Tampere University

Muhammad Hamza

IMPACTS OF CYBERATTACK THROUGH HOME AUTOMATION SYSTEM ON FINLAND'S FREQUENCY RESERVE MARKETS, MEDIUM & LOW VOLTAGE NETWORKS IN SOUTH SAVO FINLAND, AND INDIVIDUAL CUSTOMERS.

Master's Thesis
Faculty of Information Technology and Communication Sciences
Professor Sami Repo
Irina Laamanen
July 2024

ABSTRACT

Muhammad Hamza: Impacts of Cyberattack through Home Automation System on Finland's Frequency Reserve Markets, Medium & Low Voltage Networks in South Savo Finland, and Individual Customers
Master's Thesis
Tampere University
Master's Degree Education in Electrical Engineering, Smart Grids
July 2024

Modern home automation systems powered by Internet of Things (IoT) enable house residents with unprecedented controllability of loads, storage systems and distributed generation. It provides residents with convenience as well as efficiency in domestic energy management. However, extensive utilization of home automation systems is also accompanied by multitude of new vulnerabilities, particularly in the realm of cybersecurity. Such vulnerabilities may be exploited to pose threats to electricity network as well as house residents.

This study investigates in detail the impacts caused by cyberattack through home automation systems on power system frequency reserves, low and medium voltage electricity networks, and house residents. To achieve this, historical data of frequency markets of Fingrid is analyzed in detail to identify vulnerable instances of volume scarcity and price volatility which may be exploited by hacked home automated loads to destabilize power system and manipulate market functioning. Moreover, heat pumps and electric vehicles are simulated as home automated loads for houses/apartments in South Savo, Finland. It is done to study the impacts of these loads in normal operation as well as after-hacking scenarios on transformers, conductors, and service points of the chosen network. Furthermore, qualitative categorization of impacts of cyberattack through home automation system on house residents is also performed.

Keywords: Home Automation System, Frequency Markets, Volume Shortage based Risk Analysis, Price-based Risk Analysis, Heat Pumps, Electric Vehicles, Load Modelling, After Hacking Scenario Formulation, Overloading, Overvoltage, Undervoltage.

PREFACE

This thesis was done for the Master of Science degree program in Electrical Engineering, specialization in Smart Grids at Tampere University. It was commissioned by the research group under the Faculty of Information Technology and Communications (ITC), Electrical Engineering Unit of Tampere University. This thesis was Supervised by Professor Sami Repo, and was completed in collaboration with Rejlers Oy, Suur-Savon Sähkö Group, and Tietoevry.

I would like to express my immense gratitude to Professor Sami Repo for his invaluable guidance throughout the research process. He has not only been a brilliant thesis supervisor but also a true mentor who has guided me through every step of this thesis. His academic expertise, intellectual curiosity and constructive feedback has truly been vital for this thesis to achieve its research goals. I am also thankful to Tommi Siintoharju from Rejlers Oy, and Tomi Öster from Suur-Savon Sähkö Group for their valuable contributions to this research.

I am also extremely thankful to my family and friends without whom this wonderful academic journey would not have been possible. Especially to my parents, I am grateful beyond words.

I hope that this thesis proves to be gateway for further research in this rather unexplored study area and contributes to mitigate impacts of cyberattack through home automation system on any part of electricity network.

Tampere, 10 July 2024

Muhammad Hamza

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND ABBREVIATIONS

aFRR	Automatic Frequency Restoration Reserve
CDD	Cooling Degree Days
COP	Coefficient of Performance
DER	Distributed Energy Resource
DG	Distributed Generation
DSO	Distribution System Operator
EV	Electric Vehicle
FCR	Frequency Containment Reserve
FFR	Fast Frequency Reserve
HDD	Heating Degree Days
HP	Heat Pump
HVDC	High Voltage Direct Current
ICEV	Internal Combustion Engine Vehicle
IoT	Internet of Things
IT	Information Technology
KPI	Key Performance Indicator
LFC	Load Frequency Control
LG	Load Group
LV	Low Voltage
mFRR	Manual Frequency Restoration Reserve
MV	Medium Voltage
R&D	Research and Development
SPF	Seasonal Performance Factor
TSO	Transmission System Operator

$e(t)$	Actual Hourly Electricity Consumption of each Heat Pump
$e_{hacking}(t)$	Hourly Hacking Capacity of each Heat Pump
$e_{maximum}$	Size of each Heat Pump in terms of Electricity Consumption
$e_{Spaces\_Demand}\,(t)$	Hourly electricity consumption demand of each Customer for Space Heating
$e_{Spaces_{SingleHP}}(t)$	Maximum Electricity Consumption of Smallest Sized Heat Pump
f	Loss Factor of Heat Pump
$I_{HP}(t)$	Actual Hourly Heating Output of each Heat Pump
$I_{HPSpaces_{Max}}(t)$	Maximum Hourly Heating Output Capacity of each Heat Pump
$I_{Spaces\_Demand}(t)$	Hourly Space Heating Requirement of each Customer
$I_{Spaces_{SingleHP}}(t)$	Maximum Heating Output of Smallest sized Heat Pump
T_{HDD}	Indoor Temperature representing Heating Degree Day
T_{HSO}	Heating Source Temperature
T_{HSY}	Building Heating System Temperature
T_{ib}	In-blast Temperature
Q	Annual Space Heating Demand

1. INTRODUCTION

1.1 Motivation

Modern home automation systems offer unprecedented convenience and efficiency in domestic energy management. However, this technological advancement is also accompanied by multitude of new vulnerabilities especially in context of cybersecurity. These vulnerabilities pose significant threats to all parts of electricity network. Main motivation of this thesis is to identify and explore those threats.

Delving into the details, it is vital to identify the threats posed by cyberattack through home automation systems on frequency markets of Fingrid as they play integral role in maintaining stability and balance of electricity in the whole Nordic synchronous area. It is also imperative to identify the vulnerable instances where volume scarcity as well as price volatility occurs in frequency markets. This is because such instances may be exploited to affect system stability and market functionality. Furthermore, impacts of cyberattack through home automation systems must also be analysed on the increasingly interconnected electricity medium and low voltage networks. Network elements which may get effected include transformers, conductors, and service points. South Savo, with its diverse mix of residential and commercial energy consumers, along with its region's reliance on medium and low voltage networks makes it an ideal candidate for examining the localized impacts of cyberattacks on home automation systems. By analysing the specific vulnerabilities and potential consequences of such attacks in this context, this thesis aims to contribute to the broader efforts of further securing electricity networks. Additionally, the research aims to protect individual customers from the myriads of adverse effects stemming from cyber vulnerabilities, ultimately fostering a safer and more reliable energy environment.

Hence, the findings of this study are expected to inform both policymakers and industry stakeholders, offering insights into the impacts of cyber threats of home automation systems on electric power systems. Moreover, this thesis will provide valuable knowledge that can guide the development of more robust electricity networks as well as markets.

1.2 Objectives

Main objective of this thesis is to examine the possible impacts of cyberattack through automated houses on power system, electric grid, and end users. In this thesis, impacts of such attacks on individual, societal as well as system level will be analysed. This will be done in different phases. In the first phase, impacts on different frequency markets of Fingrid will be studied. Objective of such study is to explore the two-pronged potential risks of volume availability and price volatility associated with frequency market operation. Then, the impact of load manipulation through home automation cyberattack during those vulnerability instances will be studied.

In the next phase, impacts of cyberattack through home automation system on a medium and low voltage network in South-Savo Finland will be analysed. Network elements under study include service points, conductors, and transformers. For service points, parameters of average loading level, overloading, overvoltage, and undervoltage will be studied. However, for conductors and transformers, only the parameters of average loading level and overloading will be studied. For this study, two loads are selected to be simulated as home automated loads by each household: heat pumps and electric vehicles. Initially, customer specific load modelling of both these home automated loads will be done. Then these modelled loads will be added to the customer service point data depicting a future scenario. Afterwards, worse-case after-hacking scenario will be formulated through load manipulation of these home automated loads. Then, impacts of these loads in the after-addition as well as the after-hacking scenario will be studied on transformers, conductors, and service points of the whole South Savo network.

In the last phase, effects of cyberattack on individual consumers will be studied. This will be done through categorization of cybersecurity threats based on risk posed to residents' safety, security, property, privacy, and data. Moreover, type and degree of impact suffered by individual household residents depend upon hacker's level of access, actions, and intentions. Along with that, scenario formation such as heating system shutdown, uncharged EV, device malfunctioning, and triggering of false alarm is also done in order to assess the degree of discomfort suffered by the residents of automated house.

