 2018)



Kuva 2. Tyypillisen konesalin energiakulutus (Evans 2018).

ICT-laitteiden nestejäähdytystä on kehitetty nykyaikaisilla menetelmillä, esimerkiksi konesalin palvelimet upotetaan elektroniikalle vaarattomaan nesteeseen, jonka kiehumispiste on 50 °C:ssa. Nesteen kiehuminen kuljettaa lämpöä pois työskenteleviltä palvelinten prosessoreilta. Kiehuvasta nesteestä nouseva höyry muuntuu nesteeksi ja se johdetaan lauhduttimen kautta takaisin altaaseen upotettuihin palvelimiin. (Roach 2021)

Konesalin sijainnin valinta vaikuttaa käytettävän jäähdytysmenetelmän valintaan, esimerkiksi kylmissä ilmastoissa voidaan käyttää vapaata jäähdytystä kuivalla ja kylmällä ilmalla, ja vesistöjen lähellä olevissa laitoksissa voidaan käyttää vesijäähdytystä. (Vaisala 2017)

3 HVAC-OHJAUSJÄRJESTELMÄ

Rakennuksen automaatiojärjestelmän (BAS) tavoitteena on parantaa järjestelmän tehokkuutta, vähentää kuluja ja lisätä turvallisuutta. Keskitetty rakennuksen hallintajärjestelmä tuo kaikki komponentit yhdeksi kokonaisuudeksi. Komponentteihin kuuluvat sensorit, kontrollerit ja laitteet, joita on tarkoitus ohjata kontrollereilla. (Senseware Inc 2017)

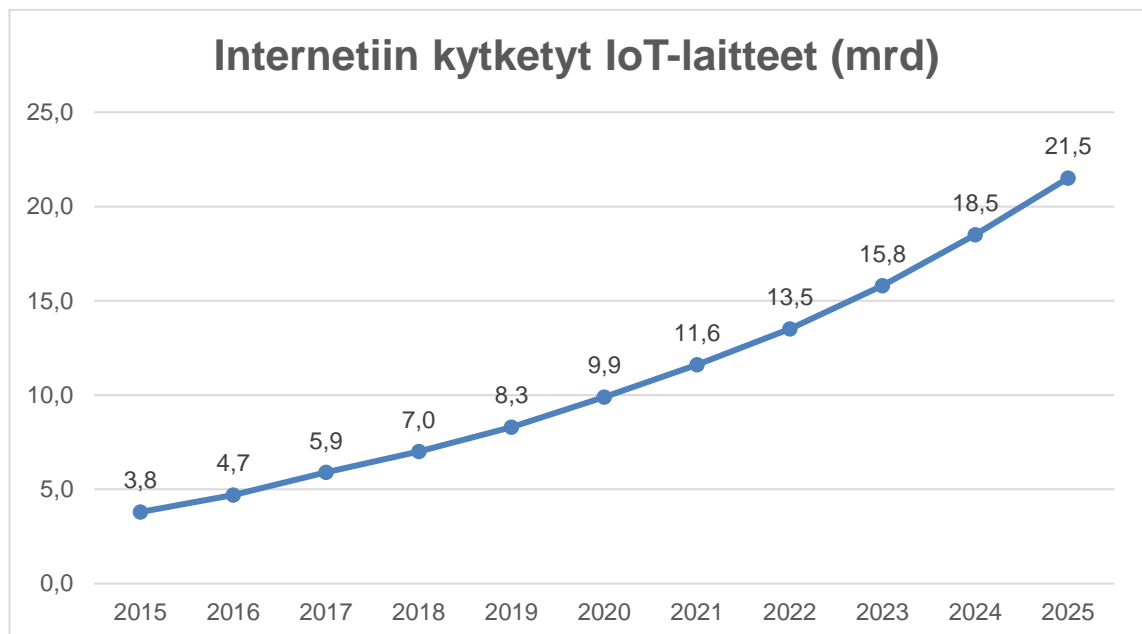
Tyypillinen HVAC-ohjausjärjestelmä koostuu toiminnallisesti ja maantieteellisesti hajautetuista ohjaimista, jotka kykenevät ohjaamaan erilaisia prosesseja rakennuksessa. Nykypäivän ohjaimilla on laaja laskennallinen kyky ja ne voivat hallita prosesseja, kuten hälytyksiä, tapahtumien käynnistämiä sovelluksia, aikaperusteisia sovelluksia ja energianhallintasovelluksia. Tietoliikenneprotokollalla ohjausjärjestelmät jakavat tietoa muiden ohjausjärjestelmien ja isäntäkoneen kanssa. (Clayton 2018)

HVAC-ohjausjärjestelmät ovat yksi neljästä keskeisestä segmentistä, jotka muodostavat koko rakennusautomaatiojärjestelmän (BAS). Loput kolme segmenttiä ovat kulunvalvonta, fyysinen turvallisuus sekä valaistuksen ohjausjärjestelmät. (Clayton 2018)

HVAC-järjestelmien automatisointi tuo hyötyjä erityisesti tehokkuuden näkökulmasta. Energiahukkaa tulee silloin, kun HVAC-järjestelmä on täydellä teholla lämmittääkseen tai jäähdyttääkseen tilaa, joka on tyhjillään sillä hetkellä. Monimutkaisen ilmavirtajärjestelmän ja siihen kytkettyjen laitteiden manuaalisesta säätämisestä voi tulla kokopäiväinen työ. (HVACSchool.org 2021)

4 IOT-LAITTEET

Internet of Things (IoT) eli esineiden internet on kiinteä osa tulevaisuuden internetiä. Se voidaan määritellä dynaamiseksi eli jatkuvasti muuttuvaksi ja kehittyväksi, maailmanlaajuiseksi verkkoinfrastruktuuriksi eli verkon perusrakenteeksi, jossa fyysisillä ja virtuaalisilla esineillä on identiteetti, fyysisiä ominaisuuksia ja virtuaalinen persoona. IoT sisältää paljon toimintamahdollisuuksia, mutta sen tietoturvallisuus on heikko tai lähes olematon, koska järjestelmät ja laitteet on kehitetty markkinoille nopeasti ja usein tietoturvallisuuden vaatimuksista tinkien. (Kotakallio, et al. 2021) Kuvan 3 mukaan maailmassa on yli 7 miljardia IoT-laitetta kytkettynä internetiin ja määrä kasvaa 21,5 miljardiin vuoteen 2025 mennessä. (Lueth 2018)



Kuva 3. Internetiin kytketyt IoT-laitteet (Lueth 2018).

