Konsta Antikainen

IoT-teknologian hyödyntäminen sähköverkon mittaustiedon keräämisessä

Opinnäytetyö
Sähkö- ja automaatiotekniikka

2019

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tekijä/Tekijät	Tutkinto	Aika
Konsta Antikainen	Insinööri (AMK)	Toukokuu 2019

Opinnäytetyön nimi

IoT-teknologian hyödyntäminen sähköverkon mittaustiedon keräämisessä

137 sivua
0 liitesivua

Toimeksiantaja

Suur-Savon Sähkö Oy

Ohjaaja

Harri Kosonen, Pekka Nurmi

Tiivistelmä

Tämän opinnäytetyön tarkoituksena oli tutkia IoT-teknologian hyödyntämistä sähköverkon mittaustiedon keräämisessä ja käytännön työnä kehittää ratkaisu Järvi-Suomen Energian sähköverkossa sijaitsevien 1 kV:n katkaisijoiden valvontaan IoT-teknologiaa hyödyntäen.

Opinnäytetyössä perehdyttiin IoT-käsitteeseen sekä tällä hetkellä käytössä ja saatavilla oleviin erilaisiin IoT-teknologioihin ja laitteisiin, joiden soveltuvuutta käytettäväksi sähköverkon mittaustiedon keräämisessä tutkittiin. Tämän perusteella kehitettiin myös 1 kV:n katkaisijoiden valvontaratkaisu kartoittamalla aluksi katkaisijoille sijoitettaville IoT-laitteille asetetut lähtövaatimukset, minkä jälkeen valittiin käyttöön soveltuvin teknologia, jota käyttäen ratkaisu kehitettiin.

Erilaisista IoT-teknologioista ja niihin soveltuvista päätelaitteista tutkittiin esimerkiksi matkapuhelinverkkojen ja niiden IoT-teknologioiden hyödyntämistä sekä erilaisia LPWAN-verkkoja, joista päätettiin ottaa käyttöön LoRaWAN-teknologia Digitan verkkoa hyödyntäen, sekä Elsys ELT-2 -anturia pilottilaitteena katkaisijalla käyttäen. Lisäksi toteutettiin Application Server -palvelin, jota käytettiin datan vastaanottoon ja muuntamiseen IEC-104-protokollalle mittaustietojen viemiseksi olemassa olevaan SCADA-järjestelmään.

Opinnäytetyön lähtötavoitteet saavutettiin ja käytännön työn tuloksena saatiin toteutettua Suur-Savon Sähkön / Järvi-Suomen Energian käyttöön ratkaisu 1 kV katkaisijoiden valvontaan, joka testattiin onnistuneesti toimivaksi käytännön olosuhteita vastaavasti.

Johtopäätöksinä voidaan todeta sähköverkoissa olevan perinteisen sähköverkkoautomaation lisäksi hyödyntämismahdollisuuksia myös IoT-teknologiaan perustuville ratkaisuille kohteissa, jotka eivät ole kriittisiä, mutta joista kuitenkin halutaan esimerkiksi kerätä mittausdataa, mikä ei olisi kannattavaa perinteisiä automaatioratkaisuja käyttäen esimerkiksi suurten investointikustannusten johdosta.

IoT-teknologian ei kuitenkaan voida ainakaan tällä hetkellä tässä opinnäytetyössä käsitellyssä muodossaan katsoa korvaavan perinteistä sähköverkkoautomaatiota sähköverkon kriittisissä kohteissa, sillä esimerkiksi tämänkaltaisen IoT-tekniikan luotettavuuden ei välttämättä voida todeta olevan siihen riittävällä tasolla.

Asiasanat

IoT, sähköverkon mittaustiedon kerääminen, 1 kV, LoRaWAN, SCADA, IEC-104

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree	Time
Konsta Antikainen	Bachelor of Engineering	May 2019

Thesis title

Utilization of IoT technology in electricity grid measurement data acquisition

137 pages
0 pages of appendices

Commissioned by

Suur-Savon Sähkö Oy

Supervisor

Harri Kosonen, Pekka Nurmi

Abstract

The objective of this thesis was to study the utilization of IoT technologies for the acquisition of electricity distribution grid measurement data. The practical part of the thesis consisted of development of a monitoring solution for 1 kV breakers utilizing IoT technology.

The definition of the IoT technology and the current availability of the different IoT end-devices and networking technologies were studied and the suitability of them for utilization in electricity grid measurement data acquisition evaluated. The development of the breaker monitoring solution was accomplished by surveying the requirements for the end-devices and selecting the most suitable, currently available IoT technology for this case.

From all the different IoT technologies and end-devices based on them, the technologies based on the cellular networks and different LPWAN networks were studied. The breaker monitoring solution was built on the LoRaWAN technology and it utilized the network operated by Digita and an Elsys ELT-2 sensor as the end-device at the breaker. An Application Server for receiving and processing of the data was also deployed and the data transmitted to the existing SCADA system using the traditional IEC-104 protocol.

The goals of the thesis were successfully achieved and as a result of the practical part, a concept for monitoring the 1 kV breakers in the electricity grid of Järvi-Suomen Energia was developed and successfully tested in conditions reflecting the real environment.

As conclusions of the thesis, potential for the utilization of IoT based data acquisition seems to be present in the electricity distribution grids. Especially the cost-effectiveness of the IoT end-devices in comparison to the traditional automation enables them to be used for gathering “not-that-critical” data from locations where it would not be reasonable to use the traditional automation systems.

Nonetheless, IoT technology cannot be directly regarded as a replacement for the traditional automation. Especially in critical parts of the electricity distribution automation which affects a high number of customers, its usage is questionable, mainly because the reliability of the IoT technology at least in this form might not necessarily be at the level required for these cases.

Keywords

IoT, electricity grid measurement data acquisition, 1 kV, LoRaWAN, SCADA, IEC-104

SISÄLLYS

LYHENNELUETTELO

3GPP	3rd Generation Partnership Project
ABP	Activation by Personalization
ACK	Acknowledgement
ADR	Adaptive Data Rate
AES	Advanced Encryption Standard
AMQP	Advanced Message Queuing Protocol
ANSI	American National Standard Institute
APCI	Application Protocol Control Information
APDU	Application Protocol Data Unit
API	Application Programming Interface
APN	Access Point Name
AS	Application Server
ASDU	Application Service Data Unit
CA	Certification Authority
CHIRP	Compressed High Intensity Radar Pulse
CLI	Command Line Interface
COA	Common Object Address
CoAP	Constrained Application Protocol
COT	Cause of Transmission
DBMS	Database Management System
DI	Digital Input
DNP	Distributed Network Protocol
DNS	Domain Name System
DR	Data Rate
EC-GSM-IoT	Extended Coverage GSM for Internet of Things
ETSI	European Telecommunications Standards Institute
EUI	Extended Unique Identifier
FSK	Frequency Shift Keying
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol

ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IIS	Internet Information Services
IOA	Information Object Address
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
JSE	Järvi-Suomen Energia
JSON	JavaScript Object Notation
LAN	Local Area Network
LoRaWAN	Long-Range Wide Area Network
LPWAN	Low-Power Wide Area Network
LRC	Long-Range Controller (Actilityn Network Server)
LTE	Long Term Evolution
MAC	Medium Access Control
MDO	Master Data Object
MIC	Message Integrity Code
MQTT	Message Queuing Telemetry Transport
MTC	Machine Type Communication
NB-IoT	Narrowband IoT
NFC	Near Field Communication
NO	Normally Open
NSSM	Non-Sucking Service Manager
ODBC	Open Database Connectivity
OPC	Open Platform Communications
OTAA	Over the Air Activation
PIR	Passive Infrared Sensor
QoS	Quality of Service
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
REST	Representational State Transfer
RF	Radio Frequency
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SDGW	Scada Data Gateway

SF	Spreading Factor
SHA	Secure Hash Algorithm
SMQTT	Secure Message Queuing Telemetry Transport
SQL	Structured Query Language
SRD	Short Range Device
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on tutkia IoT-teknologian hyödyntämistä sähköverkon mittaustiedon keräämisessä ja käytännön osuuden tavoitteena toteuttaa Järvi-Suomen Energian 1 kV:n jakeluverkossa sijaitsevien katkaisijoiden tilatietojen valvonnan mahdollistava ratkaisu kyseistä teknologiaa hyödyntäen.

Työ toteutettiin, sillä IoT-teknologian todettiin olevan hyvinkin ajankohtainen aihe, minkä hyödyntämiseen liittyy lisäksi runsaasti erilaisia tulevaisuuden visioita esimerkiksi tulevista uuden tekniikan, kuten viidennen sukupolven matkapuhelinverkkojen tarjoamista mahdollisuuksista.

Lisäksi myös sähköverkoissa ja niiden kuormitusprofiilissa on odotettavissa tulevaisuudessa tapahtuvia muutoksia esimerkiksi sähköautojen yleistymisen johdosta, mitkä mahdollisesti lisäävät tarvetta sähköverkosta kerättävälle mittaustiedolle ja erilaisille valvontakohteille, mitä ei kuitenkaan välttämättä ole kaikissa tapauksissa mahdollista tai järkevää toteuttaa aikaisemmin käytetyillä, perinteisillä sähköverkkoautomaatioratkaisuilla.

Työssä perehdytään aluksi yleisesti IoT-teknologiaan sekä IoT:n käsitteeseen ja tarkastellaan, miten tekniikkaa voitaisiin hyödyntää sähköverkon mittaustiedon keräämisessä. IoT-teknologian eri osa-alueista työssä syvennytään erityisesti tämänkaltaiseen käyttötarkoitukseen soveltuviin teknologian osa-alueisiin jättäen mahdollisesti muut osa-alueet vähemmälle huomiolle.

Opinnäytetyön käytännön osuudessa tutkitaan, onko kyseinen teknologia soveltuvaa 1 kV katkaisijoiden valvontaa varten ja voidaanko se toteuttaa tällä hetkellä saatavilla olevaa IoT-teknologiaa hyödyntäen. Lisäksi työn osana myös onnistuessaan toteutetaan kyseinen 1 kV katkaisijan valvontaratkaisu käytännössä ja todistetaan sen toiminta sekä teknologian soveltuvuus tähän käyttötarkoitukseen käytännön olosuhteita vastaavasti.

Työn pohdintaosuudessa tarkastellaan esimerkiksi työn lopputuloksia ja mahdollisia jatkokehityssuunnitelmia työn käytännön osuuden osalta, sekä pohditaan myös yleisesti IoT-teknologian käyttöä sähköverkon erilaisissa valvonta- ja mittauskohteissa työn yhteydessä saatujen kokemusten perusteella.

2 IOT-TEKNOLOGIA

Lyhenne IoT muodostuu sanoista Internet of Things, millä tarkoitetaan ”esineiden internetiä”. IoT-teknologia käsittää hyvin laajan alueen erilaisia käyttökohteita ja monenlaisia järjestelmiä, joissa teknologiaa hyödynnetään ja mahdollisesti tullaan tulevaisuudessa hyödyntämään. (Chebudie ym. 2014, 6.)

IoT:lle ei välttämättä pystytä löytämään yksiselitteistä, tarkkaa määritelmää, vaan eri standardit ja esimerkiksi laitevalmistajat tulkitsevat ja määrittelevät Internet of Thingsin eri tavoin, usein jokainen omasta näkökulmastaan kuitenkaan onnistumatta määrittelemään termiä kokonaisuudessaan (Chebudie ym. 2014, 6–7).

Tämän johdosta termi IoT esiintyykin yleisesti hyvinkin monenlaisissa yhteyksissä, kuten esimerkiksi erilaisissa laitteissa ja ohjelmistoissa sekä myös suurissa kokonaisuuksissa ja järjestelmissä (Chebudie ym. 2014, 6–7).

Esimerkiksi tarkastelemalla eri standardien mukaisia määritelmiä IoT-termille, voidaan niiden perusteella vetää johtopäätös, että IoT olisi kokonaisuus erilaisia verkottuneita ”esineitä”, jotka voidaan tunnistaa, nimetä ja määritellä niille osoitteet (Chebudie ym. 2014, 22).

Haettaessa termille kokonaisvaltaista määritelmää Chebudie ym. määrittelevät tutkimuksessaan pienehkön yksinkertaisen IoT-järjestelmän seuraavasti:

”An IoT is a network that connects uniquely identifiable “Things” to the Internet. The “Things” have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the “Thing” can be collected and the state of the ‘Thing’ can be changed from anywhere, anytime, by anything.“ (Chebudie ym. 2014, 74.)

Tämä määritelmä ei esimerkiksi ota kantaa IoT-verkon laitteiden hardwareen, tekniseen toteutukseen, ohjelmistoihin, käytettyihin tietoliikenneyhteyksiin tai muuhun infrastruktuuriin, vaan määritelmässä lähestytään aihetta laitteiden muodostaman järjestelmän mahdollistaman funktionaalisuuden kautta.

Tässä työssä IoT-teknologiaa lähestytään erityisesti siihen liittyvien päätelaitteiden ja erilaisten langattomien tiedonsiirtotekniikoiden yhdessä mahdollistamien toiminnallisuuksien kautta, joita voitaisiin hyödyntää sähköverkon mittaustiedon keräämisessä.

2.1 IoT-laitteet

Kuten aikaisemmin todettiin, IoT-termille on määrittelijästä riippuen erilaisia määritelmiä, joiden alle mahtuu erittäin suuri määrä erilaisia skenaarioita ja käyttötarkoituksia ja sitä myöten markkinoilla onkin huomattavasti erilaisia IoT-laitteita, ja laitteita, joita voidaan jonkin määritelmän mukaisesti pitää IoT-laitteena, vaikka valmistaja ei ko. termiä markkinoinnissa käyttäisikään.

Chebudien ym. tutkimuksessa IoT-laitteet ovat määritelty laitteiksi, jotka yhdistävät fyysisiä esineitä tai kokonaisuuksia Internetiin esimerkiksi erilaisten valvontaominaisuuksien kautta, jonka perusteella IoT-laitteiksi voidaan katsoa esimerkiksi seuraavat laitetyypit (Chebudie ym. 2014, 42–43):

- ”Tägit”, esimerkiksi RFID-tägit, joita käytetään esimerkiksi erilaisten esineiden tunnistamiseen.
- ”Lukijat”, joita käytetään ”tägien” sisältämän datan lukemiseen ja kirjoittamiseen sekä tiedon välittämiseen eteenpäin, esimerkiksi tietokantaan.
- ”Anturit”, jotka mahdollisesti yksilöivät fyysisen esineen (thing) ja mittaavat siitä jonkinlaista dataa, kuten esimerkiksi lämpötilaa.
- ”Toimilaitteet”, jotka kykenevät esimerkiksi vaikuttamaan fyysisen esineen fyysiseen tilaan tai sen toiminnallisuuteen.

IoT-sovelluksissa usein käytettyjä IoT-laitteita ovat esimerkiksi erilaiset anturit ja toimilaitteet, joilla joko mitataan jotain suuretta prosessista tai vaikutetaan prosessin toimintaan.

Monille IoT-laitteille on lisäksi tyypillistä langaton tietoliikenneyhteys ja akkukäyttöisyys, mutta toisaalta myös esimerkiksi kiinteitä tietoliikenneyhteyksiä ja

ulkoista sähkönsyöttöä vaativia IoT-laitteita on myös erilaisten määritelmien mukaan olemassa.

Yksinkertaisia esimerkkejä ehkä yleisesti IoT-laitteina mielletyistä IoT-laitteista ovat pienet langattomat lämpötila- tai kosteusanturit ja vastaavat. Esimerkkinä tällaisesta kuvassa 1 esitetään pientä, langattomaan lähiverkkoon liitettävää paristokäyttöistä lämpötila/kosteusanturia.

Kuva 1. WiCub "Wifi IoT" -lämpötila- ja kosteusanturi (Kickstarter 2019)

2.2 Tietoliikenne

IoT-laitteiden muodostaessa verkon on niille kaikille yhteistä tietoliikenneyhteyden tarve. IoT:n määritelmä ei kuitenkaan välttämättä ota kantaa tietoliikenneyhteyden toteutustapaan tai esimerkiksi käytettyihin protokolliin, joten IoT-laitteille onkin olemassa useita erilaisia ratkaisuja fyysisen verkkoyhteyden muodostamiseen sekä myös tiedonsiirtoon käytettäviin protokolliin.

Akkukäyttöisillä IoT-laitteilla alhaisen virrankulutuksen mahdollistamiseksi on kehitetty erilaisia langattomia Low-Power WAN -verkkoja, joiden lisäksi käytössä ovat myös esimerkiksi perinteiset ethernet-pohjaiset (LAN) ja langattomat lähiverkot (WLAN) IP-protokollineen, jotka soveltuvat hyvin jatkuvan sähkönsyötön piirissä oleville laitteille.

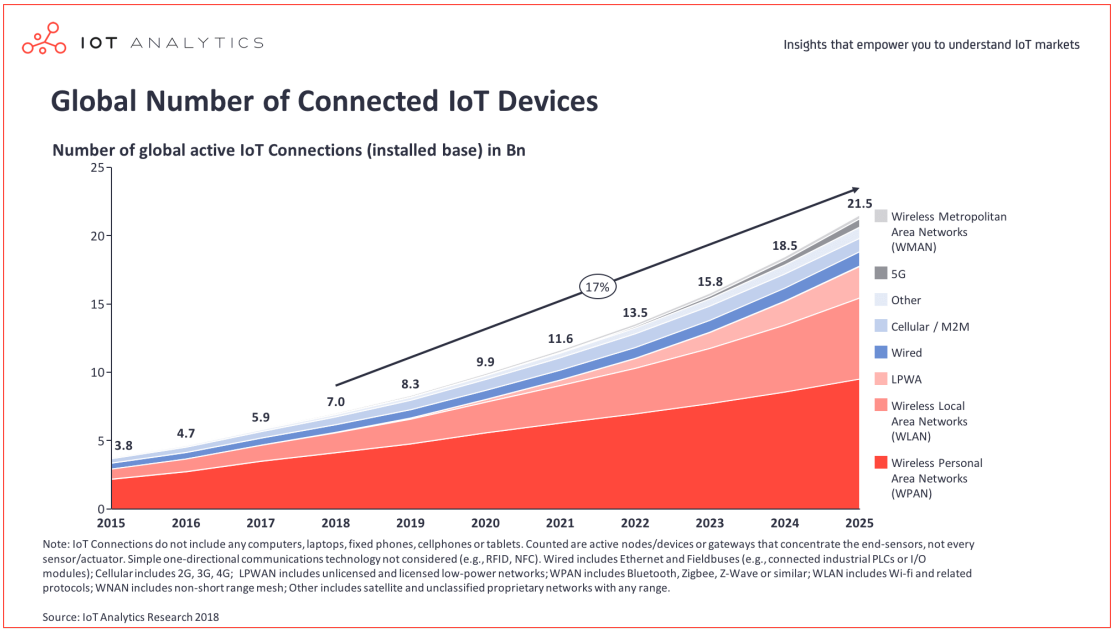
Lisäksi matkapuhelinverkoissa on otettu käyttöön uusia tekniikoita, jotka parantavat verkkojen soveltuvuutta erityisesti akkukäyttöisille IoT-laitteille alentamalla verkkoyhteyden ylläpidon vaatimaa sähkönkulutusta merkittävästi.

IoT-käyttöön tarkoitettuja WWAN-verkkoja (Wireless Wide Area Network), jotka eivät hyödynnä matkapuhelin- tai perinteisten langattomien lähiverkkojen tapaan IP-protokollaa, ovat esimerkiksi LPWAN-verkoiksi luokiteltavat suurimmat LoRaWAN ja Sigfox sekä näiden lisäksi erilaiset laitevalmistajien omat, suljetut ratkaisut.

Lisäksi käytössä on muita vastaavia lyhyen kantaman WPAN-verkkoja (Wireless Personal Area Network) esimerkiksi kotitalouksissa käytettäviä ”Smart Home” -laitteita varten. Tällaisia ovat esimerkiksi ZigBee, Z-Wave ja Bluetooth (Pasqua 2018).

Tällä hetkellä kaikkien IoT-laitteiden käyttämistä tietoliikenneratkaisuista selvästi yleisimpiä ovat WPAN- ja WLAN-verkot, mikä lienee seurausta IoT-laitteiden yleistymisestä kotitalouksissa ym. vastaavassa käytössä, missä IoT-laitteet sijaitsevat fyysisesti pienellä alueella esimerkiksi asunnossa tai henkilökohtaisessa käytössä (Pasqua 2018).

Kuvassa 2 havainnollistetaan IoT-laitteiden käyttämiä verkkoteknologioita tällä hetkellä ja ennustetaan kehitystä seuraavien vuosien aikana.



Kuva 2. IoT-laitteiden käyttämät verkkoteknologiat nyt ja tulevaisuudessa (Pasqua 2018)

2.2.1 Matkapuhelinverkkojen IoT-teknologiat

Matkapuhelinverkkoihin on kehitetty ja 3GPP:n (3rd Generation Partnership Project) toimesta standardisoitu kolme erilaista ratkaisua palvelemaan erityisesti IoT-laitteita ja niiden tarpeita (GSM Association 2016, 1).

Nämä ratkaisut ovat EC-GSM-IoT (Extended Coverage GSM for Internet of Things), LTE MTC Cat M1 (Long Term Evolution Machine Type Communications Category M1) sekä NB-IoT (Narrowband-IoT) (GSM Association 2016, 1).

Nämä teknologiat toimivat lisensoiduilla, jo entuudestaan olemassa olevan matkapuhelin/mobiilidataverkon käyttämillä taajuusalueilla, joten mobiiliverkko-operaattoreiden on helppo ottaa käyttöön ko. teknologiat omissa verkoissaan (GSM Association 2016, 26). Tämä kuitenkin tarkoittaa, että esimerkiksi yritykset eivät pysty helposti rakentamaan omia privaattiverkkoja kyseisiä tekniikoita käyttäen.

Teknologiat ovat lisäksi suunniteltu siten, etteivät ne aiheuttaisi haittavaikutuksia nykyisille matkapuhelinverkoille tai matkapuhelintukiasemien entiselle laitteistolle, jotta tekniikan käyttöönotto jo entuudestaan olemassa olevassa matkapuhelinverkossa ei aiheuttaisi ongelmia (GSM Association 2016, 16).

EC-GSM-IoT-teknologia on entisiin GSM-verkkoihin ohjelmistopäivityksillä lisättävissä oleva IoT-laitteiden käyttöön optimoitu teknologia, jossa on kiinnitetty huomiota esimerkiksi kantaman pidentämiseen ja laitteiden pitkään paristonkestoaikaan. Teknologia on suunniteltu takaisinpäin yhteensopivaksi, jotta samoja verkon resursseja voidaan käyttää myös perinteisille pakettikytkentäisille palveluille. (GSM Association 2016, 18.)

LTE MTC Cat M1 on aikaisemmista LTE MTC -standardeista parannettu versio, jossa on tavoiteltu kompleksisuuden vähentämistä edeltävästä CAT 0 -standardista, parempaa verkon kattavuutta sekä päätelaitteiden paristojen pidempää käyttöikää säilyttäen samalla mahdollisuus käyttää jo aikaisemmin asennettua laitekantaa (GSM Association 2016, 17).

NB-IoT on uusi, erityisesti kokonaan IoT-laitteita varten suunniteltu matkapuhelinverkkojen teknologia, joka kykenee tarjoamaan erityisesti pidemmän kantaman myös hankalissa olosuhteissa sekä siinä on kiinnitetty erityistä huomiota myös päätelaitteiden mahdollisimman pitkään, jopa yli 10 vuoden akkukestoon (GSM Association 2016, 19).

NB-IoT on lisäksi olemassa olevien LTE-verkkojen kanssa yhteensopiva, jolloin se voidaan ottaa käyttöön joko olemassa olevan LTE-taajuusalueen sisällä tai kokonaan omana verkkonaan. Lisäksi NB-IoT-teknologia pystyy toimimaan yhdessä myös kaikkien perinteisten matkapuhelinverkkotekniikoiden kanssa ongelmia aiheuttamatta. (GSM Association 2016, 28–29.)

Matkapuhelinverkoissa datan siirto tapahtuu normaalisti IP-protokollaa hyödyntäen, kuten internetissä yleensäkin. Verkko ei tällöin rajoita varsinaisen laitteen ja dataa vastaanottavan palvelimen välillä käytettäviä Session Layer -protokollia, joita tarkastellaan hieman myöhemmin.

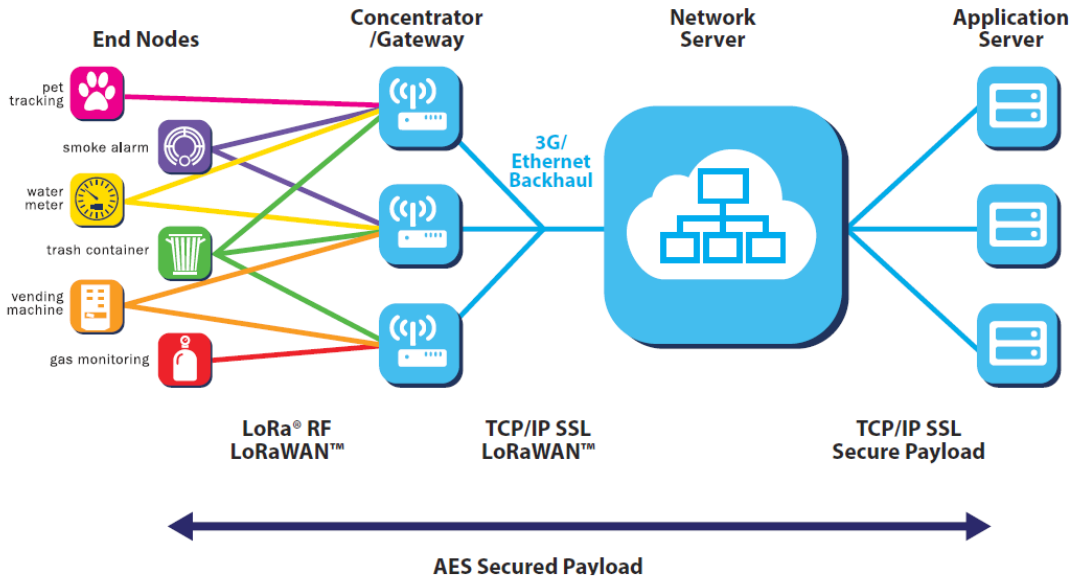
2.2.2 LoRaWAN

LoRaWAN (Long-Range Wide Area Network) on yksi IoT-laitteiden käyttöön suunnitelluista LPWAN (Low-Power Wide Area Networks)-verkkostandardeista. LoRaWAN käyttää fyysisenä yhteytenä pääosin LoRa-radioverkkoa ja määrittelee sen lisäksi verkon arkkitehtuurin ja tietoliikenteeseen käytettävän

protokollan, josta muodostuu kokonaisvaltainen verkkoratkaisu IoT-laitteiden käyttöön. (LoRa Alliance 2015, 7.)

LoRaWAN-verkko muodostuu concentrator/gateway-laitteista, joihin verkkoon liitettävät IoT-laitteet ovat yhteydessä, Network Serveristä ja näiden gateway-laitteiden ja Network Serverin välisestä IP-pohjaisesta backhaul-verkosta (LoRa Alliance 2015, 9).

LoRaWAN käsittää tietoliikenteen IoT-laitteelta Network Serverille asti, josta liikenne ohjataan jälleen IP-verkon ylitse standardeja protokollia käyttämällä sen vastaanottavalle ohjelmistolle (LoRa Alliance 2015, 9). Verkon arkkitehtuuria havainnollistetaan kuvassa 3.



Kuva 3. Havainnekuva LoRaWAN-verkon arkkitehtuurista (LoRa Alliance 2015, 8)

IoT-laitteet lähettävät dataa, jonka yksi tai useampi LoRaWAN-gateway vastaanottaa ja välittää verkon Network Serverille. Tämä palvelin ”hallitsee” liikennöintiä IoT-laitteiden ja dataa vastaanottavan palvelimen välillä ja esimerkiksi hävittää ylimääräiset paketit, jotka ovat mahdollisesti syntyneet kahden eri gateway-laitteen vastaanottaessa yhden IoT-laitteen lähettämät paketit. (LoRa Alliance 2015, 9.)

LoRaWAN-verkossa on erityisesti kiinnitetty huomiota IoT-laitteiden alhaiseen sähkönkulutukseen, mikä tekee vuosia akkujen varassa toimivien laitteiden valmistamisen mahdolliseksi (LoRa Alliance 2015, 9).

LoRaWAN-verkko on asynkroninen, ja siinä olevien laitteiden tarvitsee muodostaa yhteys verkkoon vain silloin, kun niillä on lähetettävää dataa. Tämän johdosta IoT-laitteiden, kuten esimerkiksi erilaisten sensoreiden virrankulutus on huomattavasti alhaisempi kuin esimerkiksi matkapuhelinverkossa toimivilla laitteilla. (LoRa Alliance 2015, 9.)

LoRaWAN-verkossa laitteet ovat jaoteltu kolmeen eri luokkaan käytettävissä olevan sähkön ja laitteelle päin suunnatun datan latenssin suhteen. A-luokan laitteet ovat pääasiassa akkukäyttöisiä sensoreita, jotka ovat yhteydessä verkkoon vain silloin, kun niillä on lähetettävää dataa. Tämän vuoksi myöskään tiedonsiirto sensoreille päin ei onnistu, kuin välittömästi niiltä vastaanotetun datan lähettämisen jälkeen. (LoRa Alliance 2015, 10.)

B-luokan laitteet ovat akkukäyttöisiä toimilaitteita, jotka kuuntelevat verkkoa säännöllisisin väliajoin ja vastaanottavat tällöin myös niille suunnatut ohjauskomennot. C-luokan laitteet ovat käytännössä ulkopuolisen sähkönsyötön piirissä olevia laitteita, jotka pystyvät kuuntelemaan verkkoa jatkuvasti, ja täten viivettä niille lähetetyn datan suhteen ei juurikaan esiinny. (LoRa Alliance 2015, 10.)

LoRaWANin käyttämä LoRa-radiotekniikka toimii lisensoimattomalla taajuusalueella, joka mahdollistaa myös oman LoRaWAN-verkon rakentamisen ilman taajuusalueen käyttöön tarvittavaa lupaprosessia. Oman LoRaWAN-verkon rakentaminen verkon osalta tapahtuu asentamalla riittävä määrä tukiasemia kattamaan IoT-laitteiden sijainnit, Network Server ja näiden välille tarvittavat tietoliikenneyhteydet.

LoRaWAN-verkkoja on myös saatavilla kaupallisten operaattorien tuottamina, jollaista Suomessa ylläpitää Digita. Operaattorin verkkoa käyttämällä säästytään oman verkon rakentamiselta, mikä voi osoittautua kokonaistaloudellisemmaksi ratkaisuksi esimerkiksi tilanteessa, jossa laitteita on vähän geografisesti laajalla alueella.

Digitan LoRaWAN-verkko hyödyntää pääosin jo olemassa olevia Digitan TV/Radio-lähetystoimintaan liittyviä tukiasemamastoja, ja sen tavoitteena on koko Suomen kattava peittoalue. Digita arvioi, että vuoden 2019 aikana käyttöön saadaan jo 400 tukiasemaa, vuoden 2018 luku on 150 kappaletta. (Digita 2018a, 8.)

2.2.3 Sigfox

Sigfox on LoRaWANin tavoin IoT-laitteiden käyttöön suunniteltu kaupallinen LPWAN-verkkoratkaisu, joka määrittelee sekä fyysisen siirtotien että siinä käytettävän protokollan.

Sigfox-verkoissa on kiinnitetty huomiota mahdollisimman pitkälle optimoituun protokollaan ja datan käsittelyyn pilvessä laitteiden sijasta, jonka tarkoituksena on vähentää IoT-laitteiden virrankulutusta ja mahdollistaa edellytykset pitkälle akun kestoiälle akkukäyttöisissä sovelluksissa (Sigfox 2018a).

Sigfox-verkoissa kaikki data siirretään IoT-laitteilta Sigfox Cloudiin, johon asiakkaan sovelluksen on mahdollista liittyä HTTPS-protokollaa käyttäen datan vastaanottamiseksi ja lähettämiseksi Sigfox-laitteille (Sigfox 2018b). Tämän vuoksi esimerkiksi LoRaWAN-verkosta poiketen Sigfox-tekniikalla ei ole mahdollista rakentaa omaa paikallisverkkoa, vaikka se toimiikin lisensoimattomalla taajuusalueella.

Sigfox-organisaation tarkoituksena on tarjota maailmanlaajuinen Sigfox-verkko, joka mahdollistaa esimerkiksi joustavan IoT-laitteiden liikkumisen eri valtioiden alueella ilman erillisiä roaming tms. -maksuja (Sigfox 2018c). Sigfox-verkkoa operoivat Sigfox-organisaation lisäksi eri partner-operaattorit, jollainen Suomessa on Connected Finland (Sigfox 2018d).

Connected Finlandin operoima Sigfox-verkko kattaa tällä hetkellä noin 85 % Suomen väestöstä (Connected Finland 2018).

2.2.4 Katsaus ”IoT-protokollista” IP-verkoissa

IoT-laitteiden tiedonsiirrossa voidaan käyttää perinteisen IP-pohjaisen tietoverkon päällä toimivia sekä niiden lisäksi esimerkiksi erilaisten LPWAN-verkkoratkaisujen määrittelemiä protokollia, joista tässä kappaleessa tarkastellaan IP-pohjaisessa verkossa käytettäviä Session Layer -kerroksen protokollia.

Esimerkkejä tällaisista, IP-pohjaisen verkon päällä toimivista, TCP:tä tai UDP:tä hyödyntävistä IoT-laitteiden käyttämistä protokollista ovat MQTT, AMQP, CoAP ja XMPP. Nämä ovat pääosin jo ennen nykyisenkaltaisten IoT-laitteiden aikaa olemassa olleita protokollia, joita on niiden soveltuessa alettu hyödyntämään myös IoT-laitteiden käyttöön.

MQTT (Message Queue Telemetry Transport) on IBM:n vuonna 1999 esittelemä protokolla, joka perustuu publish/subscribe -arkkitehtuuriin. Protokollaa käyttävässä järjestelmässä käytetään kolmea eri pääkomponenttia, jotka ovat dataa julkaisevat laitteet, sitä vastaanottavat laitteet ja nämä yhdistävä broker eli välittäjä. (Salman 2015, 15.) Esimerkki yleisestä tähän tarkoitukseen käytetystä välittäjäohjelmistosta on Eclipse Mosquitto.

Käytettäessä protokollaa IoT-laitteiden kanssa IoT-laitteet, kuten anturit, toimivat dataa ”julkaisevina” laitteina, jotka muodostavat ajoittain yhteyden välittäjään lähettääkseen kerätyn mittausdatan ja tämän jälkeen siirtyvät jälleen lepotilaan pariston kapasiteetin säästämiseksi (Salman 2015, 15).

Subscriberinä toimii yleensä ohjelmisto tai sovellus, joka ko. antureilta kerättyä mittausdataa käsittelee. Tämä ohjelmisto tai useampi on yhteydessä välittäjäohjelmistoon, jolta saadaan informaatio uudesta IoT-laitteilta saapuneesta datasta. (Salman 2015, 15.)

MQTT:n etuna on sen vähäinen overhead (ylimääräinen kuorma) varsinaisen datan lisäksi, joka on laitteiden sähkönkulutuksen kannalta edullista, ja sen vuoksi MQTT onkin erittäin suosittu ja eniten käytetty protokolla erilaisissa IP-pohjaista verkkoa hyödyntävissä IoT-sovelluksissa. MQTT:n SMQTT-versio tarjoaa lisäksi salauksen, joka parantaa protokollan tietoturvaa. (Salman 2015, 15.)

AMQP (Advanced Message Queuing Protocol) on MQTT:n tapainen protokolla, jonka erona on lähinnä välittäjäkomponentin arkkitehtuuri. AMQP Broker eroaa MQTT:n vastaavasta siten, että se on jaettu eri pääkomponentteihin, Exchangeen ja Queueen, joista Exchange-komponentti on vastuussa datan vastaanottamisesta ja jakamisesta eri Queue-komponenteille, joihin tilaajat yhdistävät kuten MQTT:n tapauksessa. (Salman 2015, 16.)

CoAP (Constrained Application Protocol) on protokolla, joka on kehitetty tarjoamaan normaalia kevyempi RESTful / HTTP-rajapinta IoT-laitteiden käyttöön mahdollistaen alhaisemman virrankulutuksen ja protokollan käyttämisen akkukäyttöisissä laitteissa (Salman 2015, 16).

”Tavallinen” REST (Representional State Transfer), joka on standardi rajapinta HTTP-asiakkaiden ja palvelimien välillä, kuljetetaan TCP:n päällä, kun taas CoAP:ssa käytetään UDP:tä, jolloin pakettien määrä on TCP:tä vähäisempi (Salman 2015, 16).

CoAP-arkkitehtuurissa hyödynnetään kahta alikerrosta, messaging ja request/response. Näistä messaging-kerroksen tarkoituksena on viestien perillemenon varmistaminen ja niiden toistaminen tarvittaessa, koska protokolla käyttää UDP:tä TCP:n sijasta, kun taas request/response-kerros on vastuussa muusta kommunikoinnista. (Salman 2015, 16–17.)

Tämän johdosta CoAP-protokollalla pystytään tarvittaessa toteuttamaan myös varmistamaton lähetys, joka tekee siitä pelkästään TCP:n päällä toimivaan protokollaan verrattuna monikäyttöisemmän.

XMPP (Extensible Messaging and Presence Protocol) on alun perin erilaisten chat- ja viestinvälitysohjelmistojen käyttöön tarkoitettu protokolla, joka on ajan saatossa osoittautunut hyväksi erilaisissa internet-sovelluksissa, jonka vuoksi protokollaa onkin alettu viime aikoina käyttämään myös IoT-sovelluksissa (Salman 2015, 17).

Protokollan ongelmana kuitenkin on esimerkiksi XML:n (eXtensible Markup Language) käyttäminen, joka lisää ylimääräistä overheadia ja nostaa IoT-laitteiden sähkönkulutusta, mikä onkin ongelma erityisesti akkukäyttöisten laitteiden tapauksessa. Tällä hetkellä tämän protokollan käyttö IoT-sovelluksissa on suhteellisen vähäistä. (Salman 2015, 17.)

2.3 Verkkotekniikoiden vertailua

Oikean tietoliikenneteknologian valitseminen IoT-laitteen käyttöön perustuu kyseisen sovelluksen asettamiin vaatimuksiin ja rajoitteisiin esimerkiksi tiedonsiirron luotettavuuden, laitteiden mahdollisen akunkeston, verkon kattavuuden ja myös kyseisen teknologian käyttöönottotilanteen suhteen (Mekki ym. 2017, 4).

Tiedonsiirron luotettavuuden suhteen parhain tekniikka on NB-IoT, koska kyseistä teknologiaa käytettäessä tiedonsiirto on synkronista, mitä LoRaWAN- ja Sigfox-tekniikoilla ei voida vastaavalla tavalla toteuttaa. Lisäksi NB-IoT tarjoaa myös alhaisen latenssin myös kaksisuuntaiseen kommunikointiin päätelaitteiden kanssa. Vastaavaan ominaisuuteen päästään myös LoRaWANin C-luokan laitteilla, mutta ei kuitenkaan Sigfoxilla. (Mekki ym. 2017, 4.)

Kuitenkin NB-IoT:n ja LoRaWANin C-luokan laitteiden sähkönkulutus on korkeampi kuin esimerkiksi Sigfox ja LoRaWAN A-luokan laitteilla, jonka johdosta laitteiden akun kestossa ei päästä yhtä pitkiin aikoihin (Mekki ym. 2017, 4).

Tämän vuoksi sovelluksissa, joissa akun kesto on tärkeä ominaisuus eikä esimerkiksi tiedonsiirron viiveellä erityisesti laitteen suuntaan ole suurta merkitystä, LoRaWAN A-luokka ja Sigfox ovatkin NB-IoT:tä parempia vaihtoehtoja (Mekki ym. 2017, 4).

Erityisesti Sigfoxissa on rajoitteena laitteen lähettämän datan määrä, sillä Sigfoxin maksimi payloadin koko on vain 12 tavua, kun LoRaWANissa päästään 243 tavuun ja NB-IoT:ssa 1600 tavuun. NB-IoT osoittautuukin parhaimmaksi ratkaisuksi sovelluksissa, jotka vaativat suurten datamäärien siirtoa Sigfoxin

ollessa käytännössä käyttökelvoton sen asettaessa rajoitukset myös lähetettyjen viestien maksimimäärälle 12 uplink- ja 4 downlink-viestillä vuorokaudessa LoRaWANista ja NB-IoT:stä poiketen. (Mekki ym. 2017, 3, 5.)

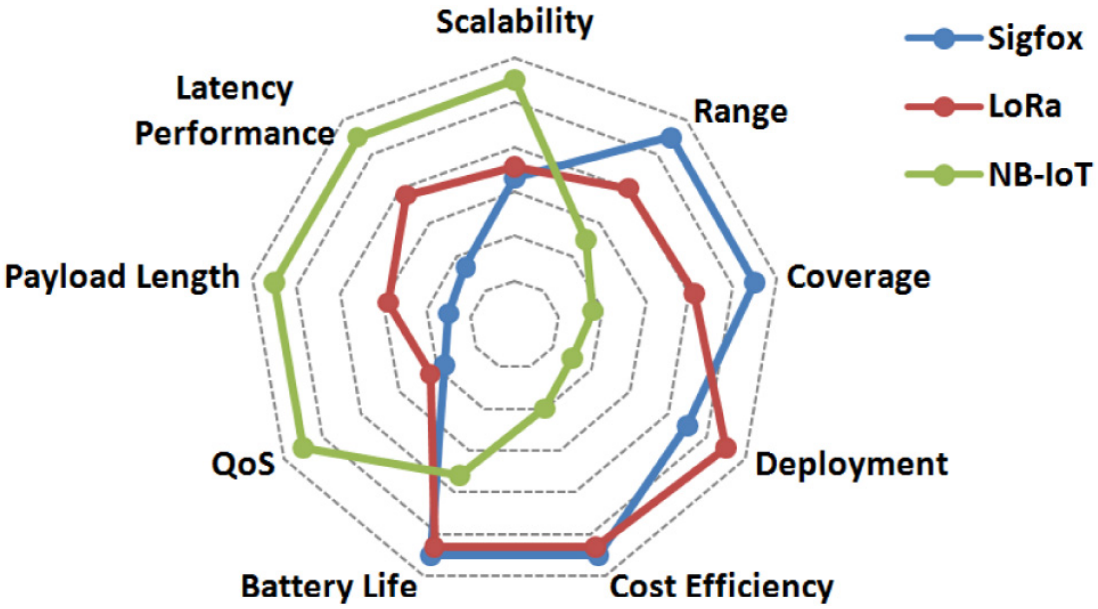
NB-IoT skaalautuu myös parhaiten erittäin suuriin laitemääriin sen kyetessä palvelemaan jopa 100 tuhatta laitetta yhtä tukiaseman solua kohden Sigfoxin ja LoRaWANin jäädessä 50 tuhanteen laitteeseen (Mekki ym. 2017, 5).

NB-IoT-tukiaseman kantama on kuitenkin näistä kolmesta tekniikasta alhaisin jääden maksimissaan noin kymmenen kilometrin säteeseen. Sigfox-tukiasema kattaa jopa 40km säteen LoRaWANin jäädessä näiden väliin noin 20 kilometrin säteellä. (Mekki ym. 2017, 5.)

Verkon rakentamisesta aiheutuvien kulujen suhteen kokonaisuutena Sigfox ja LoRaWAN tulevat edullisimmiksi vaihtoehdoiksi, koska niiden käyttämällä taajuusalueella ei tarvita lisenssimaksuja sekä laitteiden ja tukiasemien hintataso on NB-IoT:n vastaavia alhaisempi (Mekki ym. 2017, 5).

NB-IoT on uusin standardisoitu tekniikka, joten sen käyttöönotto ei ole välttämättä vielä yhtä pitkällä kuin LoRaWANin ja Sigfoxin. NB-IoT:n ja Sigfoxin käyttöönotto tapahtuu vain kaupallisten operaattorien toimesta, kun taas LoRaWANin etuna on mahdollisuus rakentaa myös oma privaattiverkko haluttaessa. (Mekki ym. 2017, 5.)

Kokonaisuutena eri teknologioiden vastaavuutta erilaisiin tarpeisiin havainnollistetaan kuvassa 4.



Kuva 4. Sigfox-, LoRaWAN- ja NB-IoT-teknologioiden vertailua eri aspektit huomioiden (Mekki ym. 2017, 5)

Aloitettaessa IoT-projekteja onkin soveltuvan verkkotekniikan valinta tehtävä paikalliset olosuhteet huomioon ottaen. Kaikissa tapauksissa kaikkia aspekteja ei kuitenkaan välttämättä tarvitse ottaa huomioon kaikilta osin.

Tällaisesta tapauksesta voidaan mainita esimerkkinä tapaus, jossa loppuasiakas suunnittelee jo olemassa olevan operaattorin verkon hyödyntämistä. Tällöin esimerkiksi kyseisen verkon perustamiskustannuksilla ja tukiasemien tarvittavalla määrällä ei ole suoraa vaikutusta loppuasiakkaan päätökseen, joskin toki kyseiset asiat todennäköisesti vaikuttavat operaattoreiden hinnoitteluun ja sitä myöten myös asiakkaan päätöksentekoon.

Lisäksi kaikissa tapauksissa kaikkia teknologioita ei ole edes mahdollista käyttää, sillä esimerkiksi eri teknologioilla toteutettujen verkkojen julkinen saatavuus vaihtelee alueittain, ja tämän vuoksi yleispätevää sääntöä tietyn tekniikan valitsemiselle voikin olla mahdotonta määritellä.