1.3 Research Questions

Main research questions are as follows:

- How many vulnerable instances exist in terms of volume scarcity in frequency markets? How can these vulnerable instances be exploited through cyberattack on home automation systems? What can be the possible methods utilized by hackers, probable outcomes of such methods, and what degree of impact can a large scale cyberattack cause on frequency markets in terms of volume availability?
- How many vulnerable instances exist in terms of price manipulation of frequency markets? How can these vulnerable instances be exploited through cyberattack on home automation systems? What can be the possible methods utilized by hackers, probable outcomes of such methods, and what degree of impact can a large scale cyberattack cause on frequency markets in terms of price manipulation?
- Can cyberattacks through home automation system cause voltage quality issues in low voltage and medium voltage networks? How many instances of over and undervoltage can be caused by certain amount of home automated loads in lower voltage and medium voltage networks?
- Can cyberattacks through home automation system cause overloading in low voltage and medium voltage networks? What are the loading levels of service points, conductors, and transformers before and after cyberattack?
- Can such cyberattacks generate artificial grid reinforcement needs? What will be outlook when ratio of home automation systems increases in future?
- What can be the possible impacts of cyberattack through home automation system on residents of the house. How different levels of hackers' access, actions and intentions create different levels of impacts on individual customers.

1.4 Overview

In modern times, information technology (IT) is being abundantly adopted in all aspects of life. Home automation systems through IoT is also a result of such fast-paced IT adaptation. Distributed generation, storage systems as well as loads in houses can be controlled remotely with ease. It provides homeowners not only with better monitoring and controllability but also plays key role in efficient energy usage. However, cybersecurity of home automation systems is also a serious concern. Most companies providing such IoT services use minimal R&D resources for software development to save budget in order to be market competitive. This causes issues such as dependency hell where one software package is dependent upon another [1], and software rot where quality of code deteriorates over time due to changes in external environment [2]. Such multitude of issues make home automation systems more susceptible to cyber-attacks. Furthermore, many companies use centralized cloud web services for control of IoT devices. If cloud web used by a service provider is compromised, then all the devices controlled through it may become vulnerable. This may give hackers access to tens or even hundreds of thousands of home automated devices. Then, these devices can be controlled through usual commands in such a way that cyber-attack remains undetected. This way, desired objectives of hackers may be achieved through load manipulation.

Impacts of cyber-attacks on home automated systems can be severe and are classified into impacts on national grid, local grid, and individual customers. In first case, national grid stability may be compromised by prevention of frequency reserve control actions, increasing volume shortage risk, or by breaking the N-1 criteria through load behavior synchronization. Moreover, price manipulation in frequency markets can also be done with the intention of either gaining profit or causing loss. For local LV and MV grids, the issues of overloading and non-compliance of voltage quality standards can be caused by a cyberattack on home automation systems. Voltage quality can be degraded especially in weak LV and MV networks by manipulation of load in such way that worst case scenario occurs. This may cause non-compliance of power quality standards which might lead to grid reinforcement needs. In case of local overloading, current limit of conductors, transformers, service points and other equipment can get exceeded through load increment if grid is already operating at high loading condition or at alternative topology. This may cause outage or thermal damage to the equipment. Furthermore, through such cyber-attacks, harm to end user can happen in the form of threat to

safety, security, property, privacy, data, and occurrence of extreme discomfort. So, cyber-attacks through home automation systems can have severe impacts on national and local power systems, installed equipment, actors in electricity markets, TSO, DSO, as well as end users.

2. THEORETICAL BACKGROUND

2.1 Home Automation Systems: Trends and Applications

A smart automated house refers to a residential building equipped with technological features enabling adaptive responses in specific scenarios to enhance energy efficiency, security as well as comfort of its inhabitants [3]. This integration is facilitated through a unified interface, establishing connectivity with external systems and services outside the home environment [4]. In home automation systems, various types of cyber-physical systems interact in multiple ways mostly through sensors and applications. These cyber-physical systems generate large amounts of complex data which is then used as feedback to improve energy efficiency, security as well as comfort of the end-user. In terms of energy efficiency, household energy consumption can be decreased by 20 percent through the use of home automation systems [5]. Moreover, for the purpose of security enhancement, multiple features can be opted such as surveillance systems, intrusion detection systems, geofencing, smart locks and smart lighting. In terms of comfortability, automated houses can provide features such as temperature control, voice control, smart entertainment systems etc. This way, home automation systems provide all-inclusive solutions for residents.

In terms of input control of smart automated homes; user commands, sensor data as well as user behavior are three main types of input. User commands can also be given remotely with multiple devices such as smart phone, laptop, and tablets. Apart from user commands, modern smart homes have functionalities which allow devices to be controlled autonomously on behalf of the end users through the use of sensor data and user behavior monitoring. Moreover, artificial intelligence models are often utilized to forecast user behavior in advance based on collected data in order to improve the quality of autonomous control.Top of Form

Let’s assume that the individual devices that are connected directly or indirectly to the gateway of internet for the purpose of control, monitoring, and regulation of different functions in houses are considered as home automation systems. Then recent trends suggest that from 2023 to 2030, Global home automation market is expected to grow at an annual rate of 27.3 percent [6]. Moreover, the number of smart homes is going to be more than 785 million by the end of 2028 [7]. For Finland in particular, the household penetration rate for smart automation homes is going to increase from 29.8% in 2024

to 69.8% in 2028 [8]. Moreover, in Finland, the market is anticipated to demonstrate a yearly growth rate of 9.38% between 2024 and 2028, leading to an estimated market size of US$474.8 million by 2028 [8].

However, this predicted increase in home automation system penetration is hugely dependent on price factor. Let's assume that aforementioned trends do not correspond to market reality in future and adaptation of home automation systems by masses remain relatively low. Even then, controllable loads and distributed energy resources are becoming increasingly prevalent in modern actively controlled grids [9]. For instance, heat pump, electric vehicle charging, and solar modules can be automated as a controllable loads/DER's which can then be connected to cloud services. In that case, these controllable loads and DER's can also be considered to be part of partially automated houses. Hence, automation systems for the houses, whether fully or partially automated, are on the upward trajectory for the future.

2.2 Cybersecurity Threats to Home Automation Systems

Kirkham et al. [10] analyses and categorizes the risks associated with data sharing between home and external services. The proposed risk model categorizes risk into three different categories: legal risk, application failure risk, and resource security risk. Legal risk focuses on evaluating the data sharing and compliance of home automation companies with privacy legislation and broader data processing laws. It employs a rule-based model, particularly innovative in its approach, to assess the extent to which service providers adhere to legal mandates. If companies do not properly adhere to laws associated with data privacy as well as data sharing, legal risk increases thus increasing cybersecurity risk as well. Secondly, the consideration of appliance failure risk is crucial for identifying potential vulnerabilities stemming from malfunctions in smart home devices. This aspect assesses environmental factors and technical deficiencies that could lead to system failures, thereby jeopardizing the contractual agreements between homeowners and service providers. It can either be caused by the appliance in use by the customer or the application through which that appliance is connected to the cloud services. Although, induction of fail-safe automation devices would reduce this risk manifolds. Finally, resource security risk analysis within the risk model is concerned with safeguarding against unauthorized access and leakage of resources within the smart home environment. This dimension encompasses threats posed by both malicious actors, such as rogue service providers, theft, human error and technical malfunctions within devices. This way, combination of all three risks indicate whether home automation system is well secured or not.

For assessment of current condition of security of home automation systems, the work of [11] suggests it is estimated that approximately 80 percent of home automation devices are vulnerable to some type of hacking. Moreover, research done by [12] helps identify main vulnerabilities within home automation systems. It identifies that encryption layer of home automation devices is not properly formulated. Moreover, outdated protocols are being followed. It is also supported by [13] that protocols and regulations have not been able to keep up with fast paced growth within IoT industry. Moreover, insecure applications and middleware platforms utilized to control smart home devices lack systematic techniques to be fully secured [14]. Also, multiple weaknesses are identified within authentication procedures of home automation systems [15][16]. Along with that, firmware failure is another cybersecurity risk of smart homes where companies keep using outdated firmware even during upgradation of other devices [12]. Any of the aforementioned risks may cause home automation system to get hacked.