Ihmispohjainen viestintä edustaa suurta osuutta koko tietovirrasta, mutta täysin automatisoitu M2M-viestintä on laajentumassa suuremmaksi valtavilla harppauksilla. Esineiden internet, jossa on fyysisiin esineisiin upotettuja antureita ja toimilaitteita, muuttaa sosio-

teknistaloudellisen ekosysteemin täysin uuteen aikakauteen, jossa vanhoja liiketoimintäsääntöjä ja ansaintamalleja päivitetään päivittäisellä tasolla. (Penttinen 2017)

4.1 IoT-laitteiden turvallisuus

IoT tuo valtavan määrän uusia mahdollisuuksia hallita, koordinoita, automatisoida ja hyötyä yleensä viestinnästä ilman ihmisen väliintuloa sekä ottamalla ihmisten vuorovaikutus tarvittaessa huomioon. Uusien mahdollisuuksien lisäksi tämä avaa myös tunnettuja ja täysin uusia turvallisuusuhkia, jotka voivat vaarantaa käyttäjien identiteetin ja tietojen luottamuksellisuuden, mikä puolestaan voi vaarantaa esimerkiksi talouden turvallisuutta ja ihmisten henkilökohtaista hyvinvointia. (Penttinen 2017)

Rikolliset murtautuvat IoT-laitteisiin käyttämällä laitteiden oletusarvoisia kirjautumistunnuksia, koska valmistajat käyttävät samoja kirjautumistunnuksia uusille laitteilleen säästääkseen kuluissa sen sijaan, että jokaisella laitteilla olisi oma salasana. Mirai-bottiverkko saastutti tuhansia IoT-laitteita käyttämällä laitteiden oletusarvoisia kirjautumistunnuksia ja laukaisi palvelunestohyökkäyksiä. (Gebhardt 2020)

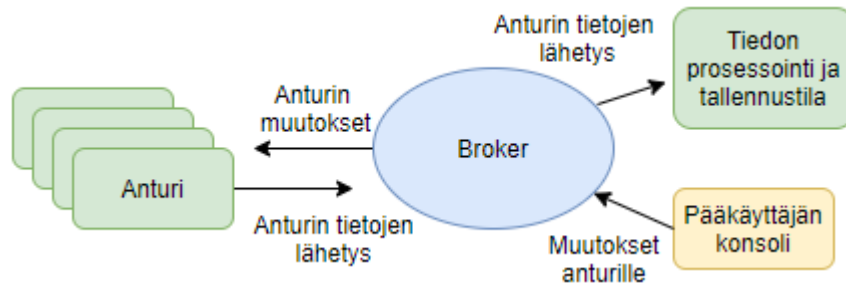
4.2 MQTT-protokollaa tukevat IoT-laitteet

MQTT (Message Queuing Telemetry Transport) on kevyt viestintäprotokolla, joka on suunniteltu lähettämään telemetriaa koneiden välillä matalan kaistanleveyden ympäristöissä. IBM on kehittänyt MQTT-protokollan vuonna 1999 ja sen alkuperäinen käyttökohde oli linkittää öljyputkien anturijärjestelmät satelliitteihin. MQTT-protokolla on nykyisin yksi käytetyimmistä protokollista IoT-laitteissa. (Cope 2021) MQTT-protokolla on standardoitu vuonna 2014 ja sitä kehittää nykyisin voittoa tavoittelematon järjestö OASIS Open. (Egli 2016)

MQTT-protokolla rakentuu kahdesta verkossa olevista entiteetistä, broker-palvelimesta ja clientistä. Broker on palvelin, joka vastaanottaa kaikki viestit clienteilta ja lähettää viestit eteenpäin toisille clienteille. Client voi olla mikä tahansa, esimerkiksi IoT-laite tai ohjelma konesalissa, joka käsittelee IoT-laitteiden tietoa. (Yuan 2020)

MQTT-protokolla on suunniteltu siten, että viestit ovat järjestelty aiheittain ja sovelluskehittäjä voi määrittää clientien oikeudet tiettyihin viesteihin. Kuvan 4 esimerkin mukaan anturit lähettävät arvoja broker-palvelimelle ja broker-palvelin lähettää ne eteenpäin

toiselle laitteelle, tiedon prosessointiin. Pääkäyttäjä voi halutessaan lähettää tietyn anturin muutokset broker-palvelimen kautta, esimerkiksi anturin herkkyyden muutokset. (Yuan 2020)