Lisäksi käytettävien IoT-laitteiden sähköenergian saatavuus saattaa asettaa huomattavia rajoituksia, mikäli esimerkiksi ulkoista sähkönsyöttöä ei ole saatavissa ja laitteiden tulee toimia omien akkujensa varassa pitkiäkin aikoja.

Teknologiakenttä IoT-markkinoilla on myös koko ajan muutoksessa, esimerkiksi viidennen sukupolven matkapuhelinverkkojen (5G) kehitys ja niihin sisältyvät mahdolliset IoT-laitteita varten suunnatut ominaisuudet tulevat todennäköisesti muuttamaan tilannetta lähitulevaisuudessa merkittävästi (Mekki ym. 2017, 6).

3 SÄHKÖVERKON MITTAUSTIEDON KERÄÄMINEN

Sähköverkon mittaustiedon keräämistä ja sen kehittämistä voidaan tarkastella verkon tämän hetkisen tilanteen ja tulevaisuudessa tapahtuvien, mahdollisesti myös sähköverkkoon vaikuttavien muutosten kannalta.

Voidaan esimerkiksi arvioida, onko sähköverkon kannalta tapahtumassa muutoksia, jotka vaatisivat nykyistä laajempaa mittaustiedon keräämistä verkosta verkon optimaalisen käytön mahdollistamiseksi ja tarkastella, miten mahdollisesti tarvittavat uudet mittaustiedot saadaan järkevästi kerättyä.

3.1 Lyhyt katsaus sähköverkkoihin vaikuttaviin muutoksiin

Tällä hetkellä sähkönjakeluverkkoja koskettavia lähitulevaisuudessa esiin tulevia asioita ovat esimerkiksi lain asettamat vaatimukset ”säävarmasta sähköverkosta” ja kuormitusprofiilin muutos esimerkiksi sähköautojen ja lämpöpumppukuormituksen lisääntyessä sekä hajautetun tuotannon yleistyessä (Partanen 2019, 2).

Vuonna 2013 voimaan tullut sähkömarkkinalaki määrittelee 51§:n mukaan ”säävarmasta sähköverkosta” seuraavasti:

”Jakeluverkko on suunniteltava ja rakennettava, ja sitä on ylläpidettävä siten, että:
….
2) jakeluverkon vioittuminen myrskyn tai lumikuorman seurauksena ei aiheuta asemakaava-alueella verkon käyttäjälle yli 6 tuntia kestävää sähkönjakelun keskeytystä;
3) jakeluverkon vioittuminen myrskyn tai lumikuorman seurauksena ei aiheuta muulla kuin 2 kohdassa tarkoitetulla alueella verkon käyttäjälle yli 36 tuntia kestävää sähkönjakelun keskeytystä” (Sähkömarkkinalaki 9.8.2013/588).

Lisäksi sähkömarkkinalain 119§ määrittelee jakeluverkon kehittämisestä ja käyttöönotosta seuraavasti:

”Jakeluverkonhaltijan on täytettävä 51 §:n 1 momentin 2 ja 3 kohdassa säädetyt vaatimukset vastuualueellaan viimeistään 31 päivänä joulukuuta 2028. Vaatimusten on täytyttävä viimeistään 31 päivänä joulukuuta 2019 vähintään 50 prosentilla jakeluverkon kaikista käyttäjistä vapaa-ajan asunnot pois lukien ja viimeistään 31 päivänä joulukuuta 2023 vähintään 75 prosentilla jakeluverkon kaikista käyttäjistä vapaa-ajan asunnot pois lukien” (Sähkömarkkinalaki 119. §).

Säävarmaan sähköverkkoon siirtyminen edellyttää jakeluyhtiöiltä esimerkiksi vikaherkkien keskijänniteavojohto-osuuksien maakaapelointia tai korvaamista mahdollisuuksien mukaan jollain muulla tekniikalla, kuten 1 kV jakelujännitteen käyttöä lisäämällä.

Lisäksi toimitusvarmuuteen pääsemiseksi vaaditaan usein muutoksia myös pienjännitejakelussa, joka muodostaa usein merkittävän osuuden sähköyhtiön jakeluverkosta. 50 % pienjännitejohtopituudesta on vain yhden asiakkaan käytössä, ja osalla asiakkaista sähkönkulutus on hyvinkin alhaista. Esimerkiksi eräiden kolmen suuren sähköyhtiön asiakkaista 15 % käyttää vähemmän kuin 500 kWh sähköä vuodessa. (Partanen 2019, 16.)

Suurten sähköverkkoinvestointien tekeminen vähän kuluttavia tai mahdollisesti tulevaisuudessa kokonaan käytöstä poistuvia liittymiä varten ei ole taloudellisesti kannattavaa, joten näissä tapauksissa on myös arvioitava, onko liittymälle ylipäätään tarvetta vai voitaisiinko se irtisanoa ja pj-verkko purkaa kokonaan, joka säästäisi investointikustannuksissa (Partanen 2019, 14–16).

Tulevaisuudessa pienikulutuksisilla haja-asutusalueilla voi tulla myös mahdollisesti kyseeseen esimerkiksi erilaiset mikroverkot, sähkön paikallinen varastointi ja tuotanto tai erilaiset varavoimaratkaisut varsinaisen jakeluverkon toimitusvarmuuden parantamiseksi (Partanen 2019, 21).

Kuormitusprofiilin muutoksen vaikutukset kohdistuvat voimakkaimmin pienjännitejakeluverkkoon sekä -muuntajiin. Sähköautojen yleistymisen voidaan arvioida johtavan vahvimmillaan vuoteen 2030 mennessä ylikuormitustilanteisiin neljäsosalla nykyisistä jakelumuuntajista sekä esimerkiksi lämpöpumppukuormien ja pientuotannon aiheuttavan jännitevaihtelujen lisääntymistä. (Partanen 2019, 17.)

3.2 “Perinteinen” sähköverkkoautomaatio

Perinteisellä sähköverkkoautomaatiolla siirtoyhtiötasolla käsitetään lähinnä keskijänniteverkon käyttöön ja valvontaan käytettyä tekniikkaa, joka koostuu pääasiallisesti käyttökeskuksessa olevasta SCADA-järjestelmästä ja siihen liitetyistä kenttälaitteista, jotka pääosin sijaitsevat keskitetysti sähköasemilla (ABB 2000, 3–5).

Sähköasematasolla automaatioon perinteisesti liitetään esimerkiksi katkaisijoiden ja erottimien ohjaukset, päämuuntajien käämikytkimet ja sähköasemalta saatavaa erilaista mittaustietoa, kuten eri johtolähtöjen virta-, jännite- ja muita sähköisten suureiden mittauksia (ABB 2000, 5).

Perinteinen sähköverkkoautomaatio keskittyy siis siirtoyhtiön tasolla lähinnä jakelun alkupäähän sähköasemille ja keskijänniteverkkoon, ja sen avulla hallitaan sähköverkon pääkomponentteja, jotka palvelevat suuria määriä asiakkaista.

Täten perinteisen sähköverkkoautomaation komponentit ovatkin pääosin ns. industrial-tason laitteita, ja ne soveltuvatkin hyvin tämänkaltaiseen käyttötarkoitukseen. Nämä perinteisen sähköverkkoautomaation käytössä olevat laitteet tarvitsevat esimerkiksi omakäyttösähköä, jatkuvan tietoliikenneyhteyden niitä hallitsevaan SCADA-järjestelmään ja lisäksi ne tulee usein sijoittaa olosuhteiltaan sopivaan laitetilaan.

Tämänkaltaisten laitteiden käyttäminen ei siis ole järin kustannustehokasta tai järkevää kohteissa, joissa esimerkiksi niiden vaatimaa omakäyttösähköä ei ole ennestään saatavilla ja mitkä palvelevat vain pientä määrää asiakkaita.

3.3 IoT-teknologian mahdollisuudet sähköverkon mittaustiedon keräämisessä

IoT-teknologiaa käyttäen voidaan sähköverkosta kerätä mittaustietoa sellaisistakin kohteista, joista tiedon kerääminen perinteisellä sähköverkkoautomaatiolla ei olisi kannattavaa. Tämän mahdollistaa erityisesti pitkiä aikoja omien akkujensa varassa, langatonta verkkoa tiedonsiirtoon käyttävät edulliset IoT-laitteet, joita hyödyntäen sähköverkon valvontaa voidaan järkevästi ja kustannustehokkaasti laajentaa myös näihin kohteisiin.

Tällaisia kohteita ovat esimerkiksi tämän opinnäytetyön käytännön osuudessa käsitellyt 1 kV katkaisijat, joiden valvontaa ei aikaisemmin ole lainkaan toteutettu, vaan katkaisijan laukeaminen on todettu pääasiassa asiakkaiden verkkoyhtiölle soittamien vikailmoitusten perusteella.

1 kV katkaisijan takana on suhteellisen pieni määrä asiakkaita, ja katkaisijoiden fyysiset sijainnit sekä toimintaympäristö asettavat rajoitteita, jotka tekisivät perinteisen sähköverkkoautomaation käytön kyseisissä kohteissa helposti huomattavan tehottomaksi siitä saatuun hyötyyn nähden.

IoT-teknologia voi mahdollistaa mittaustiedon keräämisen myös tämänkaltaisista kohteista, joka omalta osaltaan mahdollistaa automaattisen tiedonkeruun mahdollistamat hyödyt, kuten esimerkiksi vikatilanteen havaitsemisen sähköyhtiön valvomossa heti sen tapahtuessa ja viankorjauksen aloittamisen mahdollisimman nopeasti.

Nopeammalla viankorjauksella saadaan asiakkaiden kokemaa keskeytysaikaa vähennettyä sekä vikapartioiden työskentelyä tehostettua vikapaikan ollessa jo valmiiksi tiedossa. Tämä on esimerkiksi ”säävarmaan sähköverkkoon” ja keskeytysaikojen minimiointiin liittyen tärkeää, ettei vikapaikkaa tarvitse hakea turhaan laajalta alueelta.

IoT-teknologian mahdollistamalla sähköverkon tiedonkeruun laajentamisella voidaan myös monissa tapauksissa havaita alkava vika jo ennen, kuin siitä aiheutuu varsinaista vikatilannetta.

Esimerkkeinä tällaisista IoT-teknologiaa hyödyntävistä projekteista sähköverkoissa voidaan mainita ilmajohtojen lumikuorman aiheuttaman painumisen mittaaminen, pylväiden kaltevuuden ja sitä kautta niiden mahdollisen kaatumisen ennakointi sekä jakokaappien tai vastaavien tilojen ovien auki jäämisten tai muiden niille aiheutuneiden vaurioiden havaitseminen (Digita 2019).

IoT-tekniikalla ei kuitenkaan näillä näkymin pystytä korvaamaan kriittisiä, nykyisen sähköverkkoautomaation piirissä olevia komponentteja, vaan sitä voidaan lisätä perinteisen sähköverkkoautomaation rinnalle mahdollistamaan uusia valvottavia kohteita.

IoT-teknologia ei ole perinteisen sähköverkkoautomaation kanssa suoraan yhteensopivaa, sillä IoT-laitteet eivät käytä tai tue lainkaan perinteisessä sähköverkkoautomaatiossa laitteiden väliseen tiedonsiirtoon käytettyjä protokollia.

Lisäksi IoT-laitteiden käyttämät tietoliikenneyhteydet ja mahdollinen sähkönsaannin rajallisuus asettaisivat rajoituksia perinteisen sähköverkkoautomaation käyttämän järjestelmäarkkitehtuurin hyödyntämiselle, joten suora yhteensopivuus sen kanssa ei välttämättä edes olisi mahdollista toteuttaa.

IoT-laitteiden yhdistäminen perinteiseen sähköverkkoautomaatioon ja siihen liittyvien haasteiden ratkaiseminen onkin tärkeää tarkasteltaessa IoT-teknologian käytön lisäämistä jo olemassa olevissa sähköverkoissa ja niiden käytönvalvontaratkaisuissa.

IoT-teknologian käytön voidaan ainakin varovasti ennustaa lisääntyvän sähköverkoissa, sillä esimerkiksi aiemmin käsitellyt, sähköverkoissa tapahtuvat muutokset voivat vaatia entistä tarkempaa tiedonkeruuta esimerkiksi jakelumuuntamoilta ja pienjänniteverkon kaapeliosuuksilta niiden mahdollisen ylikuormittumisen riskin lisääntyessä esimerkiksi sähköajoneuvojen latauskuormien johdosta.

Tulevaisuudessa käyttöönotettavat, mahdolliset älykkäät sähköverkkoratkaisut avaavat myös todennäköisesti uudenlaisia tarpeita sekä mahdollisuuksia erilaisten mittaustietojen keräämiselle, joihin IoT-teknologia voi tietyissä tilanteissa vastata perinteistä sähköverkkoautomaatiota paremmin.

Näissä yhteyksissä IoT-teknologiaa voidaan mahdollisesti käyttää myös verkon mittaustiedon keräämisen lisäksi esimerkiksi ei-kriittisten ohjausten toteuttamiseen suoraan kuluttajien sähkölaitteistoissa kysyntäjoustoratkaisujen yhteydessä.

4 1 KV SÄHKÖNJAKELU

1 kV jännitetasoa käytetään sähkönjakeluverkoissa varsinaisen keskijännitejakelun (20 kV) ja pienjännitejakelun (0,4 kV) väliportaana silloin, kun keskijännitejakelun tuominen kulutuskohteiden läheisyyteen ei ole järkevää, mutta siirtomatka lähimmältä keskijännitejakelun liittymispisteeltä olisi pienjännitteelle liian pitkä.

1kV-järjestelmä käsittää 20/1kV-muuntajan keskijänniteverkon liittymispisteessä, 1 kV johtolähdön katkaisijan, 1 kV siirtojohdon ja 1/0,4 kV muuntajan kulutuskohteiden läheisyydessä (Saira 2009, 9).

1kV-järjestelmän rakentaminen on monessa tapauksessa investointikustannuksiltaan keskijännitejakelua huomattavasti alhaisempaa, sillä 1 kV jakeluverkkoa voidaan rakentaa pääosin samoilla menetelmillä kuin 0,4 kV verkkoa, sillä EU:n pienjännitedirektiivin 2006/95/EC mukaan pienjännitekomponentit on mitoitettava kestämään 1 kV:n jännite (Saira 2009, 8–9).

1 kV jännitteellä samoja johdinpaksuuksia käyttämällä saadaan kuitenkin siirrettyä 2,5-kertainen määrä tehoa 2,5 kertaa pidemmälle 0,4 kV:n jännitetasoon nähden (Saira 2009, 10).

1kV-verkossa ei kuitenkaan voida 0,4 kV jakeluverkon tavoin käyttää verkon suojaukseen perinteistä sulakesuojausta, sillä ko. järjestelmä on rakennettava maasta erotetuksi jonka johdosta maasulkutilanteissa maasulkuvirta jää alhaiseksi, jolloin sulakkeet eivät palaisi (Saira 2009, 13).

Sulakkeiden sijaan suojaukseen käytetään katkaisijaa, jonka laukeamisen aiheuttaa joko katkaisijaan määritellyt ylivirtasuojaukset tai erillinen maasulkusuojaus, joka voidaan toteuttaa esimerkiksi muuntajan tähtipistejännitettä maadoituselektrodia vasten mittaamalla (Saira 2009, 14).

1 kV lähdön katkaisijan lauetessa sähkönjakelu keskeytyy kaikilta ko. johtolähdön takana olevilta asiakkailta. 1 kV johtolähtö palvelee keskimäärin muutamia asiakkaita, joiden kulutus on usein pientä. Katkaisijoiden laukeamisia aiheuttavista häiriöistä ja niiden esiintymistiheydestä esimerkiksi tämän opinnäytetyön kohteena olevilla katkaisijoilla ei ole saatavilla tarkkaa informaatiota, koska katkaisijoita ei ole aikaisemmin valvottu.

5 SCADA-JÄRJESTELMÄ

SCADA (Supervisory Control and Data Acquisition System) on järjestelmä, jonka tarkoituksena on mahdollistaa esimerkiksi jonkin prosessin tai järjestelmän valvonta ja hallinta keskitetystä valvomosta riippumatta siitä, miten laaja-alainen kyseinen järjestelmä on (Thakur 2012).

SCADA-järjestelmä koostuu yleensä keskustietokoneista/palvelimista, jotka keräävät, säilövät ja prosessoivat dataa sekä liikennöivät etäasemille, HMI (Human Machine Interface)-laitteistosta, jonka avulla operaattorit pystyvät valvomaan ja ohjaamaan järjestelmää sekä kentällä/prosessissa sijaitsevista etäasemista ja näiden välisistä tietoliikenneyhteyksistä (Thakur 2012).

Sähkönsiirtoyhtiöiden tapauksessa SCADA-järjestelmän käyttäminen sähköverkon etävalvontaan ja hallintaan sekä automatisointiin on merkittävä tekijä verkon käyttökustannusten alentamiseksi ja palvelun laadun sekä saatavuuden parantamiseksi (Terezinho 2013, 2).

SCADA-järjestelmän kerätessä dataa ja mahdollistaessa ohjaukset koko verkon alueelle on operaattorin helppo esimerkiksi vikatilanteessa muodostaa kokonaiskuva siitä, mitä on tapahtunut ja tehdä tarvittavat toimenpiteet sähkönjakelun palauttamiseksi mahdollisimman suurelle osalle asiakkaita (Terezinho 2013, 3).

Ilman tämänkaltaista järjestelmää tieto viasta saataisiin mahdollisesti vasta asiakkaan ilmoittaessa sähkönpuutteesta, ja vikaa jouduttaisiin hakemaan ja rajaamaan manuaalisesti kentällä, joka olisi hidas ja kallis ratkaisu erityisesti suurempien häiriöiden tapauksessa.

SCADA-järjestelmän avulla pystytään myös havaitsemaan mahdollisia tulevia vikatilanteita, ennen kuin niistä aiheutuu jakeluhäiriöitä, kuten esimerkiksi ylikuormitusvaarassa olevat johtolähdöt tai sähkönlaatupoikkeamien normaalia suurempi esiintyminen (Terezinho 2013, 3).

Lisäksi vikatilanteiden sattuessa on mahdollista automatisoida verkon uudelleenkonfigurointi mahdollisimman nopean vianrajauksen mahdollistamiseksi ja sähköjen palauttamiseksi mahdollisimman suurelle osalle asiakkaita.

5.1 NetControl Netcon 3000

Järvi-Suomen Energialla käytetään SCADA-järjestelmänä NetControlin Netcon 3000 -järjestelmää. Netcon 3000 on client/server -arkkitehtuuriin perustuva hajautettu hyvin skaalautuva järjestelmä, jota voidaan käyttää niin pienissä kuin suurissakin järjestelmissä (Netcontrol 2018, 4).

Netcon 3000 -järjestelmä koostuu SCADA-palvelimesta tai useammasta, jotka käsittävät reaaliaikaisen prosessitietokannan ja vastaavat esimerkiksi tietoliikenteestä kenttälaitteille sekä hälytyskäsittelystä, tapahtumien lokiinkirjauksesta ja arkistoinnista (Netcontrol 2018, 4).

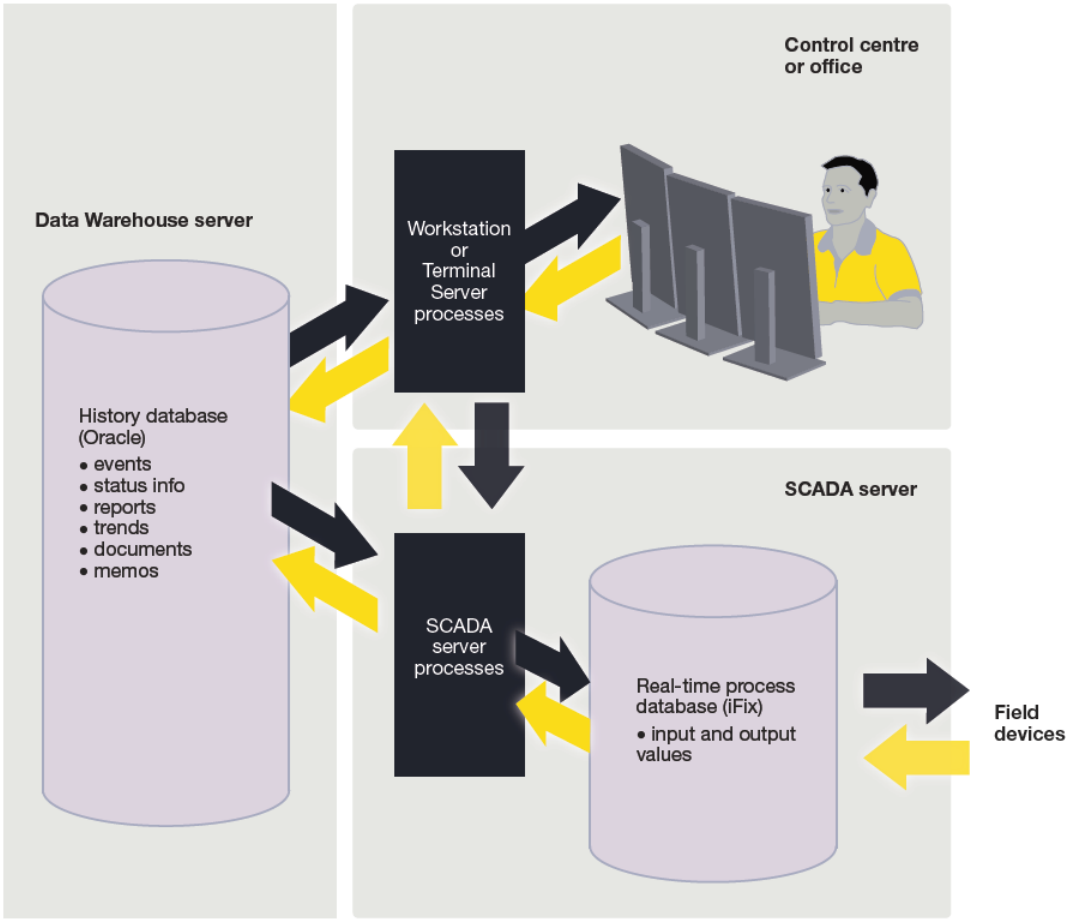
Järjestelmän käyttöliittymä perustuu client-ohjelmistoihin, jotka muodostavat yhteyden IP-verkon yli SCADA-palvelimille ja tarjoavat käyttöliittymän operaattoreille. Näillä ohjelmistoilla voidaan suorittaa kaikki käyttötoimenpiteet ja esimerkiksi esittää reaaliaikaista dataa grafiikkakuvissa, tarkastella mittausten trendikäyriä ja luoda erilaisia raportteja. (Netcontrol 2018, 4.)

Client-ohjelmistoja voidaan käyttää joko suoraan Windows-pohjaisilla tietokoneilla tai vaihtoehtoisesti RDS (Remote Desktop Services)-palvelinympäristössä, mikä mahdollistaa järjestelmän helpon etäkäytön sekä ”thin-clienttien” hyödyntämisen järjestelmän osana (Netcontrol 2018, 4).

”Thin-clientilla” tarkoitetaan kevyttä tietokonetta vastaavaa päätelaitetta, joka on optimoitu tarjoamaan alusta etätyöpöytäyhteyden muodostamiseksi virtuaalityöpöydän tarjoavalle palvelimelle sekä näyttöjen ja muiden oheislaitteiden paikalliseksi liittämiseksi (Clearcube 2019).

”Thin-clienttien” käytöllä voidaan saavuttaa etuja esimerkiksi järjestelmän hallittavuuden, tietoturvan ja kustannusten suhteen, sillä kaikki varsinainen datan käsittely, tallennus ja ohjelmien suorittaminen on keskitetty palvelimille. Tällöin päätelaitteissa ei tarvita täydellistä käyttöjärjestelmää ja lisäksi niiden laitteistovaatimukset ovat huomattavasti perinteisiä tietokoneita alhaisemmat, minkä johdosta laitteiden hankintahinta ja energiankulutus jäävät myös pienemmiksi. (Clearcube 2019.)

NetControl Netcon 3000 -järjestelmän arkkitehtuuria on havainnollistettu kuvassa 5.



Kuva 5. Netcon 3000 -järjestelmän arkkitehtuuri (Netcontrol 2018, 4)

JSE:llä käytössä olevassa Netcon 3000 -järjestelmässä kenttälaitteisiin liitytään käyttäen IEC104-protokollaa TCP/IP:n ylitse (Kauhanen, 2019a).

5.2 IEC104-protokolla

IEC104-protokolla on yksi IEC 60870-5 -standardissa määritellyistä protokollista. IEC 60870 on standardi, joka määrittelee esimerkiksi sähkönjakeluautomaatiossa kenttälaitteiden kanssa liikennöintiin käytettäviä protokollia. (Matoušek 2017, 4–5.)

IEC104, eli IEC 60870-5-104 -protokolla on IEC101-protokollan mukaista dataa TCP/IP-verkkojen yli välittämään suunniteltu protokolla. Tällöin fyysisenä verkkoyhteytenä on mahdollista käyttää monenlaisia verkkoratkaisuja, joka tekee protokollasta helposti sovellettavan geografisesti laajalle levinneiden prosessien käyttöön. (Matoušek 2017, 2.)

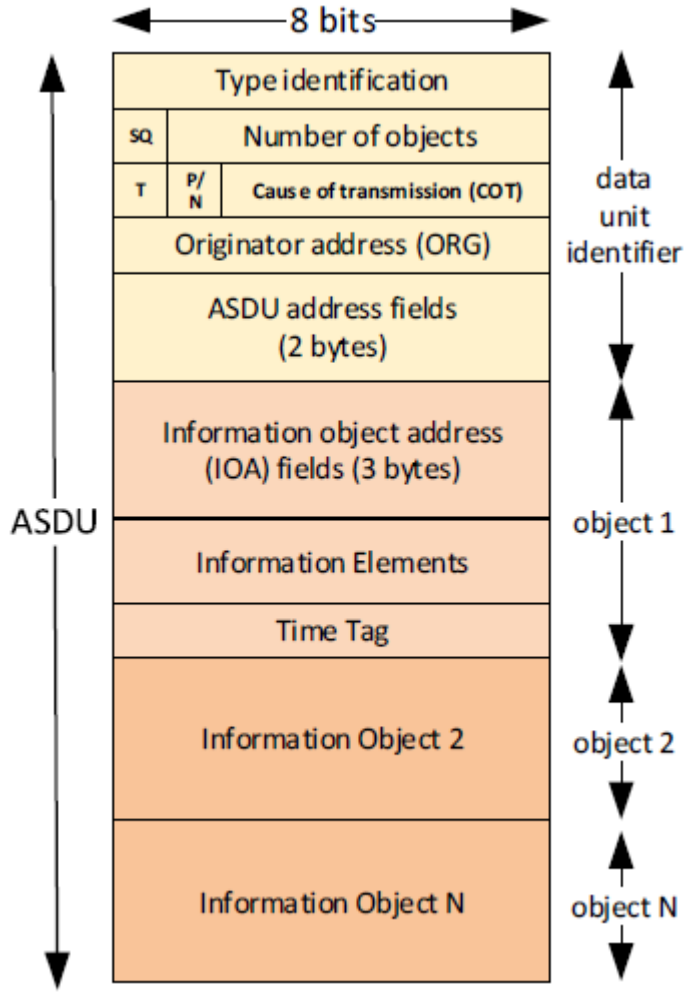
IEC60870-5-protokollissa määritellään järjestelmälle hierarkinen rakenne, jossa jokainen laite/asema on joko hallitseva tai hallittu asema. Tyypillisesti hallitsevana komponenttina toimii SCADA-järjestelmä, ja hallittuina laitteina ala-asemat. Näistä (ala-asemista) voidaan käyttää myös nimityksiä RTU (Remote Terminal Unit), Slave tai IEC104-Server. (Matoušek 2017, 7.)

IEC101 ja 104:ssa tiedonsiirron suunta määritellään pääasiallisesti hierarkian mukaisesti joko Monitor- tai Control-suuntaisesti, joista Monitor / valvonta-suunta tarkoittaa tiedonsiirtoa etäasemalta hallinta-asemalle, kuten mittausdataa kenttälaitteelta SCADA-järjestelmään ja Control / hallinta esimerkiksi ohjauskomentoja SCADA-järjestelmästä kenttälaitteelle. Lisäksi on mahdollinen Reversed Direction, jossa tiedonsiirron suunta on päinvastainen laitehierarkiaan nähden. (Matoušek 2017, 7–8.)

IEC60870-5-protokollissa varsinaisen mittaus- ym. datan siirto tapahtuu ASDU-objektien (Application Service Data Unit) kuljettamissa Information Objecteissa. ASDU-objektit koostuvat kahdesta pääosiosta, jotka ovat itse ASDU:n tunniste sekä sen sisältämä varsinainen data/Information Objectit. Tunnisteessa määritellään esimerkiksi objektin sisältämän datan tyyppi ja osoitteistus sen yksilöimiseksi. (Matoušek 2017, 12.)

Lisäksi ASDU:n tunniste sisältää esimerkiksi ASDU:n sisältäminen Information Objectien määrän ja tiedon ASDU:n lähettämisen syystä (COT, Cause of Transmission). Lähettämisen syitä voivat olla esimerkiksi säännöllinen rutiinilähetys tai mittausdatan muuttumisen aiheuttama spontaani lähetys. (Matoušek 2017, 12, 35.)

Kuvassa 6 esitetään tyypillinen ASDU-objektin rakenne.



Kuva 6. ASDU-objektin rakenne (Matoušek 2017, 13)

IEC-101-protokolla, jonka mukaista dataa IEC-104 kuljettaa, määrittelee monenlaisia tyyppejä ASDU-objekteille niiden kuljettamien Information Objectien sisältämän datan tyypin ja tiedonsiirron suunnan mukaisesti (Matoušek 2017, 13). Esimerkkinä tyypeistä voidaan katsoa ensimmäinen tyyppi nro 1, josta käytetään tunnistetta M_SP_NA_1.

Tämä datatyyppi on tarkoitettu siirtämään yksittäinen single-point information -datapiste Monitor-suuntaisesti, eli esimerkiksi kytkimen tai katkaisijan on/off-tilatieto kenttälaitteelta SCADA-järjestelmälle.

Tunnuksen ensimmäinen kirjain ”M” kertoo tiedonsiirron suunnan, joka on tässä tapauksessa Monitor. Toinen osa, ”SP” määrittelee datatyypin, Single Point, joka käytännössä tarkoittaa ”On/Off” -tilatietoa. Kolmannen osan ensimmäinen kirjain ”N” määrittelee, sisältääkö datatyyppi aikaleimaa, jota ei tässä tapauksessa ole (Not time tagged). Tämän jälkeinen ”A”-kirjain määrittelee mahdolliset muut ominaisuudet spesifikaation mukaisesti, jotka tässä tapauksessa ovat ”status and normalized, with quality”. (Matoušek 2017, 32–34.)

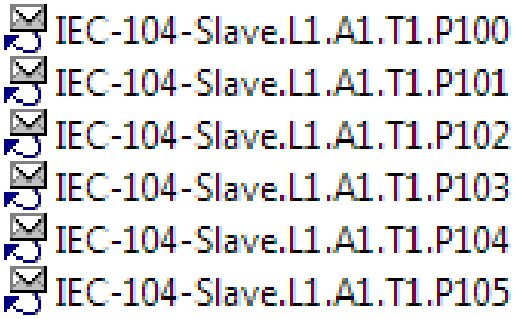
Kaikki protokollan mukaiset ASDU-tyypit ja esimerkiksi niiden Cause of Transmission -arvot ovat esitetty Matoušekin (2017) tutkimuksen ”Description and analysis of IEC 104 Protocol” liitteinä dokumentin sivuilla 32–35.

IEC104:lla myös datapisteiden osoitteistus perustuu IEC-101-protokollaan, ja määräytyy laiteosoitteen, ASDU:n osoitteen / Common Addressin, datatyypin ja yksilöllisen tunnuksen perusteella. Jokaiselle laitteelle määritellään oma laite/linkkiosoite, jonka perusteella dataa lähettävä/vastaanottava laite identifioidaan. Tästä osoitteesta voidaan myös käyttää termiä Originator Address ASDU-pakettien yhteydessä. (Matoušek 2017, 8, 16.)

IEC104:lla tämä kyseinen osoite on IEC101:stä poiketen kuitenkin tyypillisesti 2 tavun kokoinen, mikä mahdollistaa sille annetut numeeriset arvot väliltä 1–65535, kun taas IEC101:llä käytetään tyypillisesti 1 tavun kokoista osoitetta, milloin osoitealue rajautuu välille 1–255 (Matoušek 2017, 8).

Lisäksi laitteella on yksi tai useampi Common Address ASDU-objekteille, jonka alle varsinaiset datapisteet määritellään. Tästä osoitteesta käytetään myös esimerkiksi nimityksiä Common Object Address (COA) tai Common Station Address, ja sen tarkoituksena on esimerkiksi määritellä sovellus, johon kyseiset datapisteet liittyvät. Osoitteen koko ja mahdolliset numeeriset arvot ovat laite/linkkiosoitteen tapaan tyypillisesti IEC104-protokollaa käytettäessä 2 tavua ja 1–65535. (Matoušek 2017, 8–9.)

Näin jokaiselle datapisteelle saadaan täydellinen tunnus, joka koostuu laiteosoitteesta, COA:sta ja ASDU:n tyypistä sekä yksilöllisestä tunnuksesta. Esimerkkinä tästä havainnollistetaan kuvaa 7 Scada Data Gateway -ohjelmistosta.

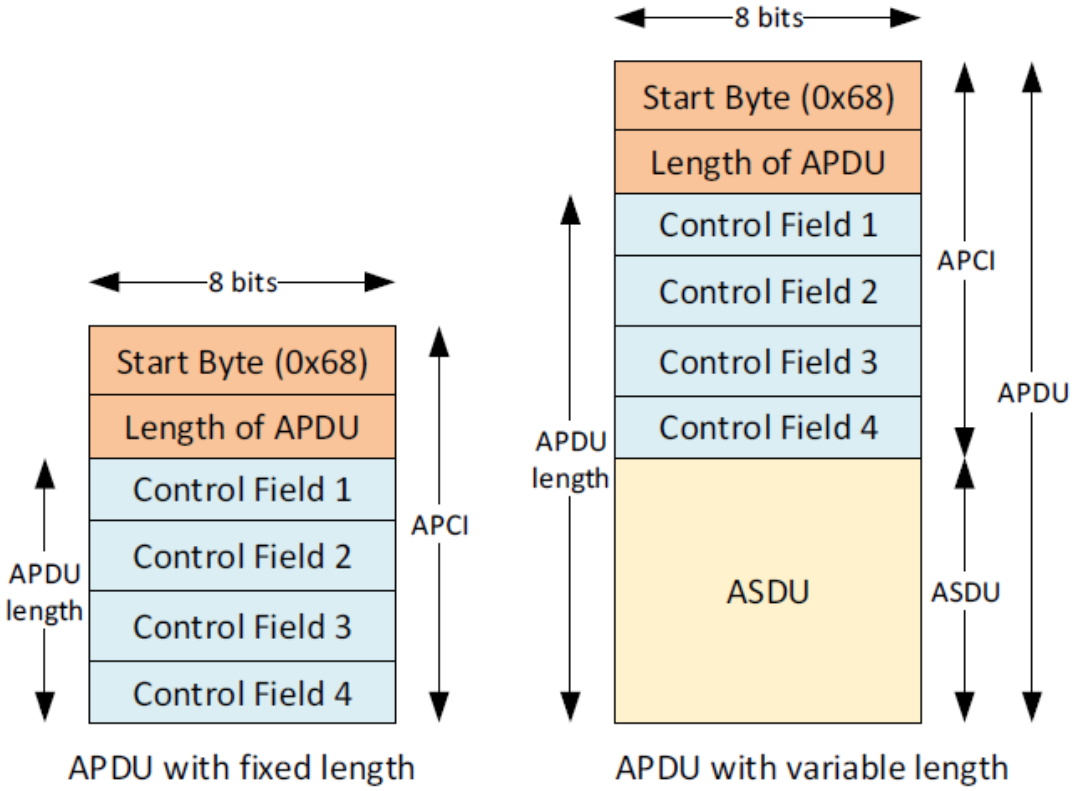


Kuva 7. IEC-104-datapisteitä esitettynä Scada Data Gateway -ohjelmistossa

Kyseisessä kuvassa esitetään datapisteet 100-105, joiden linkki/laiteosoite on 1 (L1), ASDU:n osoite/COA 1 (A1), ASDU:n tyyppi 1 (T1) ja pisteiden osoitteet (P) 100-105. Koska kyseessä on ASDU-tyyppi 1 ja IEC-104 slave, voidaan kyseessä päätellä olevan ala-asema, jolta dataa siirretään pääosin SCADA-järjestelmään.

IEC-104-protokollassa ASDU-objektit paketoidaan yhdessä APCI-objektien (Application Protocol Control Information) kanssa kehyksiin, joista käytetään nimitystä APDU (Application Protocol Data Unit). APDU-kehys voi sisältää ASDU-objektin, mutta se voi olla myös ilman ASDU-objektia sisältäen pelkän APCI-osan. (Matoušek 2017, 9–10.)

APDU-kehyksen rakennetta mallinnetaan kuvassa 8.



Kuva 8. APDU-objektin rakenne (Matoušek 2017, 10)

APCI-osan kontrollikentät määrittelevät esimerkiksi kehyksen rakenteen ja viestin suunnan sekä tyypin. Standardissa on määritelty kolme erilaista tyyppiä APDU-kehykselle, jotka ovat I, S ja U-tyyppi. (Matoušek 2017, 10.)

I-tyypin APDU-kehyksen pääasiallisena tarkoituksena on siirtää informaatiota valvovan ja valvotun aseman välillä, jolloin se luonnollisesti sisältää aina ASDU-objektin. S- ja U-tyypin APDU-kehyksillä siirretään IEC104-yhteyden vaatimaa signalointi- ym. dataa, mutta nämä eivät kuitenkaan sisällä varsinaista mittaus- tai ohjausdataa sisältäviä ASDU-objekteja. (Matoušek 2017, 10–11.)

Esimerkiksi S-tyypin APDU:a käytetään Acknowledged-viestien lähettämiseen tapauksissa, joissa varsinaista dataa siirretään muutoin vain yhteen suuntaan, ja viestien perillemenoa on määritellyin väliajoin tarkasteltava. U-tyypin APDU-kehyksillä voidaan esimerkiksi välittää pyyntö tiedonsiirron aloittamisesta tai lopettamisesta ala-asemalle tai lähettää testikehyksiä, mikäli muuta liikennettä yhteydellä ei esiinny. (Matoušek 2017, 11–12.)

6 1 KV KATKAISIJAN TILATIEDON VALVONTA

Tässä opinnäytetyössä oli käytännön työn tarkoituksena toteuttaa ratkaisu JSE:n 1 kV:n sähkönjakeluverkossa sijaitsevien katkaisijoiden tilatietojen valvontaan IoT-teknologiaa hyödyntäen ja toteuttaa pilottikohde ratkaisun toimivuuden toteamiseksi käytännössä.

6.1 Ympäristö ja lähtökohdat

Lähtökohtana työlle oli löytää ratkaisu, jolla 1kV-katkaisijan apukoskettimelta saatavan kärkitiedon tila välitetään sähköyhtiön SCADA-järjestelmään.

1kV-jakelua on käytössä koko Järvi-Suomen Energian verkon alueella pääasiallisesti harvaan asutuilla alueilla 20 kV jakelun loppupäässä. 1 kV:n katkaisijoita on tällä hetkellä käytössä Järvi-Suomen Energian verkkoalueella yhteensä noin 800 kappaletta (Kauhanen 2019b).

1kV-katkaisijat ovat asennettu 20/1 kV muuntajien yhteyteen pylväsasennuskoteloihin. Näiden katkaisijoiden yhteydessä ei ole saatavilla normaalia 230/400 V omakäyttösähköä, eikä kiinteitä tietoliikenneyhteyksiä tai varsinaista laitetilaa, johon esimerkiksi ulkolämpötilan vaihtelua rajallisemmalla käyttölämpötila-alueella käytettäväksi sallittuja laitteita voitaisiin sijoittaa.

Katkaisijan apukoskettimilta on saatavilla digitaalinen kärkitieto, jonka avulla katkaisijan tila pystytään tunnistamaan. Tämän kärkitiedon avulla voidaan tunnistaa, ovatko katkaisijan pääkoskettimet johtavassa tilassa, mutta ei kuitenkaan esimerkiksi havaita, onko katkaisijalla ylipäätään jännitettä.

Tämän kärkitiedon välittämiseen on tarkoitus käyttää IoT-laitetta, jonka tulisi olla ulkoilman lämpötilassa vallitseviin käyttöolosuhteisiin soveltuva ja sisältää riittävä akusto riittävän pitkän toiminta-ajan saavuttamiseksi.

Katkaisijoilla suoritetaan määräaikaistarkastukset 6 vuoden välein, jonka yhteydessä näiden ko. laitteiden akkuja olisi mahdollista vaihtaa uusiin, joten 6 vuoden akkukesto asetettiin laitteelle minimivaatimukseksi. Lisäksi vaatimuksena oli kärkitiedon vienti olemassa olevaan SCADA-järjestelmään IEC104-

protokollaa käyttäen ja järjestelmän tietoturvatasoa heikentämättä, jonka pohjalta sopivaa ratkaisua lähdettiin suunnittelemaan.

6.2 IoT-laitteen ja tietoliikenneratkaisun valinta

Työn käytännön osuuden suunnittelu aloitettiin tutkimalla olemassa olevaa laitetarjontaa mahdollisesti kyseiseen käyttökohteeseen soveltuvista IoT-laitteista ja niiden käyttämistä verkkotekniikoista.

Mahdollisiksi käytettäviksi sekä vertailtaviksi tietoliikennetekniikoiksi valittiin matkapuhelinverkko ja erilaiset LPWAN-verkot, kuten LoRaWAN sekä Sigfox ja esimerkiksi erilaiset laitevalmistajien omat, suljetut ratkaisut.

Aluksi ensisijaisena tarkoituksena oli hyödyntää matkapuhelinverkkoa sen käytännöllisyyden vuoksi. Matkapuhelinverkko kattaa käytännössä koko jakelualueen, ja siihen on helppo liittyä sekä datan siirto IoT-laitteelta sitä vastaanottavalle palvelimelle tapahtuisi suoraan internetin yli IP-protokollaa hyödyntäen ilman erillisiä laitteita tai palveluita.

Laitteita etsiessä ilmeni kuitenkin ongelmia käyttökohteen vaatimukset täyttävien laitteiden saatavuudessa erityisesti riittävän pitkän akkukeston suhteen. Lisäksi datan välittäminen suoraan julkisen internetin yli monilta eri laitteilta koettiin mahdollisesti tietoturvaongelmaksi, jonka poistamiseksi olisi pitänyt esimerkiksi ottaa käyttöön privateAPN (Access Point Name)-ratkaisu, jossa matkapuhelinoperaattori reitittää liikenteen kyseisiltä laitteilta suoraan asiakkaan omaan verkkoon, eivätkä laitteet ole saavutettavissa julkisesta internetistä.

Matkapuhelinverkon sijaan erilaisia LPWAN-verkkoratkaisuja hyödyntävien IoT-laitteiden akuston riittävyys havaittiin huomattavasti paremmaksi, jonka johdosta siirryttiin tutkimaan tätä vaihtoehtoa.

Lisäksi näiden verkkoratkaisujen osalta tarkasteltiin, olisiko mahdollisesti kannattavaa rakentaa omia laitetiloja ja tukiasemia kokonaan omaa, tätä tarkoitusta varten rakennettavaa LPWAN-verkkoa varten vai hyödyntää jo jotakin olemassa olevaa kaupallista verkkoa.

Omien laitetilojen rakentaminen 1kV-jakeluverkon alueelle havaittiin nopeasti kannattamattomaksi, sillä katkaisijoiden sijainnit olivat hajallaan ympäri toimialuetta, eikä esimerkiksi yksittäisellä omalla, jonkin laitevalmistajan suljetun LPWAN-ratkaisun tukiasemalla olisi käytännöllisesti pystynyt palvelemaan kuin yksittäisiä katkaisijoita. Myöskään oman LoRaWAN-verkon rakentamisen aloittamista ei tässä vaiheessa katsottu järkeväksi.

Kaupallisten LPWAN-ratkaisujen, eli Sigfoxin ja LoRaWANin välillä suurimpana erona on mahdollisuus toteuttaa haluttaessa oma verkko LoRaWAN-tekniikkaa käyttäen, mikä katsottiin LoRaWAN-teknologian eduksi Sigfoxiin nähden, vaikka tässä vaiheessa omaa verkkoa ei vielä päätettykään rakentaa.

Lisäksi LoRaWAN pystyy esimerkiksi siirtämään hieman suurempia datamääriä Sigfoxiin verrattuna sekä käyttämään suurempia tiedonsiirtonopeuksia, eikä sillä ole tiukkoja rajoituksia viestimäärien suhteen, jotka Sigfoxissa rajoittavat erityisesti mahdollista kaksisuuntaista kommunikaatiota päätelaitteiden kanssa.

Suomessa kaupallista LoRaWAN-verkkoa operoiva Digita koettiin myös luotettavaksi verkko-operaattoriksi tämänkaltaiseen sovellukseen ja Digitan LoRaWAN-verkkoa olikin jo alettu hyödyntämään esimerkiksi muiden sähköyhtiöiden toimesta vastaavankaltaisissa IoT-projekteissa.