Furthermore, in the vulnerability analysis conducted by Jacobson et al. [17], risks associated with home automation system are explored. In total, 32 risks belonging to multiple categories were identified. Out of the total, 13 risks are related to software, 5 are information related, 5 are communication related, 5 are human related, and 4 are hardware related risks. In terms of cybersecurity, any of the aforementioned risks or their combination may be utilized in order to conduct organized cyberattack.

Moreover, usually fast paced increase in any technology can only occur if it is facilitated by decrease in prices and/or increase in lifespan of such devices [18]. With ongoing increase in the demand for home automation services, market competition is very high. Companies strive to compete in the market by decreasing the prices of services as much as possible in order to gain market volume. This results in reduction of R&D costs for planning and development. Due to that, issues like software rot arise which render a system to semi functioning level because of changes in the external environment upon which the software was previously dependent. Couple this with lack of proper laws and regulation enforcement in this field, result is poorly coded software as well as malfunctioning hardware. This means that in future, with the exponential increase in home automation systems, risk of organized cyberattacks will also increase accordingly.

2.3 Load Manipulation through Cyberattack on Home Automation Systems

Dennin et al. [19] provides a method to assess security and privacy-based landscape in smart automated homes with the goal to analyze cybersecurity risks associated with home automation systems,. Three main components of this method are feasibility of conducting a cyberattack, the attractiveness of the system as a compromised platform and the damage caused by such attack. The combination of the initial two components offer insight into the potential susceptibility of the device, whereas the third factor assists in assessing the comprehensive risk profile. To further explain, feasibility of conducting a cyberattack refers to how easily hackers can exploit vulnerabilities within a system. This includes factors such as sophistication of the security measures in place, the presence of known vulnerabilities, and the level of expertise required to breach the system. Attractiveness of the system as a compromised platform pertains to the value that the system holds for cybercriminals once it is breached. Lastly, damage caused by such an attack involves the consequences and impact of a successful breach. This includes both immediate and long-term effects, such as financial losses, reputational damage, operational disruptions, and legal ramifications.

In terms of comprehensive risk profile, it depends on how much load vis-à-vis the number of houses are subject to cyberattack. If cloud system of service provider gets compromised, then multiple home automation systems may get hacked simultaneously. If large number of automated houses are hacked, then comprehensive risk vis-à-vis effects of such cyberattack increases exponentially. This is because the amount of load that can be manipulated increases. This can cause devastating effects for national as well as local grid. However, as the amount of hacked load becomes smaller, the risk factor decreases because the impact level decreases to certain part of the local grid or individual customers.

In terms of methods of load manipulation, Adrian et al. [20] executes three different techniques to study the impacts on synchronous grid of Continental Europe (UCTE grid). MATLAB/Simulink model is used to test the impacts of different load manipulation techniques on this grid. In terms of load change strategies, first is the static load attack in which power consumption of the hacked devices is increased to maximum with the intention to create frequency imbalance. The scale and effects of such imbalance depends upon the amount of hacked load increment, grid operating state, reserve capacity as well as response time. Second option of load manipulation defined in this paper is dynamic load attack in which feedback system is utilized to increase effectiveness of attack. In this method, behavior of primary control may be targeted by changing the

load continuously depending upon control response. Specifically, hackers may maximize the load and wait for the full activation of the primary control, then minimize the load and wait for the deactivation of the primary control and so on. Eventually, hacker may find a resonant frequency leading to much larger frequency change. Finally, third method of load manipulation is termed as inter-zoned attacks. In this method, tie lines which connect different areas may be targeted by increasing load on them. In this study, it was determined that inducing load shedding by breaching the threshold of 49 Hz through a static load attack requires twice the amount of ENTSO-E's reference incident at network minimum power and 3.5 times the reference incident at maximum network power. Conversely, a dynamic load attack necessitates only 1.5 times the ENTSO-E reference incident to cause a frequency deviation beyond 49 Hz at network minimum power. Therefore, it was concluded that dynamic load attacks pose a greater threat to power system stability compared to static load attacks.

Sajjad et al. [21] investigates dynamic load altering attacks (D-LAAs) and their impact on power system stability. The study categorizes D-LAAs into two distinct types: open-loop and closed-loop. In the open-loop D-LAA, the system conditions are not monitored in real-time; instead, the attack follows a pre-programmed trajectory based on historical data. In contrast, closed-loop D-LAAs involve real-time monitoring of critical system parameters, such as frequency response to load changes, which inform subsequent actions. Furthermore, D-LAAs can be executed as either single-point or multipoint attacks, depending on the number of load buses targeted. These attacks are capable of destabilizing the power system frequency, pushing it beyond nominal values. Additionally, the objective can also be to force significant generators or transmission lines out of operation, causing cascading ripple effects across the interconnected power system. In this study, various types and forms of D-LAAs are tested on the IEEE 39 bus test system, demonstrating that successful load-altering cyberattacks can induce instability in the power system under study.

Furthermore, in the work of Robert et al. [22], different load and DER manipulation scenarios are conducted to test the voltage changes on a modelled HV and MV grid. Modelled HV grid for this study is Nordic32 system which is mainly based on Nordic and Swedish system. MV grid is modelled as an approximation of modern European MV grid having combination of DER’s, storage systems and loads. Results of this study demonstrate the susceptibility of modern medium voltage (MV) grids having combination of distributed energy resources (DERs) and smart automation homes to large-scale cyberattacks. In fact when a co-ordinated cyberattack through home automation systems as well as DERs is conducted on the same MV grid, the resulting voltage shift can exceed 30%, posing a significant threat to grid stability.

It is important to note that research on this topic is very limited. Most existing studies rely on models of electricity networks and power systems. However, the approach used in this thesis is novel. It employs a unique methodology to examine past vulnerable instances in frequency markets operated by Finnish TSO where hacked home automated loads could cause adverse effects on grid stability as well as market functioning. Moreover, this study uniquely utilizes load modeling of home automated loads based on actual customer data from the local grid in South Savo, Finland, and then analysis is conducted for the impacts of these loads in different operational modes on service points, transformers, and conductors of this network, considering grid code requirements. Hence, this study is distinguished by its innovative approach.

3. IMPACTS OF CYBERATTACK THROUGH HOME AUTOMATION SYSTEMS ON FINNISH TSO'S FREQUENCY MARKETS

3.1 Explanation of Frequency within context of Nordic Power System

Nominal frequency for Nordic power system is set to operate at 50 Hz; however, actual frequency always keeps on fluctuating around the nominal value because of imbalance between production and consumption. The larger the imbalance between production and consumption, larger will be the frequency deviations. Small imbalances usually occur because of stochastic changes in production and consumption of electricity. Large imbalances may happen because of sudden disconnection of any high voltage power line or large generator. Abrupt changes in frequency caused by such imbalances are resisted by kinetic energy/inertia of the power system. This inertia is usually provided by the synchronous machines which resists sudden frequency changes by providing or absorbing electric power from their rotational kinetic energy. So, power system which has higher inertia also has higher ability to mitigate abrupt frequency changes. To further control and limit frequency within secure range, power system reserves are utilized. Reserves are in the form of power generation units, controllable loads, and energy storage systems.

Fingrid is transmission system operator of Finland. It is part of Nordic power system which consists of TSO's of Finland, Norway, Sweden, and Eastern Denmark. Collectively, they comprise of Nordic load-frequency control (LFC) block where collective action is taken in order to control and limit frequency of the whole system within desirable limits. Aim of Nordic LFC block is to keep the frequency from deviating outside standard frequency range to 10000 minutes per year [23]. In order to limit the frequency within predefined range and to keep system operation in normal state, system inertia as well as power system reserves are utilized.

3.2 Reserve Markets in Nordic Power System and Procurement mechanisms of Fingrid

3.2.1 Frequency Containment Reserve

In order to contain frequency within predefined limits, fast activated automatic reserves are utilized in proportion to frequency deviation. FCR reserves are utilized for stabilization of fluctuations and maintenance of frequency within predefined limits in case of imbalances.

If frequency fluctuations are small, FCR for Normal operation (FCR-N) are utilized to keep frequency within the range of 49.9-50.1 Hz [23]. It is activated continuously as small variations between consumption and production always exists in large power systems. FCR-N full activation time is 3 minutes [23], and it must have capability to increase as well as decrease its production or consumption. As per FINGRID report in year 2022 [24], current volume for FCR-N is set at 600 MW for the entire Nordic synchronous system. Each country's TSO has to procure certain percentage of this volume on yearly basis which is determined based on the data from previous year. Each year, on 1st January, induvial shares of each TSO are revised.