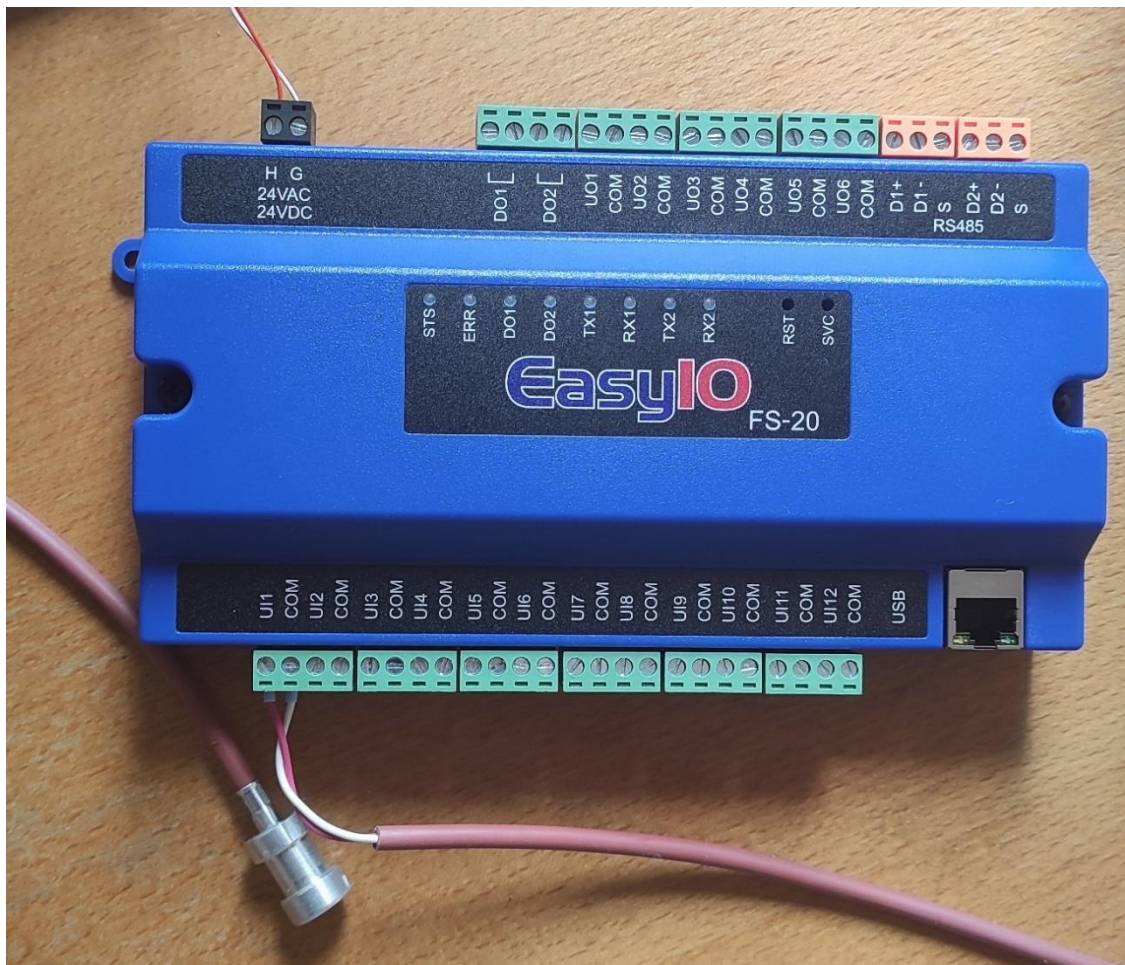


Kuva 4. MQTT-protokollan toimintaperiaate (Yuan 2020).

5 EASYIO FS-20 -KONTROLLERI

EasyIO FS-20 on rakennuksen energianhallintajärjestelmä (BEMS), joka tukee viimeisimpiä verkko- ja turvastandardeja ja rakennuksen energianhallintaan tarvittavia protokollia. Kontrollerissa on sisäänrakennettu tietokantasovellus ja web-palvelin, johon voidaan rakentaa grafiikoita HTML5- ja Javascript ohjelmointikielillä. FS-20 -kontrolleri tukee MQTT-protokollaa ja sitä varten kontrollerissa on sisäänrakennettu MQTT-ohjauspaneeli. (Johnson Controls 2021)

Kuvan 5 mukaisesti kontrollerissa on 12 universaalista sisääntuloa (UI), 6 universaalista ulostuloa (UO) ja 2 digitaalista ulostuloa (DO). Näihin ulostuloihin liitetään konesalissa olevia laitteita, kuten antureita ja puhaltimia. Ulostulojen lisäksi kontrollerissa on 2 RS485 liitäntää ja RJ45 liitäntä verkkokaapelille. Kontrolleri saa sähkövirran tavallisesta sähköverkosta.



Kuva 5. EasyIO FS-20, johon kytketty PT1000 lämpötila-anturi.

5.1 CPT-Tools

CPT Tools on avoimen lähdekoodin ohjelmointityökalu, jossa on kolmannen osapuolen kokoonpano- ja hallintatyökaluja Sedona -ympäristössä toimiville laitteille. (Johnson Controls 2021) FS-20 -kontrolleriin pääsee sisään CPT Tools -ohjelmistolla, joka puolestaan käyttää Sedona Sox -protokollaa kirjautumiseen (Kuva 6).