Tämän johdosta päädyttiin aloittamaan pilotti Digitan LoRaWAN-verkkoa hyödyntäen, minkä kuuluvuusalueen todettiin Digitan verkkosivuillaan julkaiseman kuuluvuuskartan perusteella kattavan jo tällä hetkellä ainakin osan katkaisijoiden sijainneista. Erilaisia LoRaWAN-yhteensopivia kärkitietoa lukevia laitteita todettiin lisäksi olevan saatavilla eri laitevalmistajilta suhteellisen kattavasti.

Tässä tapauksessa ensimmäiseksi pilottilaitteeksi valittiin samalla Digitan kautta saatavilla ollut Elsys ELT-2-HP -anturi. Tähän laitteeseen päädyttiin sen soveltuessa kyseiseen käyttökohteeseen ja ollessa saatavilla suoraan Digitalta, jolloin laitteen saatavuudessa ja yhteensopivuudessa ei pitäisi esiintyä ongelmia, eikä sen tilaamista tarvinnut erikseen järjestellä.

Elsys ELT-2-HP on yleiskäyttöinen LoRaWAN-laite, joka pystyy lukemaan erilaisia analogisia ja digitaalisia signaaleja. Laite sisältää sisäiset anturit lämpötilan, kosteuden, kiihtyvyyden ja ilmanpaineen mittaamiseen ja tämän lisäksi kaksi ulkoista tuloa, joihin voidaan kytkeä erilaisia tulosignaaleja, kuten esimerkiksi analogi- ja digitaali- tai pulssituloja sekä erilaisia ulkoisia sensoreita (Elsys 2017).

Kyseinen anturi on suunniteltu asennettavaksi suoraan ulko-olosuhteisiin ja sen akun käyttöikä on valmistajan mukaan jopa 10 vuotta riippuen lähetysvälistä, LoRaWAN-verkon kuuluvuudesta ja mitattavista suureista.

Osalla valvottavista katkaisijoista tiedettiin lisäksi olevan ylijännitesuojamoduuleita, joista oli vikaantumisindikointi saatavilla myöskin kärkitietona. ELT-2-HP-anturimallilla saadaan tällaisissa kohteissa valvottua myös itse katkaisijan lisäksi toisella sisääntulolla esimerkiksi näiden mahdollista vikaantumista.

Ylijännitesuojien vikaantuminen ei vaadi välitöntä toimenpidettä, kuten katkaisijan laukeaminen, joten sen vuoksi samaa kärkitietoa käyttämällä näiden valvontakohteiden yhdistäminen ei olisi optimaalista.

Elsysin ELT-sarja käsittää myös ELT-Lite-anturin, joka sisältää yhden ulkoisen tulon eikä sisäisiä antureita. Tämän anturimallin optimaalinen käyttökohde olisikin sellaisilla laiteasemilla, joilla valvottavana on vain esimerkiksi itse katkaisijan kärkitieto.

Muita vastaavankaltaiseen käyttötarkoitukseen soveltuvia esimerkkejä LoRaWAN-antureista ovat DigitalMatter SensorNode- ja Adeunis Dry Contacts -anturit.

6.3 Digitan LoRaWAN-verkko

Digitan LoRaWAN-verkkoratkaisussa Digita tarjoaa asiakkaan käyttöön LoRaWAN-verkkopalvelun, joka toimittaa asiakkaan käyttämien päätelaitteiden LoRaWAN-verkon kautta lähettämän datan asiakkaan palvelimelle internetin välityksellä rajapintamäärityksen mukaisesti (Digita 2018b, 1–2).

Digitan LoRaWAN-verkkoa voidaan käyttää kaikkien LoRaWAN-yhteensopivien päätelaitteiden kanssa, jotka asiakas voi esimerkiksi tilata Digitan valikoimasta valmiiksi verkkoon provisioituna tai vaihtoehtoisesti käyttää myös muita, miltä tahansa toimittajalta hankittuja laitteita (Digita 2018b, 2).

Digitan käyttämässä verkkoalusta Actility ThingParkissa rajapintana toimii HTTP REST API (Application Programming Interface), jolloin Actility lähettää LoRaWAN-laitteiden lähettämät uplink-paketit määritellylle Application Server -palvelimelle HTTP POST -requesteina joko JSON- (JavaScript Object Notation) tai XML-muodossa (Actility 2018a, 16).

Actility-verkkoalusta toimii kuitenkin tässä käytössä vain pakettien välittäjänä, joten asiakkaan palvelimen ollessa saavuttamattomissa, LoRaWAN-laitteilta vastaanotettu data häviää.

Järjestelmään on kuitenkin mahdollista määritellä useita erillisiä Application Server -palvelimia haluttaessa esimerkiksi varmistaa datan vastaanotto mahdollisten laiterikkojen tai tietoliikennehäiriöiden varalta, jolloin asiakas voi helposti kahdentaa omat dataa vastaanottavat järjestelmänsä.

6.4 Datan vastaanotto ja käsittely Application Server -palvelimella

Datan vastaanottopalvelimen tehtäväksi jäi vastaanottaa Digitan LoRaWAN-verkkoalustan HTTP POST -requesteina lähettämät LoRaWAN-laitteilta tulevat paketit ja saada välitettyä data LoRaWAN-antureilla valvottavien katkaisijoiden tilasta SCADA-järjestelmään IEC104-protokollaa käyttäen.

Palvelimen suunnittelu aloitettiin määrittelemällä palvelimen tyyppi, sijainti ja sille tarvittavat tietoliikenneyhteydet. Tässä tapauksessa päädyttiin hyödyntämään palvelimelle jo olemassa olevaa VMWare-virtualisointialustaa, mihin tietoliikenneyhteyksien järjestäminen olisi helppoa. Lisäksi palvelimen käyttöjärjestelmäksi päätettiin valita Windows Serverin uusin versio, joka tukisi käytettäviä ohjelmistoja.

Palvelimella käyttävien ohjelmistojen suunnittelu aloitettiin kartoittamalla internetistä, olisiko kyseiseen käyttökohteeseen soveltuvia ohjelmia mahdollisesti

jo valmiina olemassa esimerkiksi Application Serverinä toimimaan tai IEC-104-yhteyden muodostamista varten.

LoRaWAN-laitteiden harvakseltaan / epäsäännöllisesti lähettämän datan yhteensovittamiseen suoraan IEC-104-protokollalla SCADAn luettavaksi ei kuitenkaan osoittautunut löytyvän minkäänlaista valmista ohjelmistoa tai ratkaisua.

Tässä vaiheessa päädyttiin kokoamaan järjestelmä useammasta ohjelmistosta, joiden välillä rajapintana toimisi jonkinlainen tietokanta, joka sisältäisi LoRaWAN-laitteilla valvottujen kohteiden viimehetkiset tilat ja jota IEC-104-protokollaa käyttäen ”luettaisiin”.

Actility ThingParkille Application Serverinä toimivaa, suoraan soveltuvaa valmista ohjelmistoa ei myöskään löydetty, joten aluksi päädyttiin tutkimaan ratkaisua datan siirtämiseen jonkinlaisesta tietokannasta IEC-104-protokollaa käyttäen SCADA-järjestelmään ja ratkaisun löydyttyä selvittää, miten Actilityn lähettämistä paketeista saataisiin data valittuun tietokantaan.

IEC-104-slavena toimivaksi ohjelmistoksi valikoitui alustavasti Triangle Microworksin Scada Data Gateway, joka sisältää esimerkiksi ODBC-rajapinnan erilaisten tietokantojen lukemiseen sekä kykenee toimimaan sekä IEC-104 Slave- että Master-moodeissa, joten sen todettiin olevan ominaisuuksiltaan käyttötarkoitusta vastaava.

Tämänkaltaisten ohjelmistojen kaupallinen tarjonta osoittautui muutoinkin erittäin rajalliseksi, joten suoraan vastaavia vaihtoehtoja kyseiselle ohjelmalle ei oikeastaan edes löytynyt.

Datan vastaanottamiseksi Actilityltä alettiin tutkia oman palvelinsovelluksen kehittämistä esimerkiksi Microsoft IIS- tai Apache-palvelinohjelmistojen päälle. Lisäksi tutkittiin myös Actilityn tukemaa Kafka-rajapintaa ja selvitettiin, olisiko Digitalla datan vastaanottoon jo jonkinlaista valmiiksi tiedossa olevaa ratkaisua olemassa.

Digitalta löytyi valmis datan visualisointiin tarkoitettu palvelu, joka todettiin kuitenkin tähän kyseiseen käyttökohteeseen soveltumattomaksi, koska data oli tarkoitus saada vietyä sähköyhtiön olemassa olevaan SCADA-järjestelmään.

Oman palvelinsovelluksen kehittämistä suunnitellessa ja sitä varten tietoa etsiessä ilmeni, että Python-ohjelmointikieltä käyttämällä tarkoituksenmukaisen ohjelman kehittäminen olisi suhteellisen yksinkertaista ja tämä vaikutti myöskin toteuttamiskelpoiselta vaihtoehdolta, johon löytyi lisäksi vielä osittain valmiita esimerkkejä Internetistä, joten datan vastaanotto päätettiin toteuttaa ainakin alustavasti tällä ratkaisulla.

Tietokannaksi valittiin myös alustavasti MySQL-tietokanta, jonka rakenne määriteltäisiin käyttötarkoitukseen soveltuvaksi. MySQL:n havaittiin omaavan hyvän Python-rajapinnan, joka teki tietokannan hyödyntämisestä Python-sovelluksessa helppoa, ja siihen löytyy lisäksi ODBC-rajapinta, joka takaa yhteensopivuuden muiden tietokantaohjelmistojen kanssa.

6.4.1 “LoRaWAN_AppServer.py”

”LoRaWAN_AppServer.py” on juuri tähän kyseiseen käyttötarkoitukseen Pythonilla tämän työn osana kehitetty ohjelma, jonka tarkoituksena on kuunnella ja vastaanottaa Actilityltä tulevia HTTP POST -requesteja ja tallentaa niiden sisältämä vastaanotettu LoRaWAN-laitteen lähettämä data palvelimelle MySQL-tietokantaan.

Ohjelma kehitettiin pääasiallisesti vastaamaan Actilityn rajapintakuvaukseen ja sen kehityksessä otettiin lisäksi huomioon mahdollisesti tulevaisuudessa lisääntyvä laitemäärä ja esimerkiksi tietokantarakenteen skaalautuvuus sekä ohjelman varmatoimisuus mahdollisten häiriöiden, kuten tietokantapalvelimen tai tietoliikenneyhteyksien ongelmatilanteissa. Ohjelman ensimmäisen ”valmiin” version kehitystyö kesti noin viikon.

Lopullinen versio tukee Elsys-merkkisiä LoRaWAN-antureita ja kykenee dekoodaamaan ja tallentamaan niiden lähettämän datan käytettyyn MySQL-tietokantaan, jonka lisäksi 1 kV:n katkaisijoiden valvonnassa käytetyt datapisteet

tallennetaan erillisiin tietokantatauluihin, jotka käsittävät uusimmat vastaanotetut arvot, jotka viedään SCADA-järjestelmään.

Ohjelmoinnissa käytettiin tukena esimerkiksi Elsys-laitevalmistajan sivuilta löytyneitä dokumentteja Elsys-antureiden lähettämästä payload-datasta ja selainpohjaista datan decodeeria, jonka avulla varmistettiin, että Python-ohjelma käsittelee payloadin oikein ja tulokset ovat yhteneväiset käytetyllä testidatalla.

Ohjelman toimintaa testattiin lisäksi käyttämällä Actilityn rajapintakuvauksessa esitettyjä esimerkkejä järjestelmän lähettämistä uplink-viesteistä. Lisäksi varmistettiin, että ohjelma kykenee toimimaan Windows Servicenä, jolloin palvelimella ei tarvitse olla käyttäjän kirjautuneena sisään ohjelman toiminnan mahdollistamiseksi.

Lopulliseen version tuli lisäksi kyky lähettää LoRaWAN-laitteille downlink-viestejä esimerkiksi mahdollisten asetusmuutosten tekemiseksi, ja tämän datan generoimiseen kehitettiin vielä yksinkertainen GUI:lla (Graphical User Interface) varustettu ohjelma, jolla on helppo generoida tietokantaan lähetettävää dataa suurellekin määrälle LoRaWAN-laitteita.

Lisäksi ohjelmaan toteutettiin myös esimerkiksi mahdollisuus konfiguroida uudet LoRaWAN-laitteet automaattisesti triggeröimällä esimääriteltyjen asetusten lähetys downlink-viestissä vastaanotettaessa ensimmäinen viesti kyseiseltä laitteelta Application Serverille.

6.4.2 MySQL-tietokanta ja ODBC-rajapinta

MySQL on yleisin avoimeen lähdekoodiin perustuva tietokantajärjestelmä, joka on havaittu luotettavaksi ja suorituskykyiseksi jonka johdosta MySQL:ää onkin alettu käyttämään runsaasti esimerkiksi erilaisissa web-sovelluksissa, kuten Facebookin tai YouTuben taustajärjestelmissä (Oracle 2019a).

MySQL käyttää nimensä mukaisesti SQL:ää (Structured Query Language) tietokannan hallintakielenä, joka on kaikista yleisin ohjelmointikieli tietokantojen hallitsemiseksi. SQL on määritelty ANSI/ISO-standardissa, jota on kehitetty vuodesta 1986 lähtien. (Oracle 2019b.)

SQL-kyselyjä voidaan kirjoittaa suoraan vaikkapa generoitaessa raportteja tietokannassa olevaa dataa hyväksi käyttäen tai esimerkiksi sisällyttää jollakin ohjelmointikielellä kirjoitetun ohjelman lähdekoodin osaksi (Oracle 2019b).

Lyhenne ODBC tulee sanoista Open Database Connectivity, ja se on määritelmä eräälle database-API:lle. ODBC API perustuu ”Open Group” ja ISO/IEC-standardien määrittämiin CLI (Command Line Interface)-spesifikaatioihin, joihin ODBC-rajapinta on täysin vastannut versiosta 3 lähtien. (Microsoft 2017.)

ODBC-rajapinnan hyödyntämiseksi eri tietokantajärjestelmille (DBMS), kuten MySQL:lle tarvitaan vain kyseiselle tietokannalle soveltuva ODBC-ajuri. Kyseisten ajurien käyttämät funktiot asiakasohjelman suuntaan ovat standardisoitu, jolloin ODBC-yhteensopiva tietokantaa käyttävä ohjelmisto pystyy käyttämään mitä tahansa tietokantaa, jolle on olemassa ODBC-ajuri ilman itse ohjelmistoon tarvittavia muutoksia. (Microsoft 2017.)

Tämän johdosta ODBC-rajapinnan kautta onkin helppo liittyä erilaisiin tietokantoihin samaa ohjelmistoa käyttäen, eikä tietokannan tyyppiä tarvitse välttämättä speksata ohjelmistokohtaisesti, eikä eri tietokantoihin liittymiseksi tarvitse ohjelmoida itse asiakasohjelmistoon jokaiselle erikseen juuri kyseiselle kannalle soveltuvaa ”liitännäistä”.

ODBC-rajapinta ei kuitenkaan vaikuta itse tietokantajärjestelmän funktionaalisuuksiin, joten asiakasohjelmisto ei esimerkiksi pysty universaalisti hyödyntämään jotakin ominaisuutta tai toimintoa, jota ei löydy kaikista ODBC-ajurin omaavista tietokantajärjestelmistä (Microsoft 2017).

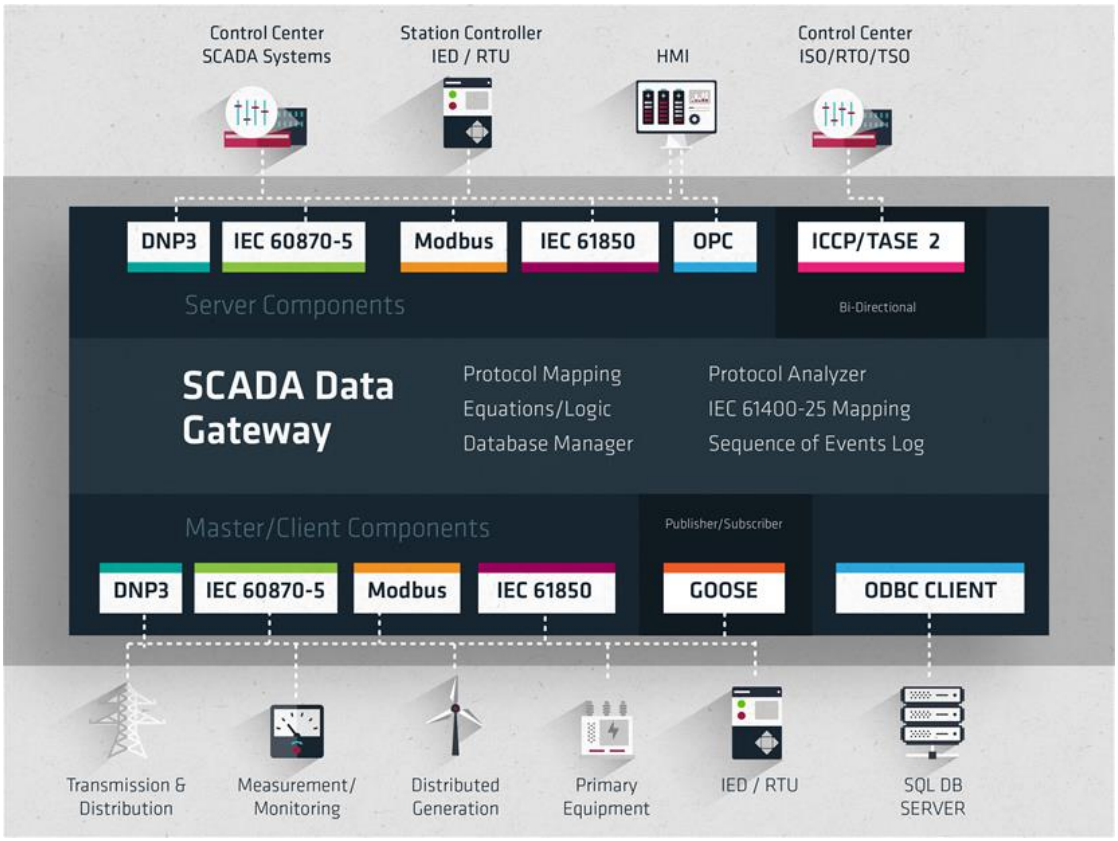
6.4.3 Triangle Microworks Scada Data Gateway

Triangle Microworks Scada Data Gateway on Windows-ohjelmisto, jota voidaan käyttää eri protokollia käyttävien järjestelmien ja kenttälaitteiden välisen kommunikoinnin mahdollistamiseen ja datan muuntamiseen protokollasta toiseen (Triangle Microworks s.a).

Scada Data Gateway tukee IEC 60870-5 -standardin IEC101- ja 104-protokollia sekä Master- että Slave-aseman roolissa. Lisäksi ohjelmistossa on tuki esimerkiksi IEC61850-, Modbus- ja DNP3- protokollille sekä ODBC-rajapinta tietokantoihin liittymiseen. (Triangle Microworks s.a.)

Ohjelmistolla pystytään joustavasti liittämään datapisteitä protokollien välillä toisiinsa, jonka lisäksi voidaan tehdä myös erilaisia loogisia tai matemaattisia operaatioita, mikäli datatyypit eivät esimerkiksi eri protokollien välillä ole suoraan yhteensopivia (Triangle Microworks s.a).

Kuvassa 9 esitetään graafisesti Scada Data Gateway -ohjelmiston tukemat protokollat ja mahdollisia sovellusesimerkkejä.



Kuva 9. Scada Data Gatewayn tukemat protokollat graafisesti esitettynä (Triangle Microworks s.a)

Tässä työssä Scada Data Gateway -ohjelmistolla on tarkoitus lukea ODBC-rajapinnan kautta LoRaWAN-laitteilta vastaanotetut viimeisimmät mittaustiedot käsittäviä MySQL-tietokannan tauluja ja viedä kyseiset tiedot olemassa olevaan SCADA-järjestelmään IEC 60870-5-104 -protokollaa käyttäen.

6.4.4 Ohjelmistojen koekäyttö ja simulointi

Ennen varsinaisen käytännön toteutuksen aloittamista alustavasti valittujen ohjelmistojen soveltuvuutta käyttötarkoitukseen tutkittiin ennakkoon rakentamalla kokeiluympäristö, jossa testattiin ohjelmistojen käytännön toimivuutta ja arvioitiin lisäksi suorituskykyä sekä käyttökelpoisuutta, mikäli valvottavia kohteita olisi käytössä esimerkiksi satoja tai tuhansia kappaleita.

Käyttökelpoisuuden arvioinnissa kiinnitettiin huomiota esimerkiksi uusien valvontakohteiden lisäämisen vaatimaan manuaaliseen konfigurointityöhön ja ylipäätään ohjelmistojen kykyyn selvitä suuremmasta laitemäärästä.

Digitan käyttämää LoRaWAN-verkkoalusta Actility ThingParkia simuloitiin lähettämällä rajapintakuvauksessa ollutta esimerkkiviestiä Insomnia-HTTP-clientilla virtuaalipalvelimelle, jolle ”LoRaWAN_AppServer.py” -ohjelmisto ja MySQL-tietokanta olivat asennettuina.

MySQL-tietokannasta dataa luettiin Scada Data Gateway -ohjelmistolla ODBC-rajapinnan kautta käyttäen MySQL/ODBC Connector -liitännäistä MySQL-tietokantaan liittymiseksi.

SCADA-järjestelmää simuloitiin FreyrSCADA IEC-60870-5-104 Client/Master Simulator -ohjelmistolla, johon datapisteet Scada Data Gateway -ohjelmistosta tuotiin IEC-104-protokollaa käyttäen.

Suurta laitemäärää mallinnettiin generoimalla MySQL-tietokantaan satunnaista dataa tuhannelle ”testilaitteelle” ”LoRaWAN_AppServer.py”:n käyttämällä tietokantarakenteella, joka tuotiin Scada Data Gateway -ohjelmistoon ja vietiin sieltä IEC-104-simulaattoriin samaan tapaan kuin varsinaisilta laitteilta saatu data.

Suurta liikennemäärää LoRaWAN-verkosta simuloitiin lähettämällä Insomnia-ohjelmistolla suuri määrä esimerkkiviestejä mahdollisimman nopeasti ja tarkkailemalla esimerkiksi palvelimen prosessorikuormaa ja HTTP request -vastausaikoja.

Ohjelmistojen testauksen aikana ”LoRaWAN_AppServer.py”-ohjelmaa kehitettiinkin suorituskykyisemmäksi esimerkiksi lisäämällä säikeistystä (threading) ja multiprosessointia hyödyntämällä, joilla saavutettiin parannuksia suorituskyvyssä ja HTTP-vastausaikojen alentumista suuren kuormituksen alla.

Lisäksi simuloitiin erilaisia virhe- ja häiriötilanteita, kuten esimerkiksi tietokantapalvelimen kaatumista pysäyttämällä kyseinen Windows-palvelu manuaalisesti ohjelman suorituksen eri vaiheissa tai tietokantakyselyjen erittäin hidasta prosessointia lisäämällä Python-ohjelmaan manuaalisesti useita sekunteja kuollutta aikaa tietokantakyselyn käsittävään funktioon.

Näiden testien perusteella kehitettiin ”LoRaWAN_AppServer.py”-ohjelmistoa siten, että se pystyy kirjoittamaan lokitiedostoon merkintöjä kyseisistä tapahtumista ja kykenee selviytymään niistä kaatumatta sekä jatkamaan normaalia toimintaansa automaattisesti varsinaisen ongelman poistuttua.

Lisäksi ohjelmasta korjattiin muutamia bugeja, joita esiintyi esimerkiksi datatyyppi- tai laitepositioiden generoinnissa tietokantapalvelimen vasteajan ollessa pitkä ja useiden viestien saapuessa Actilityltä (tai tässä tapauksessa Insomnialta) samanaikaisesti.

Tässä tapauksessa ohjelma saattoi generoida samalla laitteelle tai datatyypille useita positioita tietokantaan säikeistyksestä ja asynkronisesta prosessoinnista johtuen, mikä korjattiin lisäämällä positioiden hakemiseen ja generointiin lukot, jotka estävät näiden käsittelyn useamman kuin yhden säikeen toimesta samanaikaisesti.

Datan tuonnissa Scada Data Gateway -ohjelmistoon havaittiin testien aikana myös muutamia ongelmia. Aluksi käyttäen uusinta versiota MySQL/ODBC-connectorista, ei dataa ohjelmistoon saatu tietokannasta tuotua lainkaan, vaan tietokantakyselyä luodessa saatiin virheilmoitus, ettei tietokantataulujen sisältämää informaatiota voinut hakea.

Vanhemman MySQL/ODBC-connector liitännäisen asentaminen korjasi ongelman ja datan hakeminen tietokannasta alkoi onnistua. Ongelmaa ei tässä vai-

heessa tutkittu sen tarkemmin, vaan päätettiin katsoa, tapahtuuko sama varsinaisessa tuotantoympäristössä ja tällaisen tapauksen esiintyessä tiedettiin mahdollinen ratkaisu ongelmaan.

SDGW:n havaittiin hakevan tietokannasta kerrallaan yhden rivin, jonka sarakkeiden arvot esitetään Master Data Objecteina, jotka voidaan sitten liittää muihin protokolliin, kuten IEC-104-slaven datapisteisiin. Lisäksi kyselyssä on muuttujat esimerkiksi seuraavalle riville siirtymiseen (GetNextRecord) tai kyselyn suorittamiseen (ExecuteQuery).

Nämä muuttujat voidaan aktivoida esimerkiksi liittämällä ne toisesta järjestelmästä toista protokollaa käyttäen saapuvaan tilamuuttujaan tai ohjelman sisäiseen tilamuuttujaan, joka voidaan asettaa aktivoitumaan säännöllisin väliajoin, jolloin esimerkiksi tietokantakyselyn suorittaminen ja muuttujien arvojen päivittämisen tietokannasta tapahtuu automaattisesti tietyllä intervallilla.

Näkymä tyypillisestä yksinkertaisesta, esimerkiksi ”SELECT * from ”table”” -tietokantakyselystä Scada Data Gateway -ohjelmistossa esitetään kuvassa 10. Kuvassa 11 esitetään lisäksi vastaava tietokantakysely HeidiSQL-ohjelmistossa.

Name	Value	Type
CurrentRecord	value=1 quality=0000 time=27Mar2019 0:00:52.438(A)	(UI4)
DATA	value=3426 quality=0000 time=27Mar2019 0:00:52.438(A)	(I4)
DEV_ID	value=1 quality=0000 time=27Mar2019 0:00:52.438(A)	(I4)
ExecuteQuery	value=On quality=0000 time=27Mar2019 0:00:52.438(A)	(BOOL)
GetNextRecord	value=Off quality=0000 time=27Mar2019 0:00:42.432(A)	(BOOL)
MoveToRecord	value=0 quality=0000 time=27Mar2019 0:00:42.432(A)	(UI4)
QueryError	value=Off quality=0000 time=27Mar2019 0:01:02.206(A)	(BOOL)
RecordCount	value=1 quality=0000 time=27Mar2019 0:00:52.438(A)	(UI4)
TIMESTAMP	value=20Mar19 16:31:42.000 quality=0000 time=27Mar20...	(DATE)

Kuva 10. Tyypillinen tietokantakyselynäkymä Scada Data Gateway -ohjelmistossa

dev_id	timestamp	data
1	2019-03-20 16:31:42	3 426
3	2019-03-23 03:50:24	3 426
4	2019-03-26 17:34:11	3 607
5	2019-03-26 23:57:40	3 633

Kuva 11. Vastaava tietokantakysely esitettynä HeidiSQL-ohjelmistossa

Näiden kuvien perusteella voidaan havaita, että Scada Data Gateway -ohjelmistoon saadaan käytetystä tietokantarakenteesta tätä kyselyä käyttäen kerrallaan vain yhden laitteen datapisteet, jolloin jokaiselle laitteelle pitäisi periaatteessa muodostaa omat tietokantakyselyt.

Vaihtoehtoisesti dataa SDGW:n kautta hakevan järjestelmän olisi kyettävä erillisessä muuttujassa osoittamaan tietokannan rivi, mistä dataa milläkin hetkellä haetaan, jolloin tietokantakysely voitaisiin muodostaa dynaamiseksi kyseinen muuttuja huomioiden.

Tarkoituksena oli kuitenkin saada kaikki tilatiedot vietyä kerralla erillisiin IEC-104-datapisteisiin, mikä tarkoitti, että tietokannasta oli käytännössä saatava yhdellä kyselyllä kaikkien kyseistä mittaustietoa välittävien LoRaWAN-anturei-den viimeisimmät tilatiedot yhdellä rivillä erillisissä sarakkeissa, joissa sarakkeiden niminä on kyseisen anturin laitetunnus ja arvona esimerkiksi digitaalitulon viimeisin tilatieto.

Tietokannan sarakkeeseen määritetty datatyyppi piti myös olla määritelty esimerkiksi katkaisijan tilaa valvovan digitaalitulon tapauksessa arvoon BIT(1), jotta SDGW-ohjelmaan saatiin data oikeana datatyyppinä (boolean) liitettäväksi suoraan IEC-104-protokollan käyttämään ”Single-point information” -datatyyppiin, jollaisena tieto vietäisiin SCADA-järjestelmään.

Tämänkaltaisen tietokantarakenteen lähtökohtainen muodostaminen ei olisi kannattavaa tietokannan suorituskyvyn ja skaalautuvuuden vuoksi, joten tietokantarakenteessa päädyttiin pysymään alkuperäisesti suunnitelluissa mittaustietokohtaisissa tauluissa, joihin tallennetaan eri riveille uusimmat mittaustiedot LoRaWAN-laitteen tietokannassa käytetyllä ID:llä ja aikaleimalla varustettuna.

MySQL:ssä ei ole natiivia tukea pivot-ominaisuudelle, millä tietokantakyselyssä rivit olisi voitu kääntää sarakkeiksi, joten tietokantakyselyn muodostamisessa päädyttiin aluksi sen kirjoittamiseen manuaalisesti esimerkiksi useita ”SELECT” -ja ”SELECT AS” -kyselyitä ”WHERE” -ehtoihin yhdistäen, jotta data saatiin ulos halutussa muodossa oikea datatyyppi säilyttäen.

Kuvassa 12 esitetään tietokantakysely SDGW-ohjelmistossa halutussa muodossa, ja kuvassa 13 vastaava tietokantakysely HeidiSQL-ohjelmistossa.

Name	Value	Type
ABATTER1W	value=1994 quality=0000 time=27Mar2019 0:02:22.800(A)	(I4)
ABLENCH1H	value=1992 quality=0000 time=27Mar2019 0:02:22.800(A)	(I4)
ACARO5O	value=1999 quality=0000 time=27Mar2019 0:02:22.803(A)	(I4)
ACAZEREAU57	value=2003 quality=0000 time=27Mar2019 0:02:22.803(A)	(I4)
ACELLI5A	value=1996 quality=0000 time=27Mar2019 0:02:22.803(A)	(I4)
ADANELUT5W	value=1991 quality=0000 time=27Mar2019 0:02:22.803(A)	(I4)
ADOMENICHINI6Q	value=1986 quality=0000 time=27Mar2019 0:02:22.804(A)	(I4)
AESCOFIER6Z	value=0 quality=0080 time=26Mar2019 23:33:46.523(A)	(I4)
AFLOUNDERS4L	value=1993 quality=0000 time=27Mar2019 0:02:22.802(A)	(I4)
AFROSTDICKE2I	value=2011 quality=0000 time=27Mar2019 0:02:22.801(A)	(I4)
AGARN5	value=2006 quality=0000 time=27Mar2019 0:02:22.799(A)	(I4)
AHADNY5F	value=1997 quality=0000 time=27Mar2019 0:02:22.803(A)	(I4)

Kuva 12. Tietokantakysely Scada Data Gateway -ohjelmistossa halutussa muodossa

apykerman0	ebotton1	ymacadie2	ncastiello3	qmacwhan4	agarn5
2 008	2 003	2 012	1 999	2 007	2 006

Kuva 13. Vastaava kysely esitettynä HeidiSQL-ohjelmistossa

Tämänkaltaisen tietokantakyselyn kirjoittaminen käsin esimerkiksi tuhat laitetta sisältävän tietokannan tietojen hakemiseksi olisi kuitenkin ollut käytännössä mahdotonta ja erittäin työlästä yhtään isommalla laitemäärällä. Kyselyyn tarvittavia tietoja, kuten esimerkiksi laitetunnuksia, piti myös hakea erikseen useammasta eri tietokannan taulusta käytetystä tietokantarakenteesta johtuen.

Käsin kirjoitettaessa suuren työmäärän lisäksi virheiden mahdollisuus näin pitkässä kyselyssä olisi väkisinkin ollut suuri, sillä kyseinen kysely olisi yhtään suuremmalla laitemäärällä tullut helposti useita kymmeniä tuhansia merkkejä pitkäksi. Tämänkaltaisen kyselyn editointi tuotantojärjestelmään muutoksia tehdessä ei olisi millään muotoa järkeväksi suunniteltu toimenpide.

Lisäksi MySQL:ssä havaittiin olevan 61 liitetyn taulun hard limit, joka esti tässä tapauksessa yli 61 laitteen tilatietojen hakemisen halutussa muodossa samassa tietokantakyselyssä. Tämän havainnon jälkeen tutkittiin MySQL:n korvaamista Microsoft SQL Server Express -tietokannalla, jossa vastaavaa rajoitusta ei olisi ollut.

Microsoft SQL Server Expressin suorituskyky havaittiin kuitenkin erittäin heikoksi suoritettaessa kyseinen tietokantakysely jo muutaman sadan laitteen kyseessä ollessa. Tämä saattoi mahdollisesti johtua Express-version asettamista rajoitteista, mutta ongelman vuoksi tässä vaiheessa päätettiin vielä pääasiallisesti jatkaa MySQL:n hyödyntämismahdollisuuksien tutkimista käyttäen erilaisia tietokantarakenteita ja -kyselyitä.

Kyseinen MySQL:n rajoitus havaittiin mahdolliseksi kiertää tekemällä maksimissaan 61 kappaletta tilatietoja käsittäviä view-termillä tunnettuja tietokannan ”virtuaalinäkymiä”, joita pystyi tämän jälkeen vielä kokoamaan uuteen vastaavaan ”näkymään”, johon oli mahdollista kerätä esimerkiksi tuhannen laitteen tiedot kerralla rakentamalla se yhdistäen 17 kappaletta maksimissaan 61 laitetta käsittäviä ”alinäkymiä”.

Myöskin view-toiminnon käyttäminen ja näiden ”näkymien” kehittäminen vaativat kuitenkin edelleen pitkien tietokantakyselyiden kirjoittamista, joka olisi vaatinut runsaasti manuaalista konfigurointia ja aiheuttanut useita inhimillisen virheen mahdollisuuksia aina uusia LoRaWAN-laitteita käyttöön otettaessa.

Tämän johdosta päädyttiin ratkaisemaan ongelma kirjoittamalla uusi Python-ohjelma ”SDGW_configuration_helper.py”, joka analysoi tietokannassa ohjelman suoritushetkellä olevaa dataa ja muodostaa automaattisesti tarvittavat ”näkymät” tietokantaan ja palauttaa Scada Data Gateway -ohjelman konfiguraatioon tarvittavat tietokantakyselyt tekstitiedostoihin.

Tietojen hakeminen valmiiksi haluttua rakennetta käyttävästä view-näkymästä tapahtuu yksinkertaisella tietokantakyselyllä, kuten esimerkiksi ”SELECT * from ”view””. Myöskään MySQL-palvelimen suorituskyvyssä ei havaittu olevan ongelmia edes haettaessa kaikkien kyseisten 1000 testilaitteen tiedot kerralla, jolloin päädyttiin käyttämään tätä ratkaisua yhdessä MySQL-tietokannan kanssa.

Yritettäessä tuoda Scada Data Gateway -ohjelmistoon kyseinen 1000 laitetta sisältävä ”näkymä”, se kuitenkin poikkeuksetta kaatui. Tämän jälkeen yhteen

kyselyyn sisällytettävää laitemäärää pienennettiin, kunnes löydettiin käytännöllinen maksimimäärä, jonka SDGW kykeni yhdessä tietokantakyselyssä käsittelemään.

Tällaiseksi määräksi osoittautui kokeellisesti tutkien 250 datapistettä. Tämän jälkeen testattiin tuoda Scada Data Gateway -ohjelmistoon useita tuhansia datapisteitä tietokannasta käyttäen useita tietokantakyselyitä, joissa oli 250 pistettä kerrallaan. Kaikki kyseiset tietokantakyselyt määriteltiin lisäksi tapahtumaan samanaikaisesti tietokantapalvelimen kuormituksen maksimoimiseksi.

Osassa datapisteitä käytettiin boolean-muuttujien lisäksi datatyyppinä neljä numeroa sisältävää ”mittausdataa”, jollaista olisi esimerkiksi LoRaWAN-laitteiden lähettämät akkujännitteet millivoltteina. Testi osoittautui onnistuneeksi ja ohjelman tai MySQL-palvelimen suorituskyvyssä ei esiintynyt ongelmia useallakaan tuhannella tietokannasta samanaikaisesti haetulla datapisteellä.

Aiemmin kirjoitettua ”SDGW_configuration_helper.py”-ohjelmaa modifioitiin siten, että siihen on mahdollista ohjelmaa suoritettaessa määritellä maksimipistemäärä yhdelle tietokantakyselylle, jonka ylittyessä tietokantaan muodostettavien ”näkymien” rakennetta ja kyselyitä muokataan siten, että ohjelma palauttaa useita erillisiä kyselyitä, jotka sisältävät maksimissaan oletuksena 250 laitteen tai erikseen konfiguroidun laitemäärän tiedot.

Kyseisen Python-ohjelman avulla todettiin tietokantakyselyiden konfiguroiminen helpoksi ja käytännölliseksi myös järjestelmän käsittäessä useita tuhansia laitteita. Yksinkertaisimmillaan haluttaessa konfiguroida uusia LoRaWAN-laitteita SDGW-ohjelmistoon, ainoa tarvittava toimenpide on suorittaa kyseinen Python-ohjelma ja käynnistää SDGW-ohjelmisto tarvittaessa uudelleen, jotta uuden laitteen välittämä data tulee SDGW:n näkyviin.

”SDGW_configuration_helper.py”-ohjelman voisi tarvittaessa helposti myös ohjelmoida kutsuttavaksi Application Serverinä toimivasta ”LoRaWAN_AppServer.py”:stä sen luodessa uuden laiteposition, jolloin datapisteet saataisiin päivitettyä täysin automaattisesti suoraan SDGW-ohjelmistoon asti uuden LoRaWAN-anturin lähettäessä ensimmäisen uplink-paketin.

Tämä jätettiin tässä vaiheessa kuitenkin vielä tarkemmin harkittavaksi, onko näin pitkälle viedylle automatisoinnille ylipäätään tarvetta ja onko sellaisen käyttäminen tuotantoympäristössä muutenkaan järkevää mahdollisten virhetilanteiden varalta. Ohjelmistoja ajettiin useita vuorokausia, jonka aikana tarkkailtiin niiden toimintaa ja esimerkiksi muistinkulutusta ja prosessorikäyttöä, joiden ei havaittu kohoavan missään vaiheessa epämääräisen suuriksi.

Testien perusteella näiden kyseisten ohjelmistojen todettiin soveltuvan ainakin vähintään tuhannen LoRaWAN-laitteen järjestelmään yhdellä, riittävän suorituskykyisellä palvelininstanssilla, jonka pitäisi riittää ainakin tällä hetkellä JSE:n jakeluverkossa sijaitsevien 1 kV:n katkaisijoiden valvontaan.

Lisäksi voidaan todeta, että testien aikana kaikki datapisteet päivitettiin tietokannasta samanaikaisesti suhteellisen tiheästi, mikä ei olisi välttämättömyys varsinaisessa tuotantojärjestelmässä, vaan datapisteitä voisi päivittää hieman harvemmin niiden sisältämästä datasta riippuen ja porrastettuna, mikäli tietokantapalvelimen suorituskyky ei muuten riittäisi.

Varsinaiseen järjestelmään käyttöön tuleva palvelin asennetaan virtualisointialustalle, joten myös resurssien lisääminen siihen järjestelmän laitemäärän lisääntyessä on helppoa niin kauan kuin alustan fyysisten host-palvelimien kapasiteetti ja suorituskyky siihen riittävät.

Suuressa järjestelmässä, jossa olisi esimerkiksi kymmeniä tuhansia pisteitä, voitaisiin lisäksi hyödyntää useita palvelininstansseja, joille kuormitusta ja eri rooleja jaettaisiin, joten suurenkin järjestelmän rakentaminen käytetyillä ohjelmistoilla arvioitiin käytännössä toteutuskelpoiseksi.

7 KÄYTÄNNÖN TOTEUTUS

7.1 Digitan LoRaWAN-verkon käyttöönotto ja asetusten konfigurointi

Työssä hyödynnettiin Digitan LoRaWAN-verkkoa, joten käyttöönoton ensimmäisenä vaiheena oli kyseisen palvelun tilaaminen Digitalta. LoRaWAN-verkkopalvelun tilaamisen yhteydessä Digitalta tilattiin lisäksi ensimmäiseksi testilaitteeksi Elsys ELT-2-HP -anturi lithiumparistolla ja ympärisäteilevällä piiskaantennilla varustettuna.

Palvelun tilaus- ja toimitusprosessin valmistumisen jälkeen seuraavana vaiheena verkon käyttöönotossa oli luoda Digitan käyttämälle Actility ThingPark -verkkoalustalle tarvittavat käyttäjätunnukset ja konfiguroida asetukset LoRaWAN-laitteiden lähettämän datan reitittämiseksi sitä vastaanottavalle Application Server -palvelimelle.

Tässä ThingPark-alustalle on ensin luotava kyseinen Application Server, jonka jälkeen se voidaan liittää reititysprofiileihin, jotka taas voidaan liittää itse LoRaWAN-laitteisiin tai määritellä oletusprofiiliksi kaikkien laitteiden käyttöön, jos profiilia ei erikseen haluta laitekohtaisesti määritellä.

LoRaWAN-laitteille Actility ThingPark tukee kolmentyyppisiä Application Servereitä, jotka ovat ”LoRaWAN HTTP Application Servers”, ”Kafka clusters” sekä ”ThingPark X destinations” (Actility 2018b, 125).

”ThingPark X destinations” ovat Actilityn omia Application Servereitä, jotka LoRaWAN-verkkopalvelun toimittaja niitä käytettäessä määrittelee ThingPark-alustalle (Actility 2018b, 126). Näiden avulla voitaisiin rakentaa esimerkiksi erilaisia datan tallennus- ja käsittelypalveluita suoraan Actility-verkkoalustalle, mutta niitä ei tässä työssä käytetä.

Asiakkaan omaan käyttöön soveltuvia Application Server -tyyppejä ovat ”LoRaWAN HTTP Application Server” ja ”Kafka Cluster”, joista tässä työssä hyödynnettiin ”LoRaWAN HTTP Application Server” -tyyppiä.

Application Serverin luominen aloitetaan navigoimalla Actilityn käyttöliittymässä ”Application servers” -näkymään, josta uuden Application Serverin luominen voidaan aloittaa (Actility 2018b, 128).

Aloitettaessa uuden Application Serverin luominen ensimmäisenä sille on annettava nimi ja valittava palvelimen tyyppi. Tässä tapauksessa käyttöönottoa tehdessä varsinainen tuotantopalvelin ei ollut vielä käytettävissä, joten järjestelmän testaaminen aloitettiin hyödyntämällä ”LoRaWAN_AppServer.py”:n kehittämiseen ja testaamiseen käytettyä virtuaalipalvelinta.

Tälle ensimmäiselle Application Serverille annettiin nimeksi ”TestServer” ja tyypiksi valittiin käytetty palvelintyyppi eli ”LoRaWAN HTTP Application Server”. Varsinaisella Application Server -palvelimella tarvittavat ja muut siihen liittyvät määritykset kuvataan tarkemmin myöhemmässä vaiheessa varsinaisen tuotantopalvelimen asennusta ja konfigurointia käsittelevässä kappaleessa.

Tämän jälkeen konfiguraatioon määritettiin palvelimen vastaanottama sisältötyyppi, jossa vaihtoehtoina ovat XML ja JSON. Tässä työssä Application Serverinä käytetty ”LoRaWAN_AppServer.py” oli ohjelmoitu vastaanottamaan JSON-muotoista dataa, joten tyypiksi valittiin sen mukaisesti JSON. Tämän lisäksi kyseisen Application Serverin statuksen varmistettiin olevan ”Active”, jotta Actility lähettäisi dataa ko. palvelimelle.

Tämän jälkeen määritettiin uplink/downlink security -ominaisuus, jota käytettäessä viestit Actilityn ja Application Serverin välillä allekirjoitetaan tietyistä viestien elementeistä ja ennalta määritellystä LRC (Long-Range Controller)-AS Key -avaimesta muodostetulla SHA-256-tokenilla, joka parantaa järjestelmän tietoturvaa erityisesti downlink-viestien osalta.