If frequency fluctuations are larger, FCR for Disturbances (FCR-D) is utilized. FCR-D upregulation is activated for frequency range of 49.9-49.5 Hz [23]. FCR-D downregulation is activated for frequency range of 50.1-50-5 Hz [23]. Reference incident is the single largest disturbance that FCR-D should be able to mitigate in both upward and downward direction. To properly dimension FCR-D, following reference incidents are considered [23]:

- Single largest power generation unit
- Single largest demand facility
- Single HVDC interconnector
- Tripping of AC line
- Single failure on busbar tripping more than one consumption or generation unit.

In FINGRID report 2022 [24], total required volume for Nordic synchronous area was 1450 MW for FCR-D upregulation and 1400 MW for FCR-D downregulation. This volume is determined based on the ratio of sum of consumption and generation of a TSO to the sum of consumption and generation in the whole synchronous region. Formula

for determination of percentage of FCR reserves allotted to each TSO is as follows [24]:

$$Share_{TSO} = \frac{Consumption_{TSO} + Generation_{TSO}}{Consumption_{Synchronous\ Area} + Generation_{Synchronous\ Area}}$$

Primary source of procurement of FCR reserves from FINGRID is through the yearly market on the basis of competitive bidding. This procurement is done from the generation and consumption units located in Finland. For competitive bidding to procure volume through the yearly market, auction is held in Autumn every year. Based on the forecast, required volume is procured in advance for the upcoming whole year. [25]

As the forecasts are not entirely accurate, there is also an hourly market as well for FCR procurement. This market is utilized if additional reserves are required in case of lack of reserved volume in the yearly market. Marginal pricing principle is followed in hourly market where prices for every hour of the following day are separately defined. Moreover, Fingrid can procure FCR reserves from Estonian HVDC links, and other Nordic countries as well depending upon the level of requirement. So, overall, there are three different ways of FCR procurement. [25]

3.2.2 Frequency Restoration Reserve

Main purpose of frequency restoration reserve (FRR) is to restore frequency back to normal state in order to relieve and restore FCR capacity. FRR takes more time to get activated. FRR is mainly divided into two parts: Automatic frequency restoration reserve (aFRR) and manual frequency restoration reserve (mFRR). In Nordics, the main restoration reserve is mFRR as aFRR is still under the process of development and is still very limited in volume. [24]

mFRR is the only manual reserve under use in Nordic LFC block. Its full activation time is 15 minutes. As its activation time is longer than all other frequency reserves, it is used to relieve and restore all other reserves including FCR, FFR and aFRR. It is activated as a reaction to frequency imbalance as well as a proactive measure to prevent large imbalances. Furthermore, mFRR is dimensioned individually by TSO of each country within the Nordic LFC block. Moreover, volume procured for mFRR must be enough to cover reference incident. However, in this case, reference incident is the biggest disturbance of the control area of respective TSO. To procure balancing capacity mFRR, Fingrid utilizes three different methods. First method is utilization of reserve power plants which are activated after completion of energy bids. Second method is procurement of mFRR from capacity markets. Third method is occasional import from

Estonia. mFRR capacity is procured for both upregulation as well as downregulation. mFRR capacity market operates on weekly basis where marginal pricing principle is followed. Moreover, balancing energy mFRR market operates on hourly basis where the reserves bids are provided by reserve providers in balancing capacity market [23][24][26]

aFRR is the automatic complement to mFRR and is activated much faster. Capacities were introduced in 2013 in the Nordic synchronous area. It was done because of deteriorating frequency quality. aFRR reserves were initially procured for only morning and evening hours. However, they are now procured for almost every hour because of increasing frequency deviations. Furthermore, the procurement hours as well as volume for aFFR is determined quarterly by whole Nordic LFC block together. Then, the volume procured is divided among the TSOs in the following manner: [23][24][27]

Fingrid procures aFRR daily in its hourly market for both upregulation as well as downregulation. This procurement is done for the next day with resolution of one hour for the bids. Moreover, in procurement of aFRR, marginal pricing principle is followed. Furthermore, procurement of aFRR from Svenska Kraftnatät is also possible if needed. [24]

3.2.3 Fast Frequency Reserve

Sometimes, due to low inertia of the system, FCR-D is not fast enough to contain frequency within the normal state especially if there is any large disturbance. In order to tackle this issue, Fast Frequency Reserve was introduced in Nordic synchronous system in 2020. Until now, FFR is only being utilized for upregulation. It's the most quickly activated reserve which contains frequency until FCR-D becomes fully operational. FFR becomes fully operational from 0.7 to 1.3 seconds. It gets triggered when frequency goes below a certain activation threshold which might be set at 49.7, 49.6 or 49.5 Hz. [23][24][28]

Determination of volume of FFR required in the Nordic synchronous area is done through short term forecast of system inertia and reference incident. After that, the total capacity is distributed among Nordic TSOs. Fingrid has its own FFR market where it implies its own procurement strategy. FFR volume is procured in the hourly market based on marginal pricing method. Volume is only procured for the hours when its required based on forecasts and reference incident magnitude. Moreover, procurement from other countries is also possible if needed. [28]

3.3 Methodology for Risk Analysis of Fingrid Frequency Markets

Each country has its own mechanism of operation of its national grid along with management of associated frequency markets. In this thesis, Fingrid is the national grid upon which the impacts of cyberattack through home automation systems are studied. Two main cybersecurity threats through home automation cyberattack are identified: price manipulation and creation of volume shortage in frequency markets. Price manipulation of hourly frequency markets can be done by changing the demand through load change of hacked automated houses. This can be most impactful when the whole system has less amount of flexibility resources available to bid, and prices are already highly volatile. This can usually be done in order to gain profit, cause financial loss, create market instability, and hamper market functioning. In second method, volume shortage may be created through cyberattack. Hackers may recognize the most vulnerable hours during which volume is already scarce. After that, manipulation of hacked loads may be done in order to fuel the existing volume shortage. Furthermore, if hacked loads are already part of demand response, then prevention of their control from Fingrid might also cause further insufficiency of already scarce resources. If the amount of hacked load is large enough; unplanned outages or even nationwide blackout may occur. This is the most dangerous impact of a cyberattack through home automation systems and should be deemed important in terms of national security as well.

3.3.1 Load Group Types & Hacker Actions

There are two types of hacked home automated loads which can be used to cause harmful impacts for grid during risk hours. Let’s categorize them into load type 1 and load type 2. Load type 1 are simple hacked home automated loads which are not part of demand response. Load type 2 are those loads which are designated as demand response for a certain frequency market.

Hacker action for load type 1 can be load manipulation during risk hours. However, for load type 2, hacker action can be load manipulation and/or demand response blockage. So, hacking of load type 2 can prove to be more detrimental for frequency markets as well as National grid operation. Furthermore, strategies of static, dynamic and interzone attacks can also be utilized through both load types [20].

Table 3.1 *Hacker Actions for different Load Types*

Hacker Action	Load Type 01	Load Type 02
Load Manipulation	Yes	Yes
Demand Response Blocking	No	Yes

3.3.2 Volume Shortage Risk Analysis

Each frequency market has predetermined amount of volume which should be procured. This volume may be procured through multiple ways such as yearly market, reserve power plants, hourly market (daily or weekly procurement), and import of capacity from neighboring countries. Most of the frequency markets of Fingrid usually utilize a combination of all or some of the aforementioned methods of volume procurement. Yearly volume procurement is done based on volume requirement forecasts of the entire year. As forecasts are subject to error, remaining volume is procured through hourly markets and import of capacity.

If there is shortage of available volume in these markets, then procurement would be less than required target. It symbolizes the incapacity of Fingrid to completely control frequency under all circumstances. It also indicates risks associated with power system stability of Fingrid as well as of Nordic synchronous system.

a) Volume Shortage Analysis of FCR Markets

FCR volume procurement is done through combination of yearly market, hourly volume procurement through daily market and import of capacity from neighboring countries [25]. As predetermined amount of volume is procured based on forecasts for entire year, remaining volume is procured through hourly market and import. Their data is utilized to assess volume shortage. For any hour to be considered as risk hour in terms of volume shortage for FCR markets, following conditions must be met:

- Price of hourly procured volume from daily market should be at least twice the average hourly price.
- No capacity from that market is being exported to another country during that particular hour.
- More than 80 percent of hourly volume from daily market is procured.