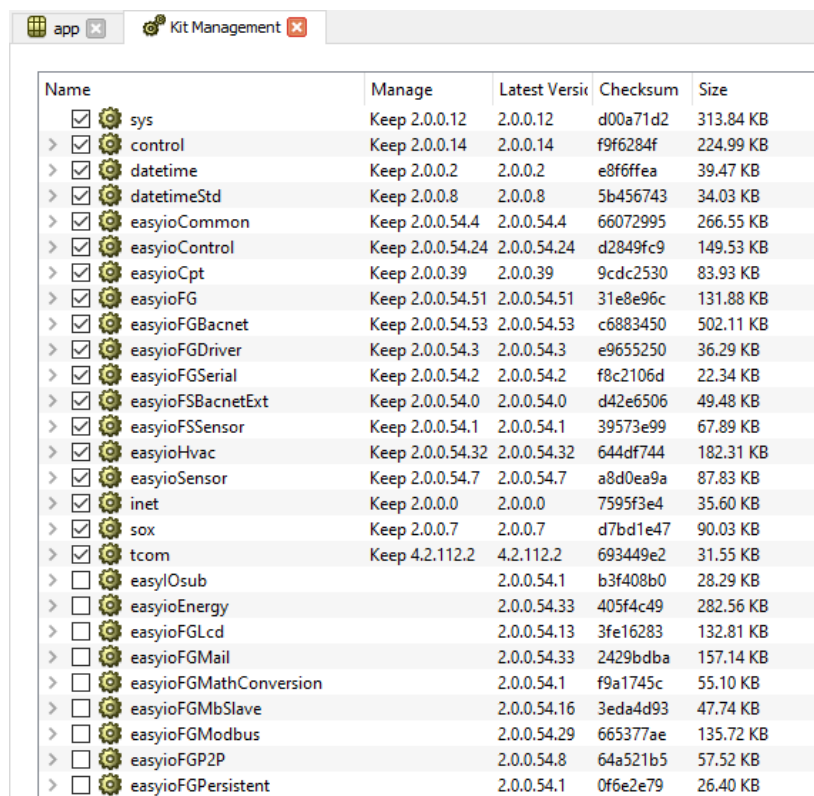
The screenshot shows the CPT Tools application window. The title bar includes a 'Recent' tab and a close button. The main interface is split into two sections. The left section, labeled 'Name', displays a list of items, currently showing 'A FS-20'. The right section contains a configuration form for logging in to an FS-20 controller. The form includes fields for 'App Desc' (FS-20), 'Protocol' (Sox), 'Host' (192.168.10.12), 'Port' (1876), 'UserName' (admin), 'Password' (with a 'Remember Password' checkbox), 'Data Folder' (SedonaFG, with an 'Add' button), and 'Web Port' (80, with an 'HTTPS' checkbox). At the bottom of the form are buttons for 'New', 'Clone', 'Delete', 'Save', and 'Open'.

Kuva 6. CPT Tools -työkalun kirjautumisosio

5.1.1 Sedona

Sedona on yhdysvaltalaisen Tridium Inc -yhtiön valmistama vapaan lähdekoodin ohjelmistoympäristö, joka on suunniteltu helpottamaan älykkäiden, verkotettujen ja sulautettujen laitteiden rakentamista, jotka soveltuvat hyvin ohjaussovellusten toteuttamiseen. Sedona -työkalun avulla sarjoissa olevat komponentit kootaan vuokaavioihin, jolloin luodaan Sedona -laitteen suorittamat sovellukset. Sedonan ohjelmointikieli soveltuu ohjausstrategioiden graafiseen esittämiseen. (Sedona Alliance 2021)

EasyIO FS-20 -kontrolleria varten on tehty erilaisia Sedona paketteja (Kuva 7). Sedona -paketeissa on rakennusautomaatiojärjestelmälle tarvittavia ominaisuuksia, joilla hallita esimerkiksi HVAC-järjestelmää. Sedona -paketteja voidaan ottaa käyttöön paketinhallintajärjestelmästä.



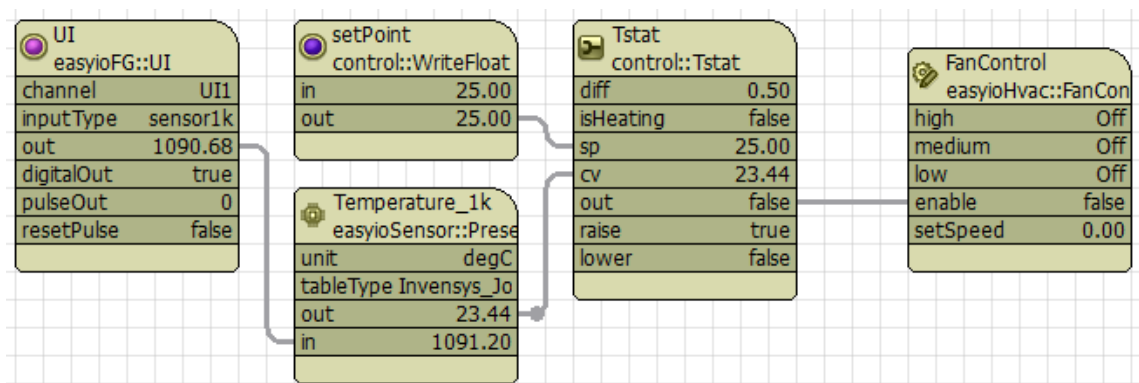
Name	Manage	Latest Version	Checksum	Size
<input checked="" type="checkbox"/> sys	Keep 2.0.0.12	2.0.0.12	d00a71d2	313.84 KB
> <input checked="" type="checkbox"/> control	Keep 2.0.0.14	2.0.0.14	f9f6284f	224.99 KB
> <input checked="" type="checkbox"/> datetime	Keep 2.0.0.2	2.0.0.2	e8f6ffea	39.47 KB
> <input checked="" type="checkbox"/> datetimeStd	Keep 2.0.0.8	2.0.0.8	5b456743	34.03 KB
> <input checked="" type="checkbox"/> easyioCommon	Keep 2.0.0.54.4	2.0.0.54.4	66072995	266.55 KB
> <input checked="" type="checkbox"/> easyioControl	Keep 2.0.0.54.24	2.0.0.54.24	d2849fc9	149.53 KB
> <input checked="" type="checkbox"/> easyioCpt	Keep 2.0.0.39	2.0.0.39	9cdc2530	83.93 KB
> <input checked="" type="checkbox"/> easyioFG	Keep 2.0.0.54.51	2.0.0.54.51	31e8e96c	131.88 KB
> <input checked="" type="checkbox"/> easyioFGBacnet	Keep 2.0.0.54.53	2.0.0.54.53	c6883450	502.11 KB
> <input checked="" type="checkbox"/> easyioFGDriver	Keep 2.0.0.54.3	2.0.0.54.3	e9655250	36.29 KB
> <input checked="" type="checkbox"/> easyioFGSerial	Keep 2.0.0.54.2	2.0.0.54.2	f8c2106d	22.34 KB
> <input checked="" type="checkbox"/> easyioFSBacnetExt	Keep 2.0.0.54.0	2.0.0.54.0	d42e6506	49.48 KB
> <input checked="" type="checkbox"/> easyioFSSensor	Keep 2.0.0.54.1	2.0.0.54.1	39573e99	67.89 KB
> <input checked="" type="checkbox"/> easyioHvac	Keep 2.0.0.54.32	2.0.0.54.32	644df744	182.31 KB
> <input checked="" type="checkbox"/> easyioSensor	Keep 2.0.0.54.7	2.0.0.54.7	a8d0ea9a	87.83 KB
> <input checked="" type="checkbox"/> inet	Keep 2.0.0.0	2.0.0.0	7595f3e4	35.60 KB
> <input checked="" type="checkbox"/> sox	Keep 2.0.0.7	2.0.0.7	d7bd1e47	90.03 KB
> <input checked="" type="checkbox"/> tcom	Keep 4.2.112.2	4.2.112.2	693449e2	31.55 KB
> <input type="checkbox"/> easyIOsub		2.0.0.54.1	b3f408b0	28.29 KB
> <input type="checkbox"/> easyioEnergy		2.0.0.54.33	405f4c49	282.56 KB
> <input type="checkbox"/> easyioFGLcd		2.0.0.54.13	3fe16283	132.81 KB
> <input type="checkbox"/> easyioFGMail		2.0.0.54.33	2429bdba	157.14 KB
> <input type="checkbox"/> easyioFGMathConversion		2.0.0.54.1	f9a1745c	55.10 KB
> <input type="checkbox"/> easyioFGMbSlave		2.0.0.54.16	3eda4d93	47.74 KB
> <input type="checkbox"/> easyioFGModbus		2.0.0.54.29	665377ae	135.72 KB
> <input type="checkbox"/> easyioFGP2P		2.0.0.54.8	64a521b5	57.52 KB
> <input type="checkbox"/> easyioFGPersistent		2.0.0.54.1	0f6e2e79	26.40 KB