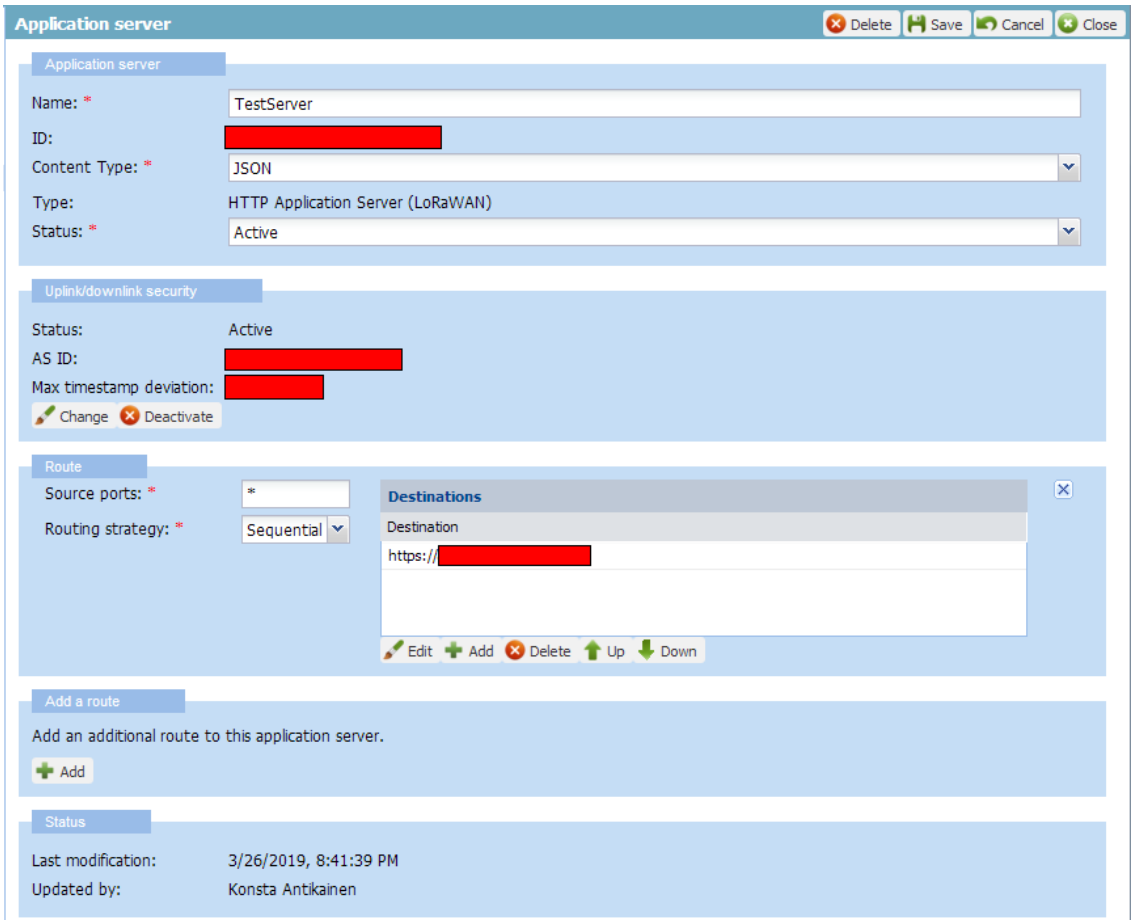
Ilman kyseistä toimintoa olisi ilkivaltaisten downlink-viestien lähettäminen antureille huomattavasti helpompaa, mikäli sopivaa taustatietoa omaava ilkivaltainen henkilö saa tietoonsa laitteen DevEUI (Extended Unique Identifier)-tunnuksen, joka esimerkiksi Elsys-antureissa on kirjoitettuna anturin pohjassa olevaan tarraan, ja anturit ovat myös ulkotiloihin asennettavaksi soveltuvia.

Ominaisuutta käyttöönotettaessa määritellään vapaavalintainen Application Server ID, 128-bittinen LRC-AS Key ja maksimi sallittu aikaero viestiä generoitaessa siihen muodostetun aikaleiman ja viestiä vastaanottavan järjestelmän senhetkisen kellonajan välillä.

Näiden lisäksi Application Serverille tulee vielä määritellä vähintään yksi URL-osoite, jossa käytetty palvelin kuuntelee HTTPS:n käyttämää porttia TCP443. Tarvittaessa osoitteita voidaan määritellä useampia, mikäli käytetään useaa palvelininstanssia esimerkiksi vikasietoisuuden varmistamiseksi.

Useamman kohdeosoitteen tapauksessa voidaan lisäksi määritellä, lähetetäänkö viesti aina kaikille palvelimille vai jossakin tietyssä järjestyksessä, kunnes jokin palvelimista vastaa. Myös lähdeportit voidaan tarvittaessa määritellä, mikä voi olla hyödyllistä esimerkiksi palomuurisääntöjen takia. Tässä tapauksessa näitä asetuksia ei kuitenkaan tarvinnut muokata.

Kuvassa 14 havainnollistetaan valmiiksi konfiguroituja Application Server asetuksia Actility ThingPark -verkkoalustalla.



Kuva 14. Valmis Application Server -konfiguraatio Actility ThingPark -verkkoalustalla

Kun valmis Application Server -konfiguraatio on tallennettu, on se valmis liitettäväksi reititysprofiileihin, joiden avulla määritellään, mihin LoRaWAN-laitteilta vastaanotettu data reititetään.

Reititysprofiilin luominen tapahtuu siirtymällä käyttöliittymässä ”AS routing profiles” -näkymään, josta uuden reititysprofiilin luominen voidaan aloittaa. Uutta reititysprofiilia luodessa on sille aluksi annettava nimi ja valittava profiilin

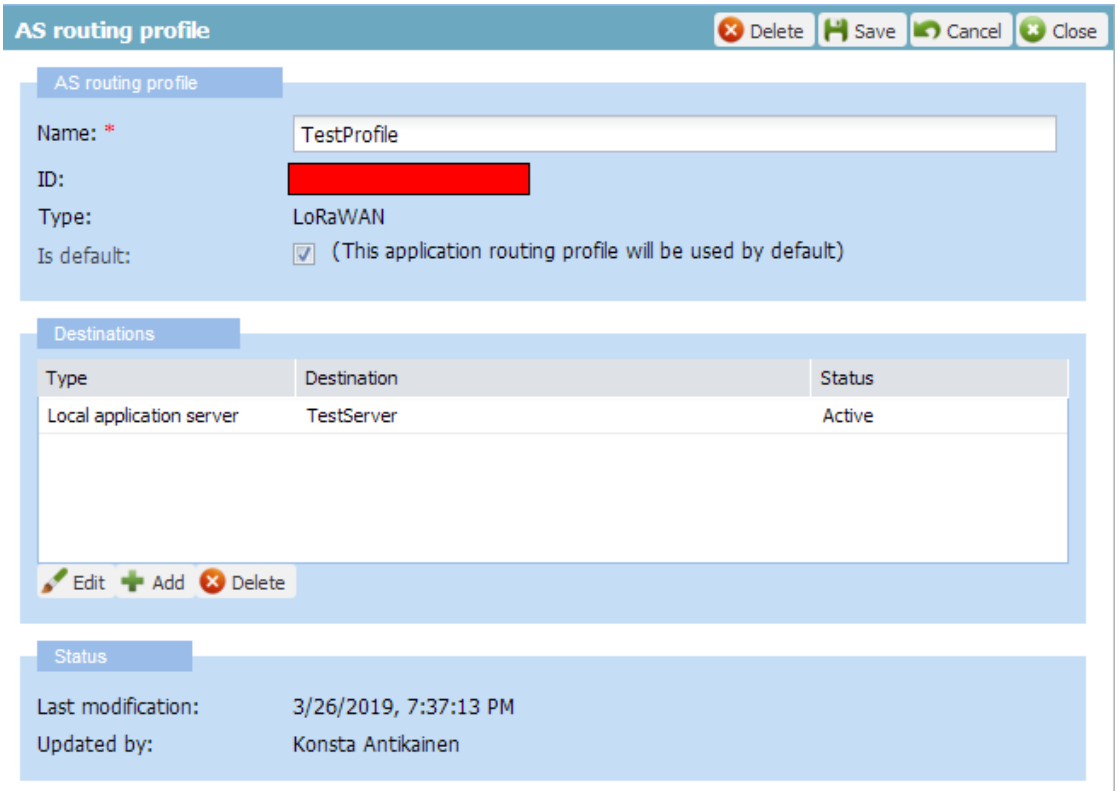
tyyppi. Actility tukee kahdentyyppisiä reititysprofiileita, ”LoRaWAN” sekä ”Cellular” (Actility 2018b, 138).

Tässä tapauksessa valittiin luonnollisesti LoRaWAN ja nimeksi profiilille annettiin ”TestProfile”. Tämän jälkeen profiilille voidaan määritellä yksi tai useampia Application Servereitä, joista valittavissa oli joko ”Local Application Server” tai ”Supplier Application Server” -tyyppinen kohdepalvelin.

Näistä Local-tyyppi tarkoittaa Actilityyn itse aiemmin kuvatun kaltaisesti luotua Application Serveriä ja Supplier jonkin palveluntarjoajan tarjoamaa, mahdollisesti useiden asiakkaiden käyttämää palvelua, joka on verkkoalustalle ennalta konfiguroitu operaattorin toimesta. Lisäksi tässä voisi olla valittavissa myös Actility ThingPark X -palvelimia, mikäli niitä olisi alustalla saatavilla. (Actility 2018b, 139.)

Tässä tapauksessa valittiin tyypiksi Local Application Server ja sen jälkeen kohdepalvelimeksi aiemmin luotu ”TestServer”. Lisäksi määriteltiin, että kyseinen reititysprofiili on oletusprofiili, joka tarkoittaa, että kaikkien LoRaWAN-laitteiden, joille ei erikseen määritellä jotain muuta profiilia, lähettämä data lähetetään ko. profiilin kohdepalvelimille.

Kuvassa 15 havainnollistetaan valmista reititysprofiilin konfiguraatiota.



Kuva 15. Valmis AS routing profile -konfiguraatio Actility ThingPark -verkkoalustalla

Näiden asetusten konfiguroinnin jälkeen Actility ThingPark -verkkoalusta oli valmiina käyttöön ja reitittämään LoRaWAN-antureilta vastaanotettua dataa kyseiselle testipalvelimelle sopivassa muodossa.

7.2 LoRaWAN-anturin käyttöönotto ja provisiointi verkkoon

LoRaWAN-anturit voidaan provisioida verkkoon käyttäen kahta eri menetelmää, jotka ovat ABP sekä OTAA. ABP muodostuu sanoista ”Activation By Personalization” ja OTAA ”Over The Air Activation”. (Oniga ym. 2017, 2.)

Provisioitavalle anturille ja verkkoalustalle on syötettävä tiettyjä parametrejä, joiden avulla verkko pystyy tunnistamaan anturin ja jotka myös mahdollistavat esimerkiksi vahvan lähetettyjen viestien salauksen, jolloin niitä ei pääse mahdollisesti ulkopuoliset lukemaan.

Käytettäessä ABP-menetelmää anturille on manuaalisesti määritettävä ”DevAddr”, ”NwkSKey” sekä ”AppSKey”. ”DevAddr” on laitteen LoRaWAN-verkossa käyttämä yksilöllinen osoite ja ”NwkSKey” on Network Session Key, jonka avulla verkko ja päätelaite esimerkiksi muodostavat ja tarkistavat jokaiselle viestille lasketun Message Integrity Coden. (Oniga ym. 2017, 2–3.)

MIC-tarkistuksen tarkoituksena on estää LoRaWAN-verkossa lähetettyjen viestien manipulointi siirron aikana ja ns. Impersonation-hyökkäykset, joissa joku yrittää lähettää viestejä esiintyen jonain toisena LoRaWAN-verkkoon provisioituna laitteena (Oniga ym. 2017, 3). Tällaisessa tapauksessa MIC-tarkistus ei mene läpi, sillä vieraalla laitteella ei ole verkon kanssa samaa Network Session Keytä.

”AppSKey” eli Application Session Key on taas vastaavasti anturin ja Application Serverin tai verkkoalustan käyttämä varsinaisen antureiden lähettämän payloadin (eli ”Application Datan”) kryptaukseen käyttämä salausavain (Oniga ym. 2017, 2–3).

OTAA-menetelmässä nämä kyseiset osoitteet ja avaimet muodostetaan dynaamisesti anturin verkkoonliittymisprosessin aikana. Tässä menetelmässä anturille tarvitsee konfiguroida vain ”AppKey” ja ”AppEUI”. ”AppKey” on avain, jota käytetään anturin liittyessä verkkoon ”join request” -viestin allekirjoittamiseen ja verkon vastatessa ”join accept” -viestin encryptaamiseen. (Oniga ym. 2017, 2.)

AppEUI:n tarkoituksena on identifioida kyseisen anturin ja sovelluksen omistaja (Oniga ym. 2017, 2), ja sitä voidaankin käyttää esimerkiksi anturin lähettämän datan ohjaamiselle oikealle Application Serverille.

OTAA-aktivointimenetelmän etuna on, ettei laitteisiin tarvitse konfiguroida manuaalisesti esimerkiksi niiden osoitteita, ja tarvittaessa LoRaWAN-verkon Network Server pystyy initioimaan uuden aktivoinnin päätelaitteen viestimäärälaskureiden saavuttaessa maksimiarvonsa, joka pienentää mahdollisuutta replay-hyökkäysten toteuttamiseen (Oniga ym. 2017, 3). Lisäksi tietoturvamielessä varsinaisia, datan salaamiseen käytettäviä session key -avaimia ei ole pysyvästi tallennettuna laitteisiin.

Replay-hyökkäys tarkoittaa saman, mahdollisesti kaapatun viestin lähettämistä uudelleen myöhempänä ajankohtana, minkä estämiseksi LoRaWAN-

verkossa käytetään pakettilaskureita, joiden avulla pidetään kirjaa päätelaitteen ja verkon välillä lähetetyistä paketeista laitteen verkkoon liittymisen jälkeen (Oniga ym. 2017, 3).

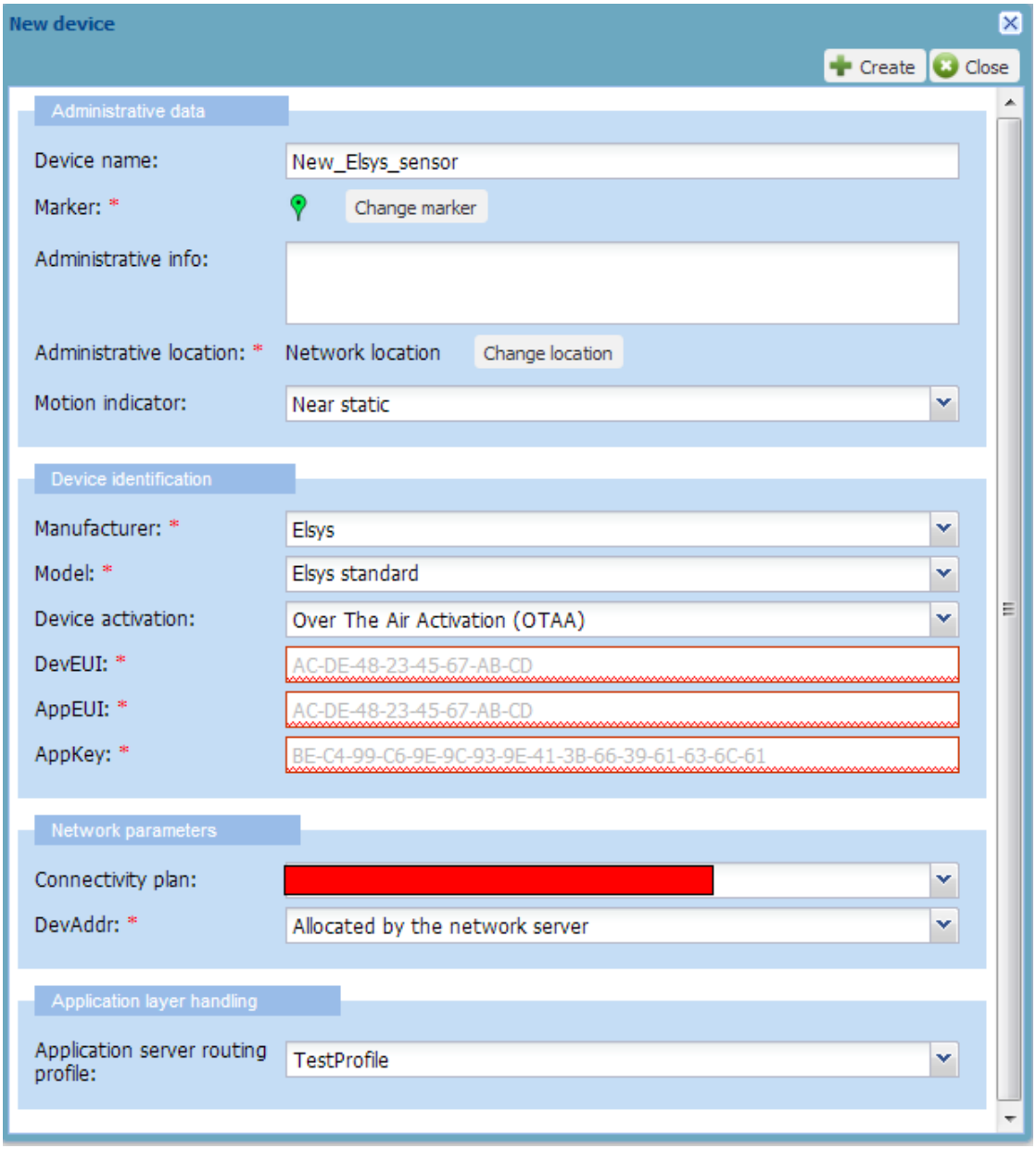
Digitan verkkoa käytettäessä Digitan kautta tilatut LoRaWAN-anturit tulevat valmiiksi verkkoon provisioituna, joten käyttöönotto anturin saapuessa tapahtuu asettamalla anturin mukana tullut antenni ja paristo paikoilleen, jonka jälkeen anturi automaattisesti liittyy Digitan LoRaWAN-verkkoon ja lähettää oletusasetustensa mukaisesti ensimmäisen payloadin default routing profileen määritellylle Application Serverille.

Mikäli käytetään omaa privaatti-LoRaWAN-verkkoa tai liitetään esimerkiksi Digitan verkkoon muita kuin Digitan kautta tilattuja antureita, on anturit provisioitava, ennen kuin verkko hyväksyy ja välittää niiden lähettämää dataa.

Vaikka kyseinen anturi saapuikin valmiiksi verkkoon provisioituna, voidaan esimerkiksi OTAA-aktivointia käyttävän vastaavan Elsys-anturin provisioinnin toteuttamista Digitan LoRaWAN-verkkoon käytännössä käsitellä akateemisessa mielessä.

Uuden anturin provisiointi Actility ThingPark -alustalle tapahtuu Actility Device-Manager -käyttöliittymässä, josta navigoidaan ”Devices”-näkymään, jossa klikataan ”Add Devices” -osiosta ”Create”, mikäli kyseessä on yksittäinen laite. Laitteita voitaisiin myös tarvittaessa tuoda Actilityyn useita kerrallaan .csv-tiedostoa käyttäen.

Actilitylle on määriteltävä laitteen valmistaja ja malli, aktivointityyppi ja sitä varten tarvittavat avaimet sekä laitteen DevEUI-tunnus, laitteen käyttämä ”Connectivity plan”, laiteosoitteen määrittelytapa sekä laitteelle käytettävä ”Application server routing profile”. Lisäksi voidaan määritellä laitteen nimi ja muuta informaatiota. Kuva 16 esittää Actilityn ”New device” -valintaikkunaa.



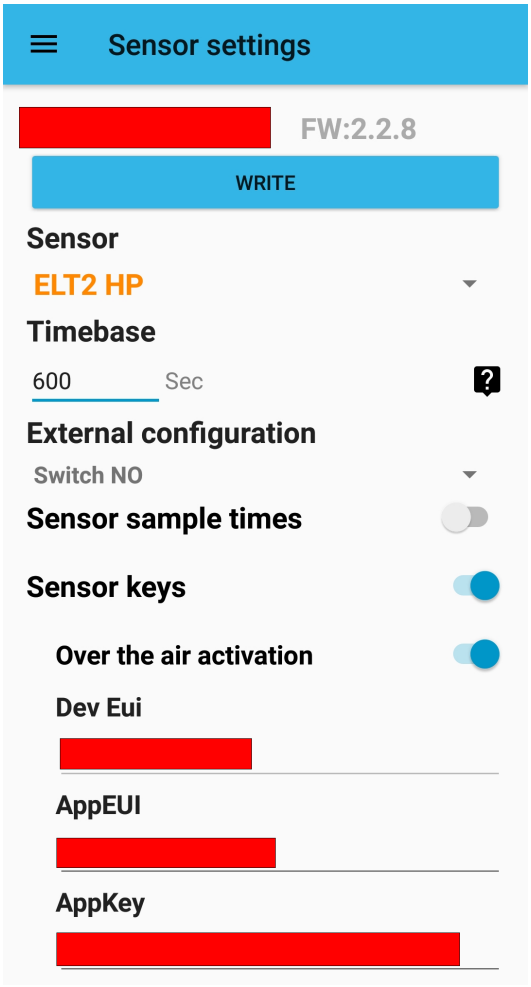
Kuva 16. Actility ThingParkin ”New device” -ikkuna käytettäessä OTAA-aktivointia

Ennen anturin provisioimista verkkoon, on sille määriteltävä AppEUI- ja AppKey-avaimet sekä selvitettävä anturin DevEUI-tunnus Actilityyn syöttämistä varten. Elsys-anturin tapauksessa tähän voidaan käyttää Android-puhelimissa toimivaa mobiilisovellusta, jolla antureiden asetuksia voidaan konfiguroida NFC:tä hyödyntäen.

Mobiilisovelluksen käynnistämisen jälkeen tuomalla Elsys-anturi puhelimen NFC-antennin läheisyyteen, kyseinen sovellus lukee sillä hetkellä anturin muistissa olevat asetusarvot. Tämän jälkeen sovelluksesta voidaan avata ”Sensor keys” -valikko, josta nähdään laitteen DevEUI-tunnus, ja voidaan määritellä tarvittavat AppEUI sekä AppKey.

Tämän lisäksi ”Version 2 features” -valikosta kannattaa tarkistaa, että käytetty ”Frequency plan” on oikea, jotta anturi ylipäätään käyttää alueen tukiasemien kanssa samaa taajuutta. Esimerkiksi Suomessa käytetään ”3 EU868” -valintaa, jolloin anturi käyttää 868 Mhz taajuusaluetta, millä Suomessa käytetyt LoRaWAN-tukiasemat toimivat.

Kuvassa 17 esitetään ”Sensor settings” -mobiilisovelluksen näkymä ”Sensor keys” -valikosta.



Kuva 17. Elsys sensor settings -mobiilisovelluksen ”Sensor keys” -valikko

Kun tarvittavat asetukset on määritelty ja laite luotu Actilityyn, sovelluksessa klikataan ”WRITE”-painiketta, jonka jälkeen puhelimen NFC-antenni viedään anturin NFC-antennin läheisyyteen, jolloin muokatut asetukset siirtyvät anturille ja anturi käynnistyy uudelleen.

Tämän jälkeen anturin pitäisi liittyä Digitan LoRaWAN-verkkoon, joka voidaan tarkistaa esimerkiksi Actilityn Wireless Loggeria hyödyntäen tai käytetyltä Application Serveriltä.

7.3 “LoRaWAN_AppServer.py”:n toimintakokeet Actilityn kanssa

LoRaWAN-anturin käyttöönottamisen jälkeen aloitettiin “LoRaWAN_AppServer.py”-ohjelmiston ensimmäiset toimintakokeet Actility ThingPark -verkkoalustan kanssa.

Tässä vaiheessa tuotantopalvelin ei ollut vielä käytettävissä, joten kokeet suoritettiin testipalvelinta hyödyntäen, jonka julkista IP-osoitetta vastaava ISP:n automaattisesti generoima DNS-osoite oli jo aiemmin määritelty Actility ThingParkin asetuksiin LoRaWAN-verkkoa käyttöönotettaessa.

Tälle kyseiselle testiympäristön palvelimelle oli jo sen asennusvaiheessa liitetty suoraan julkisen IP-osoitteen omaava virtuaaliverkkosovitin, joten verkkoyhteyksien konfigurointia ei enää tässä vaiheessa tarvinnut tehdä kyseisen sovittimen päälle kytkemisen lisäksi.

Actility ThingParkin ja ”LoRaWAN_AppServer.py”:n välillä käytetään HTTPS-yhteyttä, joten testiä varten “AppServerille” oli haettava käytettyä DNS-osoitetta vastaava julkisesti luotettu SSL-sertifikaatti, johon tässä vaiheessa käytettiin ”Let’s Encrypt” -palvelua, millä voidaan helposti ja nopeasti luoda ilmaisia SSL-sertifikaatteja esimerkiksi tämänkaltaiseen käyttötarkoitukseen.

Lisäksi ”LoRaWAN_AppServer.py” -ohjelmalle konfiguroitiin LRC-AS Key- ja AS-ID-parametrit vastaavasti, kuten Actilityyn oli aiemmin konfiguroitu. Testipalvelimen julkinen virtuaaliverkkosovitin oli liitetty suoraan ISP:n verkkoon sillattuun VLAN:iin, joten tarvittavat palomuurisäännöt pystyttiin määrittelemään suoraan palvelimen Windows Firewall -asetuksissa.

Palomuuriin määriteltiin sääntö, joka sallii liikenteen palvelimen porttiin 443 Digitan ilmoittamista Actilityn käyttämistä IP-osoitteista, jonka lisäksi sallittiin myös ”Echo Request ICMPv4-In”, jotta palvelin vastaisi pingiin myös julkisesta osoitteesta. Lisäksi sisäverkon virtuaaliverkkosovittimelta poistettiin gateway-

osoite ja määritettiin staattinen reititys muille sisäverkon aliverkoille, jotta palvelin varmasti käyttäisi omaa julkista IP-osoitettaan liikennöidessään internetiin.

Asetusten konfiguroinnin jälkeen käynnistettiin kyseinen ohjelma ja odotettiin LoRaWAN-anturin lähettämää pakettia ja tarkkailtiin tietokantaa sekä ohjelman konsoli-ikkunaa sekä lokitiedostoja mahdollisten virheilmoitusten varalta.

Actilityn lähetettyä ensimmäisen paketin havaittiin lokitiedostossa virheilmoitus uplink/downlink security -ominaisuuden perusteella muodostetun tokenin epäkelpoisuudesta, jonka vuoksi vastaanotettu data oli hylätty. Asiaa tutkittaessa varmistettiin, että sama LRC-AS Key on varmasti konfiguroitu sekä Actilityyn että AS:lle sekä varmistettiin ohjelmoidun palvelinohjelmiston toteutuksen olevan Actilityn rajapintakuvausten mukainen.

Tässä vaiheessa Actilityn rajapintakuvauksessa huomattiin maininta LRC-AS Keyn syöttämisestä SHA256-hashin generoivaan funktioon pieniä kirjaimia käyttäen, joka havaittiin toteuttamattomaksi ”LoRaWAN_AppServer.py”-ohjelmassa.

Rajapintakuvauksen esimerkeissä oli käytetty valmiiksi vain pieniä kirjaimia sisältävää LRC-AS Keytä, mutta todellisuudessa nyt käytössä oli sekä isoja- että pieniä kirjaimia sisältävä key, jonka vuoksi Actilityn vain pieniä kirjaimia ja AS:n todellisia kirjainkokoja käyttäen generoimat tokenit eivät olleet yhteneväiset ja autentikaatio ei onnistunut, vaikka se olikin testivaiheessa toiminut.

Ongelma korjattiin lisäämällä ”LoRaWAN_AppServer.py” ohjelmaan Pythonin ”.lower()” -funktio kyseisen LRC-AS Keyn käsittelyyn, minkä jälkeen ongelma korjaantui ja viestin autentikointi onnistui sekä dataa alkoi kertyä tietokantaan. Samassa yhteydessä kyseisen virhetilanteen logitusta parannettiin, jotta tämänkaltainen ongelma olisi jatkossa helpommin diagnosoitavissa.

Tämän jälkeen tietokantaan ilmestynyttä dataa analysoitaessa ilmeni, ettei AS kirjoita mitään 1 kV katkaisijoiden valvontaan käytetyt tilatiedot käsittäviin tauluihin, vaikka LoRaWAN-anturi lähettää dataa käyttäen kyseiselle toiminnolle konfiguroitua Fport-arvoa.

Ongelmaksi paljastui vastaanotetun datan ja ohjelmaan konfiguroidun Fport arvon yhteneväisyyttä tarkastelevassa if-funktiossa string-muotoisen datan vertailu integerin kanssa, jonka vuoksi funktio ei toiminut. Ongelma korjattiin pakottamalla molemmat muuttujat integer-tyyppisiksi Pythonin ”int()”-funktiota käyttämällä.

Näiden bugfixien jälkeen ohjelman todettiin toimivan suunnitellusti. Up-link/downlink security -ominaisuuden toiminta varmistettiin vielä konfiguroimalla Actilityyn tietoisesti väärä LRC-AS Key ja toteamalla, että AS hylkäsi kyseiset viestit.

Lisäksi ominaisuuteen kuuluva aikaleimojen tarkastelu todettiin toimivaksi muokkaamalla palvelimen kellonaika eriäväksi todellisesta kellonajasta enemmän kuin maksimiksi oli ohjelman konfiguraatioon määritetty ja toteamalla, että ohjelma hylkäsi viestit asiaankuuluvan virheilmoituksen lokitiedostoon kirjoittaen.

Downlink-ominaisuuden toiminta tarkastettiin syöttämällä ohjelman lukemaan tietokantaan testikäytössä olleelle LoRaWAN-anturille suunnattu payload, jonka tulisi käynnistää kyseinen testianturi uudelleen.

Tämän jälkeen tarkastettiin, lähettikö ohjelma viestin Actilitylle ja päivitti tietokantaa vastaavasti, minkä lisäksi tarkastettiin, menikö viesti perille LoRaWAN-laitteelle tarkkailemalla laitteen sisällä ollutta led-merkkivaloa, joka indikoisi laitteen uudelleenkäynnistymisen.

Nämä testit osoittautuivat onnistuneeksi, joten ohjelman todettiin alustavasti toimivan ja olevan valmis käyttöön. Ohjelman kehitystyötä ja bugien korjaamista kuitenkin jatkettiin vielä muiden kokeiden yhteydessä havaittujen ongelmien ja mahdollisten parannusideoiden esiintyessä ja tullaan todennäköisesti jatkamaan vielä myöhemminkin.

7.4 Elsys ELT-2-HP -anturin konfigurointi ja testaaminen

7.4.1 Anturin konfigurointimenetelmät ja konfiguroitavat asetukset

Elsys ELT-2 -anturin konfigurointiin on kaksi erilaista menetelmää. Anturi voidaan konfiguroida NFC-ominaisuudella varustetussa Android-puhelimessa käytettävän ”Elsys sensor settings” -mobiilisovelluksen avulla tai LoRaWAN-verkon downlink-viestejä hyödyntäen, mikäli anturi on jo provisioitu LoRaWAN-verkkoon (Elsys s.a.a).

Android-sovelluksella saadaan nopea katsaus anturin kaikkiin mahdollisiin asetusarvoihin, ja tämän avulla konfigurointi tapahtuu helposti ja nopeasti, mikäli anturille on fyysinen pääsy, ja kyseisen sovelluksen käyttäminen onkin eri asetusten tutkimiseen ja testaamiseen paras vaihtoehto.

LoRaWAN-verkon downlink-viestien avulla anturin asetuksiin taas voidaan tehdä muutoksia helposti myös silloin, kun anturiin ei päästä helposti fyysisesti käsiksi, ja erityisen kätevä downlink-viesti on, mikäli käytössä on esimerkiksi useita satoja antureita samanlaisissa käyttökohteissa ja kaikkiin halutaan tehdä jokin asetusmuutos.

Kyseisen anturin ollessa LoRaWAN A-luokan laite downlink-viestien lähetys sille on mahdollista vain välittömästi anturin lähettämän uplink-viestin jälkeen avautuvassa vastaanottoikkunassa, joten downlink-viesteillä tapahtuva konfigurointi on anturin lähetysvälistä riippuen kuitenkin huomattavan paljon hitaampaa kuin paikallisesti matkapuhelimella suoritettuna.

Downlink-viesteillä tapahtuvassa konfiguroinnissa halutut uudet asetusarvot on lähettävä anturille Elsysin downlink payload -kuvauksen mukaisesti heksadesimaalimuodossa käyttäen seuraavaa LoRaWANin Fportia anturin varsinaisesta, uplink-viesteille käyttämästä portista (Elsys 2019a).

Kyseisen payloadin generoimiseen tarvittavat arvot eri asetuksille voidaan lukea esimerkiksi ”Elsys sensor settings” -mobiilisovelluksesta määritellen siihen halutut asetusarvot ja käyttäen debug-toimintoa, joka näyttää kyseiset asetuk-

set ja niille konfiguroitavat arvot desimaalimuodossa. Lisäksi kyseisistä arvoista ja niiden mahdollisista määrittelyistä on saatavilla Elsysin julkaisema dokumentti ”Sensor settings parameters” (Elsys 2019b).

Näiden arvojen perusteella tarvittava payload voidaan yksinkertaisimmillaan generoida esimerkiksi Elsysin verkkosivuilta löytyvällä ”Downlink payload generator”:lla tai kehittää ”downlink payload” -kuvauksen mukaiset toiminnat Application Server -palvelimella käytettävään ohjelmistoon, millä downlink-viestien lähetystä hoidetaan, kuten toimittiin tämän opinnäytetyön yhteydessä.

Elsys ELT-2 -anturille määriteltäviä asetuksia aikaisemmassa kohdassa käsiteltyjen LoRaWAN-verkkoon liittymiseen tarvittavien avainten lisäksi ovat esimerkiksi

- Sensor sample times
    - Timebase
    - Temperature period
    - Humidity period
    - External period
    - External startup time
    - Trigger timeout
    - Accelerometer period
    - Battery period
    - Pressure period
    - Transmit period
- External configuration
- Advanced
    - PIR sensitivity
    - Datarate default
    - Datarate max
    - Datarate min
    - Port
- Version 2 features
    - Confirmed message
    - Sample queue size
    - Queue offset
    - Queue purge
    - Link Period
    - Link Threshold
    - Accelerometer configuration

Tässä tapauksessa anturille tullaan konfiguroimaan esimerkiksi Sensor sample times -asetukset, jotka liittyvät erilaisten mittaustietojen ”sämpläys” ja lähetysväleihin sekä ”External configuration”, joka liittyy anturin ulkoisten tulojen konfiguraatioon.

Myös mahdollisesti muita asetuksia tullaan määrittelemään anturille suoritettujen toimintakokeiden johdosta tehtyjen havaintojen perusteella. Lisäksi kyseisen anturin lukitseminen koodilla asetusmuutosten ehkäisemiseksi ilkivaltatarkoituksessa anturin sijaitessa ulkona on mahdollista sekä mobiilisovelluksen että downlink-viestien avulla, jota mahdollisesti tullaan myöskin hyödyntämään anturin asennustavasta riippuen.

7.4.2 Anturin toiminnan testaaminen

Elsys ELT-2 -anturille suoritettiin aluksi erilaisia kokeita anturin toiminnan tutkimiseksi ja testaamiseksi, jonka jälkeen alettiin optimoida anturin konfiguraatiota lopullista käyttökohdetta varten 1 kV katkaisijoilla.

Aluksi anturi sijoitettiin sisätiloihin ja lähetysvälinä käytettiin 10 minuuttia. Anturin lähettämää dataa tarkkailtiin sekä Actilityn Wireless Loggerissa että Application Serverin tietokannassa ja tutkittiin, kuinka luotettavasti paketit saapuvat perille LoRaWAN-verkkoon ja Application Serverille asti sekä miten esimerkiksi anturin sijoittelu sisätiloissa vaikuttaa verkon kuuluvuuteen ja signaaliarvoihin.

Lisäksi tarkasteltiin eri asetusarvojen vaikutuksia anturin toimintaan ja tehtiin esimerkiksi kokeita anturin käyttämän dataraten ja Acknowledged uplink -toiminnon vaikutuksista viestien perillemenon luotettavuuteen. Myös anturin ulkoisten tulojen käytettävissä olevia erilaisia moodeja tarkasteltiin ja kokeellisesti todennettiin niiden toimivuutta ja soveltuvuutta tähän käyttötarkoitukseen.

Samassa yhteydessä tarkasteltiin ja arvioitiin ”LoRaWAN_AppServer.py”-ohjelmiston ja tietokannan toimivuutta ja tehtiin tarvittaessa bugfixejä ja implementoitiin uusia ominaisuuksia, kuten esimerkiksi uusien, valmiiksi verkkoon provisioitujen antureiden automaattinen konfigurointi LoRaWANin downlink-viestejä käyttäen, jolloin asentajien ei tarvitse erikseen muokata antureiden asetuksia.

Kokeiden tulosten perusteella muodostettiin käsitys anturin ja LoRaWAN-verkon käyttäytymisestä, jonka pohjalta suunniteltiin anturille optimaalinen konfiguraatio 1 kV:n katkaisijoiden valvontasovellusta varten huomioiden esimerkiksi LoRaWAN-verkon ja anturin paristokapasiteetin asettamat rajoitteet pyrkien kuitenkin saavuttamaan mahdollisimman luotettava ja nopea indikaatio katkaisijan laukeamisesta.

Ennen koetulosten käsittelyä ja niiden perusteella vedettäviä johtopäätöksiä ja laitteen konfiguroinnin optimoimista, on kuitenkin perehdyttävä LoRaWANin käyttämään LoRa-radiotekniikkaan ja sen asettamiin rajoituksiin sekä konfiguroinnin optimoinnin periaatteisiin hieman tarkemmin.

7.4.3 LoRaWANin käyttämä tekniikka ja sen asettamat rajoitukset

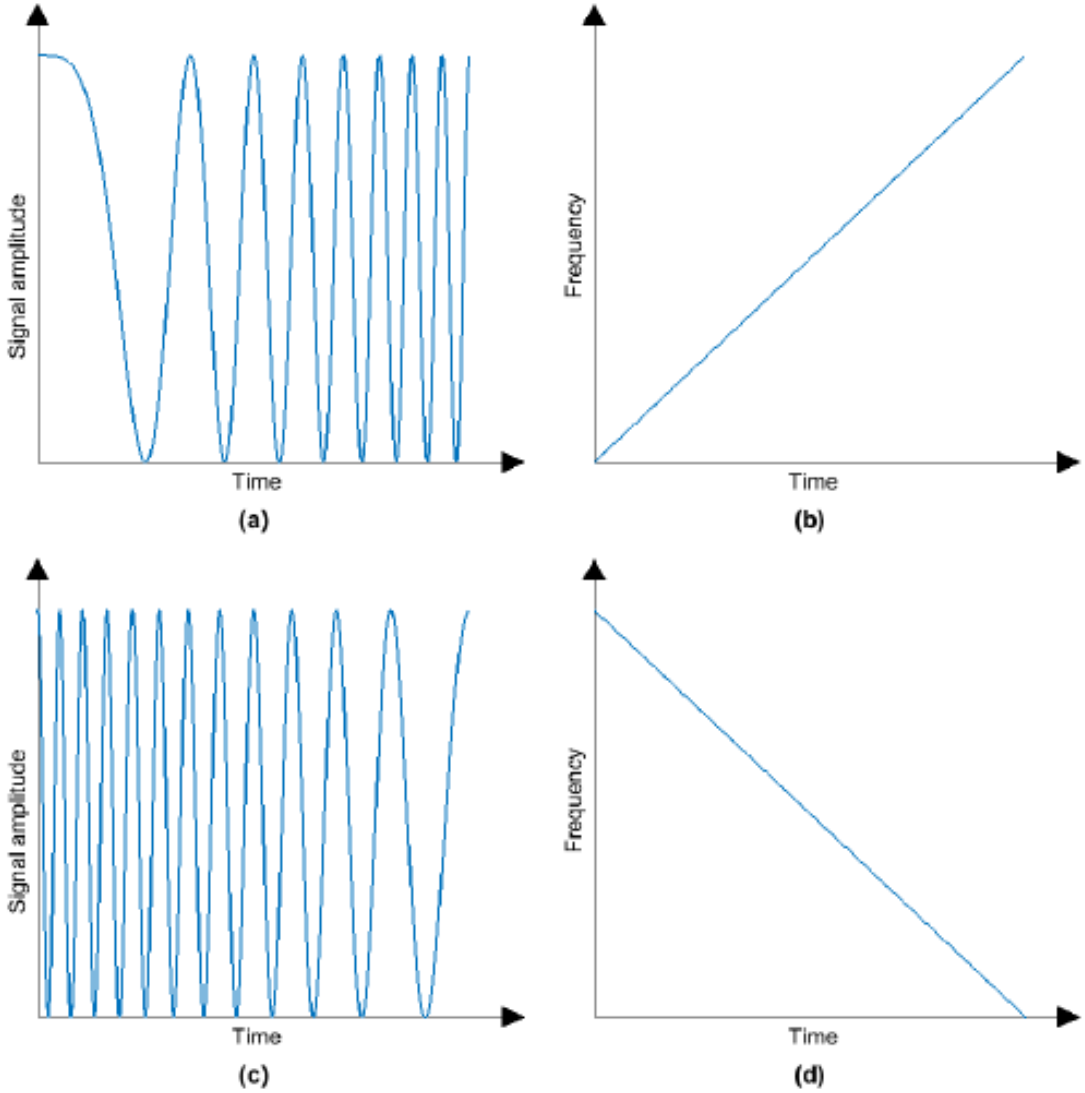
LoRaWAN-verkko toimii lisensoimattomalla taajuusalueella, joka määrittelee tukiasemille ja päätelaitteille erilaisia rajoituksia viranomaisten toimesta, jonka lisäksi myös laitteilla itsellään on ominaisuuksia, jotka tulee ottaa huomioon LoRaWAN-sovelluksia suunnitellessa verkon kapasiteetin ja laitteiden toiminnan optimoimiseksi.

LoRaWAN-verkko käyttää LoRa-radiotekniikkaa, joka on Chirp Spread Spectrum -modulaatiota hyödyntävä tekniikka. Kyseinen tekniikka on kehitetty 1940-luvulla ja sen jälkeen havaittu hyväksi esimerkiksi armeija- ja avaruustekniikan vaatimissa kommunikaatiosovelluksissa sen hyvän häiriönsiedon ja kantaman vuoksi. (Hakkenberg 2016, 14.)

Spread spectrum -modulaatiota käyttävässä järjestelmässä lähetettävä signaali levitetään huomattavasti suuremmalle kokonaistaajuusalueelle kuin sen sisältämän datan lähettämiseen minimissään tarvittaisiin. Tämän johdosta tekniikka on hyvin sekä erilaisia kapea- että laajakaistaisia ja muita radiohäiriöitä sietävä. Lisäksi tekniikan hyvinä puolina on myös esimerkiksi vähäinen radioiden energiantarve ja kyky demoduloida signaali myös sen ollessa kohinatason alapuolella. (Hakkenberg 2016, 14.)

Käytännössä signaalin ”levittäminen” (spreading) taajuudelle tapahtuu generoimalla signaali, jonka taajuus joko kasvaa tai laskee lineaarisesti ajan funktiona käytettyä kaistanleveyttä vastaavasti. Tästä muodostuu perusmuotoinen, joko nouseva tai laskeva chirp (Compressed High Intensity Radar Pulse). Nopeudesta, millä kyseistä signaalin taajuutta muutetaan, käytetään termiä Spreading Factor. (Hakkenberg 2016, 14–15.)

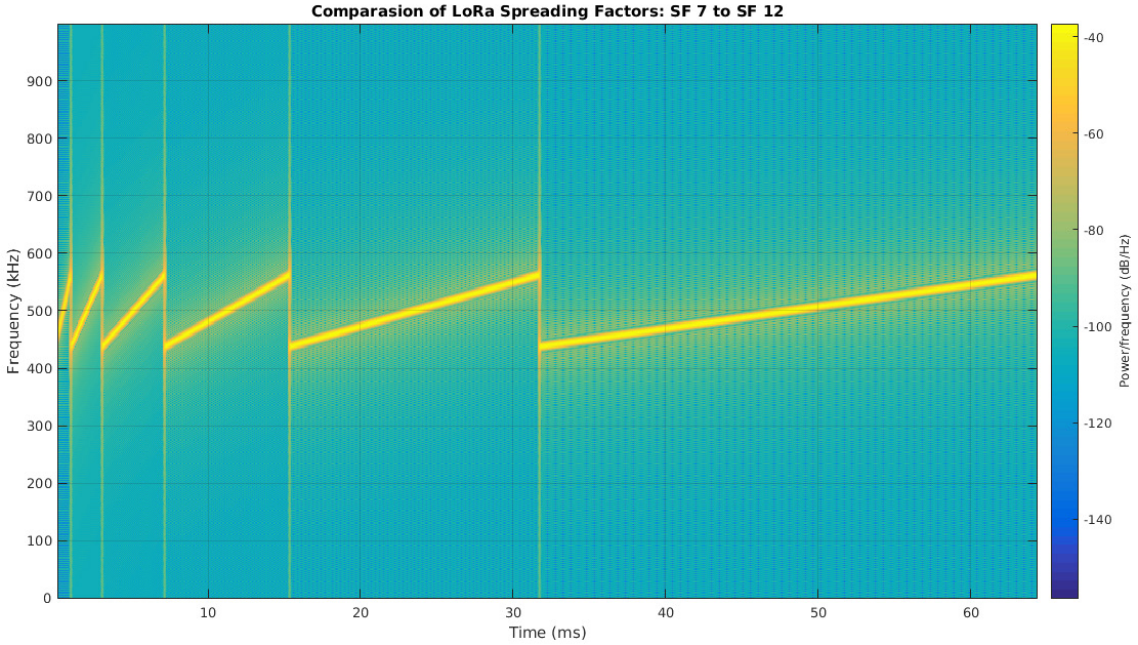
Perusmuotoista chirpiä havainnollistetaan sekä signaalin amplitudin että taajuuden osalta kuvassa 18.