This combination of conditions symbolize shortage of available volume in FCR markets. Price condition is kept in order to ensure that volume is urgently required even at high prices. Condition of no export of capacity from Finland ensures volume require-

ment within the country. Last and the most important condition is that more than 80 percent of hourly volume from daily market gets procured. If all of the three aforementioned conditions are fulfilled, an hour can be characterized as risk hour in terms of volume shortage. Furthermore, along with the prerequisite that first two conditions are being met, if 80-90% of hourly market volume is procured, that hour is termed as low risk hour. If this percentage is 90-95%, that hour is medium risk hour. If more than 95% of hourly bids get procured, then an hour is indicated as high-risk hour.

b) Volume Shortage Analysis of Balancing Capacity mFRR market

Balancing capacity mFRR market was initiated by Fingrid in 2016. This market was initiated to ensure the sufficiency of manual frequency restoration reserves in case of dimensioning fault. Reserve providers whose capacity bids are accepted in this market are obliged to provide energy bids to the balancing energy market for financial compensation. According to Fingrid [26], main procurement method for balancing capacity mFRR reserves is through reserve power plants. After that, remaining capacity is procured through capacity markets which operate on weekly basis. Furthermore, if volume is still required, it is procured through import from neighboring countries. Based on the available data (weekly market and import of capacity), following conditions must be met for any hour to be considered as risk hour in terms of volume shortage:

- Price of hourly procured volume from weekly capacity market should be at least twice the average hourly price of the market under study.
- No capacity is being exported to another country during that particular hour.
- More than 80 percent of hourly volume from weekly capacity market is procured for that particular hour through weekly market.

Along with no export condition and price limit, if 80-90% of volume is procured for an hour through weekly market, that hour is termed as low risk hour. If this percentage is 90-95%, that hour is medium risk hour. If more than 95% of bids get procured for an hour, then that hour is indicated as high risk hour.

c) Volume Shortage Analysis of Balancing Energy mFRR market

According to Fingrid [26], balancing energy market organized by Fingrid is part of Nordic balancing energy market which is also termed as regulating power market. Balancing energy market is used to balance generation and consumption in real time through utilization of manual frequency restoration reserves. Balancing energy market mainly

operates through the reserves bid by reserve providers in balancing capacity market. Moreover, balancing energy is procured through the hourly market where prices and bids are published with one hour delay. Moreover, price structure for this market is different from other frequency markets. For upregulation, price in the balancing energy market is the price of most expensive bid used in the market during a particular hour; however, it is at least the day ahead market price. For volume shortage analysis of balancing energy mFRR upregulation market, following criteria is set:

- If 80-90% of volume from the total bids offered by Finnish parties in balancing energy market mFRR upregulation in Finland is ordered for an hour through the hourly market, that hour is termed as low risk hour. If this percentage is 90-95%, that hour is medium risk hour. If more than 95% of bids get ordered for an hour, then that hour is indicated as high-risk hour. It must be noted that for this market, for some hours, ordered bids may exceed offered bids by Finnish parties in the market. Those hours are also considered within the category of high risk hours.
- Price of that particular hour is at least twice the mean hourly price throughout the years.

For volume shortage analysis of balancing energy mFRR downregulation market, price is not considered. For this market, hourly price is the cheapest bid used in the market during a particular hour; however, it is at most the Elspot Finland price. Moreover, hourly price in this market goes negative on many occasions. Hence, volume shortage analysis of balancing energy mFRR downregulation market, following criteria is set:

- If 80-90% of volume from the total bids offered by Finnish parties in balancing energy mFRR downregulation market in Finland is ordered for an hour through the hourly market, that hour is termed as low risk hour. If this percentage is 90-95%, that hour is medium risk hour. If more than 95% of bids get ordered for an hour, then that hour is indicated as high-risk hour. It must be noted that for this market, for some hours, ordered bids may exceed offered bids by Finnish parties in the market. Those hours are also considered within the category of high-risk hours.

d) Volume Shortage Analysis of FFR market

According to Fingrid [28], hourly procurement for FRR is done through daily market. If more reserves are needed for a particular hour, import from other countries can also be

done. However, no trade data is available on Fingrid open data site. So, volume shortage analysis for FFR market is conducted through two conditions which are as follows:

- Price of hourly procured volume from daily market should be at least twice the average hourly price.
- More than 80 percent of hourly volume is procured for that particular hour through daily market. If 80-90% of volume is procured for an hour through weekly market, that hour is termed as low risk hour. If this percentage is 90-95%, that hour is medium risk hour. If more than 95% of bids get procured for an hour, then an hour is indicated as high risk hour.

e) Hacker Actions & their Impacts during Volume Shortage Risk Hours

If large amount of home automated loads get hacked, these loads can be used to destabilize the power system especially during volume shortage risk hours. During these hours, availability of enough amount of volume is already a problem. If hacked loads belong to load type 1, load manipulation can be done by hackers during volume shortage risk hours. However, if hacked loads are part of demand response (load type 02), then blockage of desired operation of such loads can also be done by hackers. Furthermore, load manipulation and demand response blocking may be done simultaneously to cause most devastating effects.

At small scale, such a scenario may result in unplanned outages. However, if large number of loads get hacked during volume availability based high risk hours, then whole power system may get effected causing nationwide or even systemwide blackout. Such a scenario poses a serious risk not only to power system stability of Finland but also to whole Nordic synchronous area. It also poses a threat to the national security of Nordic countries.

3.3.3 Price Based Risk Analysis

If frequency markets operated perfectly, then price volatility would be minimum, and prices would always correspond to actual volume availability. However, that is not always the case because of multiple reasons including market's structural deficiencies, inaccurate weather forecasts, expensive electricity production sources, power inadequacy, anticipation, and profit maximization efforts of market actors [29]. Severity of any or combination of aforementioned issues may cause unrealistic price hikes. Such unrealistically high-priced hours are termed as price based risk hours.

For FCR markets, price-based analysis is conducted on hourly markets which are used for volume procurement on daily basis. Similarly, for FFR market, hourly prices of day ahead market are utilized for this analysis. However, for balancing capacity mFRR market, analysis is conducted for hourly prices for volume procured through weekly market. Furthermore, for balancing energy mFRR upregulation market, hourly prices are utilized which are published after one hour delay. For all of the aforementioned markets, in order to assess the number of risk hours during a particular time frame, average hourly market price is calculated throughout the years. Based on average price, risk hours are identified. All the hours having price equal to or less than five times the average price are considered to be at no risk as this degree of market volatility is considered to be normal. If the procurement price for an hour is between five to ten times the average hourly market price, that hour is considered as low risk hour. If this price is between ten to twenty times the average price, that hour is characterized as medium risk hour. If price for hourly procured volume is more than 20 times the overall average market price, then such hour is characterized to be high risk hour.

However, price-based risk analysis is assessed differently for balancing energy mFRR downregulation market. It is assessed differently because market operation is different than all other markets. Here, prices often become negative due to which same formula cannot be used as for all other markets. Hence, for this market, initially mean and standard deviation of hourly price is calculated since data has become available. Then, following formula based on normal distribution is devised:

$No\ Risk\ Hours$:

$$x = \mu \pm 4\sigma$$

$Low\ Risk\ Hours$:

$$(\mu - 8\sigma) \leq x < (\mu - 4\sigma)\ or\ \ (\mu + 4\sigma) < x \leq (\mu + 8\sigma)$$

$Medium\ Risk\ Hours$:

$$(\mu - 16\sigma) \leq x < (\mu - 8\sigma)\ or\ (\mu + 8\sigma) < x \leq (\mu + 16\sigma)$$

$High\ Risk\ Hours$:

$x < (\mu - 16\sigma)\ or\ x > (\mu + 16\sigma)$

where

μ is the mean price of the hourly market throughout the years.

σ is the standard deviation of hourly market prices throughout the years.

x represents risk hours in the market.

a) Hacker Actions & their Impacts during Price based Risk Hours

Risk of market manipulation through hacked home automated loads increases manifolds if a market has lot of high or medium risk hours. As during those hours, even mediocre amount of load manipulation and/or demand response control blockage may cause prices to reach market caps. Such high prices may create market panic, render market functioning to be unstable, increase financial profits and/or cause monetary loss to certain parties or Fingrid. Very high increase in market prices indicate poor planning as well as inadequate market structure. This may also indicate lack of capacity of frequency market to properly control frequency at all times.