Kuva 7. Sedona-pakettihallintajärjestelmä

5.1.2 Vuokaavio

Vuokaaviossa voidaan luoda sääntöjä, joita käytetään automaatioissa. Esimerkiksi lämpötila-anturilta saatava tieto voidaan määrittää kytkemään rakennuksen HVAC-järjestelmän laitteita päälle ja säätää jäähdytyksen tehoa.

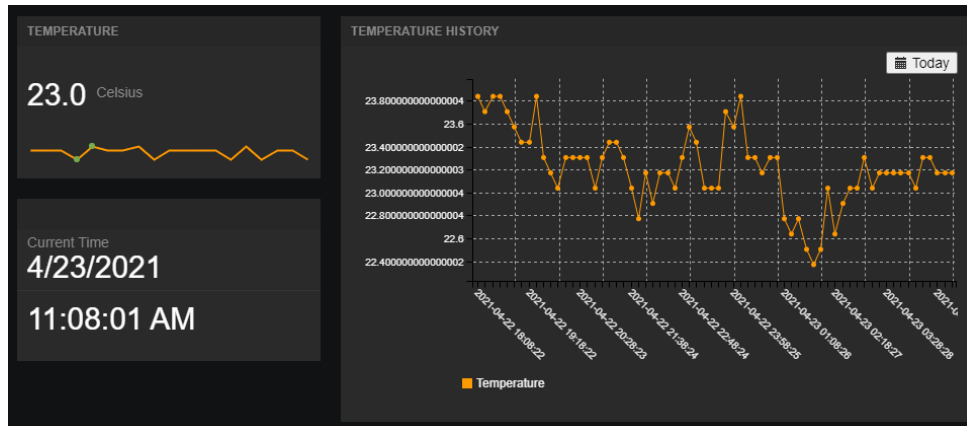
Kontrolleriin voidaan liittää erilaisia laitteita ja sähkönsyöttöä voidaan säätää resistanssin, virran tai jännitteen mukaan. Lämpötila-antureita on erilaisia, ja niillä on omat resistanssinsa. Anturit saavat lämpötilan resistanssilla ja resistanssi muunnetaan celsius- tai fahrenheitasteiksi vuokaaviossa (Kuva 8).



Kuva 8. Lämpötila-anturi kytkettynä vuokaavioon.

5.1.3 Grafiikat

EasyIO FS-20 kontrolleri sisältää sisäänrakennetun web-palvelimen, joka tukee HTML5- ja Javascript ohjelmointikieliä, mikä mahdollistaa grafiikkojen luomisen. Grafiikkojen avulla voidaan visualisoida vuokaavioon liitettyjä sedona -paketteja ja tehdä erilaisia toiminnallisuuksia FS-20 -kontrollerille ja siihen kytketyille laitteille. Grafiikka muodostuu siten, että se hakee vuokaaviosta tietoja laitteilta. Esimerkiksi lämpötilan seurantaan varten voidaan tehdä grafiikkaa lämpötilan seurannan helpottamiseksi (Kuva 9).



Kuva 9. Lämpötila-anturille tehty grafiikka.

5.1.4 Käyttäjähallinta

Käyttäjähallinnan avulla voidaan määrittää tietyt oikeudet käyttäjille grafiikoihin (Kuva 10). Järjestelmänvalvoja voi määrittää kullekin käyttäjälle oikeudet tietyn grafiikan katseluun tai muokkaamiseen. Grafiikkojen lisäksi käyttäjälle voidaan antaa oikeudet avata tiettyjä ominaisuuksia, esimerkiksi MQTT-hallintapaneelia.