Kuva 18. Havainnekuva LoRa-signaalin amplitudista ja taajuuden muuttumisesta ajan funktiona sekä nousevan että laskevan chirpin tapauksessa (Hakkenberg 2016, 15)

Spreading Factorin vaikutusta perusmuotoiseen, nousevaan chirpiin havainnollistetaan kuvassa 19. Tästä kuvasta voidaan erityisesti huomata, kuinka

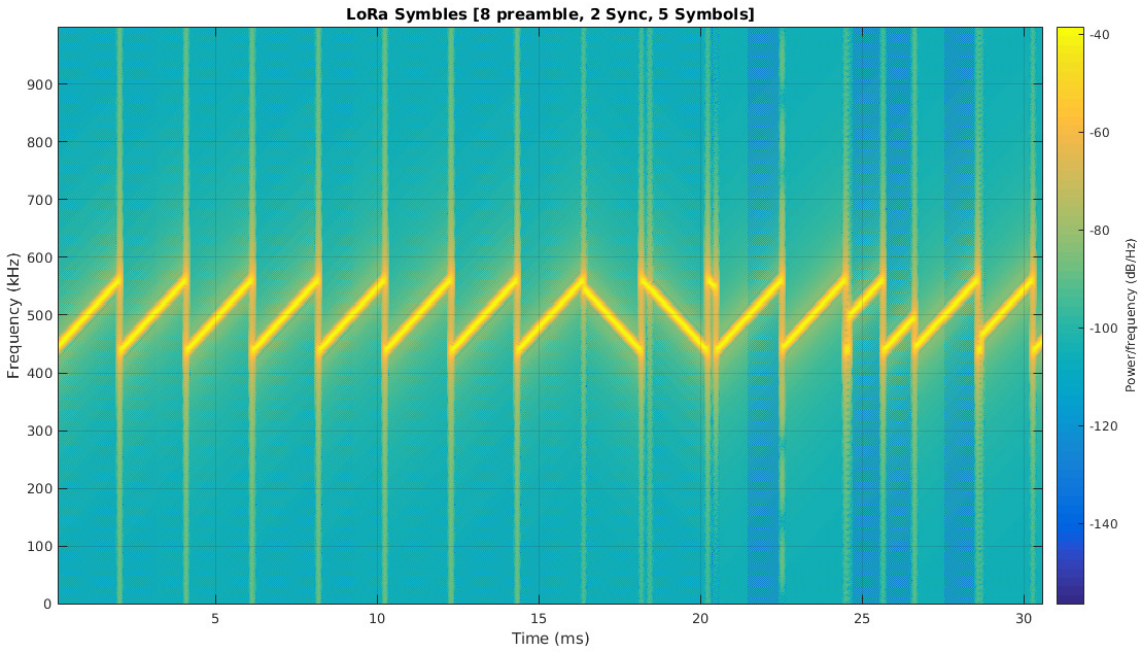
Spreading Factorin suurentaminen lisää yksittäisen chirpin lähetykseen kuluvaa aikaa.



Kuva 19. Perusmuotoinen, nouseva chirp esitettynä ajan ja signaalin taajuuden funktiona eri Spreading Factor -arvoja väliltä SF7–SF12 käyttäen (Ghoslya s.a.a)

Chirpin käyttämä kokonaiskaistanleveys on kuitenkin aina vakio, kuten myös kuvasta 19 voidaan havaita, ja kyseisenä arvona käytetään yleensä 125 kHz. Yksittäinen chirp-symboli, joka siis muodostuu kyseisestä signaalin taajuuden muutoksesta ajan funktiona, kykenee kuljettamaan 7–12 siihen enkoodattua bittiä SF-arvonsa mukaisesti. (Hakkenberg 2016, 15, 18.)

Yksinkertaistettuna tämä kyseinen datan modulointi chirp-symbolin sisään tapahtuu tekemällä perusmuotoiseen joko nousevaan tai laskevaan signaaliin nopeita taajuusmuutoksia kuitenkaan vaikuttamatta signaalin Spreading Factorin määrittelemään nousu- tai laskunopeuteen. Tätä havainnollistetaan kuvassa 20.



Kuva 20. Havainnekuva datan moduloinnista chirp-symboleihin. Ensin esitetään 8 nousevaa, perusmuotoista preamble chirpiä, sen jälkeen kaksi laskevaa synkronointia varten ja viisi moduloitua, varsinaisen datan sisältävää chirpiä (Ghoslya s.a.a)

Kasvatettaessa Spreading Factoria signaalin taajuutta muutetaan hitaammin, jolloin yhden chirpin lähetykseen tarvittava aika kasvaa, radioiden energiankulutus lisääntyy ja myös saavutettu tiedonsiirtonopeus alentuu (Hakkenberg 2016, 15).

Tiedonsiirtonopeuden alentuminen ja sitä myöten myös On the Air -ajan suurentuminen sekä energiankulutuksen lisääntyminen johtuvat yksittäisen chirpin lähettämiseen kuluvan ajan kasvamisesta huomattavasti nopeammin kuin sen kuljettamien bittien määrän Spreading Factoria kasvatettaessa.

Spreading Factorin noustessa yhdellä pykälällä kasvaa chirpin lähettämiseen kulunut aika kaksinkertaiseksi, mutta sen sisältämän datan määrä vain yhdellä bitillä. Esimerkiksi kahdessa SF7:lla lähetetyssä chirpissä pystytään siirtämään yhteensä 7 + 7 = 14 bittiä dataa, kun taas SF8:lla lähetetyssä chirpissä, jonka lähettäminen kestää yhteensä kahden SF7-chirpin ajan, vain 8 bittiä.

Tämän vuoksi LoRan Spreading Factor onkin kääntäen verrannollinen saavutettuun tiedonsiirron nopeuteen, eli datarateen, joka on eri Spreading Factorin ja kokonaiskaistanleveyden perusteella saavutetuille tiedonsiirtonopeuksille

standardisoitu arvo. Tiedonsiirtonopeutta voidaan lisäksi käsitellä myös suoraan esimerkiksi bitteinä sekunnissa. Eri datarate-arvoja vastaavia Spreading Factorin, kaistanleveyden, tiedonsiirtonopeuden ja suurimman mahdollisen lähetettävän payloadin arvoja Euroopassa käytetyllä taajuusalueella esitetään taulukossa 1.

Taulukko 1. Dataraten standardisoituja arvoja vastaavat LoRan Spreading Factorin ja kaistanleveyden arvot sekä tiedonsiirtonopeudet bit/s ja payloadin maksimikoot (Ghoslya s.a.c)

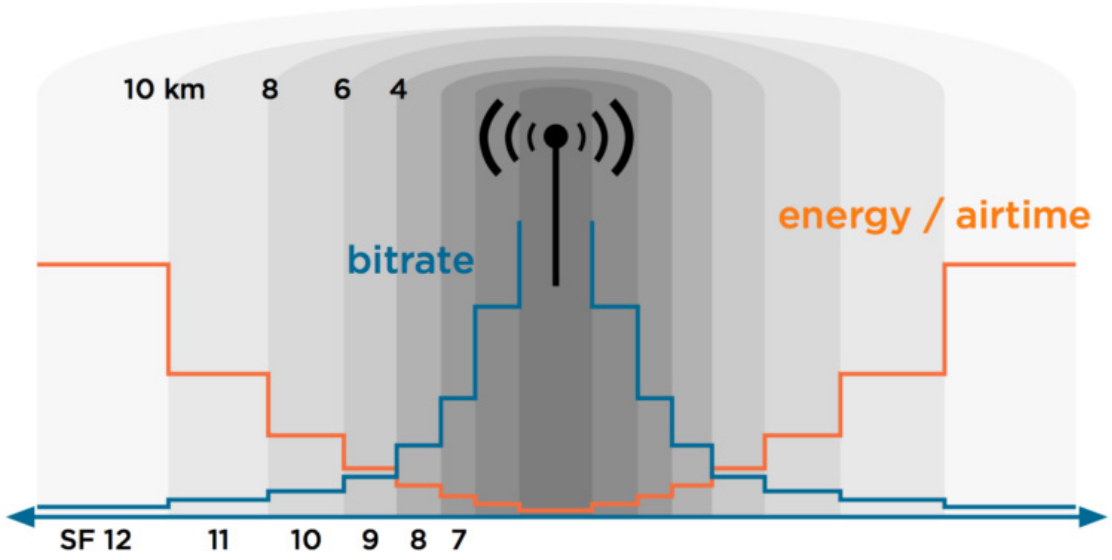
Data Rate	Configuration		Physical bit rate	Max. MAC Payload size	Max. Frame Payload Size
	Modulation	Bandwidth			
0	SF12	125kHz	250	59	51
1	SF11	125kHz	440	59	51
2	SF10	125kHz	980	59	51
3	SF09	125kHz	1760	123	115
4	SF08	125kHz	3125	230	222
5	SF07	125kHz	5470	230	222
6	SF07	250kHz	11000	230	222
7	FSK	50kbps	50000	230	222
8-15	RFU				

Kuitenkin suuremmalla Spreading Factorilla saavutetaan etuna signaalin pidempi kantama ja varmempi tiedonsiirto, koska taajuuden muutoksen tapahtuessa hitaammin signaali on saatavilla huomattavasti pidempään ja lisäksi siinä on tämän johdosta enemmän ”ylimääräistä” sisältöä, koska signaali kuljettaa lähestulkoon saman määrän dataa (Hakkenberg 2016, 15).

Taulukosta 1 voidaan lisäksi huomata, että datarate 6 käyttää LoRa-modulaatiota 125 kHz:n sijasta 250 kHz kaistanleveydellä ja datarate 7 LoRan sijasta FSK (Frequency-Shift Keying)-modulaatiota. Tästä voidaankin tehdä johtopäätös, että LoRaWAN-verkkoteknologia ei nimestään huolimatta tukeudu kokonaisuudessaan LoRa-radiotekniikkaan, vaikkakin sitä pääosin käytetään, eivätkä termit ole synonyymejä toisilleen.

Näitä kyseisiä kahta dataraten arvoa ja FSK-modulaatiota ei kuitenkaan käsitellä tässä kappaleessa sen tarkemmin, sillä pääosin LoRaWANissa käytetään nimenomaan LoRa-radiotekniikkaa 125 kHz:n kaistanleveydellä Euroopassa käytetyllä taajuusalueella.

Spreading Factorin, bitraten, radioiden energiankulutuksen, On the Air -ajan ja signaalin kantaman vaikutusta toisiinsa havainnollistetaan lisäksi kuvassa 21.



Kuva 21. LoRan Spreading Factorin vaikutus tiedonsiirron nopeuteen (bitrate/datarate), radioiden kuluttamaan energiaan ja signaalin kantamaan (Bassetti 2018, muokattu). Keskellä kuvaa oleva symboli esittää LoRaWAN-tukiasemaa ja X-akseli päätelaitteen etäisyyttä tukiasemasta.

Lisäksi käytetty datarate / Spreading Factor vaikuttaa yhdessä viestissä lähetettävän payloadin maksimikokoon, kuten taulukosta 1 voidaan havaita. Tämän johdosta suurten datamäärien lähettäminen alhaisella dataratella voi vaatia niiden jakamisen useampaan erilliseen viestiin.

Euroopassa käytetyllä SRD860 (Short Range Device)-taajuusalueella, joka käsittää taajuudet 863 ja 870 MHz:n välillä, on yleisesti ETSI:n (European Telecommunications Standards Institute) toimesta määriteltyjä rajoituksia laitteiden käyttämän maksimilähetystehon ja duty cyclen suhteen (Hakkenberg 2016, 16).

Pääsääntöisesti maksimilähetysteho tällä taajuusalueella on 14dBm ja maksimi duty cycle 0,1 %. Esimerkiksi 0,1 %:n duty cyclellä, yksittäinen laite ei voi lähettää samalla taajuudella enempää kuin 3,6 sekuntia tunnissa. Tämä rajoitus koskee kaikkia laitteita mukaan lukien LoRaWAN-tukiasemat, jotka lähettävät kyseisellä taajuudella.

Kyseisellä alueella on kuitenkin neljä alitaajuusaluetta, joilla on osittain huomattavasti sallivammat rajoitukset. Esimerkiksi band G3:lla maximum duty cycle on 10 % ja sallittu lähetysteho 27 dBm (Hakkenberg 2016, 16). Tätä havainnollistetaan taulukossa 2.

Taulukko 2. LoRaWANin käyttämällä taajuusalueella esiintyvät ETSI:n määrittelemät rajoitukset (Hakkenberg 2016, 16)

Band name	Range	Maximum transmission power (dBm)	Maximum duty cycle
G	863,0 – 870,0 MHz	25 mW EIRP (14 dBm)	0,1%
G1	868,0 – 868,6 MHz	25 mW EIRP (14 dBm)	1%
G2	868,7 – 869,2 MHz	25 mW EIRP (14 dBm)	0,1%
G3	869,4 – 869,65 MHz	500 mW EIRP (27 dBm)	10%
G4	869,7 – 870,0 MHz	25 mW EIRP (14 dBm)	1%

Kyseiset taajuusaluetta koskevat rajoitukset määrittelevät maksimaalisen lähetystiheyden laitteille, sillä ne eivät voi ylittää käytetylle taajuusalueelle määritettyjä rajoituksia, vaan duty cyclen määrittelemän rajan tullessa vastaan laitteen on odotettava ennen seuraavan viestin lähettämistä (Hakkenberg 2016, 16).

Laitteet voivat kuitenkin lähettää alitaajuusalueita vaihdellen, jolloin toisen taajuusalueen ollessa rajoitettu pois käytöstä duty cycle -rajoitusten vuoksi lähetys kuitenkin onnistuu käyttäen toista aluetta ja lähetystiheyttä voidaan huomattavasti kasvattaa, mikäli laite kykenee käyttämään useita eri taajuuksia (Hakkenberg 2016, 16).

Kuten aiemmin todettiin, tietyn datamäärän lähetyksen kestoaikaan ja sitä myöten laitteen käyttämään duty cycleen sekä sen radioiden virrankulutukseen vaikuttaa suoraan laitteen käyttämä LoRan SF eli Spreading Factor -arvo, joka taas vaikuttaa päinvastaisesti signaalin kantamaan ja tiedonsiirron luotettavuuteen.

Tämän vuoksi LoRaWAN-laitteiden paristonkesto on suoraan riippuvainen etäisyydestä tukiasemaan, sillä suuremmalla etäisyydellä on pakko käyttää suurempaa Spreading Factoria tiedonsiirron onnistumiseksi, jolloin jokaisen

lähetyksen yhteydessä laitteen radio on aktiivisempi pidempään mikä taas johtaa suurempaan paristonkulutukseen.

Duty cycle -rajoitukset eivät useampien alitaajuusalueiden käyttämisen vuoksi aiheuta kovin helposti ongelmia yksittäiselle LoRaWAN-laitteelle, joka lähettää uplink-paketteja tukiasemalle erityisesti, mikäli kyseinen laite on paristokäyttöinen, sillä suuri On the Air -aika lyhentäisi paristonkestoa merkittävästi.

LoRa-teknologiassa kuitenkaan tukiasemat eivät pysty erottelemaan samalla taajuudella, kokonaiskaistanleveydellä ja Spreading Factor -arvolla samanaikaisesti eri laitteiden lähettämiä paketteja, milloin tapahtuu päällekkäisyyksiä jotka johtavat usein vähintään toisen paketin häviämiseen. Erityisesti, mikäli alueella on suuri määrä LoRaWAN-laitteita, suuren Spreading Factorin käytön aiheuttama laitteiden On the Air -ajan lisääntyminen voi merkittävästi vaikuttaa törmäyksistä johtuvaan pakettien häviämiseen. (Hakkenberg 2016, 74–75.)

Duty cycle -rajoitukset koskettavatkin voimakkaimmin tukiasemia, joiden palvelemana on suuria määriä erillisiä laitteita, joille pitäisi lähettää jatkuvasti viestejä. Downlink-viestejä tukiasemalta laitteille aiheuttaa esimerkiksi laitteiden mahdollisesti pyytämät varmistusviestit uplink-pakettien perillemenosta.

A-luokan laitteilla, joille downlink-viestejä voidaan lähettää vain heti uplink-viestien jälkeen, on kaksi vastaanottoikkunaa, joista ensimmäinen käyttää samaa kanavaa ja dataratea kuin uplink-viesti, ja sen lisäksi toinen, joka käyttää yleensä kiinteää, hitainta mahdollista dataratea ja G3-taajuusalueelle sattuvaa taajuutta, joka on duty cycle- ja lähetystehorajoitusten vuoksi paras mahdollinen valinta downlink-viestien lähettämiseen (Hakkenberg 2016, 20).

Tukiasema, joka käyttää molempia ikkunoita downlink-viestien lähettämiseen, pystyy duty cycle -rajoitusten vuoksi huonoimmassa tapauksessa, jossa kaikki viestit lähetetään Spreading Factorin arvoa SF12 käyttäen, lähettämään laitteille vain 311 ”Acknowledged” downlink -pakettia tunnissa ja parhaimmassakin vain 1184 kappaletta (Hakkenberg 2016, 36–37).

Mikäli downlink-paketit sisältävät payloadin, niiden koko on suurempi, jolloin myös lähetys kestää pidempään, mikä vähentää määriä entisestään.

Lisäksi ainakin osa LoRaWAN-tukiasemista käyttää half-duplex-radioita, mikä tarkoittaa, etteivät ne pysty kuuntelemaan saapuvia paketteja samanaikaisesti kuin ne lähettävät viestejä, kuten esimerkiksi Acknowledgement-paketteja laitteille (Hakkenberg 2016, 78).

Suuri määrä downlink-liikennettä suurentaa siten myös uplink-pakettien häviämisen riskiä erityisesti tilanteissa, joissa LoRaWAN-laitteita on paljon ja niiden lähettämät paketit tavoittavat vain yhden tukiaseman.

Näiden tekniikan rajoitusten vuoksi olisikin verkon kapasiteetin maksimoimiseksi ja myös anturin paristonkeston optimoimiseksi antureilla pyrittävä käyttämään mahdollisimman suurta dataratea eli alhaista Spreading Factoria, jolloin anturin datan lähetys tapahtuu mahdollisimman nopeasti ja lisäksi pyrittävä myös pitämään downlink-pakettien määrä alhaisena, jotta tukiasemat eivät ruuhkautuisi liikaa, erityisesti jos alueella on paljon LoRaWAN-laitteita.

LoRaWANissa on lisäksi käytössä Adaptive Data Rate -ominaisuus, mitä käytettäessä verkkoalusta pystyy lähettämään päätelaitteille downlink-paketeissa määrittelyjä esimerkiksi tarvittavasta lähetystehosta ja käytettävästä Spreading Factorista. Tällöin päätelaitteen paristonkesto ja verkon suorituskyky saadaan optimoitua automaattisesti signaaliolosuhteiden mukaisesti. (Hakkenberg 2016, 19.)

Adaptive Data Rate on päätelaitteessa konfiguroitava ominaisuus, jota laite voi pyytää verkolta. Tällöin päätelaite lähettää uplink-viestissä bitin, jossa se pyytää verkkoa tarvittaessa pyytämään suurempaa dataratea, eli pienempää Spreading Factoria ja määrittelemään käytettävän lähetystehon. Lisäksi verkko määrittelee myös esimerkiksi uplink-viestien lähetyskertojen määrän ja lähetykseen käytettävät taajuudet (kanavat). (Ghoslya s.a.b.)

Päätelaite lisäksi lähettää aika-ajoin verkolle viestin, johon verkon tulee vastata downlink-viestillä tietyssä aikaikkunassa tarkistaakseen, saavuttaako uplink-viestit tukiasemaa. Tarvittaessa päätelaite itse nostaa Spreading Factoria asteittain, mikäli verkko ei vastaa ja viestit katsotaan hävinneiksi, verkko ei koskaan pyydä Spreading Factorin nostoa. (Ghoslya s.a.b.)

Näiden ominaisuuksien perusteella ADR-toimintoa käyttäen saavutetaan suurimmassa osassa tapauksista optimaalisin konfiguraatio kyseisten parametrien suhteen, erityisesti mikäli laitteet ovat kiinteästi asennettuja. Liikuteltavien laitteiden kanssa ADR ei kuitenkaan välttämättä kerkeä säätämään lähetystehoa ja Spreading Factoria yhtä nopeasti kuin olisi tarpeellista lähetysvälistä riippuen, ja tämä voi johtaa suurempaan pakettien häviämiseen.

Kuitenkin joissain tapauksissa, kuten esimerkiksi erittäin suuren laitemäärän sijaitessa lähellä tukiasemaa, voi sen käyttö kaikilla päätelaitteilla johtaa aiemmin käsiteltyjen samalla taajuudella ja Spreading Factorilla lähetettyjen pakettien törmäyksien johdosta heikompaan lopputulokseen (Bassetti 2018).

Kyseistä ongelmaa voidaan rajoittaa esimerkiksi konfiguroimalla manuaalisesti osalle päätelaitteista kiinteä, alhaisinta mahdollista korkeampi Spreading Factor, millä voidaan mahdollisesti vähentää pakettien häviämistä, vaikka osalla laitteista On the Air -aika kasvaisikin.

Lisäksi kyseiseen ongelmaan vastaamiseen on kehitetty uudenlaisia algoritmejä, joiden avulla verkko pystyy automaattisesti optimoimaan päätelaitteiden konfiguraatiota myös tällaisissa tapauksissa (Bassetti 2018).

7.4.4 Kokeiden tulokset ja laitekonfiguraation optimointi

Ensimmäisten kokeiden tulosten perusteella havaittiin anturin käyttäessä automaattista SF/dataratea oletusasetuksilla LoRaWANin ADR-toimintoa hyödyntäen pakettien ajoittaista häviämistä ja jopa useamman tunnin mittaisia jaksoja, jolloin paketit eivät saapuneet lainkaan perille.

Anturin sijaitessa sisätiloissa havaittiin myös anturin sijoittelulla olevan vaikutusta Packet Error Rateen (prosentuaalinen arvo pakettien välityksen epäonnistumisesta), vaikka LoRaWAN-verkon kuuluvuus pysyi koko ajan SF7:n mahdollistamalla tasolla.

Näiden havaintojen jälkeen toteutettiin koe pakottaen anturi käyttämään hitaampaa kuin suurinta mahdollista dataratea ja tarkasteltiin pakettien mahdollista häviämistä tässä tapauksessa. Tuloksissa havaittiin parannusta, esimerkiksi useamman tunnin mittaisia katkoja pakettien saapumisessa ei enää esiintynyt, mutta siitä huolimatta todettiin yksittäisten pakettien ajoittain katoavan.

Valvottaessa 1 kV katkaisijan tilaa tieto katkaisijan laukeamisesta olisi saatava mahdollisimman nopeasti, koska tällöin kyseisen katkaisijan takana olevan verkon syöttämiltä asiakkailta on sähkönjakelu keskeytynyt. Tämän vuoksi todettiin, että tässä sovelluksessa tämänkaltainen pakettien katoamisen riski on kriittinen.

Elsys ELT-2 -anturissa on käytettävissä Acknowledge-toiminto, jota käytettäessä anturi lähettää kaikki uplink-viestit pyytäen LoRaWAN-verkolta varmistusviestin siitä, että anturin lähettämä viesti on vastaanotettu, ja tarvittaessa lähettää viestit uudelleen, mikäli paketti sattuu katoamaan matkalla.

Kuten aikaisemmin todettiin, LoRaWAN-verkon rajoitteista johtuen suuri määrä downlink-liikennettä ruuhkauttaa verkkoa tukiasemien ominaisuuksista ja viranomaismääräyksistä johtuen, minkä vuoksi esimerkiksi Ack-toiminnolla lähetettyjen uplink-viestien määrä tulisi kuitenkin pitää suhteellisen alhaisena, koska tukiaseman on lähetettävä tällöin jatkuvasti downlink-viestejä anturille.

Tässä tapauksessa anturin konfiguraatiossa kuitenkin voitaisiin pyrkiä mahdollisimman vähäiseen viestien määrään, mikäli niiden perillemeno olisi varmistettua, jolloin se ei aiheuttaisi liikaa downlink-viestejä. Acknowledged uplink -toimintoa käyttäen suoritettiin myös muutaman vuorokauden mittainen koe, jonka aikana todettiin kaikkien lähetettyjen pakettien saapuneen perille, eli toiminnon todettiin toimivan kuten pitääkin.

Anturin ulkoisten tulojen erilaisista konfiguraatiovaihtoehdoista tähän tarkoitukseen sopivimmaksi havaittiin ”Switch NO” sekä ”Switch NO dual edge trigg”. Näillä kyseisillä konfiguraatioilla ”Switch NO” -valintaa käyttäen ulkoisen kärkitiedon sulkeutuminen ja ”dual edge trigg” -valintaa käyttäen sekä kärkitiedon

sulkeutuminen, että avautuminen aiheuttavat välittömän LoRaWAN-viestin lähetyksen anturin varsinaisesta lähetysvälistä riippumatta.

Kyseisellä konfiguraatiolla kytkettäessä anturi katkaisijan lauetessa sulkeutuvalle apukoskettimelle se lähettää välittömästi LoRaWAN-viestin tapahtuneesta, jolloin digitaalitulon muuttunut tila saadaan välittömästi Application Serverille. Lisäksi ”dual edge trigg” -toiminnolla saadaan välitön viesti myös katkaisijan palauttamisesta ja vian poistumisesta.

Käytettäessä normaalia, varmistamatonta lähetystä ei kyseisten triggeröityjen viestien perillemeno ole kuitenkaan varmaa, joten tämän lisäksi anturi tulisi konfiguroida käyttämään tiheintä mahdollista lähetysväliä paristonkesto huomioiden, jotta mahdollisesti paketin kadotessa hälytys katkaisijan laukeamisesta saataisiin siitä huolimatta mahdollisimman nopeasti.

Anturin paristonkestoa erilaisia konfiguraatioita käyttäen arvioitiin alustavasti teoreettisella tasolla laitevalmistajan verkkosivuilta löytyvää ”Battery life calculator” -laskuria hyödyntäen.

Alustavien tulosten mukaisesti, heikoimmalla mahdollisella, eli SF12 Spreading Factorin vaativalla kuuluvuusalueella olisi ollut mahdollista lähettää maksimissaan yksi viesti tunnissa. Parhaimmalla kuuluvuusalueella, SF7:llä, olisi kuitenkin mahdollista paristonkesto huomioiden lähettää viesti esimerkiksi 5 minuutin välein.

Käytännön olosuhteissa SF7-tasolle ei tulla kaikilla katkaisija-asemilla kuitenkaan mitenkään pääsemään, ja ratkaisun olisi syytä soveltua parhaalla mahdollisella tavalla kaikille katkaisijoille, joten kyseistä konfiguraatiota ei katsottu optimaalisimmaksi mahdolliseksi, sillä se olisi vaatinut asetusten määrittelyn antureille erikseen käyttöpaikkakohtaisesti ja asettanut LoRaWAN-verkon kuuluvuudesta riippuen asiakkaat eriarvoiseen asemaan keskeytysaikojen suhteen mahdollisen triggerpaketin hävitessä.

Lisäksi valvontaratkaisu katsottiin mahdollisesti hyödyttömäksi, mikäli on riski esimerkiksi useamman tunnin viiveeseen ennen hälytystiedon saamista use-

amman paketin hävitessä peräkkäin, sillä asiakkaat kerkeäisivät todennäköisesti soittamaan kyseisessä ajassa siirtoyhtiön päivystykseen ja päivystäjä voisi päätellä katkaisijan lauenneen näiden vikailmoitusten perusteella.

Tämän johdosta päädyttiin harkitsemaan Acknowledged uplink -toiminnon käyttöä, jolloin triggeröityjen viestien perillemeno olisi varmaa, ja anturin säännöllinen lähetysväli voitaisiin määritellä huomattavasti harvemmaksi kuin missään tilanteessa käytettäessä normaalia, varmistamatonta lähetystä.

Asian suhteen konsultoitiin myös verkko-operaattori Digitaa, ja tultiin siihen tulokseen, että Acknowledged uplink olisi tähän tarkoitukseen soveltuva konfiguraatio. Anturille päädyttiin myös määrittelemään mahdollisimman harva säännöllinen lähetysväli, jollaiseksi kaavailtiin alustavasti maksimissaan yhtä viestiä vuorokaudessa.

Vaikka varsinaiset tapahtumat aiheuttaisivatkin välittömän lähetyksen, on anturin silti syytä lähettää viestejä säännöllisesti, jotta voidaan varmistua anturin toimivuudesta sekä tarvittaessa tehdä siihen asetusmuutoksia downlink-viestejä käyttämällä, koska downlink-viestien lähetys anturille on mahdollista vain uplink-viestien jälkeisen vastaanottoikkunan aikana.

Käytettäessä tämänkaltaista harvaa lähetysväliä LoRaWAN-verkon tukiasemien kuormitus olisi myös downlink-viestien osalta todennäköisesti jopa alhaisempaa Ack-toiminnosta huolimatta kuin esimerkiksi 15 minuutin välein normaalin, varmistamattoman uplink-viestin lähettävän laitteen osalta.

Tämä johtuu LoRaWANin ADR-ominaisuuden lähettämien MAC-pakettien (Medium Access Control) määrästä, jonka käytännön kokeissa havaittiin tiheästi uplink-viestejä lähettävälle laitteelle olevan käytännössä suurempi kuin kerran vuorokaudessa varmistetun paketin lähettävälle laitteelle.

Elsysin ”Battery life calculator”:n mukaisesti tämänkaltaisella konfiguraatiolla myöskään paristonkestossa ei tulisi minkäänlaisia ongelmia edes huonoimmalla mahdollisella, Spreading Factor -arvon SF12 vaatimalla kuuluvuusalueella 6 vuoden paristonvaihtoväliä ajatellen.

Laskurin mukaisesti kerran vuorokaudessa lähetetyillä viesteillä teoreettinen paristonkesto olisi SF12:ta käyttäen jopa 26,9 vuotta, mikäli Elsys ELT-2:n sisäisiä antureita ei käytettäisi.

Ack-toiminnon aiheuttamasta paristonkulutuksen lisääntymisestä ei kuitenkaan ollut varmuutta, joten pariston riittävän käyttöiän varmistamiseksi päätettiin vielä suorittaa käytännön kokeita ja valita lopullinen käytettävä konfiguraatio näiden kokeiden tulosten perusteella.

7.4.5 Anturin paristonkulutuksen kokeellinen tarkastelu

Anturin todellista paristonkulutusta arvioitiin lisäksi suorittamalla käytännön kokeita mitaten kyseisen anturin virrankulutusta erilaisten käyttötilanteiden aikana Fluke 289 -yleismittarilla.

Käytännön kokeiden tarkoituksena oli varmistaa, vastaavatko valmistajan ilmoittamat anturin virrankulutuksen arvot todellisuutta, ja tutkia, vaikuttaako esimerkiksi varmistetun lähetyksen käyttö anturin virrankulutukseen.

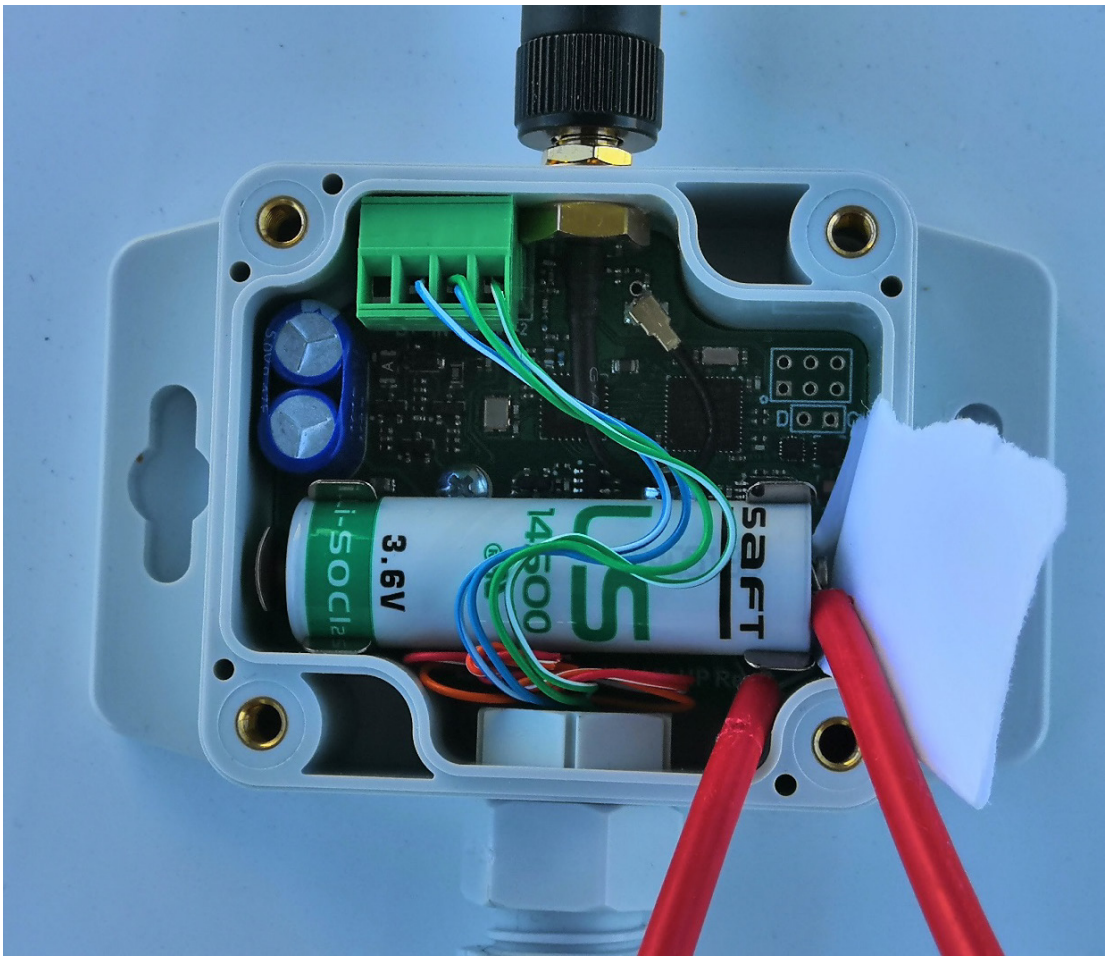
Anturin virrankulutuksen tarkastelemiseksi toteutettiin kokeet sekä Ack-lähetystä että normaalia varmistamatonta lähetystä käyttäen, jossa mitattiin 10 paketin lähetykseen 5 minuutin lähetysvälillä kulunut energia sekä Spreading Factorin SF8- että SF12-arvoja käyttäen.

Virran mittaus toteutettiin kytkemällä Fluke 289 -yleismittari Elsys ELT-2 -anturin pariston +-navan ja itse anturin vastekappaleen väliin. Fluke 289 -mittariin päädyttiin, koska sellainen löytyi XAMK:n laboratoriosta sekä mittarin ominaisuudet olivat käyttötarkoitukseen soveltuvat.

Muita mahdollisuuksia mittauksen toteuttamiseen olisi ollut esimerkiksi oskilloskoopin käyttäminen sopivalla current probella varustettuna tai mittaamalla jännitettä soveltuvan shunttivastuksen ylitse.

Kytkemiseen käytettiin joustavia koukkumittapäitä, joilla havaittiin saatavan hyvä kontakti sekä paristoon että vastekappaleeseen, joiden väliin asetettiin

pala kopiopaperia suoran kontaktin eristämiseksi, jotta pariston virtapiirissä kulkeva virta kulkisi mittarin kautta. Kytkentää esitetään kuvassa 22.



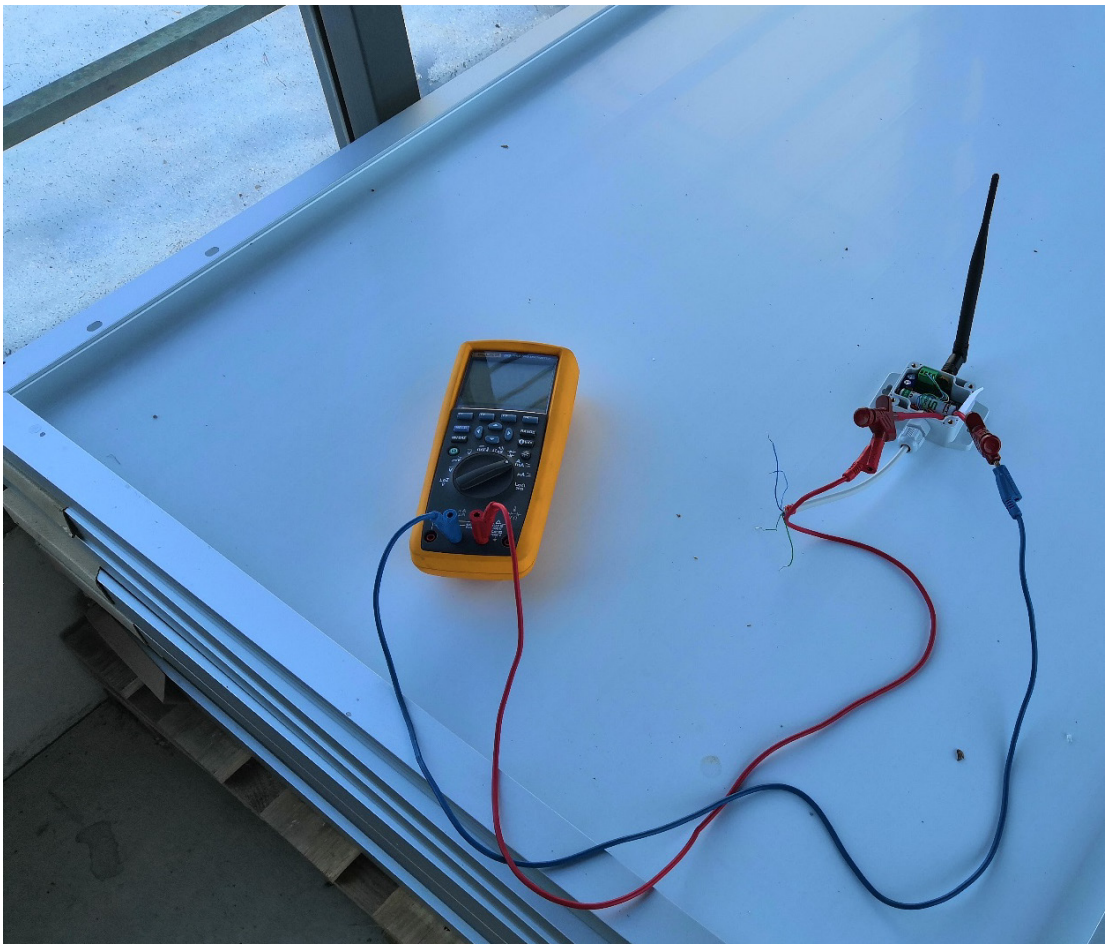
Kuva 22. Fluke 289 -mittarin kytkentä ELT-2-anturin virtapiiriin

Mittarissa käytettiin peak record -ominaisuutta, jolloin tämän kyseisen mittarin vasteaika on 250 µs, ja mittaus pidettiin käynnissä anturin uudelleenkäynnistyksen jälkeen lähettämän ensimmäisen paketin saapumisen jälkeen siihen asti, kunnes mittauksen aikana oli vastaanotettu kaikkiaan 10 pakettia.

Tilannetta tarkkailtiin mittausten aikana tietokoneelta Application Server -palvelimen tietokantaa ja Actility ThingPark Wireless Loggeria hyödyntäen.

Mittaus oli alun perin tarkoitus suorittaa XAMK:n sähkölaboratoriossa, jossa havaittiin kuitenkin mittausajankohtana ongelmia LoRaWAN-verkon kuuluvuudessa, ja anturi ei saanut lainkaan yhteyttä verkkoon. Sähkölaboratorio sijaitsi osittain maan alaisessa kellarikerroksessa, joka osaltaan saattoi vaikuttaa ongelmien syntyyn.

Tämän vuoksi mittaus päädyttiin suorittamaan kampuksen A-rakennuksen katolla, jossa havaittiin olevan riittävä verkon kuuluvuus kaikkien tarvittavien mittausten toteuttamiseksi. Lisäksi kyseisen rakennuksen katto on tasainen ja siellä on katettu käytävätila, joten mittausta ei tarvinnut suorittaa kuitenkaan ulkoilmassa eikä siitä aiheutunut katolta putoamisen riskiä. Kuva 23 esittää mittausjärjestelyjä kokeiden aikana.



Kuva 23. ELT-2-anturin paristonkulutuksen mittausjärjestelyt

Aluksi anturi bootattiin ”Elsys sensor settings” -mobiilisovellusta hyödyntäen, minkä jälkeen odotettiin sen käynnistymistä ja verkkoon liittymistä, minkä jälkeen odotettiin vielä hetki paristosta otettavan virran tasaantumista.

Anturin havaittiin oletusasetuksilla käyttävän mittaustilanteessa pääosin Spreading Factorin arvoa SF8, jonka katsottiin olevan suhteellisen hyvin käytännön olosuhteita LoRaWAN-verkon hyvän kuuluvuuden alueella vastaava, joten anturin asetuksiin ei tehty tämän osalta tässä vaiheessa muutoksia.

Heikomman verkon kuuluvuuden simuloimiseksi anturin asetuksista se pakotettiin käyttämään kaikista hitainta mahdollista dataratea, joka pakotti myös Spreading Factorin arvoon SF12. Kokeiden aikana lisäksi lähistön eräässä LoRaWAN-verkon tukiasemassa esiintyi ongelmia, mikä mahdollisti käytetyillä koejärjestelyillä myös erittäin heikkoa kuuluvuusaluetta vastaavat kokeet anturin paikkaa juurikaan muuttamatta.

Erityisesti SF12 Ack -kokeen aikana havaittiin LoRaWAN-verkon kuuluvuuden olevan toimivuuden rajoilla, sillä pakettien saapumisessa esiintyi viiveitä ja varmistusviestejä lähti anturille runsaita määriä. Tämä on käytännön toteutuksen kannalta kaikista hankalin tilanne paristonkulutuksen suhteen, joten on tärkeää, että pariston kesto saadaan varmistettua myös tässä tapauksessa.

Lisäksi mitattiin erikseen anturin lepotilassa kuluttama virta ajoittain varsinaisten kokeiden välillä, jotta lähetyksiin kulunut energia saatiin laskettua. Anturin sisäisten kondensaattoreiden hitaan latautumisen vuoksi todellisen kokonaisvirrankulutuksen laskemiseksi olisi jouduttu tekemään useiden vuorokausien mittainen koe, jonka tekeminen tässä vaiheessa katsottiin kuitenkin vielä tarpeettomaksi. Mittaustulokset esitetään taulukossa 3.

Taulukko 3. ELT-2-anturin virrankulutusmittausten tulokset. *LoRaWAN-verkon kuuluvuus toimivuuden rajoilla

Konfiguraatio	Koeaika	Paketteja	Virta (AVG)	Lepovirta
SF8, no Ack	0:46:53,8	10kpl	0,06mA	0,021mA
SF8, Ack	0:48:42,4	10kpl	0,06mA	0,021mA
SF12, no Ack	0:50:56,4	10kpl	0,37mA	0,023mA
SF12, Ack*	1:36:08,5	10kpl	1,37mA	0,023mA

Mittaustuloksista tarkasteltiin mittausjakson keskimääräistä anturin käyttämää virtaa, josta vähennettiin erikseen mittausjakson jälkeen mitattu lepotilassa kulunut virta, jonka jälkeen oletettiin lopun energian kuluneen radioiden ja sisäisten anturien käyttöön.

Tämän jälkeen laskettiin yhden paketin lähetykseen kulunut energia, jota verrattiin valmistajan ilmoittamaan arvoon. Anturi lähetti mittausarvoina molem-

pien digitaalitulojen arvot sekä sisäisen lämpötilan, kosteuden ja akkujännitteen, joten Elsysin verkkosivuilla ollut laskuri konfiguroitiin todellista koetta vastaavasti.

Ack-toiminnon aiheuttamasta lisäkulutuksesta ei ole mahdollista tehdä arviota valmistajan laskuria käyttäen, koska mahdollisten uudelleenlähetysten määrää ei voida ennustaa, joten tässä tapauksessa alustavasti verrattiin vain ilman Ack:ta tehtyjä kokeita valmistajan laskurista saatuihin tuloksiin.

Tulokset mitatuista arvoista pakettia kohden kuluvasta energiasta sekä valmistajan laskurista saaduista arvoista esitetään taulukossa 4.

Taulukko 4. ELT-2-anturin virrankulutusmittausten tulokset. *LoRaWAN-verkon kuuluvuus toimivuuden rajoilla

Konfiguraatio	µAh/paketti	Valmistajan laskuri	Erotus
SF8, no Ack	3,05 µAh	2,4 µAh	+0,65 µAh, 27%
SF8, Ack	3,17 µAh	Not available	
SF12, no Ack	29,46 µAh	28 µAh	+1,46 µAh, 5,2%
SF12, Ack*	215,84 µAh	Not available	

Taulukossa 5 on lisäksi laskettu mitattujen arvojen perusteella lähettämiseen kuluva pariston energia vuorokaudessa käytettäessä eripituisia lähetysvälejä.

Taulukko 5. ELT-2-anturin lähetyksiin käyttämä pariston energia vuorokaudessa. *LoRaWAN-verkon kuuluvuus toimivuuden rajoilla

Lähetysväli	48h	24h	12h	2h
SF8, no Ack	1,03 µAh	3,05 µAh	6,10 µAh	36,60 µAh
SF8, Ack	1,59 µAh	3,17 µAh	6,34 µAh	38,04 µAh
SF12, no Ack	14,73 µAh	29,46 µAh	58,92 µAh	353,52 µAh
SF12, Ack*	107,92 µAh	215,84 µAh	431,68 µAh	2590,08 µAh

Lähetysten kuluttaman virran lisäksi ELT-2-anturissa kuluu virtaa lepotilassa sekä esimerkiksi tässä sovelluksessa mahdollisten siihen kytkettyjen ulkoisten kytkintietojen ollessa kiinni-asennossa, jolloin digitaalitulon pull-up -vastuksen kautta piirissä kulkee tietynsuuruinen virta.