Furthermore, high risk price hours may coincide with high risk volume shortage hours. Hacker actions of load manipulation and/or demand response blocking in such hours would cause effect on frequency market as well as grid. In this scenario, market as well as grid may get affected simultaneously as a result of any cyberattack.

3.4 Results for Risk Analysis of Fingrid Frequency Markets

3.4.1 FCR-D Upregulation

FCR-D Upregulation market analysis is conducted based on the data available for hourly market bids, procurement from hourly market, hourly market prices, and foreign trade. The aforementioned data is available from 2019 which is the year since when the analysis has been conducted. Analysis is conducted for each year from 1st January to 31st December. However, for year 2023, analysis is conducted from 1st January until 31st July due to data availability and project timeline. [25][30]

It can be seen from the table 3.2 that year 2022 has had the most number of risk hours in terms of price based risk analysis. However, table 3.3 shows that in terms of volume shortage risk analysis, year 2023 has had most number of risk hours. Moreover, trends from tables below also shows that throughout the years, instead of FCR-D Upregulation market operation getting better, it has gone worse as the number of total risk hours increase according to both analyses. Hence, market operation has deteriorated over time not only in terms of prices but also volume availability in the hourly market. [30]

Table 3.2 *Price based Risk Analysis of FCR-D Upregulation Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2019	4	7	58
2020	4	2	50
2021	7	8	163
2022	75	87	248
2023	4	87	333

Table 3.3 *Volume Shortage based Risk Analysis of FCR-D Upregulation Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2019	4	0	0
2020	4	0	0
2021	8	2	9
2022	7	12	53
2023	16	17	80

As of December 2023, more than 40 % of overall certified FCR-D Upregulation capacity for Fingrid is through consumption sources for demand response categorized as load type 02 [25]. These consumption sources may contain certain amount of domestic home automated loads as well which may be utilized for cyberattack. However, Load type 1 can only be utilized for load increment as this load is not part of allocated demand response.

Furthermore, to cause price manipulation in FCR-D Upregulation market, presence of fault in the system is not necessary. However, to create grid instability through hacked loads, there must be a massive frequency dip in the system during risk hours. Such frequency dip may be caused by power flow conditions close to stability limits or large scale fault causing outage of a critical component of the system such as large generation unit or transmission line. In terms of faults on HV grid, ten-year annual average (2013-2022) of number of disturbances is 418 in 100-400 kV grids for Fingrid [31]. Alone in 2022, there were 572 grid disturbances for 100-400 kV grids in Finland [31]. If any of those large scale disturbances aren't handled well by system protection and cause frequency deviation, hackers may exploit that opportunity to create further grid instability. However, impact of such instability also depends on scale of such fault, level of frequency dip, scarcity level of available volume in the market, amount of hacked loads, and the exact timing of hacker action during volume shortage risk hours. Worst case scenario may occur when there is dimensioning fault causing major outage of a critical component of power system during market volume shortage high risk hours,

and large amount of home automated loads are hacked. Such a scenario may cause frequency to drop beyond controllable limits which may lead to outages or even black-outs. However, probability of occurrence of such event is not known. Moreover, determination of the exact amount of load in accordance with load type to simulate any outage or blackout is beyond the scope of this study.

Table 3.4 *Fault Conditions for Risk creation through FCR-D Upregulation Market*

Risk	Large Scale Fault Requirement
Price Manipulation Risk	No
Volume Shortage Risk	Yes

Figure 3.1 shows the visual representation of price-based risk analysis for FCR-D Up-regulation for the year 2022. Volume shortage index on x-axis is the ratio of hourly procured volume to hourly offered volume in the daily market. Price of hourly procured volume is shown on y-axis. It can be seen from the figure that this year has had lots of risk hours representing very high price volatility in the market. Blue pointers represent no risk hours where price was within 5 times the overall average hourly market price. Then, as the price keeps on getting higher, level of risk keeps on increasing. Moreover, a market trend is also evident that prices show direct correlation to volume shortage index. This trend is represented through the arrow in the graph below. (To further analyze such trends for other years, graphs can be found in attachment document of this thesis [32])

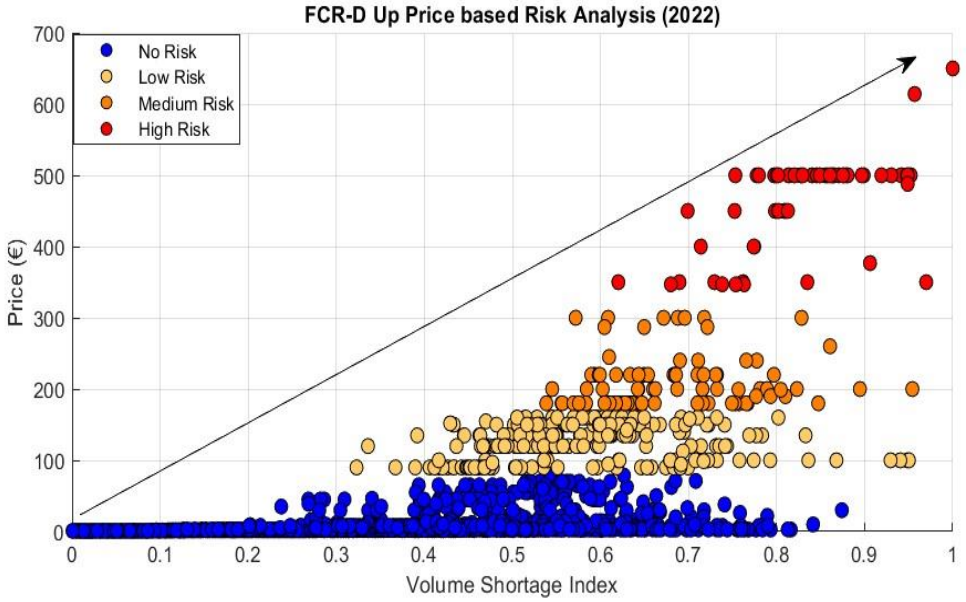


Figure 3.1 *FCR-D Up Price based Risk Analysis (2022)*

Figure 3.2 shows the visual representation of volume shortage-based risk analysis for FCR-D upregulation for the year 2023. It can be seen from the figure that this year has

had the greatest number of risk hours in terms of volume scarcity. Blue pointers represent no risk hours where volume shortage index was less than 0.8. Then, as the volume shortage index increases, scale of risk increases as well. Moreover, market trend of direct correlation between volume shortage index and price is evident here as well. (To further analyze such trends for other years, graphs can be found in attachment document of this thesis [32])

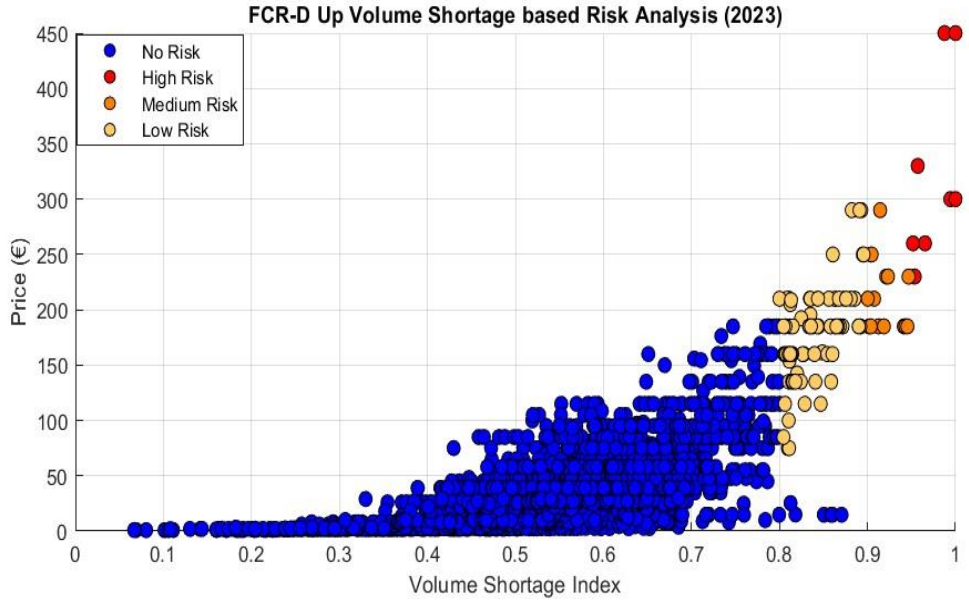


Figure 3.2 *FCR-D Up Volume Shortage based Risk Analysis (2023)*

3.4.2 FCR-D Downregulation

Main purpose of FCR-D Downregulation is to bring down frequency to normal range during disturbances. This market was initiated by Fingrid in 2022. Analysis is conducted for whole year of 2022, and for 2023 from January until September. [25][30]