Manage

Permissions Accounts Create Session AuthKey

	Path	NoAccess	ReadOnly	ReadWrite	Home
admin	test	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Engineer	Kontrollerit	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	
Manager	FS-20	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Operator	temp	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Viewer	adjustVoltage	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Developer Permission

Save

Kuva 10. Käyttäjaoikeuksien hallinta.

5.2 Palvelut

FS-20 -kontrolleri sisältää erilaisia palveluja, joita avataan kontrollerin ominaisuuksia varten (Kuva 11). Turvallisuuden vuoksi on erityisen tärkeää sulkea sellaiset palvelut, joita ei tarvita. Palveluissa olevat ohjelmat voivat sisältää haavoittuvuuksia, joita hyödyntämällä rikolliset pääsevät sisään järjestelmään ja sitä kautta häiritä konesalin toimintaa erilaisilla hyökkäyksillä. Siksi ulkopuolisten pääsy konesalin verkkoihin on estettävä minimoimalla päällä olevia palveluja ja eristettävä automaatiojärjestelmä muista kriittisistä järjestelmistä.

Service Control Panel		
Name	Status	Action
HTTP	Disabled	Enable
HTTPS	Enabled	Disable
Ftp	Enabled	Disable
SSH	Disabled	Enable
OpenVPN	Disabled	Enable
NTP	Enabled	Disable
MQTT	Enabled	Disable
Samba	Disabled	Enable

Kuva 11. Kontrollerin ohjauspaneeli palveluille.

FS-20 -kontrollerissa on vanhentuneita sovelluksia ja osasta löytyy vakavia haavoittuvuuksia, joita hyödyntämällä ulkopuoliset voivat aiheuttaa ongelmia konesalin toiminnalle, esimerkiksi asentamalla haittaohjelmia kontrollerille.

Porttiskannauksella saadaan tietoa kontrollerin käyttämistä porteista ja sen palveluista (Kuva 12). Osa porteista lähettää tietoja palveluista, kuten versiotiedot ja asetustiedot. Porttiskannaussovellukselle voidaan liittää erilaisia komentosarjoja, joiden avulla saadaan enemmän tietoja palveluista, esimerkiksi ohjelmiston haavoittuvuuksia. Haavoittuvuuksia voidaan korjata tekemällä laitteistopäivityksiä FS-20 -kontrollerille.

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
OS	Host					
192.168.10.12						
Port	Protocol	State	Service	Version		
21	tcp	open	ftp	Pure-FTPd		
22	tcp	open	ssh	OpenSSH 7.9 (protocol 2.0)		
80	tcp	open	http	nginx 1.16.1		
139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)		
443	tcp	open	http	nginx 1.16.1		
445	tcp	open	netbios-ssn	Samba smbd 4.4.5 (workgroup: WORKGROUP)		

Kuva 12. Nmap -työkalulla tehty porttiskannaus.

Porttiskannaus paljasti SMB-palvelimessa (Server Message Block) olevan Samba-ohjelmiston version olevan 4.4.5 (Kuva 13). Tässä versiossa löytyy vakava haavoittuvuus, joka mahdollistaa koodin etäsuorittamiselle, jolloin ulkopuolinen voi ladata haitallista koodia SMB-palvelimelle ja saada palvelimen lataamaan ja suorittamaan haitallisen koodin. (Özkan 2018)

Target: 192.168.10.12
Profile:
Scan Cancel

Command: nmap -p 445 --script smb-vuln-cve-2017-7494 --script-args smb-vuln-cve-2017-7494.check-version 192.168.10.12

Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans

Service
microsoft-ds
netbios-ssn

nmap -p 445 --script smb-vuln-cve-2017-7494 --script-args smb-vuln-cve-2017-7494.check-... Details

Starting Nmap 7.91 (<https://nmap.org>) at 2021-04-28 11:28 FLE Daylight Time
Nmap scan report for 192.168.10.12
Host is up (0.00013s latency).

PORT	STATE	SERVICE
445/tcp	open	microsoft-ds

MAC Address: 38:D1:35:01:32:00 (EasyIO Sdn. Bhd.)

Host script results:
| smb-vuln-cve-2017-7494:
| VULNERABLE:
| SAMBA Remote Code Execution from Writable Share
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2017-7494
| Risk factor: HIGH CVSSv3: 7.5 (HIGH) (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
| All versions of Samba from 3.5.0 onwards are vulnerable to a remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.
|
| Disclosure date: 2017-05-24
| Check results:
| Samba Version: 4.4.5
| References:
| <https://www.samba.org/samba/security/CVE-2017-7494.html>
| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7494>
|
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds

Kuva 13. Nmap -työkalulla löydetty haavoittuvuus SMB portissa.

Tätä haavoittuvuutta ei voida hyödyntää FS-20 -kontrollerissa, sillä sen SMB-palvelinta ei ole tarkoitettu tiedostojen jakamiseen, eikä palvelimelta löydy jakokansiota, jota haavoittuvuus tarvitsee. Tästä huolimatta kontrollerissa olevat palvelut pitäisi päivittää uupimpiin versioihin, koska uusia haavoittuvuuksia voidaan löytää tulevaisuudessa.

5.3 MQTT-ohjauspaneeli

MQTT-protokollaa voidaan hyödyntää FS-20 -kontrollerissa olevan MQTT-ohjauspaneelilla. MQTT-ohjauspaneelissa voidaan määritellä, millaisia tietoja halutaan lähettää kontrollerista MQTT-brokerille, esimerkiksi lämpötila-antureiden tietoja. MQTT-broker voi lähettää tiedot toiselle clientille, esimerkiksi tiedonkäsittelijälle. Tällä tavalla saadaan turvallisesti tieto konesalin toiminnasta internetin välityksellä, eikä MQTT -protokollan kautta voi vaikuttaa konesalin toimintaan.

MQTT-ohjauspaneelissa määritellään aiheet aiheiden hallinnan kautta (Kuva 14). Esimerkiksi lämpötila-anturin tietoja varten tarvitaan aiheen tilaus (subscribe) ja julkistus (publish). Tällöin broker tietää, mitä aiheita client julkistaa ja tilaa.