Pull-up -vastuksen kautta laskennallisesti kulkevaksi virraksi saatiin 72 µA ja mitatuksi virraksi 76,31 µA. Mitattu suurempi virta on mahdollisesti johtunut mittarin tarkkuudesta, laitteen pull-up -vastuksen arvon tarkkuudesta ja paristo n hieman nimellistä suuremmasta jännitteestä.

Mittaustulosten analysoinnin perusteella todettiin, että lähetyksien aiheuttama virrankulutus on absoluuttisesti suhteellisen lähellä valmistajan ilmoittamaa, mutta prosentuaalisesti erityisesti ensimmäisessä SF8-kokeessa esiintyy suuri poikkeama.

Tämän arveltiin johtuvan mahdollisesti laitteen kondensaattorien latautumisen aiheuttamasta virrankulutuksesta, koska kyseessä oli ensimmäinen koe mittarin kytkemisen jälkeen, ja lepovirrankulutus mitattiin ensimmäisen kerran vasta molempien SF8-kokeiden jälkeen.

Tarkoituksena ei muutenkaan tässä kokeessa ollut määrittää absoluuttisen tarkkaa anturin virrankulutusta, sillä tarvittavaan mittaustarkkuuteen pääseminen olisi ollut haastavaa, vaan lähinnä tutkia Ack-toiminnon vaikutusta paristonkulutukseen ja verrata saatuja tuloksia valmistajan ilmoittamiin arvoihin.

Tämän vuoksi SF12-kokeen tuloksia voidaan erotuksen valmistajan arvoihin nähden osalta pitää luotettavampana kuin SF8-kokeen. Lisäksi SF12 Ack -kokeessa havaitaan selvästi, kuinka anturin sijainti erityisesti varmistettuja viestejä käytettäessä heikosti kuuluvan LoRaWAN-verkon alueella lisää pariston kulutusta.

SF8-kokeissa ei Ack:n käytöllä havaita yhtä merkittävää eroa, sillä verkon kuuluvuus oli hyvä eikä pakettien uudelleenlähetyksiä juurikaan tarvittu kuten SF12 Ack -kokeessa.

Tämä voidaan havaita myös kokeiden kestoajasta, 10 paketin lähettäminen kesti SF12 Ack:lla noin 48 minuuttia kauemmin kuin ilman sitä, kun taas SF8-kokeessa vaikutus oli alle 2 minuuttia, mikä voidaan katsoa merkityksettömäksi, sillä mittauksen etenemistä valvottiin rakennuksen alemmassa kerrok-

sessa sijainneelta tietokoneelta, ja mittaus käynnistettiin sekä pysäytettiin manuaalisesti, jolloin jo siirtyminen valvontapaikalta mittauspaikalle on voinut aiheuttaa epätarkkuuksia kokeen kestoaikaan.

Actility ThingPark Wireless Loggerista voidaan arvioida, että SF8 Ack -kokeen aikana olisi tapahtunut kaksi uudelleenlähetystä, koska Ack-viestit tukiasemalta eivät tavoittaneet anturia. Tämä voidaan havaita tukiaseman anturille lähettämistä toistuvista Ack-viesteistä uplink-paketin vastaanottamisen jälkeen, mitä havainnollistetaan kuvassa 24.

FCnt ⇑	NFCnt ⇓	AFCnt ⇓	RSSI	SNR	ESP	SF/DR
10			-109.0	4.0	-110.45...	SF9
	13					SF9
	12					SF9
	11					SF9
9			-109.0	4.0	-110.45...	SF8

Kuva 24. SF8 Ack -kokeen aikana tapahtuneet kaksi todennäköistä uplink-paketin no. 9 uudelleenlähetystä Actility ThingPark Wireless Loggerin näkymässä tarkasteltuna

Otettaessa nämä uudelleenlähetykset huomioon saadaan pakettia kohden kuluneeksi todennäköiseksi energiaksi 2,63 µAh, jolloin absoluuttiseksi erotukseksi valmistajan laskurin mukaiseen arvoon jää +0,23 µAh ja prosentuaaliseksi noin 1 %.

Lisäksi kuten myös kuvasta 24 havaitaan, on anturi lähettänyt yhden paketin käyttäen Spreading Factorin arvoa SF9, joka lisää kulutusta SF8:aan nähden. Tämänkaltainen vaihtelu on kuitenkin käytännön olosuhteissa mahdollista, joten kokeen todettiin vastaavan nimenomaisesti käytännön tilannetta, eikä sitä uusittu pakottaen Spreading Factoria SF8-tasolle.

Lepovirrankulutuksen todelliseksi mittaamiseksi olisi pitänyt suorittaa pitkä koe, koska laitteen sisäiset kondensaattorit latautuvat erittäin hitaasti. Lisäksi kokeessa mitattu virta olisi ollut erittäin pieni, jonka johdosta mittaustulosten luotettavuus olisi helposti jäänyt hieman kyseenalaiseksi, ja laitteen toimitta-

jalta saatiin tieto, että tämä oli jo aiemmin mittauksin todettu, joten tässä tapauksessa päätettiin tämän osalta luottaa valmistajan ilmoittamaan 4 µA:n kulutukseen, sillä pakettien lähettämiseen kuluva energia vaikutti vastaavan suhteellisen hyvin valmistajan ilmoittamaa.

Valmistajan laskurin mukaan pariston itsepurkautumisvirta olisi noin 4 µA. Laitteessa on käytössä SAFT 14500 -lithiumparisto, jonka datalehden mukaisesti pariston itsepurkautuminen on alle 1 % kapasiteetista vuodessa varastoitaessa paristoa 20 asteen lämpötilassa (SAFT 2019). Pariston nimelliskapasiteetti on 2,6 Ah, jolloin datalehden mukaiseksi itsepurkautumisvirraksi saadaan laskettua keskimäärin 2,97 µA.

Pariston itsepurkautumisvirraksi päätettiin kuitenkin ottaa valmistajan antama, hieman pariston datalehteä suurempi arvo 4 µA, koska antureissa voidaan mahdollisesti käyttää esimerkiksi erimerkkisiä paristoja, joiden itsepurkautumisvirta on hieman esimerkkilaitteen paristoa suurempi, sekä mahdollinen lämpötilanvaihtelu voi myös vaikuttaa pariston itsepurkautumiseen. Tällöin anturin lepovirrankulutus ja pariston itsepurkautuminen aiheuttavat yhteensä jatkuvan 8 µA:n virran, josta muodostuu 192 µAh:n kulutus vuorokaudessa.

Pull-up -vastuksen kautta kulkevan virran ja triggeröityjen lähetystapahtumien aiheuttaman kulutuksen arvioiminen etukäteen on tarkkaan mahdotonta, sillä se riippuu katkaisijan laukeamisten määrästä ja viankorjausajoista pariston vaihtovälin aikana.

Yhtä tapahtumaa kohden voidaan kuitenkin arvioida kuluvan kahden viestin lähettämiseen tarvittava energia katkaisijan laukeamisen ja kuittaamisen yhteydessä, sekä näiden välisenä aikana piirissä pull-up -vastuksen aiheuttaman virran kuluttama energia. Arviointi on suoritettu taulukossa 6.

Taulukko 6. Valvotun 1 kV katkaisijan laukeamisen aiheuttama ELT-2-anturin kuluttama pariston energia heikolla LoRaWAN-kuuluvuusalueella Ack-toimintoa käyttäen

Tapahtumat	Energia	Kumulatiivinen
Katkaisijan laukeaminen, triggerviesti	215,84 µAh	215,84 µAh
Pull-up -virta, 4 tuntia	305,24 µAh	521,08 µAh
Vian kuittaantuminen, triggerviesti	215,84 µAh	736,92 µAh
Kokonaisenergia		**736,92 µAh**

Taulukossa 7 on esitettynä tässä sovelluksessa käytettävälle 6 vuoden akunvaihtovälille laskettu kokonaisenergiankulutus milliampeeritunteina huomioiden mitatut pakettien lähetykseen kuluvat energiat ja valmistajan ilmoittama lepovirrankulutus sekä pariston itsepurkautumisvirta, mutta ei kuitenkaan mahdollisia triggerviestejä.

Taulukko 7. ELT-2-anturin käyttämä pariston energia 6 vuoden aikana ilman triggerviestejä *LoRaWAN-verkon kuuluvuus toimivuuden rajoilla

Lähetysväli	48h	24h	12h	2h
SF8, no Ack	424 mAh	427 mAh	434 mAh	501 mAh
SF8, Ack	424 mAh	427 mAh	434 mAh	504 mAh
SF12, no Ack	453 mAh	485 mAh	550 mAh	1195 mAh
SF12, Ack*	657 mAh	893 mAh	1366 mAh	6093 mAh

Pariston kapasiteetin riittävyyttä kyseiseen sovellukseen tarkasteltaessa on asiaa tarkasteltava suurimman energiankulutuksen aiheuttavan asennuspaikan näkökulmasta, jotta voidaan taata pariston riittävä kestoikä kaikissa asennuskohteissa.

Käytännön olosuhteissa voidaan odottaa, että vähintään muutamilla katkaisija-asemilla LoRaWAN-verkon kuuluvuus on toimivuuden rajoilla, joten tarkastelu suoritetaan SF12-kokeiden tuloksia käyttäen.

Pariston riittävyyttä tarkastellaan ensisijaisesti ottamatta huomioon triggerviestien aiheuttamaa kulutusta, sillä näiden tapahtumien yhteydessä on asentajan aina käytävä katkaisija-asemalla, jolloin ääritapauksissa on mahdollista myös

vaihtaa anturin paristo, mikäli tarkastelun perusteella se osoittautuisi tarpeelliseksi. Konfiguraation valinnassa pyritään kuitenkin siihen, ettei pariston vaihto näissä tapauksissa olisi normaaliolosuhteissa tarpeellista.

Katkaisijan laukeamistapahtumien määrän vaikutusta pariston kulutukseen 6 vuoden paristonvaihtovälin aikana SF12 Spreading Factoria ja Ack-viestejä käyttäen arvioidaan taulukossa 8. Tulokset ovat ylöspäin pyöristettyjä seuraavaan milliampeerituntiin asti.

Taulukko 8. Katkaisijan laukeamistiheyden perusteella laskettu kyseisten tapahtumien aiheuttama ELT-2-anturin pariston kulutus 6 vuoden aikana

Katkaisijan laukeamistiheys	Pariston kulutus
Vuosittain	5 mAh
Kuukausittain	54 mAh
Kerran kahdessa viikossa	115 mAh
Viikoittain	230 mAh

Lisäksi optiona tarkastellaan mahdollisen toisella digitaalitulolla valvotun ”ei-kriittisen” kohteen, kuten esimerkiksi ylijännitesuojan vioittumisen aiheuttamaa pariston kulutusta.

Tämänkaltaisen tapahtuman jälkeen anturin pariston vaihto tarvittaessa olisi käytännössä todennäköisesti myös helpommin hyväksyttävissä, sillä katkaisijan laukeamisen aiheuttama vika on korjattava välittömästi, eikä siinä yhteydessä paikalle tulevalla päivystäjällä ole välttämättä paristoja mukana, ja prioriteettina on saada vika korjattua mahdollisimman nopeasti tarvitsematta huolehtia anturin paristoista.

Ylijännitesuojan vaihto tai vastaava ei-kriittinen korjaustoimenpide suoritetaan kuitenkin aina normaalina työaikana, ja anturin pariston vaihto voitaisiin ehkä tarvittaessa ottaa käytännöksi tämänkaltaisia korjauksia suoritettaessa.

Tapahtuma on muutoin katkaisijan laukeamista vastaava, mutta pull-up -vastuksen kautta kulkevan virran aiheuttama kulutus on huomattavasti suurempi,

sillä viankorjausaikakin on tällaisessa tapauksessa pidempi. Taulukossa 9 ennustetaan ylijännitesuojan vioittumisen aiheuttamaan paristonkulutusta tilanteessa, jossa viankorjausaika olisi kaksi viikkoa.

Taulukko 9. Ylijännitesuojan vioittumisen aiheuttama ELT-2-anturin pariston kulutus

Tapahtumat	Energia	Kumulatiivinen
Suojan vioittuminen, triggerviesti	215,84 µAh	215,84 µAh
Pull-up -virta, 2 viikkoa	25640,16 µAh	25856,00 µAh
Vian kuittaantuminen, triggerviesti	215,84 µAh	26071,84 µAh
Kokonaisenergia		**26071,84 µAh**

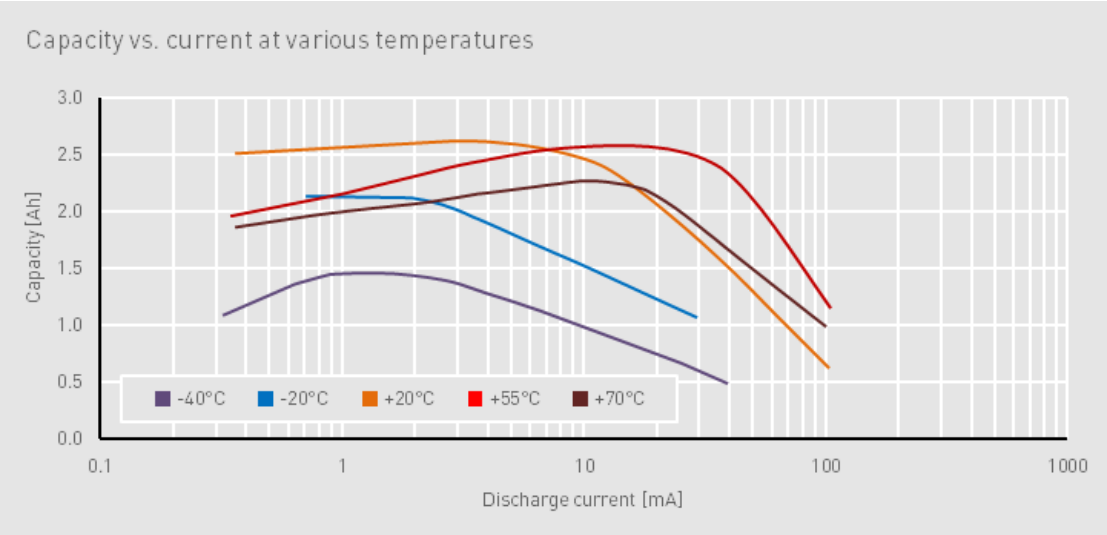
Tulosten perusteella voidaan arvioida yhden vastaavan tapahtuman kuluttavan noin 26 mAh. Arvioitaessa tarvetta pariston vaihtoon vastaavien tapahtumien jälkeen, voidaan ensin tarkastella paristoon 6 vuoden käytön jälkeen ilman kyseisiä tapahtumia jäävää kapasiteettia ja sen perusteella arvioida, onko pariston vaihdolle mahdollisesti tarvetta tietyn tapahtumamäärän jälkeen.

Taulukossa 10 tarkastellaan pariston kokonaiskulutusta 6 vuoden vaihtovälin aikana SF12 Ack -kokeen tuloksia hyödyntäen eri lähetysvälien sekä katkaisijan laukeamistiheyksien funktiona pyöristettynä ylöspäin seuraavaan milliampeerituntiin asti.

Taulukko 10. ELT-2-anturin pariston kulutus 6 vuoden paristonvaihtovälillä lähetysvälin ja katkaisijan laukeamistiheyden funktiona käytettäessä Ack-lähetystä LoRaWAN-verkon kuuluvuuden ollessa SF12 Spreading Factorin vaatimalla alueella toimivuuden rajoilla

Katkaisijan laukeamistiheys	Lähetysväli			
	48h	24h	12h	2h
Vuosittain	661 mAh	898 mAh	1370 mAh	6097 mAh
Kuukausittain	710 mAh	946 mAh	1419 mAh	6146 mAh
Kerran kahdessa viikossa	772 mAh	1008 mAh	1481 mAh	6208 mAh
Viikoittain	887 mAh	1123 mAh	1596 mAh	6323 mAh

Kyseisessä anturissa käytettävän SAFT 14500 -pariston käytettävissä oleva kapasiteetti riippuu lämpötilasta ja purkausvirrasta datalehdessä esitetyn kuvan 25 mukaisesti. Lisäksi valmistaja ilmoittaa pariston nimelliskapasiteetiksi 2,6 Ah, mikäli sitä puretaan alle 2 mA:n virralla +20 asteen lämpötilassa.



Kuva 25. SAFT 14500 -pariston käytettävissä oleva kapasiteetti purkausvirran ja lämpötilan funktiona (SAFT 2019, 2)

Mikäli anturin lähetysvälinä käytettäisiin 24 tuntia ja katkaisijan laukeamistiheys olisi keskimäärin vuosittain, taulukon 10 mukaisesti pariston energiaa kuluisi 6 vuoden paristonvaihtovälin aikana 898 mAh LoRaWAN-verkon kuuluvuuden ollessa heikolla tasolla.

Pariston datalehden kapasiteettikäyrien mukaisesti (2 voltin cut-off -jännitteellä) kyseinen paristo kykenee luovuttamaan tämän energiamäärän -40 asteen lämpötilassa noin 10 mA:n purkausvirralla ja esimerkiksi -20 asteen lämpötilassa jopa 30 mA:n purkausvirralla.

Keskimääräinen purkausvirta tässä tapauksessa on hyvin matala sisältäen kuitenkin hieman korkeampia pulsseja anturin lähettäessä viestejä. Anturin nukkuessa purkausvirta valmistajan laskurin mukaan on aikaisemmin todettu 4 µA, ja lähetyksen aikana mitattu suurin hetkellinen pariston purkausvirta noin 30 mA.

Valmistajan laskurin mukaan laitteen radio kuluttaisi 60 mA, mutta laitteen sisäiset kondensaattorit tasaavat paristosta otettavaa virtaa. On myös hieman epäselvää, kuinka pariston kapasiteettikäyriä tämänkaltaisen purkausvirran osalta pitäisi tarkastella, mutta niistä voidaan todeta, että kyseinen energiamäärä pitäisi olla varmuudella saatavilla noin 20–30 mA purkausvirralla -30 asteen lämpötilassa.

Kondensaattoreiden vaikutus paristosta otettavaan virtaan on myös todennäköisesti suurempi pariston virranantokyvyn pudotessa, jolloin paristosta otettava suurin mahdollinen purkausvirtakin on tässä tilanteessa pienempi. Paristojännitteen pysyessä korkeana myös suuremmalla virralla pariston purkausvirta pysyy suurempana, vaikka anturi kykenisikin toimimaan kondensaattorien avulla alhaisemmalla pariston purkausvirralla.

Kyseisen tarkastelun perusteella voidaan pariston kapasiteetin kuitenkin todeta olevan jokseenkin luotettavasti riittävä kaikkiin 1 kV katkaisijoiden valvontakohteisiin, mikäli anturi konfiguroidaan käyttämään 24 tunnin säännöllistä lähetysväliä Ack:ta käyttäen ja katkaisijan laukeamisia sattuu noin kerran vuodessa.

Vaikeimmilla kohteilla voitaisiin lisäksi käyttää myös 48 tunnin lähetysväliä, mikäli pariston kapasiteetin riittävyydestä herää epäilyksiä. Mikäli pariston käytettävissä olevan kapasiteetti arvioitaisiin noin yhdeksi ampeerituniksi, jäisi paristoon sen vaihtovälin päättyessä vielä noin 100 milliampeerituntia hyödynnettävää kapasiteettia.

Yhden ylijännitesuojan laukeamisen todettiin aiemmin aiheuttavan taulukon 9 mukaan noin 26 mAh:n suuruisen kulutuksen, jolloin pariston vaihto olisi syytä suorittaa viimeistään neljännen vastaavan, kahden viikon viankorjausajan käsittäneen ylijännitesuojan vioittumistapahtuman jälkeen.

Useimmilla asennuskohteilla kuitenkin pariston kulutus on huomattavasti alhaisempaa, kuten havaittiin SF8 Ack- ja SF12 No ack -kokeiden perusteella, ja kaikista vaikeimmissa tapauksissa esimerkiksi lähetysvälin pidentäminen 24:stä 48 tuntiin vapauttaisi jo 237 mAh kapasiteettia, joka vastaisi noin yhdeksää ylijännitesuojan laukeamistapahtumaa.

Ylijännitesuojien tarkasta vikatiheydestä ja kyseisten vikojen korjausajoista ei ole tarkkaa tietoa. Myöskin paristonkulutusmittauksissa saadut tulokset ovat hieman valmistajan ilmoittamia arvoja suurempia todennäköisesti laitteen sisäisten kondensaattoreiden latautumisesta johtuen, ja todellisesta tilanteesta poiketen, ELT-2-anturin sisäiset lämpötila- ja kosteusanturit olivat aktiivisia.

Myös nämä huomioon ottaen voidaan tehdä johtopäätös, että normaaliolosuhteissa antureiden pariston kapasiteetin pitäisi riittää 6 vuoden paristonvaihtovälille ongelmitta myös vaikeimmissa olosuhteissa, erityisesti mikäli katkaisijalla ei tapahdu poikkeuksellisen suurta määrää vikatilanteita.

Äärimmäisen suuren vikatilannemäärän tapauksessa katkaisijalla joudutaan tekemään jatkuvasti asentajakäyntejä, joiden yhteydessä tämänkaltaisessa harvinaisessa yksittäistapauksessa voitaisiin myös vaihtaa lopulta anturin paristo.

7.4.6 Anturin konfiguraatio

Kokeiden perusteella 1kV-katkaisijoiden valvontaan Elsys ELT-2 -anturille määriteltiin käytettäväksi seuraavat asetukset:

- Sensor sample times
  - Timebase: 86400sec
  - Temperature period: 0
  - Humidity period: 0
  - External period: 1
  - External startup time: 0
  - Trigger timeout: 100ms
  - Accelerometer period: 0
  - Battery period: 1
  - Pressure period: 0
  - Transmit period: 1
- External configuration
  - ”Switch NO dual edge trigg”
- Advanced
  - PIR sensitivity: Low (Not applicable)
  - Datarate default: DR5
  - Datarate max: DR5
  - Datarate min: DR0
  - Port: As in Application Server settings
- Version 2 features
  - Confirmed message: Enabled
  - Sample queue size: 1
  - Queue offset: Disabled
  - Queue purge: Enabled
  - Link Period: 0
  - Link Threshold: 0
  - Accelerometer configuration: 0

LoRaWAN-verkkoon liittyvät asetukset on käsitelty aikaisemmin anturin provisiointia koskevassa osiossa. Asetuksissa kaikki sisäiset anturit akkujännitteen

mittausta lukuun ottamatta ovat poiskytketty, ulkoiset tulot määritelty Switch NO -tilaan ”dual edge trigg” -ominaisuudella, jolloin sekä kytkintiedon sulkeutumisesta, että avautumisesta saadaan triggeröidyt viestit ja lisäksi säännöllisenä lähetysvälinä on 24 tuntia.

Säännöllisissä lähetyksissä on määritelty lähetettäväksi sekä akkujännite että ulkoisten tulojen tilat. Anturi on määritelty käyttämään automaattista dataratea ja Spreading Factoria välillä DR5–DR0, mikä vastaa LoRan Spreading Factorin arvoja SF7–SF12 sekä Acknowledged uplink -toiminto on kytketty päälle.

Viestit lähetetään aikaisemmin ”LoRaWAN_AppServer.py”:n asetuksiin määritellyssä LoRaWANin portissa. Mikäli LoRaWAN-verkkoa hyödyntäviä sovelluksia olisi käytössä useampi, niille voitaisiin käyttää omia porttejaan ja näin erottaa eri sovelluksiin liittyvä verkosta vastaanotettu data toisistaan, vaikka ko. sovelluksissa käytettäisiinkin samanlaisia laitteita.

Lisäksi anturin ”Sample queue” on määritelty sisältämään vain yksi mittaus, sillä tässä käyttötarkoituksessa halutaan mahdollisimman nopeaa reaaliaikaista tietoa tapahtumista, ja tapahtumat lähetetään heti varmistettuina viesteinä jolloin niiden säilömiselle jonoon myöhempää lähetystä varten ei ole tarvetta.

LinkCheck-toiminto, jolla anturi varmistaa ajoittain downlink-viestiä pyytämällä verkon vastaanottavan sen lähettämät viestit ja tarvittaessa triggeröi anturin uudelleenkäynnistymisen, mikäli downlink-viestejä verkolta ei vastaanoteta, jätettiin myös ainakin toistaiseksi pois käytöstä.

Anturilla oli käytössä jo Adaptive Data Rate- sekä Acknowledged uplink -toiminnot, jotka molemmat osaltaan varmistavat viestien perillemenoa ja joiden perusteella anturi pystyy esimerkiksi lisäämään käytettyä lähetystehoa ja suurentamaan Spreading Factoria, mikäli viestit eivät mene perille.

Esimerkiksi tämä toiminto on kuitenkin mahdollista tarvittaessa ottaa jatkossa käyttöön lähettämällä tarvittava asetusmuutos jo asennetuille antureille downlink-viestinä, joten mikäli havaitaan, että toiminnolle on tarvetta, se tullaan ot-

tamaan käyttöön myöhemmin. Anturin NFC-toiminnallisuus päätettiin myös lukita lukituskoodilla ilkivaltaisten asetusmuutosten tai asetusarvojen lukemisen ehkäisemiseksi.

Kyseiset asetukset voidaan konfiguroida anturille paikallisesti aiemmin todetun mukaisesti matkapuhelimella NFC:n ja mobiilisovelluksen avulla tai lähettää heksadesimaalimuodossa LoRaWAN-verkon kautta downlink-viestinä.

Käytettäessä Digitan LoRaWAN-verkossa Digitan kautta tilattuja, valmiiksi verkkoon provisioituja antureita niiden konfigurointi voidaan myös automatisoida määrittelemällä Application Server lähettämään uusille antureille automaattisesti sovelluksessa käytetyt oletusasetukset niiden lähetettyä ensimmäisen viestin, joka tapahtuu anturin pariston kytkemisen jälkeen.

Käytettäessä downlink-viesteihin perustuvaa automaattista konfigurointia asentajan ei tarvitse tehdä (valmiiksi provisioidulle) anturille erikseen asetusmuutoksia matkapuhelimella asennuksen yhteydessä, mikä vähentää asennusaikaa ja -kustannuksia sekä pienentää inhimillisten virheiden riskiä konfigurointiprosessissa.

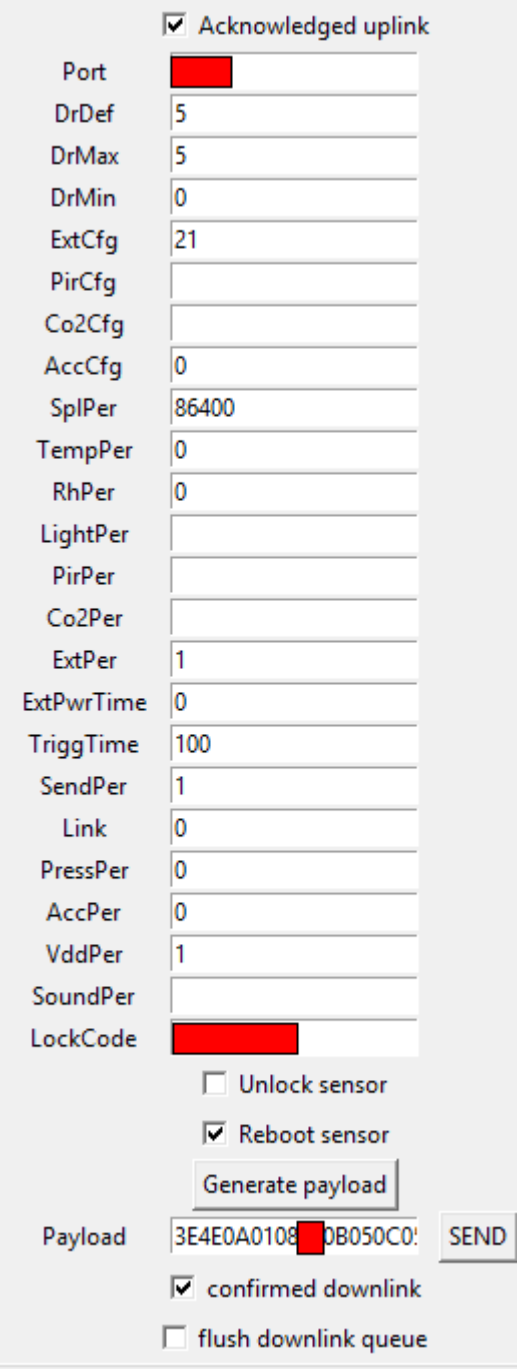
Pahimmassa tapauksessa virheellinen konfiguraatio estää onnistuneen tiedonsiirron anturin ja LoRaWAN-verkon välillä, jolloin myöhemmin ongelma havaittaessa jouduttaisiin anturille tekemään vielä erillinen asentajakäynti. Lisäksi asentajien nykyiset matkapuhelimet eivät välttämättä tue NFC-ominaisuutta, missä tapauksessa antureita asentaville henkilöille jouduttaisiin hankkimaan lisäksi uudet puhelimet.

Näiden seikkojen vuoksi antureiden konfiguroinnissa onkin järkevää pyrkiä pääosin automatisointiin ja asetusten lähettämiseen anturille downlink-viestissä. Tällainen viesti, joka sisältäisi edellä mainitut, anturille määriteltävät asetukset, sisältää seuraavan payloadin:

”*3E4E0A0108XX0B050C050D00101513000000001400015180150000000016000000001A00000011B000000001C000000641D000000001E000000011F000000012200000000230000000020XXXXXXXXFE*”

Payloadissa lähetetyn portin ja anturin lukituskoodin arvoja havainnollistetaan tässä tapauksessa X-kirjaimilla. Kuvassa 26 lisäksi havainnollistetaan kyseisen viestin generointia opinnäytetyön yhteydessä ohjelmoidussa, downlink-viestien generoimiseksi kehitetyssä ohjelmassa.

Kyseisessä ohjelmassa käytetyt lyhenteet ja esimerkiksi ”External configuration” / ”ExtCfg”-parametrin sanallisia kuvauksia vastaavat desimaaliarvot ovat saatavilla Elsysin ”Sensor settings parameters” -dokumentista (Elsys 2019b).



Kuva 26. 1kV-katkaisijan valvonnassa käytettävälle Elsys-anturille lähetettävät oletusasetukset havainnollistettuna opinnäytetyön yhteydessä ko. viestien generoimiseen ja lähettämiseen

kehitetyn ohjelman tämän kappaleen kirjoitushetkellä käytössä olleessa versiossa. Ohjelma tukee myös muita Elsys-antureita, jonka johdosta kaikkia mahdollisia parametrejä ei tässä yhteydessä käytetä.

Kyseisen payloadin voidaan havaita sisältävän 160 heksadesimaalimerkkiä, jolloin sen koko on 80 tavua, koska yhteen tavuun mahtuu kaksi heksadesimaalimerkkiä (yksi heksadesimaalimerkki vastaa 4 bittiä, ja yksi tavu 8 bittiä).

Kuten aiemmin todettiin ja taulukosta 1 voidaan lukea, SF10–12 Spreading Factoria käytettäessä yksi LoRaWAN-viesti voi kuitenkin sisältää vain maksimissaan 51 tavun kokoisen payloadin, jolloin esimerkiksi tätä asetusviestiä ei voitaisi tällaisenaan suoraan lähettää.

Koska on odotettavissa, että käytännön olosuhteissa vähintään muutamia antureita sijaitsee vähintään SF10:n vaatimalla alueella, on asetusviestit määritettävä maksimissaan 51 tavun kokoisiksi, jotta niiden lähetys varmasti onnistuu kaikille käytetyille laitteille. Tämän johdosta suurin mahdollinen payloadin pituus on 102 heksadesimaalimerkkiä, joka tarkoittaa, että asetukset on mahdollisesti jaettava kahteen erilliseen viestiin.

Koska kyseiset anturit saapuvat Digitan kautta tilattaessa tietyillä oletusasetuksilla verkkoon provisioituna, on osa asetuksista kuitenkin mahdollisesti jo valmiiksi määriteltynä, jolloin näitä ei välttämättä tarvitse enää lähettää antureille uudelleen. Lisäksi kaikkia ominaisuuksia ei käytetä, jolloin esimerkiksi kaikkia sample time -asetuksia ei tarvitse määritellä, mikäli kyseinen toiminto ei anturissa ole muutoin käytössä.

Vertailtaessa haluttua konfiguraatiota anturin toimitushetken konfiguraatioon voitaisiin esimerkiksi datarate-arvojen määrittelyt poistaa, sillä ne olivat jo valmiiksi konfiguroitu halutulla tavalla. Lisäksi esimerkiksi ”Accelerometer period” -arvoa ei tarvitsisi lähettää, koska kyseinen anturi on kytketty pois päältä ”Accelerometer configuration” -asetuksella.

Myöskin tämä kyseinen arvo oli jo toimitushetkellä valmiiksi määritelty, joten kumpaakaan kiihtyvyysanturiin vaikuttavaa asetusarvoa ei tarvitsisi lähettää,

sekä myöskin akkujännitteen mittausväli (VddPer) sekä viestien lähetysväli (SendPer) olivat jo valmiiksi halutuissa arvoissaan.

Uudemmissa Elsys-antureissa lisäksi lämpötila- ja kosteusanturit ovat yhdistetty, joten erillinen kosteusanturin mittausvälin arvo ei enää vaikuta mihinkään, vaan se noudattaa lämpötilan mittausvälin arvoa, jolloin myöskään tätä asetusarvoa ei tarvitse erikseen lähettää (Elsys s.a.b).

Optimoimalla lähetettävät asetukset vertaamalla anturin toimitushetken konfiguraatioon, todetaan seuraavan payloadin sisältävällä LoRaWAN-viestillä päästävän haluttuun lopulliseen konfiguraatioon:

”*3E2F0A0108XX10151400015180150000000016000000001A000000011B00 0000001C0000006423000000020XXXXXXXXFE*”

Kyseisen viestin voidaan todeta sisältävän 98 heksadesimaalimerkkiä, jolloin sen koko on 49 tavua, joka mahdollistaa tarvittavien asetusten lähettämisen yhdessä viestissä kaikkia Spreading Factorin arvoja käyttäen.

Anturien toimitushetken asetusten täydellisestä vastaavuudesta testilaitteeseen ja esimerkiksi mahdollisesti myöhemmin hankittujen, uudempien anturei-den asetuksista ei kuitenkaan voida olla täysin varmoja, joten asetukset voidaan varmuuden vuoksi lähettää myös kahta downlink-viestiä käyttäen alkuperäisen suunnitelman mukaisesti.

Nämä viestit sisältävät esimerkiksi seuraavat payloadit:

”*3E220A010B050C050D00130000000016000000001D000000001E00000001 2200000000FE”*

”*3E2F0A0108XX10151400015180150000000001A000000011B000000001C00 0000641F0000000123000000020XXXXXXXXFE*”

Kyseiset viestit ovat määritelty huomioiden vikatilanne, jossa ensimmäinen viesti katoaa ennen jälkimmäisen vastaanottamista, ja esimerkiksi anturin lä-

hetysvälin muuttaminen toimitushetken oletuksesta 10 minuutista 24 tuntiin tapahtuu vasta jälkimmäisessä viestissä. Lisäksi molemmissa viesteissä esiintyy anturin uudelleenkäynnistys ja Acknowledged uplink -toiminnon päällekytkentä.

Lisäksi 1 kV katkaisijan valvonnalle (tai muulle sovellukselle) essentiaalit asetukset ovat samassa, jälkimmäisessä viestissä, jolloin voidaan olla varmoja siitä, että katkaisijan valvonta on käytössä siinä vaiheessa, kun kyseinen viesti menee perille ja lähetysväli muuttuu vuorokauteen, jolloin myös downlink-viestien lähetysikkunat rajoittuvat yhteen kertaan vuorokaudessa.

Muokattaessa anturin käyttämää porttia on esimerkiksi Elsys-antureiden tapauksessa Application Serverin downlink-viestien uudelleenlähetyslogiikassa huomioitava, että tässä tapauksessa ensimmäisen viestin uudelleenlähetys jälkimmäisen viestin perillemenon jälkeen vaatii viestin lähettämisen eri portissa, kuin alkuperäisen. Tämä otettiin huomioon myös tämän opinnäytetyön yhteydessä ohjelmoidussa, myös downlink-viestien lähetystä hoitavassa ”LoRaWAN_AppServer.py”-ohjelmassa.

7.5 Application Server -palvelimen asennus ja konfigurointi

7.5.1 Palvelimen käyttöönotto ja esivalmistelut

Application Server -palvelimen käyttöönotto aloitettiin asentamalla olemassa olevalle VMWare-virtualisointialustalle Windows Server 2016 -palvelininstanssi. Kyseiselle virtuaalipalvelimelle varattiin resursseja 4 prosessoriydintä, 10GB RAM-muistia sekä 150GB:n kiintolevyosio, jotka olivat tähän käyttötarkoitukseen hyvinkin riittävät.

Palvelimelle varattiin verkon palomuurilta julkinen IP-osoite, jonka takaa ohjattiin portti TCP443 kyseisen palvelimen privaattiin IP-osoitteeseen ja liikenne porttiin sallittiin Digitan ilmoittamista Actility-verkkoalustan käyttämistä IP-osoitteista. Lisäksi kyseiselle IP-osoitteelle rekisteröitiin DNS-tietue julkiseen DNS-palveluun, jotta HTTPS:n käyttö olisi mahdollista.

Palvelimelle asennettiin ohjelmistojen vaatimat Python, MySQL Server, MySQL Workbench sekä MySQL Connector/Python ja MySQL Connector/ODBC. Lisäksi asennettiin muita tarvittavia ohjelmistoja, kuten esimerkiksi kyseisessä ympäristössä käytetty endpoint protection -ohjelmisto tietoturvan parantamiseksi, Wireshark verkkoliikenteen tutkimiseen ongelmatilanteissa sekä Notepad++ esimerkiksi Python-ohjelmatiedostojen ja muiden konfiguraatiotiedostojen muokkaamista varten.

Lisäksi palvelimelle asennettiin kaikki asennushetkellä Microsoft Updatesta saatavilla olleet päivitykset. Palvelimelle määritettiin myös RDP-etätyöpöytäyhteys sen helpon etähallinnan mahdollistamiseksi.

7.5.2 “LoRaWAN_AppServer.py”:n asennus ja konfigurointi

Sovellusohjelmistojen asennus aloitettiin ”LoRaWAN_AppServer.py”-ohjelmistosta. Kyseisen ohjelmiston asennus tapahtui luomalla palvelimen C:\ -asemalle kansio, johon ohjelman tiedostot kopioitiin aikaisemmalta testiympäristön virtuaalipalvelimelta, jossa ohjelmaa oli kehitetty ja testattu.

Tämän jälkeen valmisteltiin MySQL-tietokantapalvelin kyseisen ohjelmiston käyttöön avaamalla MySQL Workbench ja luomalla ohjelmaa varten tietokantaan sille käyttäjätunnus, jolle annettiin tarvittavat käyttöoikeudet uuden tietokannan luomiseksi ja tarvittavat kantakohtaiset oikeudet kyseisen tietokannan käyttöön.

Lisäksi valmisteltiin käytetty SSL-sertifikaatti kyseistä ohjelmistoa varten. ”LoRaWAN AppServer.py” oli ohjelmoitu käyttämään erillisessä ”.pem”-tiedostossa olevaa sertifikaattia. Käytössä oli koko kyseisen domainin kattava wildcard-sertifikaatti, joka saatiin kopioitua valmiiksi sopivassa muodossa toiselta palvelimelta, joka käytti vastaavan muotoista sertifikaattia.

Näiden esivalmistelujen jälkeen konfiguroitiin kyseisen ohjelman asetukset vastaamaan käytettyä ympäristöä esimerkiksi tietokanta-asetusten ja sertifikaattitiedostojen osalta. Kuvassa 27 esitetään ohjelman tämän kappaleen kirjoitushetkellä käytössä olleelle versiolle konfiguroitavia asetuksia.

```
#LoRaWAN Fport used for 1kV breaker monitoring
Fport1kV = [redacted]
#ApplicationServer-ID
AsID = [redacted]
#Downlink URL
DownlinkURL = [redacted]
#LRC-AsKey
LrcAsKey = [redacted]
#Maximum timestamp deviation in seconds
TimeDev = [redacted]
#MySQL server
DbServer = '127.0.0.1'
#MySQL database
DbName = [redacted]
#MySQL username
DbUserName = [redacted]
#MySQL password
DbPassword = [redacted]
#HTTP server listen IP address
listenip = '0.0.0.0'
#HTTP server listen port
listenport = '443'
#Certificate file
CertFile = [redacted]
#Private key file
PrivateKeyFile = [redacted]
#Log file names
LogFile = 'LoRaWAN AppServer.log'
DownLinkClientLogFile = 'LoRaWAN DownLinkClient.log'
#Maximum log file size in megabytes
LogFileMaxSize = '20'
#Maximum number of stored log files
MaxNumberOfLogfiles = '5'
```

Kuva 27. LoRaWAN_AppServer.py:n konfiguroitavia asetuksia

Palvelimella oli käytössä lisäksi Windows Firewall, joten siihen tehtiin vielä uusi sääntö, jolla sallittiin liikenne TCP porttiin 443 Digitan käyttämiltä IP-osoitteilta.

Tämän jälkeen ohjelman testaaminen aloitettiin luomalla työpöydälle pikakuvake, jolla ohjelma käynnistettiin ja käynnistämällä kyseinen ohjelma. Ohjelman konsoli-ikkunasta todettiin, että ohjelma oli käynnistynyt normaalisti, jonka jälkeen tutkittiin tietokannan sisältöä MySQL Workbench -ohjelmistolla, ja varmistettiin, että ohjelma oli luonut sinne tarvittavat taulut.

Lisäksi ”netstat -a”-komennolla tarkastettiin, että palvelimella on porttia 443 kuunteleva ohjelma käynnissä. Liikenteen ohjaamiseksi Digitan LoRaWAN-

verkosta palvelimelle, käytiin muokkaamassa aiemmin määriteltyä Application Serveriä Actility ThingParkin käyttöliittymässä.

Täältä muokattiin palvelimen kohdeosoite vastaamaan tämän palvelimen julkista DNS-osoitetta ja määriteltiin uplink/downlink security -ominaisuutta varten uudet AS-ID- ja LRC-AS Key -parametrit vastaamaan tällä palvelimella sijaitsevan ”LoRaWAN_AppServer.py”-ohjelman konfiguraatiota.

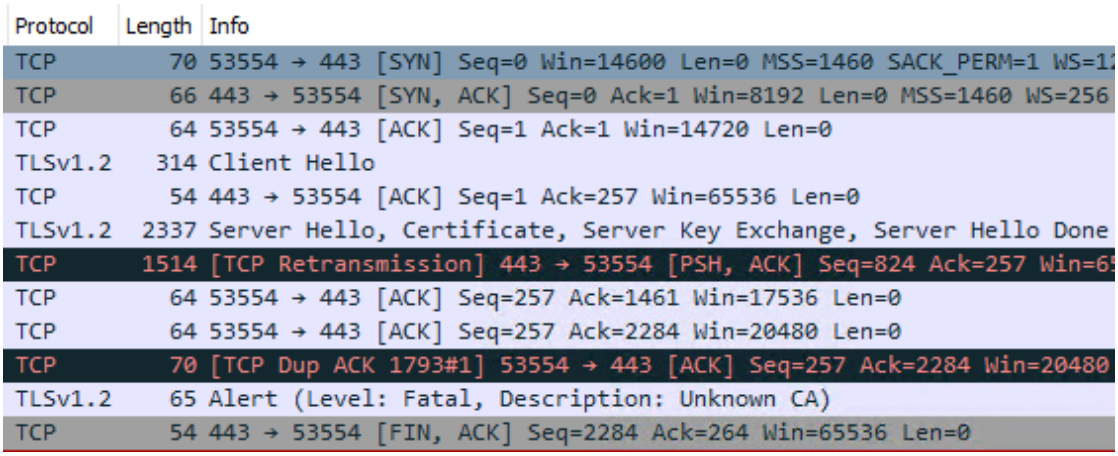
Dataa ei kuitenkaan saatu tietokantaan, vaikka Actility ThingParkin Wireless Loggerissa esiintyi LoRaWAN-anturin lähettämiä paketteja. Myöskään ohjelman konsoli-ikkunassa ei esiintynyt minkäänlaisia merkkejä, että ohjelma olisi vastaanottanut HTTP POST -requesteja Actilityltä.

Ongelman epäiltiin aluksi johtuvan esimerkiksi virheellisestä palomuurikonfiguraatiosta tai jostain muusta syystä, mikä estäisi tietoliikenteen Actilityltä kyseiselle palvelimelle.

Actilityssä ei ole Application Serverin diagnosoimiseen käytettävissä minkäänlaisia työkaluja, joten ongelmaa lähdettiin aluksi selvittämään tutkimalla palvelimen verkkoliikennettä Wireshark-ohjelmistolla samanaikaisesti, kun LoRaWAN-anturilta triggeröitiin paketin lähetys kärkitieto sulkemalla.

Wiresharkiin määriteltiin capture filter, jotta vain paikalliseen porttiin 443 kohdistuva liikenne kaapattaisiin ja esitettäisiin ikkunassa, jolloin tarkkailu oli helpompaa, sillä Actilityltä mahdollisesti saapuvaa liikennettä ei tarvinnut yrittää etsiä kaiken muun verkkoliikenteen seasta.