It can be seen from the table 3.5 and table 3.6 that year 2022 was more concerning in terms of price volatility, and year 2023 was more concerning in terms of volume shortage risk. Price volatility remained high during 2022 but risk level remained low. However, volume shortage instances during 2023 were severe. Fingrid needs to improve FCR-D downregulation market operation especially in terms of volume procurement. [30]

Table 3.5 *Price based Risk Analysis of FCR-D Downregulation Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2022	0	2	461
2023	0	0	43

Table 3.6 *Volume Shortage based Risk Analysis of FCR-D Downregulation Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2022	0	2	5
2023	35	12	89

According to Fingrid data, 18.18% of sources utilized for FCR-D Downregulation are of consumption category which are categorized as load type 2 [25]. Hackers may utilize these loads for load decrement as well as demand response blockage. However, load type 1 can only be utilized for load decrement as this load is not part of allocated demand response.

Fault requirement is same as of FCR-D Upregulation. For creation of market instability, it is not necessary that fault occurs in the grid. However, to create national grid instability, large scale fault or major frequency rise in the network must be present especially during risk hours.

Table 3.7 *Fault Conditions for Risk creation through FCR-D Downregulation Market*

Risk	Large Scale Fault Requirement
Price Manipulation Risk	No
Volume Shortage Risk	Yes

Figure 3.3 shows the visual representation of price based risk analysis for FCR-D downregulation for the year 2022. Volume shortage index on x-axis is the ratio of hourly procured volume to hourly offered volume in the daily market. Price of hourly procured volume is shown on y-axis. It can be seen from the figure that this year has had lot of low and medium risk hours representing high price volatility in the market. Blue pointers represent no risk hours where price was within 5 times the overall average hourly market price. Then, as the price keeps on getting higher, level of risk keeps on increasing. Moreover, the direct correlation between price and volume shortage index does not seem to be very strong for this year. (To further analyze such trends for other years, graphs can be found in attachment document of this thesis [32])

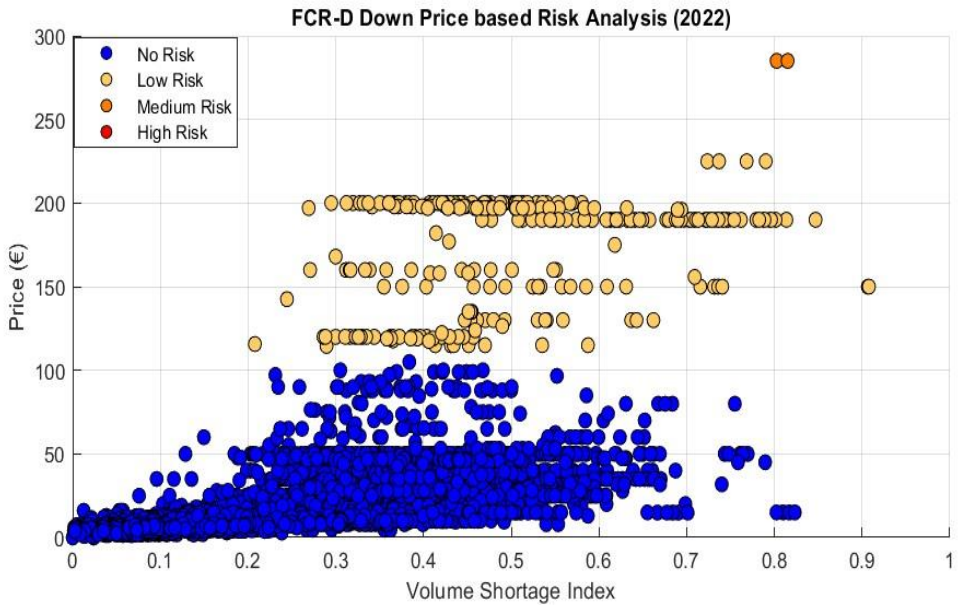


Figure 3.3 *FCR-D Down Price based Risk Analysis (2022)*

Figure 3.4 shows the visual representation of volume shortage-based risk analysis for FCR-D downwards regulation for the year 2023. It can be seen from the figure that this year has had the greatest number of risk hours in terms of volume scarcity. Blue pointers represent no risk hours where volume shortage index was less than 0.8. Then, as the volume shortage index increases, scale of risk increases as well. Moreover, market trend of direct correlation between volume shortage index and price is stronger for this year as compared to 2022. (To further analyze such trends for other years, graphs can be found in attachment document of this thesis [32])

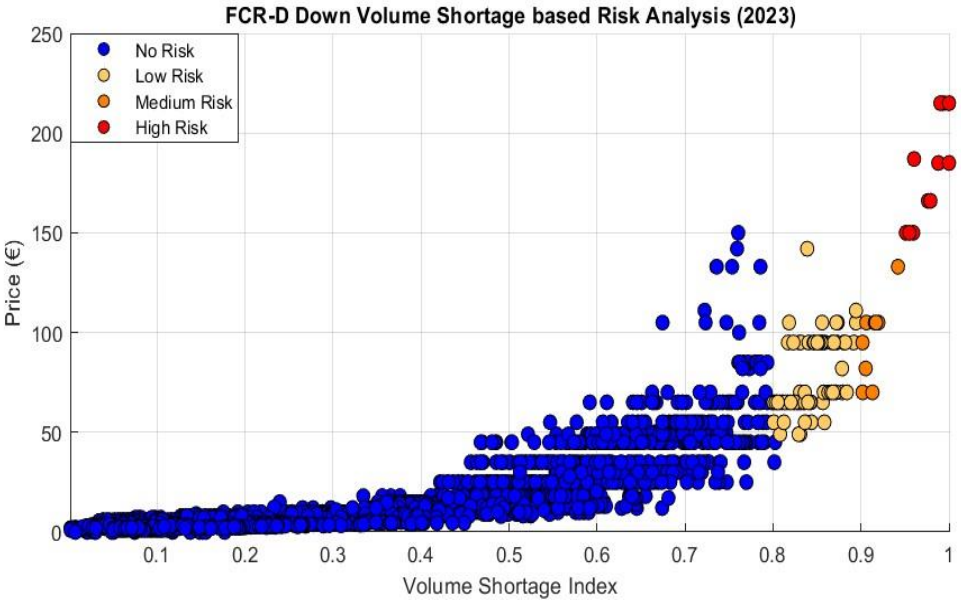


Figure 3.4 *FCR-D Down Volume Shortage based Risk Analysis (2023)*

3.4.3 FCR-N

FCR-N market analysis is conducted based on the data available for hourly market bids, procurement from hourly market, hourly market prices, and foreign trade. The aforementioned data is available from 2019 which is the year since when the analysis has been conducted. Analysis is conducted from 2019 for each year from 1st January to 31st December. However, for year 2023, analysis is conducted from 1st January until 31st May due to data availability and project timeline. [25] [30]

FCR-N market operation is very important from grid operation perspective as its capacity is operating at all times to keep frequency within normal range. As it can be seen from the tables below, FCR-N market has much lower amount of high and medium risk hours as compared to FCR-D Up and Downregulation markets. From price perspective, hourly market has never had a high-risk year during analysis timespan. However, price volatility was high for year 2022 which is evident by number of low-risk years which can be observed from table 3.8. Moreover, table 3.9 shows that, from volume availability perspective, some high-risk hours were present for some of the years, but their number is quite small. Moreover, there is neither any consistency nor any pattern for volume scarcity in the hourly market. [30]

Table 3.8 *Price based Risk Analysis of FCR-N Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2019	0	6	32
2020	0	0	0
2021	0	0	18
2022	0	0	411
2023	0	4	108

Table 3.9 *Volume Shortage based Risk Analysis of FCR-N Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2019	4	17	28
2020	0	0	8
2021	3	3	18
2022	0	0	0
2023	1	1	34

According to Fingrid data, 2.25% of sources utilized for FCR-N are of consumption category which are categorized as load type 2 [25]. They can be utilized for load manipulation as well as demand response blocking by hackers. The amount of load type 2 is too small to create any major market or grid impact from hacker's point of view. How-

ever, Load type 1 can only be utilized for load manipulation as this load is not part of allocated demand response. The level of impact created through load type 01 depends upon the amount of hacked load. However, very less amount of risk hours are available for hackers to cause serious concern.