Name	Broker	Category	Action
temp_pub	mqtt	Publish	<button>Enabled</button>
temp_sub	mqtt	Subscribe	<button>Enabled</button>

MQTT Topic

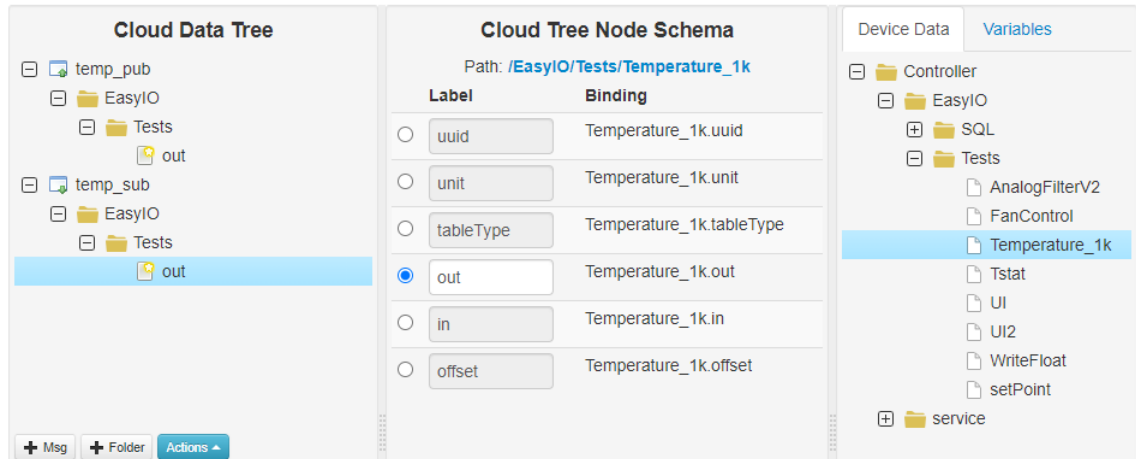
Topic Name:

Topic Path:

Topic Category:

Kuva 14. Aiheiden hallinta -toiminnallisuus, jossa määriteltä aiheet.

Kuvassa 15 aiheet lisätään MQTT-ohjauspaneelin viestienhallintaan, jossa määritellään aiheiden sisälle tarvittavat viestit, esimerkiksi lämpötila-anturista tulevat tiedot.



Kuva 15. Viestienhallinta -toiminnallisuus, jossa määriteltä viestit aiheiden sisään.

Yhteys broker-palvelimelle muodostetaan broker-hallinnan kautta (Kuva 16). Yhteyden muodostamiseksi tarvitaan brokerin verkko-osoite ja sen porttinumero, kirjautumistunnukset brokerille ja clientin tunnus. Liikenteen salaamiseksi voidaan käyttää SSL/TLS-salausta.

Name	Type	State	Action
Mosquitto	General MQTT	Success	Enabled

General MQTT

Broker Name:

Host:

Port:

Client ID:

User:

Password:

QoS:

SSL/TLS

☐ Enable TLS

CA File:

Certificate File:

Key File:

Publish Interval

Publish Interval: second

Kuva 16. Yhteyden muodostaminen broker-palvelimelle.

Lokien hallinnasta saadaan tietoja FS-20 -kontrollerin ja broker-palvelimien välisistä yhteyksistä ja viesteistä, joita lähetetään broker-palvelimille (Kuva 17). Broker-palvelin voi lähettää lämpötila-anturin tietoja eteenpäin tiedon käsittelyyn tarkoitettulle palvelimelle.

```
2021-04-24 16:28:09 INFO [6408:mqtt] data_api.c:455: Succeed in get response for url: https://127.0.0.1/sdcard/cpt/app/data_api.php
2021-04-24 16:28:08 INFO [6408:mqtt] data_api.c:443: Send write data request to https://127.0.0.1/sdcard/cpt/app/data_api.php
2021-04-24 16:28:08 INFO [6408:mqtt] mqtt.c:70: On message: /EasyIO/Tests/ {"EasyIO": {"Tests": {"out": 21.837616000000001}}}
2021-04-24 16:28:08 INFO [6408:mqtt] mqtt.c:40: Publish to topic: /EasyIO/Tests/, payload: {"EasyIO": {"Tests": {"out": 21.837616000000001}}}
```

Kuva 17. Lämpötila-anturin tietojen lähetys MQTT-brokerille

6 LOPPUPÄÄTELMÄT

Opinnäytetyön tavoitteena oli selvittää EasyIO FS-20 -kontrollerin soveltuvuus korkean turvatason konesalin automaatiojärjestelmäksi. Kontrollerin soveltuvuus testattiin tutustumalla sen ominaisuuksiin, joita otettiin käyttöön ja näitä ominaisuuksia testattiin penetraatiotestein.

EasyIO FS-20 -kontrolleri soveltuu varsin hyvin konesalin automaatiojärjestelmäksi. Se sisältää kaiken tarvittavan laitteiden ohjaamiseen ja nykyaikaisilla teknologioilla hyödynnettynä siitä voidaan saada monipuolinen ja tehokas järjestelmä automaatioon ja valvontaan.

Vaikka FS-20 -kontrolleri mahdollistaa laitteiden ohjauksen internetin välityksellä, on se turvallisuuden vuoksi laitettava omaan verkkoon, joka ei ole kytketty internetiin tai muihin järjestelmiin. Automaatiojärjestelmästä voidaan lähettää tietoja internetin saataville MQTT-protokollan avulla, mutta internetin kautta ei pääse vaikuttamaan automaatiojärjestelmän toimintoihin.