Triggeröitäessä lähetys LoRaWAN-laitteelta Wiresharkissa havaittiin liikennettä Actilityn IP-osoitteesta ja SSL-handshake Actilityn ja AS:n välillä. Tämän aikana kuitenkin havaittiin Actilityltä ”TLSv1.2 Alert” -paketti, jonka descriptionina oli ”Unknown CA”. Liikennettä Actilityn ja Application Serverin välillä sekä kyseistä esiintynyttä virhettä Wiresharkilla tarkasteltuna esitetään kuvassa 28.



Kuva 28. Epäonnistunut SSL-handshake Actilityn ja Application Serverin välillä

Virheilmoituksen mukaan Actility ei tunnistanut palvelimella käytetyn SSL-sertifikaatin myöntäjää. Digitalta oli aikaisemmin saatu tieto Actilityn käyttämästä Root CA (Certification Authority)-listan sisältävästä Red Hat Packagesta, joten ongelman selvittäminen aloitettiin lataamalla kyseinen paketti internetistä ja purkamalla se auki sekä etsimällä sisältä kyseinen Root CA:t sisältävä lista.

Tätä verrattiin käytetyn sertifikaatin chain of trustiin, jonka perusteella löydettiin Root CA:n sertifikaatti Actilityn käyttämästä paketista, mutta ei kuitenkaan Intermediate-sertifikaattia. Asiaa selvitettäessä ilmeni, että tällaisessa tapauksessa palvelimen on lähetettävä koko ketju Root CA:n myöntämään sertifikaattiin asti sisältäen myös Intermediate-sertifikaatit, jotta todennus onnistuisi.

Tutkittaessa ”LoRaWAN_AppServer.py”:n käyttöön otettua sertifikaattitiedostoa sen ei havaittu kuitenkaan sisältävän kyseistä sertifikaattia, joten Actility ei kyennyt tunnistamaan sertifikaatin myöntäjää, sillä Intermediate-sertifikaatin puuttumisen vuoksi varsinaisen sertifikaatin chain of trust jäi vaillinaiseksi.

Kyseinen ongelma ratkaistiin lisäämällä sertifikaattitiedostoon myös kyseinen Intermediate-sertifikaatti, jonka jälkeen varmenneketju aina Root CA:n sertifikaattiin asti muodostui täydelliseksi, Actility tunnisti sekä hyväksyi käytetyn sertifikaatin ja LoRaWAN-laitteelta tullut data alkoi ilmestyä tietokantaan.

Kuvassa 29 esitetään LoRaWAN-anturilta onnistuneesti tietokantaan vastaanotettua, dekoodattua dataa HeidiSQL-ohjelmistossa.

timestamp	dev_id	fport	data_type	data
2019-04-02 13:33:45	1		1	01010602130 70d740d0014000f940c1a00
2019-04-02 13:33:45	1		2	0
2019-04-02 13:33:45	1		3	0
2019-04-02 13:33:45	1		4	26.2
2019-04-02 13:33:45	1		5	19
2019-04-02 13:33:45	1		6	3444
2019-04-02 13:33:45	1		7	1020.94

Kuva 29. LoRaWAN-anturilta vastaanotettua ja dekoodattua dataa ”LoRaWAN_AppServer.py”:n tietokannan historiadatan sisältävässä taulussa

”LoRaWAN_AppServer.py”:n toimivaksi toteamisen jälkeen se konfiguroitiin toimimaan Windows Servicenä, jotta käyttäjän kirjautuminen ulos kyseiseltä palvelimelta ei aiheuttaisi ohjelmiston suorituksen pysähtymistä.

Tähän päätettiin käyttää NSSM-ohjelmaa, jolla esimerkiksi erilaisia batch-skriptejä ym. ohjelmia pystytään ajamaan Windows Servicenä, vaikka kyseisillä ohjelmilla ei tällaista natiivitukea olisikaan (Patterson s.a).

NSSM kopioitiin palvelimelle system32–järjestelmäkansioon ja kyseinen ”LoRaWAN AppServer” -palvelu asennettiin sitä hyödyntäen. Lisäksi tehtiin muita määrityksiä, kuten esimerkiksi servicen käyttäjätiliksi määriteltiin ”Local Service” oletuksena olevan ”Local System”:n sijaan tietoturvan parantamiseksi, sillä ”Local Service” -järjestelmätilillä on huomattavasti alhaisemmat käyttöoikeudet kuin ”Local System”:llä.

Tämän jälkeen kyseinen palvelu käynnistettiin ”services.msc”-konsolista ja lokitiedostoista tarkastettiin ohjelman käynnistyneen odotetusti. Lisäksi vielä tarkistettiin, että tietokantaan ilmestyy LoRaWAN-laitteen lähettämää dataa myös ohjelman toimiessa servicenä. Näiden testien jälkeen ”LoRaWAN_AppServer.py”:n asennus ja konfigurointi voitiin katsoa suoritetuksi.

7.5.3 Scada Data Gatewayn asennus ja konfigurointi

Scada Data Gateway -ohjelmiston perusasennus Application Server -palvelimelle tapahtui normaalisti Windows-ohjelmistojen tapaan suorittamalla kyseisen ohjelman asennustiedosto ja seuraamalla asennusohjelman ohjeita.

Palvelimen asennusvaiheessa oli jo esiasennettu 32-bittinen MySQL ODBC Connector, jota tarvitaan SDGW:n tietokantakyselyjen mahdollistamiseksi. SDGW:n asennuksen jälkeen ohjelman konfigurointi aloitettiin aluksi konfiguroimalla tietojen haku tietokannasta, jonka jälkeen voitiin määritellä IEC-104-yhteyden vaatimat asetukset ja tehdä tarvittavat datapistemappaukset.

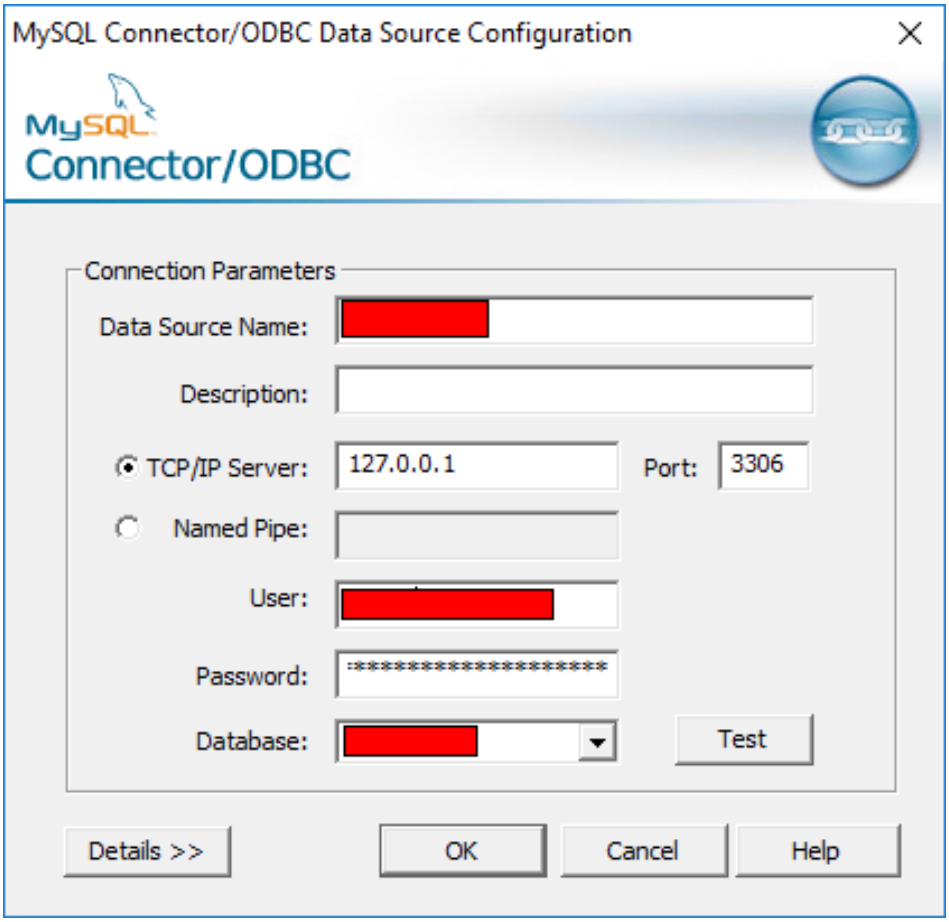
Tietojen hakeminen tietokannasta tapahtuu ODBC-rajapinnan kautta, joten konfigurointi aloitettiin luomalla uusi ”ODBC Client”, jonka alle tarvittavat tietokantakyselyt voidaan lisätä.

Tämä tapahtuu SDGW:n konfiguraatiossa ”Add ODBC Client” -toiminnolla, jonka jälkeen uudelle ODBC-clientille voidaan antaa nimi (Alias) ja hakea haluttu ODBC-ajuri valitsemalla ”Find ODBC Server”. Mikäli palvelimelle on jo aikaisemmin konfiguroitu ODBC Data Sourceja, niitä voidaan ottaa käyttöön suoraan tai lisätä tarvittaessa uusia.

Koska tässä tapauksessa näitä ei vielä ollut, aloitettiin uuden Data Sourcen lisääminen. Tyypiksi valittiin System Data Source, sillä SDGW:tä voidaan suorittaa sekä Windows Servicenä että user modessa, jolloin sama Data Source on käytettävissä molemmissa tapauksissa, vaikka ohjelman suoritus tapahtuisikin välillä eri käyttäjätilin alla.

Tietokanta-ajurin tyypiksi valittiin MySQL ODBC 5.3 ANSI Driver, mikä on uusin kyseisen ajurin versio, minkä kanssa SDGW toimii. ANSI-ajuria käytettiin, sillä se on hieman Unicode-ajuria nopeampi, eikä pelkkää numerotietoa käsiteltäessä ANSI-ajurin Unicodea rajallisempi merkistötuki aiheuta ongelmia (Oracle 2019c).

Uudelle Data Sourcelle annettiin MySQL ODBC -ajurin asetuksissa nimi, tietokantapalvelimen osoite ja tietokantaan ohjelmaa varten määritellyt käyttäjätunnukset. Lisäksi oletustietokannaksi valittiin ”LoRaWAN_AppServer.py”:n generoima tietokanta. Yhteys lisäksi testattiin ajurin ”Test”-toimintoa käyttäen. MySQL ODBC Connectorin konfiguraatiota havainnollistetaan kuvassa 30.



Kuva 30. MySQL ODBC Connectorin konfiguraatioikkuna

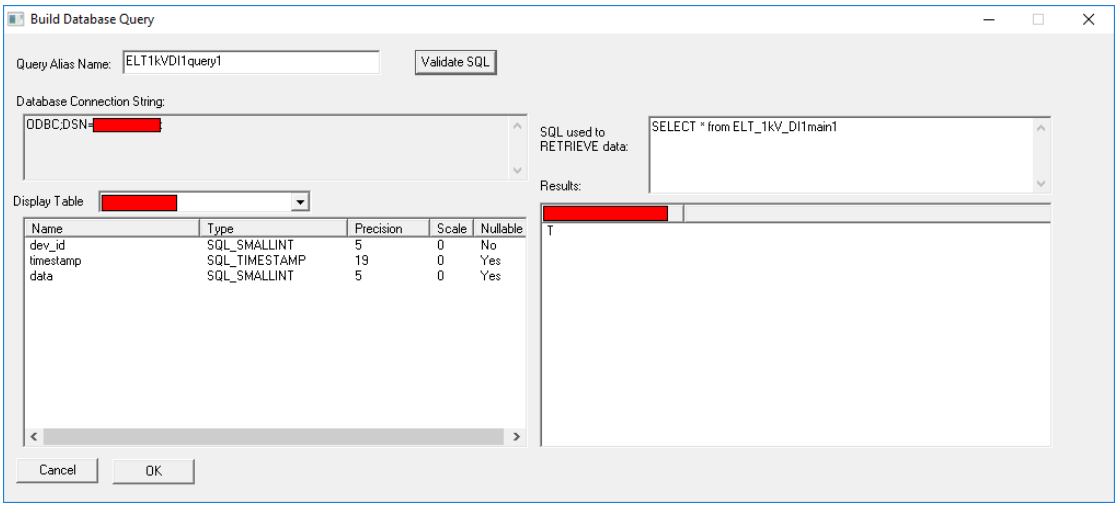
Näiden toimenpiteiden jälkeen varsinainen tietokantayhteys oli valmiina käyttöön ja seuraavina toimenpiteinä tietokantakyselyjen konfigurointi, IEC-104-yhteyden konfigurointi ja datapisteiden mappaus näiden välille.

Tietokantakysely luodaan ODBC Clientin alle toiminolla ”Add ODBC query”. Tietokantakyselylle pitää antaa nimi (Query Alias Name) ja SQL-kysely, joka palauttaa halutun datan tietokannasta. Lisäksi ”Build Database Query” -ikkunassa voidaan tarkastella tietokannassa olevien taulujen rakennetta ja halutessa hyödyntää esimerkiksi ”Validate SQL” -toimintoa, jolla tietokantakyselyn toimivuus ja tulokset voidaan esikatsella ennen kyselyn tallentamista.

Tässä tapauksessa SQL-kyselyn luomiseen käytettiin aiemmin ohjelmistojen testivaiheessa ohjelmoitua ”SDGW_configuration_helper.py”-ohjelmaa, joka generoi tietokantaan oikeanmuotoisen rakenteen ja palautti tarvittavat kyselyt tekstitiedostoihin.

Kyseisen ohjelman suorittamisen jälkeen tietokantakyselyt kopioitiin ohjelman kirjoittamista tekstitiedostoista SDGW:n sekä ”DI1” -että ”DI2”- tauluille, joiden kautta saadaan kyseisen ELT-2-anturin molempien digitaalitulojen tilatiedot.

Tietokantakyselyille annettiin nimiksi ”ELT1kVDI1query1” sekä ”ELT1kVDI2query1”. Lisäksi myöhemmin muodostettiin vielä vastaavalla tavalla kolmas kysely laitteiden akkujännitteitä varten. Tietokantakyselyn konfiguraatiota SDGW:ssa havainnollistetaan kuvassa 31.



Kuva 31. Tietokantakyselyn konfigurointi SDGW-ohjelmistossa

SDGW:ssa tietokantakysely suoritetaan, ja sen tulokset päivitetään kyseisen kyselyn alla olevan ”ExecuteQuery”-muuttujan tilan vaihtuessa. Lisäksi kysely voidaan määritellä suoritettavaksi myös tietokannasta haettavaa riviä osoittavan muuttujan tilan vaihtuessa tmwgtway.ini-tiedoston parametrejä muokkaamalla.

Käyttötarkoituksesta riippuen kyseiset muuttujat voidaan linkittää esimerkiksi jostain muusta järjestelmästä toista protokollaa käyttäen tuotavaan muuttujaan tai SDGW:n sisäiseen muuttujaan, jota käytetään esimerkiksi pollattaessa tietokantaa automaattisesti tietyn väliajoin.

Tätä tarkoitusta varten tilaa automaattisesti vaihtava sisäinen muuttuja voidaan luoda ohjelmistoon ”Add Equation” -toiminnolla, jolla generoidaan Square Equation ”square(0,1,5000)” (Triangle Microworks 2017, 190). Kyseisellä konfiguraatiolla varustettu muuttuja generoi square - eli kanttiaaltoa ensimmäisten kahden arvon välillä kolmannen arvon määrittelemin väliajoin.

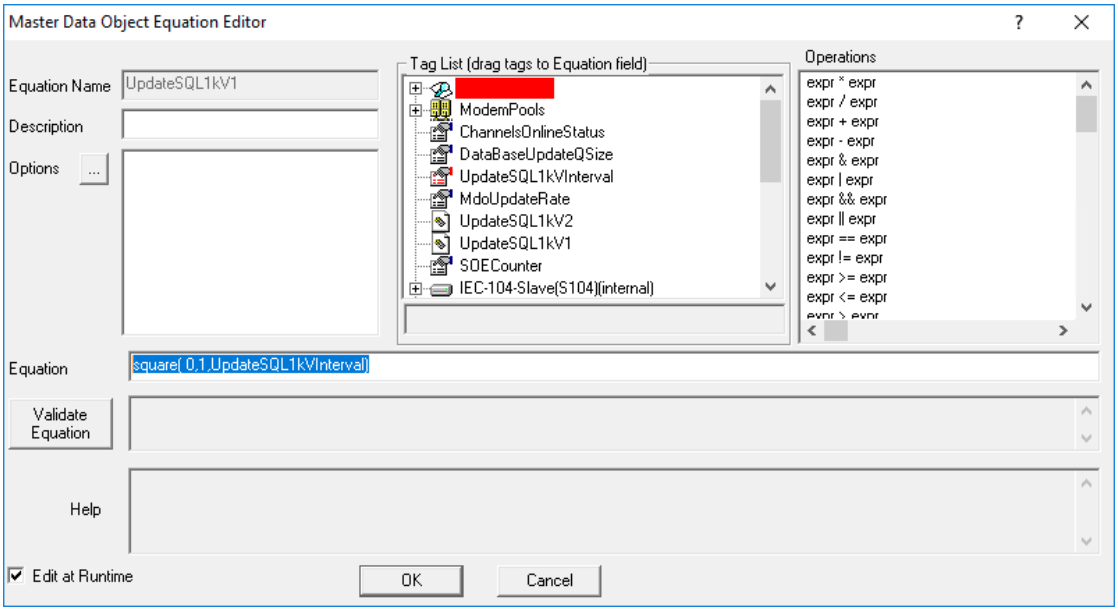
Tässä tapauksessa lopputuloksena on 0 ja 1 välillä tilaa 5000 millisekunnin välein vaihtava muuttuja, jolla voidaan esimerkiksi triggeröidä ExecuteQuery-muuttujaa tietokantakyselyissä. SDGW:ssa ei voida muokata enää toisiin datapisteisiin linkitettyä Equation-objektia, joten mikäli tietokannan pollausväliä halutaan myöhemmin helposti muokata, voidaan intervalaika tuoda Equationiin myös ulkoisesta MDO-objektista (Master Data Object).

Tässä tapauksessa kyseisen ajan muokkaaminen katsottiin mahdollisesti tarpeelliseksi ainakin aluksi konfigurointivaiheessa, joten ennen Equation-muuttujan luontia luotiin ”Add Internal MDO” -toiminnolla sisäinen, UI4 (unsigned long)-tyyppinen muuttuja, jolle annettiin arvoksi 2000 (millisekuntia). Tämän muuttujan nimeksi annettiin ”UpdateSQL1kVInterval”.

Tämän jälkeen luotiin varsinainen Equation-muuttuja, jolle annettiin nimeksi ”UpdateSQL1kV1” ja Equationiksi ”square(0,1,UpdateSQL1kVInterval)”, joka vastaa muutoin ohjelman dokumentaatiossa esitettyä, paitsi että intervalaika haetaan määritellystä, aiemmin luodusta erillisestä muuttujasta.

Lisäksi luotiin myös toinen vastaava Equation, jonka nimeksi annettiin ”UpdateSQL1kV2”, minkä tarkoituksena on vaihtaa tilaa eri aikaan ”UpdateSQL1kV1”-muuttujan kanssa ja millä voidaan haluttaessa tasata tietokantapalvelimen kuormaa suoritettaessa osa tietokantakyselyistä hieman eri aikoihin.

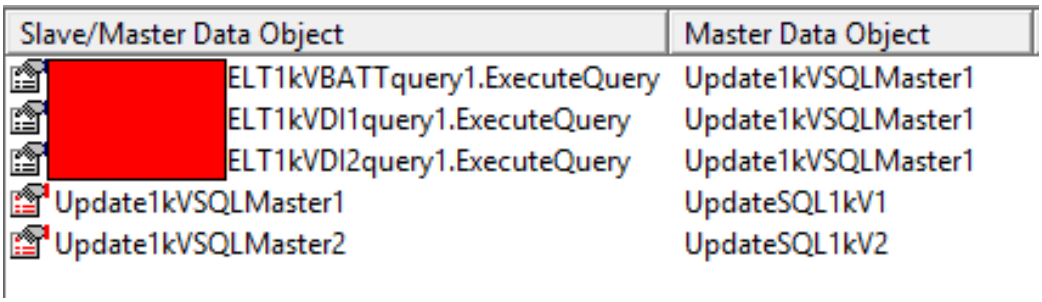
Tämä muodostettiin myös SDGW-ohjelman Equation Operation -toimintoja hyödyntämällä. ”UpdateSQL1kV1”-muuttujan konfiguraatiota havainnollistetaan kuvassa 32.



Kuva 32. ”UpdateSQL1kV1”-muuttujan konfiguraatio SDGW-ohjelmistossa

Jotta kyseistä muuttujaa voitiin käyttää useampiin tietokantakyselyihin samanaikaisesti, luotiin vielä BOOL-tyyppinen Internal MDO, jolle annettiin nimeksi ”Update1kVSQLMaster1”. Tämän jälkeen ”UpdateSQL1kV1”-muuttuja linkitettiin aluksi ”Update1kVSQLMaster1”-muuttujaan, joka taas vastaavasti linkitettiin tietokantakyselyiden ExecuteQuery-muuttujiin.

Vastaavat toimenpiteet tehtiin myös ”UpdateSQL1kV2”-muuttujalle, jota ei kuitenkaan vielä tässä vaiheessa käytetty varsinaisiin tietokantakyselyihin, vaan se jätettiin tulevaisuuden varalle, mikäli kyselyjen määrä lisääntyy merkittävästi. Kaikki tietokantakyselyjen suorittamiseksi tehdyt linkitykset esitetään kuvassa 33.

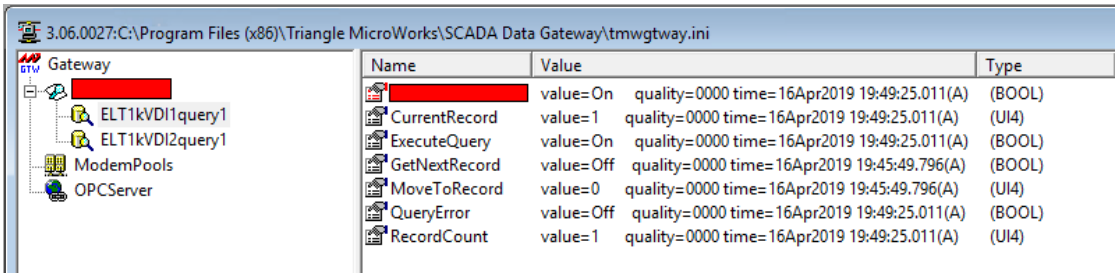


Kuva 33. UpdateSQL-objektien linkitykset tietokantakyselyiden ExecuteQuery-muuttujiin

Equation-tyyppisen muuttujan suora linkittäminen useampaan tietokantakyselyyn olisi aiheuttanut ohjelmiston käynnistyessä virheilmoituksen ja linkityksien poistumisen, jonka vuoksi linkittämisessä käytettiin apuna näitä Internal MDO -tyyppisiä muuttujia.

Näiden toimenpiteiden jälkeen SDGW oli konfiguroitu hakemaan tietokannasta kyseisiin tauluihin tallennettavat LoRaWAN-antureiden lähettämät viimeisimmät digitaalitulojen tilatiedot. Valmista tietokantakyselyä ja sen hetkistä testianturin DI1-tulolla valvotun katkaisijan tilaa havainnollistetaan kuvassa 34.

Kyseisessä kuvassa kärkitiedon tila on ”1/On”, mutta kyseinen parametri invertoidaan ”LoRaWAN_AppServer.py”-ohjelmassa anturin lähettämän payloadin käsittelyn yhteydessä, joten todellisuudessa kärkitieto oli auki. Kytkettäessä anturi katkaisijan lauetessa sulkeutuvalle apukoskettimelle, katkaisijan lauetessa kärkitieto sulkeutuu ja tilatieto ohjelmassa muuttuu ”0/Off”:ksi.



Kuva 34. Valmis tietokantakysely esitettynä SDGW-ohjelmistossa

Tietokantakyselyiden konfiguroimisen jälkeen Scada Data Gateway -ohjelmistoon piti vielä konfiguroida IEC-104-yhteys varsinaiseen SCADA-järjestelmään liittymistä varten, konfiguroida IEC-104-yhteyden vaatimat parametrit, luoda halutut IEC-104-datapisteet ja linkittää ne tietokantakyselyiden LoRaWAN-anturin digitaalitulojen arvot sisältäviin datapisteisiin.

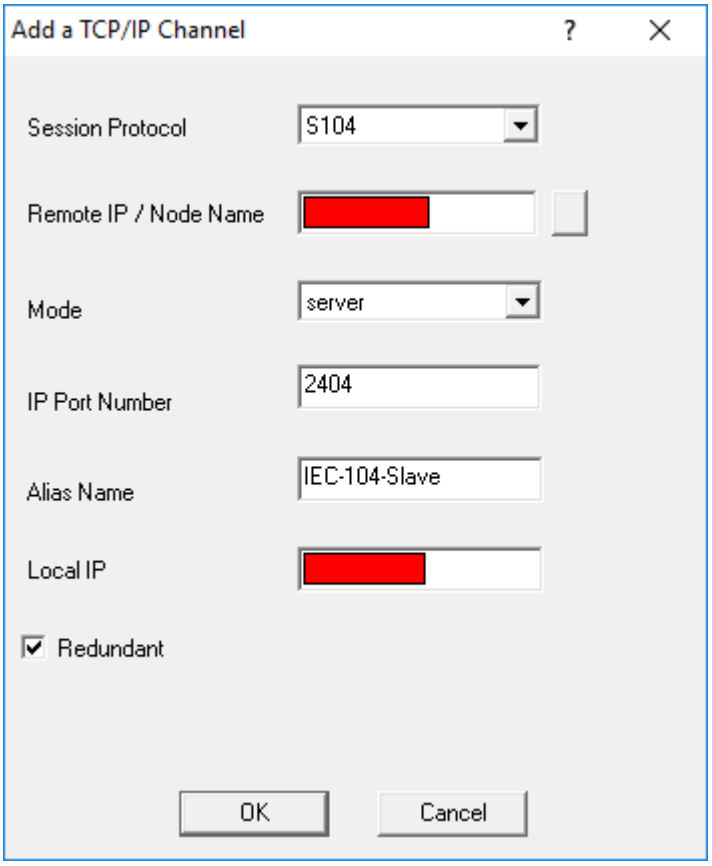
IEC-104-yhteyden konfigurointi ohjelmistoon tapahtuu ”Add TCP Channel” -toimintoa käyttämällä, jossa valitaan Session Protocol ”S104”, jolloin yhteys toimii IEC-104 slave -moodissa. Tämän jälkeen voidaan vielä varmistaa, että käytettynä modena on ”server”, TCP-portti on oikea (2404) ja määritellä ympäristössä käytettävät IP-osoitteet.

Remote IP -osoitteella tarkoitetaan kyseistä palvelinta pollaavan SCADA-järjestelmän palvelimen IP-osoitetta ja Local IP -osoitteella paikallista IP-osoitetta, jota luotava TCP Channel kuuntelee. Tähän voidaan määritellä myös arvoksi 0.0.0.0, mikäli halutaan, että ohjelmisto kuuntelee kaikkien palvelimen verkkosovittimien IP-osoitteita.

Lisäksi valitaan vielä ”Redundant”-optio, jolloin voidaan muodostaa Redundancy Group konfiguroimalla useita vaihtoehtoisia IEC-104-yhteyksiä useille eri SCADA-järjestelmän palvelimille siltä varalta, että johonkin niistä tulee häiriöitä tai tietoliikenne kyseiseltä palvelimelta on jostain syystä estynyt.

Redundancy Groupia käytettäessä tällaisessa tapauksessa liikenne siirtyy automaattisesti käyttämään jotain varalla olleista yhteyksistä. Redundancy Groupin lisäyhteydet ja yhteyksien nimet voidaan konfiguroida ohjelmistossa myöhemmin ensimmäisen yhteyden konfiguroimisen jälkeen.

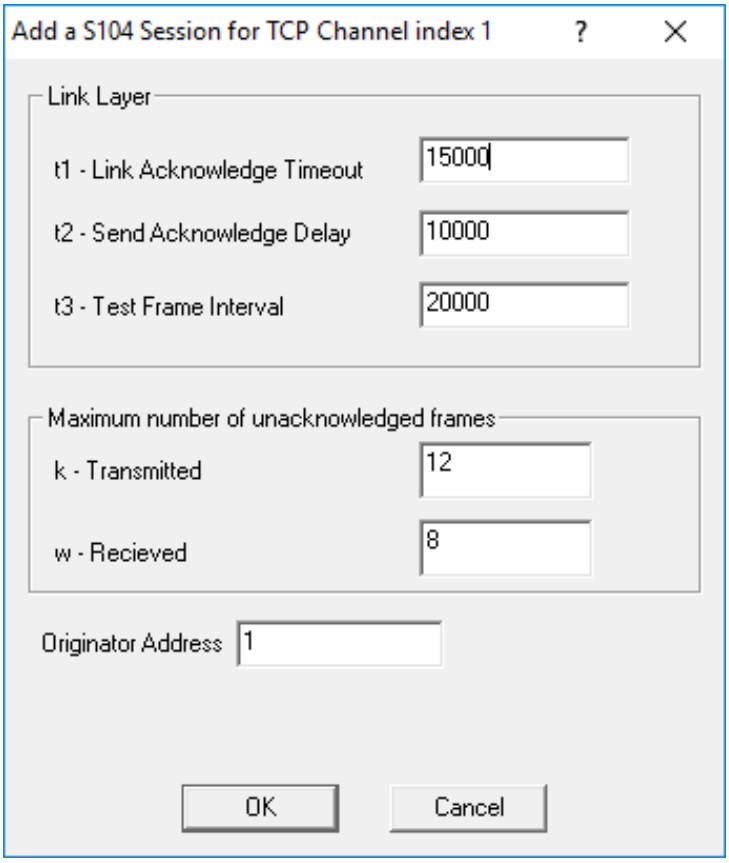
IEC-104 slave -yhteyden konfiguraatiota havainnollistetaan kuvassa 35.



Kuva 35. ”IEC-104 Slave” -yhteyden lisääminen SDGW-ohjelmistoon

Lisäksi IEC-104-yhteydelle on määritettävä vähintään yksi sessio, jolle on määritettävä protokollan vaatimat linkkiparametrit ja linkki/laiteosoite, josta tässä tapauksessa käytetään nimitystä ”Originator Address”.

Kuvassa 36 havainnollistetaan näitä asetuksia Scada Data Gateway -ohjelmiston antamia oletusarvoja käyttäen.



Kuva 36. IEC-104 slave -session parametrit SDGW-ohjelmiston oletusasetuksilla

Kyseisten parametrien selitykset esitetään taulukossa 11.

Taulukko 11. IEC-104-yhteyden parametrien selitykset (Triangle Microworks 2017, 89)

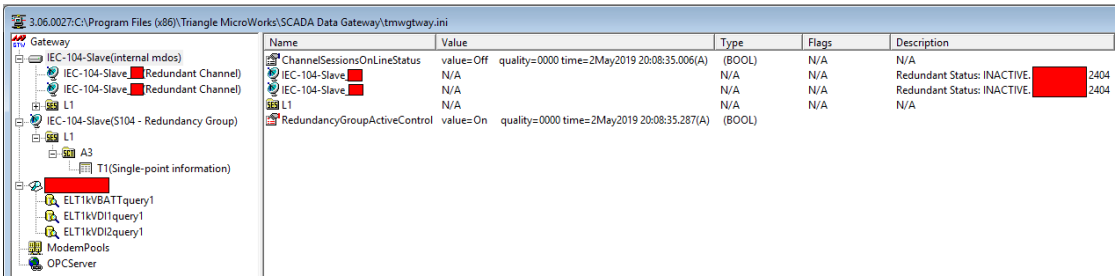
Parameter	Description
T1 - Link Acknowledge Timeout	The maximum amount of time (in milliseconds) to wait for a confirmation of frame
T2 – Send Acknowledge Delay	Maximum time (in milliseconds) to wait to send an Acknowledge frame
T3 – Test Frame Interval	Time (in milliseconds) for the Test Frame interval
K – Transmitted	Maximum number of unacknowledged transmit frames
W – Received	Maximum number of unacknowledged received frames

Parametrien konfiguroinnissa on huomioitava, että Master- ja Slave-asemille konfiguroidut arvot vastaavat toisiaan eivätkä ole ristiriidassa toistensa

kanssa. Esimerkiksi, mikäli toisen pään ”t2”-parametri olisi suurempi kuin toisen pään ”t1”, toinen laite voisi katsoa yhteyden jo katkenneeksi ennen kuin toinen edes lähettäisi Acknowledge-kehystä (IEC-104:n S-tyypin APDU:ssa).

Lisäksi laitteiden välisen verkkoyhteyden latenssin vaikutus tulee myös ottaa huomioon konfiguroitaessa kyseisiä arvoja. Normaalisti voidaan käyttää standardin mukaisia oletusarvoja mitkä SDGW-ohjelmisto automaattisesti valitsee, mikäli SCADA-järjestelmässä ei ole tehty näihin muutoksia, tai haluta esimerkiksi minimoida käytön mukaan laskutettavan verkkoyhteyden yli siirrettävää dataa ei-kriittisen yhteyden tapauksessa, milloin voitaisiin esimerkiksi suurentaa ”t3”-arvoa.

Näiden lisäksi luotuun Redundancy Groupiin lisättiin toinen yhteys ”Add Redundant Channel” -toiminnon avulla. Vaihtoehtoisten yhteyksien konfigurointi tapahtuu tämän jälkeen muutoin samaan tapaan kuin ensimmäisenkin yhteyden. Valmiin IEC-104 Redundancy Groupin konfiguraatiota esitetään kuvassa 37.



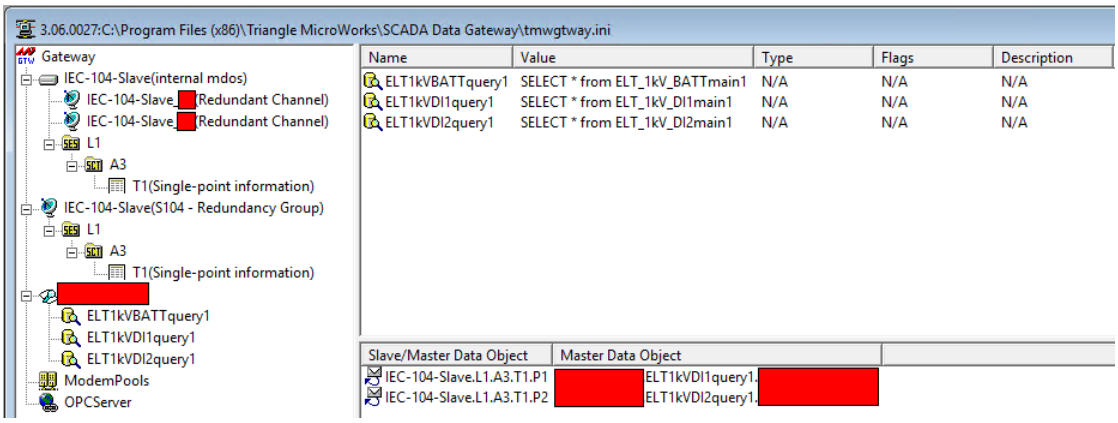
Kuva 37. IEC-104 Redundancy Group -konfiguraatio SDGW-ohjelmistossa. Kuvassa molemmat konfiguroidut yhteydet vielä ei-aktiivisia, koska tietoliikenneyhteys SCADAan ei ollut kyseisellä hetkellä palomuurista sallittu.

Näiden parametrien konfiguroinnin jälkeen SDGW-ohjelmistolle tarvitsee enää antaa aiemmin luodun session/linkkiosoitteen alle ensimmäinen käytettävä Sector Address, eli ASDU:n Common Address sekä ASDU:n datatyyppi.

Tässä tapauksessa datatyypiksi valittiin ”T1 (Single-point information)”, joka tarkoittaa IEC-104-datatyyppiä M_SP_NA_1. Kyseinen datatyyppi välittää On/Off-informaatiota Monitor-suuntaan, eli esimerkiksi ala-asemalta SCADA-järjestelmään.

Myöhemmin saman IEC-104 slave -yhteyden alle voidaan myös lisätä uusia Sector Addresseja tai ASDU:n datatyyppejä. Varsinainen datapisteiden liittäminen toisiinsa tapahtuu navigoimalla käyttöliittymässä Master Data Objectit eli liitettävät objektit sisältävään näkymään, josta objektit voidaan liittää IEC-104-slaven datapisteisiin vetämällä ne hiirellä halutun Sector Addressin alla olevan datatyypin kohdalle.

Tässä tapauksessa siirryttiin aiemmin luotuihin tietokantakyselynäkymiin, joista vedettiin testianturilta saatavat DI1- ja DI2-digitaalitulojen tilat IEC-104-slaven T1-datatyypin alle. Tämän jälkeen ohjelmisto kysyy vielä uusille IEC-104-datapisteille määritettäviä pisteosoitteita, joiksi annettiin tässä tapauksessa 1 ja 2. Valmista SDGW-ohjelmiston konfiguraatiota ja liitettyjä datapisteitä havainnollistetaan kuvassa 38.



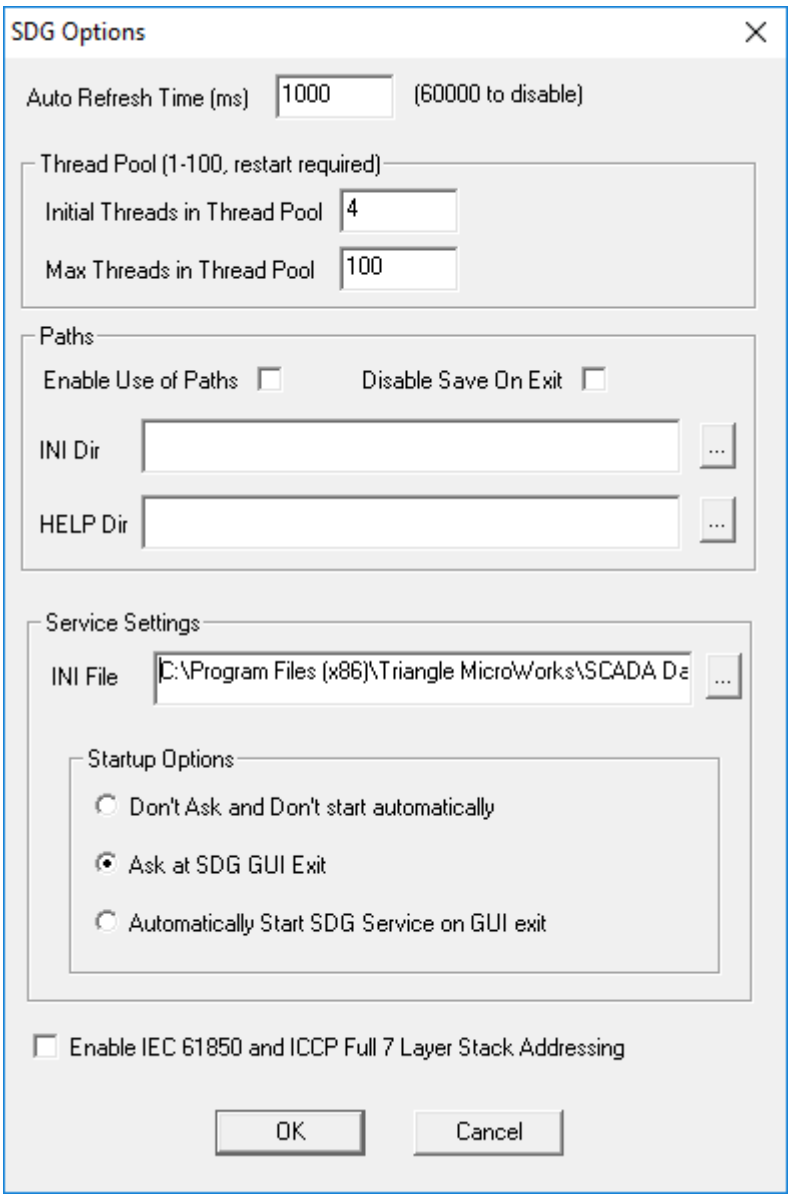
Kuva 38. Havainnekuva valmiista SDGW-ohjelmiston konfiguraatiosta tietokantakyselyiden ja IEC-104 slave -yhteyden sekä näiden välille liitettyjen datapisteiden osalta

Suuria määriä voitaisiin myös konfiguroida mahdollisesti skriptaamalla ohjelman käyttämien konfiguraatiotiedostojen editointia, jota ei kuitenkaan tämän opinnäytetyön yhteydessä toistaiseksi toteutettu, sillä manuaalista konfigurointia tarvitaan kuitenkin esimerkiksi SCADA-järjestelmän osalta.

Tämä saatetaan kuitenkin toteuttaa myöhemmin, mikäli jatkokehitysprojektien yhteydessä havaitaan esiintyvän tarvetta konfiguroida nopeasti suuria laitemääriä.

Tietokantakyselyiden, IEC-104 slave -yhteyden ja näiden välisten datapisteiden konfiguroinnin jälkeen SDGW-ohjelmisto pitää vielä määrittää käynnistymään Windows Servicenä, jotta ohjelmisto pystyy toimimaan, vaikka palvelimelle ei olisi käyttäjä kirjautuneena.

Tämä tapahtuu ”SDG Options” -valintaikkunasta, jossa määritellään servicelle käytettävä asetustiedosto, joka yleensä on sama kuin GUI:ssa käytetty. Tämä kyseinen tiedosto on oletuksena nimeltään tmwgtway.ini ja sijaitsee ohjelmiston asennushakemistossa. Tämän lisäksi määritellään vielä tarvittaessa servicen käynnistäminen automaattisesti tai kysyttäessä suljettaessa GUI-ikkuna. Näitä asetuksia havainnollistetaan kuvassa 39.

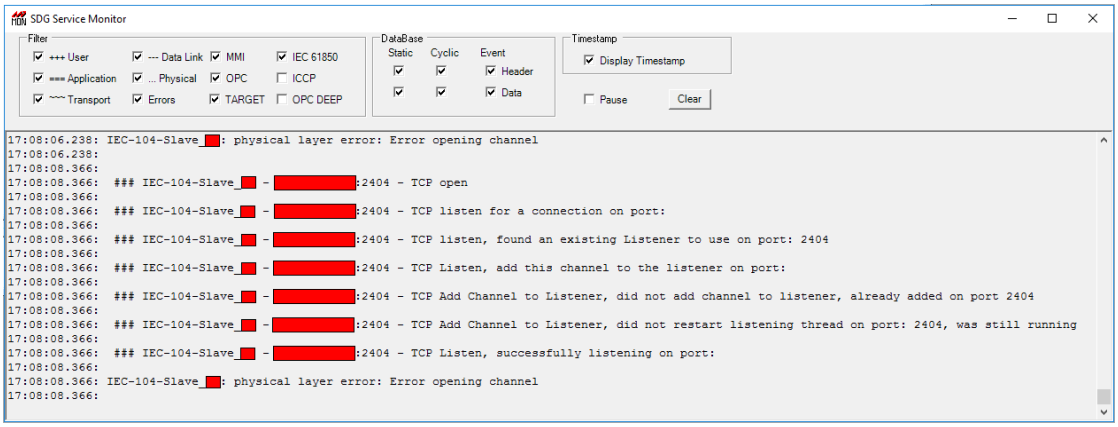


Kuva 39. SDGW-ohjelmiston Windows Servicen määrittelyt

Windowsin ”services.msc”-konsolista voidaan vielä käydä tarkistamassa ”GTWService”:n Startup type ja varmistaa, että se käynnistyy automaattisesti Windowsin mukana palvelimen käynnistyessä. Lisäksi konsolista voidaan tarkastella servicen sen hetkistä tilaa sekä tarvittaessa käynnistää ja pysäyttää kyseinen palvelu. Toimintaa voidaan myös tarkkailla ”SDG Service Monitor” -työkalulla, joka asentuu SDGW-ohjelmiston mukana.

SDG Service Monitorilla pystytään esimerkiksi tarkkailemaan IEC-104-yhteyksien tilaa ja havaitsemaan niissä olevat mahdolliset ongelmat tarvitsematta avata varsinaista GUI-käyttöliittymää, joka pysäyttäisi servicenä suoritettavan SDGW-instanssin, joka taas voisi mahdollisesti aiheuttaa hetkellisiä virheilmoituksia muissa siihen yhteydessä olevissa järjestelmissä.

Kuvassa 40 havainnollistetaan SDG Service Monitorin käyttöä vikatilannetta selvitettäessä, kyseisessä havainnekuvassa IEC-104-yhteydet SCADA-järjestelmään ovat poikki, joka voi johtua esimerkiksi puutteellisesta palomuuri- tai SCADA-järjestelmän konfiguraatiosta.



Kuva 40. IEC-104-yhteyksien vikatilanne esitettynä ”SDG Service Monitor” -työkalun näkymässä

Lisäksi toiminnan tarkastelemiseksi on mahdollista esimerkiksi ”netstat -nb” -komentoa hyödyntämällä katsoa, onko SDGW-ohjelmistosta avoimia yhteyksiä tietokantaan tai SCADA-järjestelmään MySQL:n (TCP3306) tai IEC-104:n (TCP2404) käyttämissä porteissa.

Lopullinen ohjelman toimivuus ja konfiguraation oikeellisuus kuitenkin selviävät myös SCADA-järjestelmän konfiguroimisen ja järjestelmän testaamisen yhteydessä.

7.6 SCADA-järjestelmän konfigurointi ja toiminnan testaaminen

SCADA-järjestelmän konfigurointi suoritettiin suoraan olemassa olevaan tuotantojärjestelmään yhteistyössä järjestelmän pääkäyttäjän kanssa, eikä sitä tulla käsittelemään tässä opinnäytetyössä yksityiskohtaisesti.

Pääpiirteittäin esivalmisteluina SCADA-järjestelmän palvelimilta sallittiin verkon palomuureista yhteys Application Serverille IEC-104-protokollan käyttämään porttiin TCP2404 ja määritettiin yhteydelle tarvittavat reitit ykset.

Tämän jälkeen SCADA-järjestelmään määriteltiin Application Serverillä suoritettavalta Scada Data Gateway -ohjelmistolta haettavat, aikaisemmassa kohdassa luodut IEC-104-datapisteet, jotka sisältävät LoRaWAN-laitteilta vastaanotetut viimeisimmät mittausarvot.

Näiden datapisteiden konfigurointi SCADA-järjestelmän osalta tapahtui tavalliseen tapaan aivan kuten minkä tahansa standardia IEC-104-protokollaa käyttävän sähköverkkoautomaatiolaitteen tapauksessa.

Lisäksi kyseisille pisteille määritettiin myös esimerkiksi tarvittavat hälytys- ym. asetukset, joiden avulla SCADA-järjestelmä osaa luoda esimerkiksi tarvittavat tapahtumat ja antaa hälytykset esimerkiksi valvottujen 1 kV katkaisijoiden lauetessa. SCADA-järjestelmään tehtiin myös grafiikkakuva, jossa esitetään valvottujen katkaisijoiden tilatietoja.

SCADA-järjestelmän konfiguroinnin jälkeen todettiin järjestelmän toimivuus toteamalla, että Application Serverin ja SCADA-järjestelmän väliset IEC-104-yhteydet muuttuivat aktiivisiksi sekä SDGW-ohjelmistoon määriteltyjen datapisteiden sisältämät tietokannasta haetut arvot siirtyivät onnistuneesti SCADA-järjestelmään.

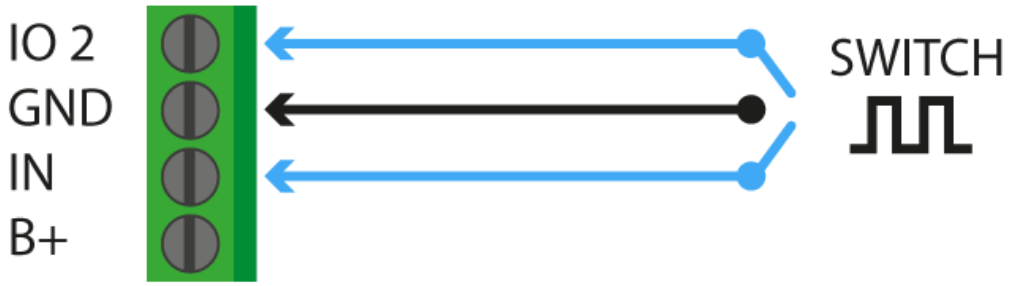
Lisäksi toteutettiin käytännön toimivuuskoe kytkemällä LoRaWAN-anturin digitaalituloon 1 kV katkaisijan apukosketinta mallintava johdonsuojakatkaisija, joka laukaistiin käsin ja todettiin, että SCADA-järjestelmään tuotu kyseisen testianturin valvoma ”katkaisijan tilatieto” muuttui vastaavasti ja esimerkiksi järjestelmään konfiguroidut hälytykset toimivat suunnitellusti.

Kyseisen kokeen tulosten perusteella ratkaisu 1 kV katkaisijan tai minkä tahansa muun digitaalisen tilatiedon siirtämiseksi LoRaWAN-anturilta SCADA-järjestelmään todettiin kokonaisuudessaan toimivaksi.

7.7 Anturin asennus 1 kV:n katkaisijalle

Anturin sähköinen kytkentä 1 kV katkaisijalle tapahtuu johdottamalla anturin ulkoinen input katkaisijan lauetessa sulkeutuvalle apukoskettimelle. Katkaisijan lauetessa sulkeutuvaa, normaalisti auki olevaa kosketinta käytetään, jotta normaalitilanteessa pull-up -virta ei aiheuta tarpeetonta paristonkulutusta anturilla.

Käytetyssä Elsys ELT-2 -anturissa digitaalitulot ”Switch NO” -moodissa ovat vedetty ylös anturin sisäisillä pull-up -vastuksilla, jolloin valvottavat koskettimet tulee kytkeä anturin GND-nastan ja sisääntulojen välille. Kytkentäkaavio kytkintiedoille on nähtävillä kuvassa 41.



Kuva 41. Havainnekuva kärkitietojen kytkennästä Elsys ELT-2 -anturille sisääntulojen pull-up -tilaa käytettäessä (Elsys s.a.a, muokattu)

Toiselle sisääntulolle voidaan lisäksi johdottaa esimerkiksi katkaisijan yhteydessä sijaitsevan ylijännitesuojan vioittumista ilmaiseva tai maasulkulaukai-

suelektroniikalta saatava maasulun yhteydessä laukeava kärkitieto, jolloin voidaan valvomossa erottaa katkaisijan ylivirta- ja maasulkulaukaisut toisistaan tai saada tieto ylijännitesuojan vikaantumisesta.

Toista anturin digitaalituloa voidaan käyttää maasulkulaukaisun lisäksi myös osittain esimerkiksi ylijännitesuojan vikaantumisen selvittämiseksi ottamalla asia huomioon Application Serverin ohjelmoinnissa, mutta tässä tapauksessa ylijännitesuojan ollessa jo valmiiksi vikaantunut ei maasulkulaukaisua kyetä erottamaan, sekä mahdollinen katkaisijan virhetoiminto maasulkulaukaisun yhteydessä saattaa indikoitua ylijännitesuojavikana.

Elsys ELT-2 -anturissa on ulkoisten tulojen kytkemiseksi M12x1,5-holkkitiiviste kaapelin läpivientiä varten. Kyseisenlainen holkkitiiviste soveltuu halkaisijaltaan 4,5–7 mm:n kaapelille (Lapp Group 2016). Kytkettäessä kaksi kärkitietoa on kaapelissa oltava vähintään kolme johdinta ja haluttaessa tuoda molemmat kärkitiedot suoraan anturin liittimille, 4 johdinta.

Tämänkaltaiseen käyttötarkoitukseen soveltuva kaapeli on esimerkiksi MHS 3x2x0.5 tai KLMA 4x0.8, joissa on MHS:ssä kolme kappaletta kahden 0,5 mm^2 johtimen muodostamaa paria ja KLMA:ssa neljä 0,8 mm^2 johdinta sekä molempien kaapeleiden ulkohalkaisija on 5,5 mm (Prysmian Group 2018a; Prysmian Group 2018b).

Molempien kaapeleiden johtimien poikkipinta-ala riittää tähän käyttötarkoitukseen, sillä johtimessa kulkee maksimissaan laskennallisesti 144 mikroampeerin virta yhteisessä GND-johtimessa sitä käytettäessä ja molempien kärkitietojen ollessa suljettuna.

Nämä kaapelit ovat kuitenkin sisäasennukseen tarkoitettu, jolloin niiden käyttäminen asennettaessa anturi ulos ei ole suositeltavaa. Asennettaessa anturi ulos on vastaava soveltuva kaapeli esimerkiksi aiemmin mainittua MHS-kaapelia vastaava VMOHBU 3x2x0.5, jonka ulkohalkaisija on 9,5 mm (Prysmian Group 2018c).

Tämänkaltaisen kaapelin asentaminen M12x1,5-holkkitiivisteeseen on kaapelin hieman liian suuresta ulkohalkaisijasta johtuen kuitenkin todennäköisesti

suhteellisen vaikeaa, ellei jopa mahdotonta, ja voisi onnistuessaankin vaatia kyseisen holkkitiivisteen modifiointia esimerkiksi kaapelin läpimenoaukkoa suurentamalla.

Mikäli holkkitiivisteeseen soveltuvaa vastaavaa ulkoasennuskaapelia ei ole saatavilla, voitaisiin mahdollisesti myös ulos asennettaessa käyttää esimerkiksi aiemmin mainittuja sisäasennuskaapeleita suojaamalla kaapeli JAPP-putkella tai muulla vastaavalla menetelmällä ja suorittamalla asennus kesäaikana ulkolämpötilan ollessa riittävän korkea, milloin kaapeli todennäköisesti kestäisi myös ulkokäytössä.

Anturin fyysinen asennus katkaisijalle on mahdollista esimerkiksi asentamalla anturi kokonaisuudessaan ulos ja ruuvaamalla se kiinni pylvääseen tai katkaisijan sisältävään pylväsasennuskoteloon ja johdottamalla kaapeli anturilta pylväsasennuskotelon sisälle normaalisti läpivientien kautta.

Asennus voitaisiin myös suorittaa sijoittamalla anturi itsessään pylväsasennuskotelon sisälle ja tuomalla vain antenni ulos joko erillisellä jatkokaapelilla tai suoraan pujottamalla se ulos pylväsasennuskoteloon poratun reiän kautta. Tässä menetelmässä anturi itsessään olisi paremmin suojassa esimerkiksi sääolosuhteiden vaikutuksilta ja mahdolliselta ilkivallalta.

Ilkivallalta suojautumiseksi anturin asennus olisi ainakin teoriassa mahdollista myös ylemmäs pylvääseen, joka voisi myös parantaa verkon kuuluvuutta antennikorkeuden kasvaessa. Tässä tapauksessa kuitenkin esimerkiksi anturin pariston vaihtamista varten asentajan olisi mahdollisesti kiivettävä pylvääseen, joka vaikeuttaisi huoltotoimenpiteiden suorittamista ja lisäisi niistä aiheutuvia kustannuksia.

Käytettäessä jatkokaapelia antennissa on myös huomioitava antennikaapelin aiheuttama vaimennus ja tarvittaessa käytettävä suuremmalla vahvistuksella varustettua antennia riittävän lähetystehon säilyttämiseksi. Antennin valinnassa tulee kuitenkin huomioida LoRaWANin käyttämän taajuusalueen lähetystehorajoitukset, ettei mahdollisesti huomattavasti alkuperäistä suurempi antennin vahvistus aiheuta sallittua suurempaa lähetystehoa antennikaapelin vaimennuksesta huolimatta.

Tarkkaa anturin fyysistä asennustapaa ei tulla määrittelemään tämän opinnäytetyön yhteydessä, vaan se tullaan suunnittelemaan myöhemmin verkon kuuluvuuskokeiden yhteydessä, jolloin tutkitaan myös laitteen ja antennin sijoittelun vaikutusta verkon kuuluvuuteen ja voidaan ottaa nämä huomioon anturin asennustavan määrittelyssä.

8 LOPPUTULOS

Opinnäytetyön käytännön osuuden tuloksena saatiin toteutettua Suur-Savon Sähkön / Järvi-Suomen Energian käyttöön IoT-teknologiaan perustuva valvontaratkaisu 1 kV:n katkaisijoille LoRaWAN-tekniikkaa käyttäen, kuten lähtötavoitteissa oli määritelty. Opinnäytetyön tavoitteet voidaan siis katsoa tämän osalta saavutetuiksi.

Ratkaisussa käytettiin pilottilaitteena katkaisijoille soveltuvaa Elsys ELT-2-HP -anturia, jolla pystytään esimerkiksi lukemaan ulkoisia digitaalitietoja, jollaisena tieto katkaisijan tilasta on saatavilla. Lisäksi käytetyssä anturissa on toisen ulkoisen tulon johdosta myös mahdollisuus esimerkiksi katkaisijan yhteydessä olevien ylijännitesuojien vikatiedon tai maasulkuelektroniikan antaman maasulkulaukaisun indikoinnin valvomiseen. Vastaavia antureita on myös saatavilla muilta valmistajilta sekä myöskin tätä kyseistä käytettyä anturimallia voidaan hyödyntää kattavasti myös monissa muissa, erilaisissa kohteissa.

Opinnäytetyön yhteydessä perehdyttiin erilaisiin IoT-teknologioihin ja erityisesti valittuun LoRaWAN-teknologiaan teoreettisella tasolla, minkä pohjalta optimoitiin anturin konfiguraatio kyseiseen käyttötarkoitukseen parhaiten soveltuvaksi. LoRaWAN-verkkona hyödynnettiin Digitan kaupallista verkkoa, joka kattaa jo opinnäytetyön tekohetkellä osan Järvi-Suomen Energian verkkoalueella olevien 1 kV katkaisijoiden sijainneista.

Lisäksi toteutettiin Application Server -palvelin datan vastaanottoon Digitan käyttämältä Actility ThingPark -verkkoalustalta ja sen jatkokäsittelyyn, tietokantaan tallentamiseen sekä katkaisijoiden tilatietojen viemiseen olemassa olevaan SCADA-järjestelmään IEC-104-protokollaa käyttäen, kuten lähtötavoitteeksi oli määritelty.

Ratkaisun toimivuus testattiin myös kokonaisuudessaan käytännön olosuhteita vastaavasti, ja järjestelmä todettiin toimivaksi sekä kyseiseen käyttötarkoitukseen soveltuvaksi. Lisäksi sitä verrattiin perinteisellä sähköverkkoautomaatiolla toteutettuun vastaavaan ratkaisuun, ja todettiin IoT-teknologialla toteutettu ratkaisu tähän verrattuna huomattavasti käyttökelpoisemmaksi tämänkaltaisiin kohteisiin.

Opinnäytetyön yhteydessä kehitetty ratkaisu tarjoaa lisäksi hyvän pohjan lähteä laajentamaan esimerkiksi LoRaWAN-tekniikan käyttöä myös mahdollisesti muihin käyttökohteisiin tai ottaa käyttöön joitain toisia IoT-teknologioita ja saada niitä käyttäviltä laitteilta tietoa siirrettyä SCADA-järjestelmään. Esimerkkejä näistä jatkokehityssuunnitelmia käsitellään seuraavassa pääkappaleessa.

8.1 Vertailu valvontaratkaisuun perinteisellä sähköverkkoautomaatiolla

Vastaavan valvontaratkaisun rakentaminen 1 kV katkaisijalle perinteistä sähköverkkoautomaatiota käyttäen olisi vaatinut katkaisijan tilatiedon valvontaan tarvittavan, IEC-104-protokollaa käyttävän digitaalituloja sisältävän RTU-laitteen sekä mahdollisesti erillisen, tietoliikenneyhteyden muodostamiseen tarvittavan laitteen, näiden vaatiman virtalähteen sekä akuston jännitteensyötön katkeamisen varalta.

Tämänkaltaisten laitteiden sijoittaminen ei myöskään olisi välttämättä ollut mahdollista olemassa olevaan pylväsasennuskoteloon, vaan niille olisi jouduttu rakentamaan erillinen laitetila laitteiden määrän ja tilantarpeen johdosta.

Lisäksi laitteille olisi pitänyt järjestää myös 230 V omakäyttösähkö, joka olisi joko jouduttu tekemään paikallisesti omakäyttömuuntajalla 20 kV- tai 1 kV -verkosta tai tuomaan kauempaa 0,4 kV -verkon piiristä, mikäli katkaisija-asemalla ei sitä valmiiksi olisi muuten ollut saatavilla.

Tämänkaltaisen automaation käyttämisen ei siis voida olettaa olevan kovin kustannustehokasta esimerkiksi 1kV-katkaisijalla siitä saatavaan hyötyyn näh-

den. 1 kV:n katkaisijan takana on pääosin vain muutamia asiakkaita, joten kyseisen automaatioinvestoinnin tekeminen jokaiselle katkaisijalle ei olisi välttämättä kovinkaan perusteltua.

IoT-teknologiaan perustuvalla ratkaisulla katkaisijalle tarvitsee sijoittaa vain yksi, jo olemassa olevaan pylväsasennuskoteloon helposti sijoitettavissa oleva laite, eikä esimerkiksi erillistä akustoa tai omakäyttösähköä tarvita. Tämän johdosta IoT-teknologiaan perustuvan valvontaratkaisun käyttöönottokustannukset jäävät perinteiseen sähköverkkoautomaatioon verrattuna alhaisemmaksi, mikä mahdollistaa valvonnan käyttöönoton myös tämänkaltaisilla kohteilla, jotka eivät palvele suuria asiakasmääriä.

IoT-laitteen sisäinen akku joudutaan vaihtamaan määräaikaistarkastusten yhteydessä, mutta myös perinteisellä automaatioratkaisulla akusto olisi uusittava määräajoin riittävän varakäyntiajan turvaamiseksi. Molemmissa ratkaisuissa tarvitaan myös tietoliikenneyhteys jollakin tekniikalla, josta aiheutuu kuluja, joita ei kuitenkaan tämän pääpiirteittäisen tarkastelun yhteydessä ole tarvetta eritellä sen tarkemmin eri tekniikoiden välillä, eikä sitä myöskään voitaisi suorittaa tarkkoja arvoja käyttäen kyseisen informaation ollessa luottamuksellista.

Perinteisellä sähköverkkoautomaatiolla toteutettu ratkaisu voidaan kuitenkin mieltää luotettavammaksi kuin tämänkaltaisella IoT-teknologialla toteutettu, sillä perinteisen sähköverkkoautomaation laitteet ovat esimerkiksi jatkuvassa yhteydessä SCADA-järjestelmään ja pienetkin ongelmat ja poikkeamat esimerkiksi tietoliikenneyhteyksissä tai laitteiden toiminnassa havaitaan välittömästi.

Tässä tapauksessa kuitenkaan esimerkiksi nämä 1 kV katkaisijoiden tilatiedot eivät ole niin kriittisiä, että mahdollisesti joskus tapahtuvat yksittäiset vikatapaukset valvonnassa aiheuttaisivat tarvetta perinteisen sähköverkkoautomaation mahdollistamalle luotettavuudelle, sillä esimerkiksi tällä hetkellä valvontaa ei 1 kV katkaisijoilla ole lainkaan.

IoT-teknologia tässä muodossaan voidaankin katsoa juuri tämänkaltaisiin käyttökohteisiin hyvin soveltuvaksi ja käyttökelpoiseksi sähköverkoissa perinteisen automaation lisänä niissä kohteissa, joissa perinteisen automaation

käyttäminen ei olisi järkevää ja mitkä ovat mahdollisesti tämän johdosta tällä hetkellä kokonaan ilman valvontaa.

9 JATKOKEHITYSSUUNNITELMIA

1 kV katkaisijoiden valvonnan suhteen aletaan todennäköisesti asentaa LoRaWAN-antureita katkaisija-asemille seuraavien määräaikaistarkastusten yhteydessä. Tämän yhteydessä tullaan myös mahdollisesti testaamaan ja käyttämään muutamia erilaisia LoRaWAN-antureita useamman eri laitevalmistajan valikoimasta.

Useamman eri valmistajan tuotteita käyttämällä voidaan hankkia kenttäkokemuksia eri tuotteista ja pienentää esimerkiksi mahdollisesti jossain tuotantoerässä olevan viallisen komponentin aiheuttaman antureiden ennenaikaisen hajoamisen vaikutuksia, mikäli kaikki asennetut anturit eivät ole samanlaisia.

LoRaWAN-verkon kuuluvuuden suhteen tullaan lisäksi tekemään kokeita ja näiden perusteella tarkastelemaan jakelualueen 1 kV:n katkaisijoiden sijoittumista olemassa oleviin Digitan LoRaWAN-tukiasemiin nähden ja mahdollista lisätukiasemien tarvetta ja niiden sijoittelua. Tässä voidaan käyttää apuna lisäksi Digitan LoRaWAN-verkon peittoaluekarttaa, jonka määrittelemään peittoalueeseen toteutuneita tuloksia voidaan verrata.

Lisäksi LoRaWAN-tekniikan käyttöaluetta tullaan mahdollisesti laajentamaan myös muihin, uusiin valvontakohteisiin 1 kV katkaisijoiden lisäksi, erityisesti kun ”infra” sen käyttöön on jo pääpiirteittäin olemassa. Vastaavalla, kärkitiedon lukemiseen perustuvalla konseptilla voidaan myös suoraan valvoa esimerkiksi maastoon sijoitettuja, käsikäyttöisiä 110 kV erottimia, joilla ei myöskään ole tällä hetkellä mitään valvontaa.

Muita valvontakohteita voisivat olla esimerkiksi katujakokaappien valvonta mahdollisesti kiihtyvyys- ja/tai valoisuusantureiden avulla, joilla voitaisiin havaita esimerkiksi lumenauraustöiden yhteydessä tai ilkivallan vuoksi vaurioituneet kaapit, joissa jännitteelliset osat ovat mahdollisesti paljaana kosketeltavissa.

Kiihtyvyysantureiden käyttö myös esimerkiksi erilaisten radiomastojen värähtelyn mittaamiseen ja tästä saatava mittausdata voisi olla hyödyllistä esimerkiksi mastojen lumikuormatilanteen seuraamiseksi ja mahdollistaa joidenkin alkavien vaurioiden havaitsemisen riittävän ajoissa.

LoRaWAN-tekniikkaan perustuvia antureita voitaisiin mahdollisesti käyttää myös yhdessä virta- ja jännitemuuntajien kanssa esimerkiksi sähkönlaatuongelmien selvittämisessä, mikäli riittävään mittaustarkkuuteen yltäviä antureita on olemassa tai tulee tulevaisuudessa markkinoille. Näissä tapauksissa voitaisiin myös tarkastella esimerkiksi matkapuhelinverkkoa hyödyntäviä antureita, mitkä voisivat olla tämänkaltaiseen käyttötarkoitukseen soveltuvampia.

Mahdollisesti myös sähköasema-alueilla voi olla runsaasti erilaisia mittauskohteita, joita ei tällä hetkellä valvota ja joihin tekniikkaa voitaisiin hyödyntää. Sähköasema-alueilla edellytykset myös perinteisellä sähköverkkoautomaatiolla toteutetulle valvonnalle ovat toki huomattavasti paremmat kuin esimerkiksi 1 kV katkaisijoilla, mutta siitä huolimatta myös näillä alueilla voi olla valvontakohteita, joiden toteuttaminen perinteisellä automaatiolla ei kuitenkaan ole järkevää.

Sähköasema-alueita ja muita vastaavia, mahdollisesti tulevaisuudessa suuren laitemäärän sisältäviä alueita ja niiden lähiympäristöä palvelemaan voitaisiin mahdollisesti perustaa myös omaa LoRaWAN-verkkoa, jota voitaisiin myös tarvittaessa ulottaa kattamaan kaikkien LoRaWAN-laitteiden sijainnit, mikäli tukiasemia voidaan järkevästi sijoitella riittävä määrä kyseisten laitteiden sijaintialueen kattamiseksi.

Lisäksi datan vastaanotto- ja käsittelypalvelimelle kehitettyjä ratkaisuja voidaan myös osin hyödyntää esimerkiksi muiden IoT-teknologioiden hyödyntämiseksi ja datan siirtämiseen laitteilta SCADA-järjestelmään, mikäli näille soveltuvia käyttökohteita ilmaantuu ja niihin soveltuvia laitteita tulee markkinoille ja otetaan käyttöön tulevaisuudessa.

Datan vastaanotto- ja käsittelypalvelimia voidaan myös järjestelmän laajentuessa ja mahdollisesti kriittisempien valvontakohteiden lisääntyessä asentaa

useampia kappaleita vikasietoisuuden ja järjestelmän suorituskyvyn parantamiseksi.

10 POHDINTA

Opinnäytetyön lähtökohtana oli tutustua IoT-teknologiaan ja toteuttaa Suur-Savon Sähkön / Järvi-Suomen Energian verkossa sijaitseville 1 kV:n katkaisijoille soveltuva ratkaisu niiden tilatiedon valvontaan IoT-teknologiaa käyttäen.

Opinnäytetyöprosessi aloitettiin tutustumalla IoT-teknologiaan ja samalla aloitettiin käytännön osuuden suunnittelu etsimällä tietoa esimerkiksi saatavilla olevista, käyttökohteeseen soveltuvista laitteista ja suunnittelemalla niiltä saatavan datan käsittelyä ja liittymistä perinteistä sähköverkkoautomaatiota edustavaan, jo olemassa olevaan SCADA-järjestelmään.

IoT-teknologia käsitteenä osoittautui heti työn alkuvaiheessa tekijän aloitushypoteesin mukaisesti olevan tarkasti määrittelemätön ja soveltuvan hyvin suureen määrään erilaisia laitteita ja ratkaisuja hieman määrittelijästä riippuen.

Joidenkin määritelmien mukaisesti myös esimerkiksi perinteinen, laajalti käytössä oleva sähköverkkoautomaatio ja siihen liittyvät laitteet voitaisiin katsoa jollakin tavalla ”IoT-teknologiaksi”, jolloin käytännön työnä kehitetty katkaisijan valvonta olisi voitu toteuttaa jo olemassa olevalla konseptilla ja vain todeta sen olevan jostakin lähteestä haetun ”IoT-määritelmän” mukainen. Tällöin kuitenkaan varsinaisia tavoitteita ei olisi millään tavoin saavutettu.

IoT-teknologian eri määritelmien havaittiin käsittävän erittäin suuren määrän erilaisia laitteita, useita erilaisia verkkoteknologioita ja muita ratkaisuja. ”Bachelor’s thesis” -tason opinnäytetyön laajuuden puitteissa esimerkiksi kaikkia mahdollisia olemassa olevia tekniikoita ja niihin perustuvia ratkaisuja ei kuitenkaan voitu työn yhteydessä analysoida täysin kattavasti.

Opinnäytetyön aloitusvaiheessa haasteena olikin käsitellä erilaisia tekniikoita niiden vertailemiseksi ja tähän kyseiseen käytännön sovellukseen soveltuvan tekniikan valitsemiseksi sopivalla tasolla kuitenkin pyrkien käsittelemään eri

vaihtoehtoja riittävästi, ettei valintaa suoritettaisi esimerkiksi jonkin mahdollisesti epävarmaan tietoon perustuvan hypoteesin perusteella.

Lisäksi tavoitteena oli saavuttaa ratkaisu tällä hetkellä saatavilla olevaa teknologiaa ja laitteita käyttäen, joka mahdollisesti rajasi pois useita erilaisia vaihtoehtoja, jotka eivät vielä olleet opinnäytetyön tekohetkellä riittävän laajalti käyttöönotettu ja saatavilla. IoT-teknologian voidaankin todeta olevan hyvin nopeasti kehittyvää, ja erilaisia projekteja aloitettaessa onkin tarkasteltava sen hetken tilannetta erilaisten saatavilla olevien mahdollisuuksien osalta.

On myös huomioitava, että tällaisessa tapauksessa teknologia voi olla myös nopeasti vanhenevaa, ja tämänkaltaisen ratkaisun laitteiden käyttöiän olevan kuitenkin jopa kymmeniä vuosia. Tämän vuoksi työtä suunnitellessa oli pyrittävä ottamaan huomioon esimerkiksi yksittäiseen laitevalmistajaan tai palveluntarjoajaan sitoutumisen riskit, sillä näitä ei välttämättä olisi esimerkiksi kymmenen vuoden päästä enää olemassa, vaikka järjestelmä itsessään olisi vielä käytössä.

Käytännön ratkaisun kehittämisessä oli alkuvaiheessa haasteena myös epätietoisuus tämän hetken teknologian tarjoamista mahdollisuuksista, jolloin ei ollut ylipäätään varmuutta siitä, onnistuuko tämänkaltaisen konseptin kehittäminen määritettyjen vaatimusten mukaisesti ja valmiiksi kaupallisesti saatavilla olevaa tekniikkaa hyödyntäen ollenkaan.

Erilaisista, IoT-verkkoteknologioina useiden eri lähteiden perusteella pidettävistä teknologioista tähän kyseiseen käyttötarkoitukseen havaittiin soveltuvimmaksi LoRaWAN-verkkoon perustuva ratkaisu. Tekniikan valinnan jälkeen opinnäytetyön erityisesti käytännön osuuden aihe tarkentuikin erityisesti LoRaWAN-teknologian hyödyntämiseen sähköverkon mittaustiedon keräämisessä, minkä jälkeen työssä perehdyttiin erityisesti kyseiseen teknologiaan ja siihen sekä sen käyttöönottoon liittyviin haasteisiin.

Perinteisen sähköverkkoautomaation ja erilaisten IoT-teknologioiden, kuten esimerkiksi LoRaWAN-teknologian integroimiseen tässä työssä halutulla tavalla havaittiin liittyvän myös haasteita, eikä esimerkiksi valmiita kaupallisia

ratkaisuja tai tämänkaltaiseen projektiin keskittynyttä opinnäytetyötä vaikuttanut löytyvän.

Trendinä näytti pikemminkin olevan perinteisten automaatiolaitteiden integrointi osaksi isompaa ”IoT/”big data”-ratkaisua ja perinteisiä automaatioprotokollia käyttävien laitteiden tuottaman datan muuntaminen erilaisille ”IoT-protokollille”.

Tämän johdosta työn onnistuneeksi toteuttamiseksi jouduttiin myös mm. kirjoittamaan kokonaan uusia palvelinohjelmia LoRaWAN-antureilta vastaanotetun datan viemiseksi SCADA-järjestelmään, joka oli määritelty yhdeksi opinnäytetyön yhteydessä kehitettävän valvontaratkaisun vaatimukseksi ja tavoitteeksi.

Opinnäytetyössä voidaan siis todeta käsitellyn monia erilaisia asioita ja pääkohtia, jotka eivät kaikki myöskään liity suoraan sähkötekniikkaan, mutta jotka olivat kuitenkin välttämättömiä vähintään jossain laajuudessa työn onnistuneen lopputuloksen kannalta. Tarkasteltaessa näitä asioita voidaan todeta, että ainakin osasta olisi voinut mahdollisesti tehdä jo itsestään opinnäytetyön, mikäli asiaa olisi käsitelty hieman laajemmin. Aiheet olisivat lisäksi voineet osittain olla enemmänkin esimerkiksi ICT- kuin sähköalan työhön soveltuvia.

Opinnäytetyöstä tuli myös ehkä hieman alun perin aiottua laajempi ainakin sivumäärän perusteella tarkasteltuna, ja edellä mainituista syistä johtuen kaikkia mahdollisia asioita ei siitä huolimatta voitu kuitenkaan käsitellä siinä laajuudessa, kuin olisi ollut mahdollista johonkin osa-alueeseen keskittyvässä opinnäytetyössä. Tässä opinnäytetyössä käsiteltyjä asioita voidaankin myös pitää aiheena uudelle, esimerkiksi tarkemmin johonkin tiettyyn osa-alueeseen syvällisesti perehtyvälle opinnäytetyölle.

Tämän johdosta opinnäytetyö ei myöskään ehkä pysty vastaamaan asiaa entuudestaan yhtään tuntemattoman lukijan tarpeisiin täydellisesti ilman täydentävää informaatiota esimerkiksi opinnäytetyössä käytetyistä lähteistä, eikä työtä voida pitää myöskään valmiina step-by-step-ohjeena vastaavanlaisen kuin opinnäytetyön yhteydessä tehdyn käytännön ratkaisun toteuttamiseen,

sillä esimerkiksi kaikkia työssä käytettyjä ydinkomponentteja, kuten itse kirjoitettuja palvelinohjelmistoja, ei ole kaupallisesti tai muutenkaan lainkaan yleisesti saatavilla, eikä niitä ole käsitelty riittävässä laajuudessa täysin vastaavien kehittämiseksi pelkästään tämän työn pohjalta.

Opinnäytetyön perusteella kuitenkin esimerkiksi vastaavan ratkaisun suunnitteleminen ja rakentaminen on todennäköisesti helpompaa kuin ilman työn lukemista. Mikäli vastaavanlainen, juuri tämän opinnäytetyön yhteydessä tehtyyn käytännön työhön liittynyt opinnäytetyö olisi ollut tätä työtä tehdessä julkisesti saatavilla, olisi siitä mahdollisesti voinut olla hyötyä.

Toisaalta on mahdollista, että kyseisenkaltainen työ on jo jossain julkaistu, mutta sitä ei ole kirjoitettu englanniksi edes abstractin osalta, ja sen vuoksi työtä ei tässä tapauksessa ollut mahdollista lainkaan löytää. Sama ongelma koskettaa nyt osittain tietysti myös tätä työtä, ja tätä ajatellen työn olisikin voinut kirjoittaa englanniksi.

Opinnäytetyön tekemiseen kului myös hieman enemmän aikaa kuin alun perin oli suunniteltu, jota olisi kuitenkin mahdollisesti voinut nopeuttaa ajankäyttöä tarkemmin suunnittelemalla ja käynnistämällä päällekkäin tai aikaisemmin erilaisia prosesseja, jotka eivät olleet toisistaan riippuvaisia ja joiden etenemisaikataulusta, johon ei ollut mahdollista erityisemmin vaikuttaa, aiheutui itse opinnäytetyön osana suoritettuun käytännön työhön erilaisia viiveitä.

Tässä olisi kuitenkin ollut riskinä mahdollisesti tarpeettoman tai väärillä lähtötiedoilla käynnistetyn prosessin turha suorittaminen, mikäli siihen vaikuttavia asioita ei olisi tutkittu tarpeeksi huolellisesti ennen päätösten tekemistä, joten tämän johdosta harkittu etenemistapa voidaan katsoa sen osalta onnistuneeksi, ettei opinnäytetyön yhteydessä esimerkiksi aiheutunut käytännössä ollenkaan työn yhteydessä tarvittuihin yhteistyökumppaneihin tai eri henkilöihin vaikuttaneita tarpeettomia tai epäonnistuneita projekteja.

LÄHTEET

ABB. 2000. TTT-käsikirja 2000-07, luku 15, sähkönjakeluverkon automaatio. PDF-dokumentti. Päivitetty 13.9.2000. Saatavilla: www.oamk.fi/~kurki/automaatiolabrat/TTT/15_S%84hk%94njakeluverkon%20automaatio.pdf [viitattu 6.5.2019].

Actility. 2018a. Actility ThingPark LRC-AS Tunnel Interface Developer Guide (LoRaWAN). PDF-dokumentti. Päivitetty 4.7.2018. Dokumentti yrityksen sisäisessä käytössä.

Actility. 2018b. Actility ThingPark Wireless Device Manager User Guide. PDF-dokumentti. Päivitetty 26.10.2018. Dokumentti yrityksen sisäisessä käytössä.

Bassetti, E. 2018. LoRaWAN spreading factor allocation in a multiple-gateway environment. WWW-dokumentti. Saatavilla: https://www.enricobassetti.it/wp/2018/02/lorawan-spreading-factor-allocation-in-a-multiple-gateway-environment [viitattu 14.4.2019].

Chebudie, A., Rotondi, D. & Minerva, R. 2014. Towards a definition of the Internet of Things (IoT). PDF-dokumentti. Päivitetty 27.5.2015. Saatavilla: https://www.researchgate.net/profile/Abiy_Biru_Chebudie/publication/317588072_Towards_a_definition_of_the_Internet_of_Things_IoT/links/5941853ea6fdcc13d688be36/Towards-a-definition-of-the-Internet-of-Things-IoT.pdf [viitattu 28.1.2019].

Clearcube. 2019. What is a Thin Client, its Uses and Benefits? WWW-dokumentti. Saatavilla: https://www.clearcube.com/posts/what-is-a-thin-client/ [viitattu 9.5.2019].

Connected Finland. 2018. Coverage. WWW-dokumentti. Saatavilla: http://www.connectedfinland.fi/en/coverage/ [viitattu 9.2.2019].

Digita. 2018a. Digita's IoT solutions – enabler of the effective business. PDF-dokumentti. Päivitetty 1.6.2018. Saatavilla: https://www.digita.fi/files/2081/Digita_IoT_presentation_ENG.pdf [viitattu 8.2.2019].

Digita. 2018b. Digita IoT palvelukuvaus – LoRaWAN verkkoyhteys. PDF-dokumentti. Päivitetty 01.09.2018. Dokumentti yrityksen sisäisessä käytössä.

Digita. 2019. Miten IoT auttaa sähköyhtiötä. PDF-dokumentti. Päivitetty 1.4.2019. Saatavilla: https:/digitamahdollistaa.fi/wp-content/uploads/2019/04/Digita_IoT_S%C3%A4hkoesite.pdf [viitattu 8.5.2019].

Elsys s.a.a. LoRa® ELT 2. WWW-dokumentti. Saatavilla: https://www.elsys.se/en/lora-elt-2/ [viitattu 7.4.2019].

Elsys s.a.b. Android Help. WWW-dokumentti. Saatavilla: https://www.elsys.se/en/android-help/ [viitattu 30.4.2019].

Elsys. 2017. Elsys ELT-2-HP LoRaWAN wireless IP-65 GPIO transceiver. PDF-dokumentti. Päivitetty 10.5.2017. Saatavilla: https://www.elsys.se/en/wp-content/uploads/sites/3/2016/09/ELT-2-folder.pdf [viitattu 23.3.2019].

Elsys. 2019a. Sensor downlink payload. PDF-dokumentti. Päivitetty 22.3.2019. Saatavilla: https://www.elsys.se/en/wp-content/uploads/sites/3/2016/09/ELSYS_downlink_payload_v2-1.pdf [viitattu 2.4.2019].

Elsys. 2019b. Sensor settings parameters. PDF-dokumentti. Päivitetty 10.4.2019. Saatavilla: https://www.elsys.se/en/wp-content/uploads/sites/3/2016/09/sensor_settings_parameter_v2.pdf [viitattu 27.4.2019].

Ghoslya, S. s.a.a. LoRa: Symbol Generation. WWW-dokumentti. Saatavilla: https://www.sghoslya.com/p/lora-is-chirp-spread-spectrum.html [viitattu 10.4.2019].

Ghoslya, S. s.a.b. How does LoRaWAN Adaptive Data Rate work? WWW-dokumentti. Saatavilla: https://www.sghoslya.com/p/how-does-lorawan-nodes-changes-their.html [viitattu 10.4.2019].

Ghoslya, S. s.a.c. LoRa/LoRaWAN Important Tables. WWW-dokumentti. Saatavilla: https://www.sghoslya.com/p/table-01-data-rate-configuration.html [viitattu 16.4.2019].

GSM Association. 2016. 3GPP Low Power Wide Area Technologies. PDF-dokumentti. Päivitetty 4.10.2016. Saatavilla: https://www.gsma.com/iot/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf [viitattu 9.2.2019].

Hakkenberg, C. 2016. EXPERIMENTAL EVALUATION OF LORA(WAN) IN INDOOR AND OUTDOOR ENVIRONMENTS. Master's thesis. Päivitetty 17.8.2016. Saatavilla: http://essay.utwente.nl/71133/1/Hakkenberg_MA_EWI.pdf [viitattu 2.4.2019].

Kauhanen, A. 2019a. Verkostoinsinööri. Sähköpostiviesti 21.1.2019. Suur-Savon Sähkö Oy.

Kauhanen, A. 2019b. Verkostoinsinööri. Sähköpostiviesti 11.2.2019. Suur-Savon Sähkö Oy.

Kickstarter. 2019. WiCub: WiFi Temperature & Humidity Sensor. WWW-dokumentti. Saatavilla: https://www.kickstarter.com/projects/911457810/wicub-wifi-temperature-and-humidity-sensor [viitattu 26.4.2019].

Lapp Group 2016. Data Sheet - SKINTOP® ST-M / STR-M. PDF-dokumentti. Päivitetty 26.1.2016. Saatavilla: http://www.farnell.com/datasheets/2124455.pdf [viitattu 29.4.2019].

LoRa Alliance. 2015. A technical overview of LoRa and LoRaWAN. PDF-dokumentti. Päivitetty 10.11.2015. Saatavilla: https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf [viitattu 8.2.2019].

Matoušek, P. 2017. Description and analysis of IEC 104 Protocol. PDF-dokumentti. Päivitetty 20.12.2017. Saatavilla: http://www.fit.vutbr.cz/research/pubs/tr.php.en?file=%2Fpub%2F11570%2FTR-IEC104.pdf&id=11570 [viitattu 9.2.2019].

Mekki, K., Bajic, E., Chaxel, F. & Meyer, F. 2017. A comparative study of LPWAN technologies for large-scale IoT deployment. PDF-dokumentti. Päivitetty 21.9.2017. Saatavilla: https://www.sciencedirect.com/science/article/pii/S2405959517302953 [viitattu 3.4.2019].

Microsoft. 2017. What Is ODBC? WWW-dokumentti. Päivitetty 19.1.2017. Saatavilla: https://docs.microsoft.com/en-us/sql/odbc/reference/what-is-odbc [viitattu 23.3.2019].

Netcontrol. 2018. Netcon 3000 – Resourceful SCADA system. PDF-dokumentti. Päivitetty 14.3.2018. Saatavilla: https://www.netcontrol.com/index.php/download_file/view/556/232/ [viitattu 9.2.2019].

Oniga, B., Dadarlat, V., De Poorter, E. & Munteanu, A. 2017. Analysis, design and implementation of secure LoRaWAN sensor networks. PDF-dokumentti. Päivitetty 4.7.2018. Saatavilla: http://hdl.handle.net/1854/LU-8567542 [viitattu 2.4.2019].

Oracle. 2019a. About MySQL. WWW-dokumentti. Saatavilla: https://www.mysql.com/about/ [viitattu 23.3.2019].

Oracle. 2019b. MySQL 8.0 Reference Manual. 1.3.1 What is MySQL? WWW-dokumentti. Saatavilla: https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html [viitattu 23.3.2019].

Oracle. 2019c. MySQL Connector/ODBC Developer Guide. Chapter 4 Connector/ODBC Installation. WWW-dokumentti. Saatavilla: https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation.html [viitattu 27.4.2019].

Partanen, J. 2019. Sähköasiakas ja sähköverkko 2030. PDF-dokumentti. Päivitetty 30.1.2019. Saatavilla: https://energia.fi/files/3375/Partanen_Jarmo.pdf [viitattu 23.3.2019].

Pasqua, E. 2018. LPWAN technologies: How cellular MNOs are placing their bets. WWW-dokumentti. Päivitetty 23.10.2018. Saatavilla: https://iot-analytics.com/lpwan-technologies-cellular-mnos/ [viitattu 24.3.2019].

Patterson, I. s.a. NSSM – the Non-Sucking Service Manager, Use cases. WWW-dokumentti. Saatavilla: https://nssm.cc/scenarios [viitattu 9.4.2019].

Prysmian Group. 2018a. MHS. PDF-dokumentti. Päivitetty 19.2.2018. Saatavilla: https://fi.prysmiangroup.com/api/product_attachment/?pdf=11832 [viitattu 29.4.2019].

Prysmian Group. 2018b. KLMA-HF Dca. PDF-dokumentti. Päivitetty 15.1.2018. Saatavilla: https://fi.prysmiangroup.com/api/product_attachment/?pdf=11768 [viitattu 29.4.2019].

Prysmian Group. 2018c. VMOHBU-TL. PDF-dokumentti. Päivitetty 19.2.2018. Saatavilla: https://fi.prysmiangroup.com/api/product_attachment/?pdf=11834 [viitattu 29.4.2019].

SAFT. 2019. LS 14500 product datasheet. PDF-dokumentti. Päivitetty 2.4.2019. Saatavilla: https://www.saftbatteries.com/download_file/6X7JMGAnv3Fm6HdmtEv%252B2gtlbZ1bRRV-HkjS11M6md92GD2EF7vU%252F3Oybbz3WOIG%252BxR8srpA5iCdJ%252FV3IQzTVHQyiTucngZKEg9KkYCLkowAvgaG1huqyXUIQvO1qUk-ZjGCfaa8Bj8zATp1fXJiJXWOMWYOmKIKGI%252B2HKVzqrqCHhO-SacXA%253D%253D/LS14500_EN_31072_0319.pdf [viitattu 6.4.2019].

Saira, V. 2009. ”1000 V JAKELUJÄNNITTEEN KÄYTTÖMAHDOLLISUUDET-KYMENLAAKSON SÄHKÖVERKKO OY:SSÄ”. Diplomityö. Päivitetty 15.1.2010. Saatavilla: http://urn.fi/URN:NBN:fi-fe201002231406 [viitattu 22.2.2019].

Salman, T. 2015. Networking Protocols and Standards for Internet of Things. PDF-dokumentti. Päivitetty 30.11.2015. Saatavilla: https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot.pdf [viitattu 6.2.2019].

Sigfox. 2018a. Sigfox Technology Overview. WWW-dokumentti. Saatavilla: https://www.sigfox.com/en/sigfox-iot-technology-overview [viitattu 8.2.2019].

Sigfox. 2018b. “Get started”. WWW-dokumentti. Saatavilla: https://www.sigfox.com/en/technology/get-started [viitattu 8.2.2019].

Sigfox. 2018c. Our vision. WWW-dokumentti. Saatavilla: https://www.sigfox.com/en/our-vision [viitattu 8.5.2019].

Sigfox. 2018d. Coverage. WWW-dokumentti. Saatavilla: https://www.sigfox.com/en/coverage [viitattu 8.5.2019].

Sähkömarkkinalaki 9.8.2013/588.

Terezinho, F. 2013. SCADA Systems Automate Electrical Distribution. PDF-dokumentti. Päivitetty 9.7.2013. Saatavilla: https://www.automation.com/pdf_articles/SCADA_white_paper.pdf [viitattu 9.2.2019].

Thakur, A. 2012. ”What is SCADA system”. WWW-dokumentti. Saatavilla: https://www.engineersgarage.com/articles/scada-systems [viitattu 9.2.2019].

Triangle Microworks s.a. SCADA Data Gateway. WWW-dokumentti. Saatavilla: http://www.trianglemicroworks.com/products/scada-data-gateway [viitattu 23.3.2019].

Triangle Microworks. 2017. SCADA Data Gateway Implementation Guide. PDF-dokumentti. Päivitetty 12.9.2017. Saatavilla ohjelmiston asennuspaketin mukana.