FS-20 -kontrollerille tehdyt penetraatiotestit osoittivat kontrollerin sisältävän vanhoja, haavoittuvaisia ohjelmistoja, mutta haavoittuvuuksia ei voitu hyödyntää, koska ohjelmissa puuttuu komponentteja, joita haavoittuvuus tarvitsee. Tästä huolimatta FS-20 -kontrolleri soveltuu tarkoitukseensa hyvin, sillä haavoittuvaiset palvelut voidaan kytkeä pois päältä.

Työn tulosten perusteella FS-20 -kontrolleri otetaan käyttöön konesalin automaatiojärjestelmäksi, jonka tehtävänä on hallita konesalin lämpötiloja. Tämän jälkeen automaatiojärjestelmä laajennetaan muihin infrastruktuureihin, esimerkiksi kulunvalvontaan.

LÄHTEET

- Carroll, Alex. 2021. *How to Be Prepared for the Top Four Data Center Disasters*. 29. Huhtikuu. Haettu 29. Huhtikuu 2021. <https://lifelinedatacenters.com/data-center/how-to-be-prepared-for-the-top-4-data-center-disasters/>.
- Cisco Systems. 2021. *What Is a Data Center*. 3. Huhtikuu. Haettu 3. Huhtikuu 2021. <https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html>.
- Clayton, David. 2018. *HVAC Automation & Control Systems Defined*. 4. Tammikuu. Haettu 13. Huhtikuu 2021. <https://www.arcweb.com/blog/hvac-automation-control-systems-defined>.
- Cope, Steve. 2021. *Beginners Guide to The MQTT Protocol*. 10. Huhtikuu. Haettu 10. Huhtikuu 2021. <http://www.steves-internet-guide.com/mqtt/>.
- Egli, Peter R. 2016. "AN INTRODUCTION TO MQTT, A PROTOCOL FOR M2M AND IoT APPLICATIONS." *Indigoo*. 4. Heinäkuu. Haettu 11. Huhtikuu 2021. http://www.indigoo.com/dox/wsmw/1_Middleware/MQTT.pdf.
- Evans, Paul. 2018. *Data center HVAC cooling systems*. 19. Huhtikuu. Haettu 16. Huhtikuu 2021. <https://theengineeringmindset.com/data-center-hvac-cooling-systems/>.
- Forcepoint. 2021. *What is Data Center Security?* 6. Huhtikuu. Haettu 6. Huhtikuu 2021. <https://www.forcepoint.com/cyber-edu/data-center-security>.
- Gebhardt, Patrick. 2020. *We should Talk about IoT Security*. 20. Helmikuu. Haettu 15. Huhtikuu 2021. <https://blog.paessler.com/we-should-talk-about-iot-security>.
- Geng, Hwaiyu. 2014. *Data Center Handbook*. Palo Alto, California: John Wiley & Sons.
- HVACSchool.org. 2021. *BUILDING AUTOMATION SYSTEMS ARE CHANGING THE HVAC CONTROLS LANDSCAPE*. 15. Huhtikuu. Haettu 15. Huhtikuu 2021. <https://www.hvacschool.org/building-automation-systems/>.
- Johnson Controls. 2021. *CPT Tools*. 18. Huhtikuu. Haettu 18. Huhtikuu 2021. <https://easyio.eu/cpt-tools/>.

- . 2021. "EasyIO FS-20." 4. Huhtikuu. Haettu 2. Huhtikuu 2021. https://easyio.eu/wp-content/uploads/2021/02/fs20_eng.pdf.
- Kotakallio, Juho, Kimmo Frilander, Eija Hatanpää, Pauliina Hirvonen, Tuukka Kivioja, Sisko Minkkinen, Panu Moilanen, Tarja Rusi, Minna Uusitalo, ja Tiina Vestman. 2021. *Internet of Things (IoT) eli esineiden internet*. 28. Tammikuu. Haettu 30. Maaliskuu 2021. <https://peda.net/jyu/it/do/kkv/6kvjvt/6tth/iotieei2>.
- Lueth, Knud Lasse. 2018. *State of the IoT 2018: Number of IoT devices now at 7B - Market accelerating*. 8. Elokuu. Haettu 11. Huhtikuu 2021. <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>.
- Özkan, Serkan. 2018. *CVE-2017-7494*. 21. Lokakuu. Haettu 26. Huhtikuu 2021. <https://www.cvedetails.com/cve/CVE-2017-7494/>.
- Penttinen, Jyrki T. J. 2017. *Wireless communications security : solutions for the internet of things*. New Jersey: John Wiley & Sons.
- Roach, John. 2021. *To cool datacenter servers, Microsoft turns to boiling liquid*. 6. Huhtikuu. Haettu 8. Huhtikuu 2021. <https://news.microsoft.com/innovation-stories/datacenter-liquid-cooling/>.
- Sedona Alliance. 2021. *What is Sedona?* 19. Huhtikuu. Haettu 19. Huhtikuu 2021. <https://www.sedona-alliance.org/aboutsedona.htm>.
- Senseware Inc. 2017. *How Building Automation Systems Work*. 10. Huhtikuu. Haettu 17. Huhtikuu 2021. <https://blog.senseware.co/2017/04/10/building-automation-systems-work>.
- Shailaja, C. 2020. *Physical security of a data center*. 31. Maaliskuu. Haettu 6. Huhtikuu 2021. <https://www.isa.org/intech-home/2020/march-april/departments/physical-security-of-a-data-center>.
- Vaisala. 2017. *Datakeskusten konesalien jäähdytys*. 1. Kesäkuu. Haettu 2. Huhtikuu 2021. <https://www.vaisala.com/fi/case/datakeskusten-konesalien-jaahdytys>.
- Yuan, Michael. 2020. *Getting to know MQTT*. 7. Tammikuu. Haettu 10. Huhtikuu 2021. <https://developer.ibm.com/components/mqtt/articles/iot-mqtt-why-good-for-iot>.