There is no fault requirement for hacker in order to cause problems for FCR-N market reserves. Existence of large-scale fault may make the situation worse, but it is not a prerequisite either for price manipulation or creation of grid instability. One possible scenario is that due to hacker actions during volume scarce hours, frequency can't be limited by FCR-N, and it goes beyond the normal range. Then, other reserves such as FCR-D and mFRR would be required for frequency containment and restoration.

Table 3.10 *Fault Conditions for Risk creation through FCR-N Market*

Risk	Large Scale Fault Requirement
Price Manipulation Risk	No
Volume Shortage Risk	No

Figures 3.5 and 3.6 provide visual representation of price-based as well as volume shortage risk analysis for FCR-N for the year 2023. In both these figures, volume shortage index on x-axis is the ratio of procured volume to offered volume in the daily market. Moreover. price of hourly procured volume is represented on y-axis.

For price-based risk analysis, it can be seen that prices below five times the overall average hourly price cause no risk. Then, as the price keeps on getting higher, level of risk keeps on increasing. Moreover, market trend of direct correlation between volume shortage index and price is evident here as well. (To further analyze such trends for other years, graphs can be found in attachment document of this thesis [32])

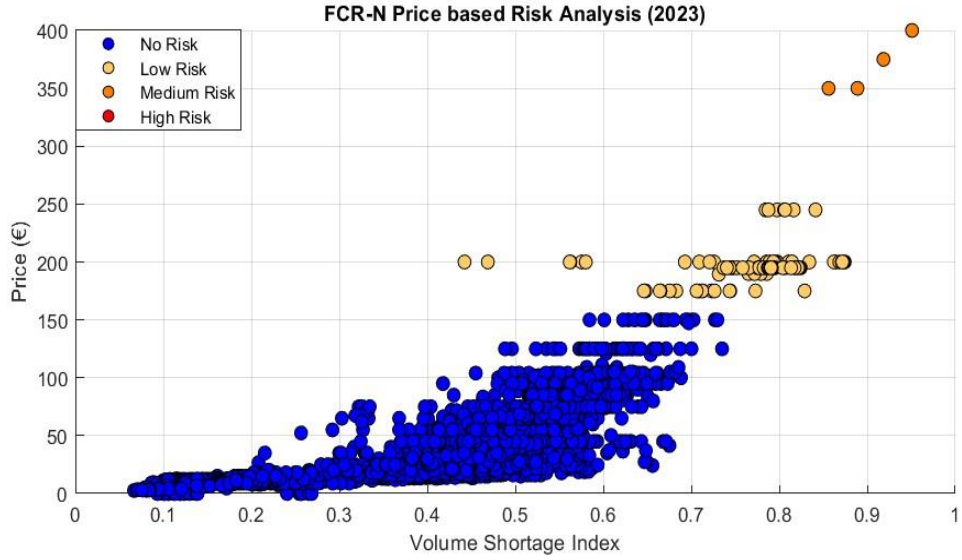


Figure 3.5 *FCR-N Price based Risk Analysis (2023)*

For volume shortage-based risk analysis for this year, blue pointers represent no risk hours where volume shortage index was less than 0.8. Then, as the volume shortage index increases, scale of volume scarcity risk increases as well.

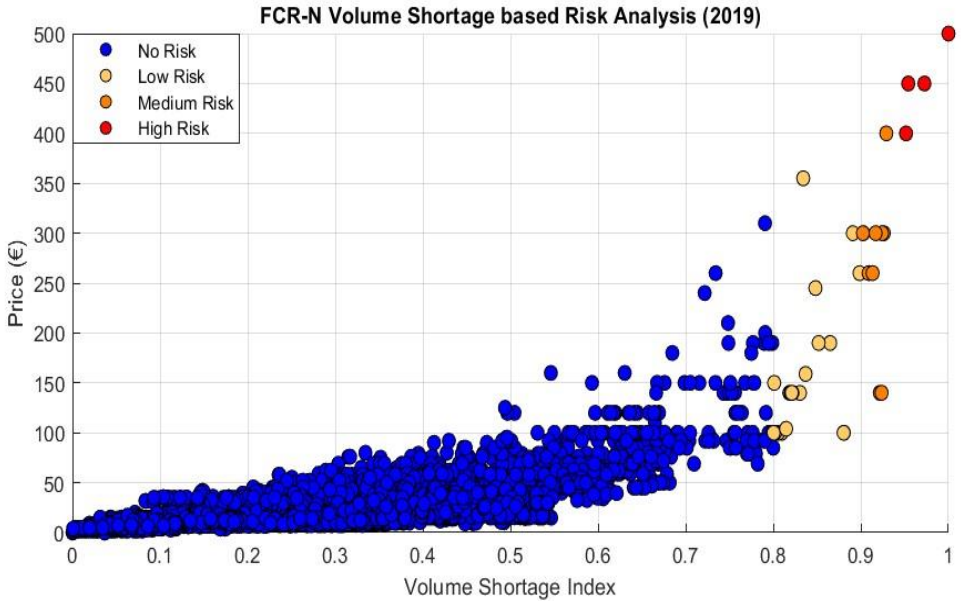


Figure 3.6 *FCR-N Volume Shortage based Risk Analysis (2019)*

3.4.4 Balancing Capacity mFRR Upregulation

Main purpose of mFRR is to restore frequency to normal range, and relieve FCR and FFR reserves. Procurement of balancing capacity for mFRR Upregulation is done through reserve power plants, weekly capacity market and occasional import from neighboring countries. Required data for analysis was available for year 2023 from January until September for which the analysis has been conducted. This market was initiated in 2016, and data before this time period has been termed as test data by Fingrid. [26][30]

Table 3.11 shows that in terms of price based risk, Balancing Capacity mFRR Upregulation market has no high risk hours during the analysis period. Although price has been volatile for many hours but degree of volatility has remained low. Table 3.12 shows that in terms of volume shortage, there has been some high and medium risk hours but their numbers have been quite low. However, low risk hours for volume shortage have been quite significant in number. Overall, there is not major alarming situation for Balancing Capacity mFRR Upregulation market but sufficiency of volume at lower prices should be improved further. [30]

Table 3.11 *Price based Risk Analysis of Balancing Capacity mFRR Upregulation Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2023	0	19	397

Table 3.12 *Volume Shortage based Risk Analysis of Balancing Capacity mFRR Upregulation* Market

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2023	4	2	287

Fingrid has not shared information as to how much consumption sources are being utilized for Balancing Capacity mFRR Upregulation. If there are consumption sources being utilized, then both load types can be used by hackers to disrupt market functioning and destabilize National grid. However, if no consumption units are being utilized by Fingrid for Balancing Capacity mFRR Upregulation, only load type 1 can be used by hackers as this load would not be part of designated demand response. This action would prove to be less effective as compared to use of load type 2. However, if the amount of hacked load is high, then it can cause damaging effects as well.

Moreover, no fault is required for price manipulation of capacity market. However, for causing National grid instability, fault may or may not be present in the system. Usually, Balancing Capacity mFRR Upregulation is operated after fault has been removed but that is not always the case. Main purpose of creation of grid instability requires that frequency is not restored to normal range within designated time irrespective of fault existence or not. Hence, exact fault condition does not exist in that case.

Table 3.13 *Fault Conditions for Risk creation through Balancing Capacity mFRR Upregulation Market*

Risk	Large Scale Fault Requirement
Price Manipulation Risk	No
Volume Shortage Risk	Yes/No

Figures 3.7 and 3.8 provide the visual representation of price based as well as volume shortage risk analysis for Balancing Capacity mFRR Upregulation for the year 2023. In both these figures, volume shortage index on x-axis is the ratio of hourly procured volume to hourly offered volume in the weekly market. Moreover. price of this hourly procured volume is represented on y-axis.

For price-based risk analysis, prices below five times the overall average hourly price causes no risk. Then, as the price keeps on getting higher, level of risk keeps on increasing. Moreover, market trend of direct correlation between volume shortage index

and price exists but some irregularities are also evident. These irregularities are more evident in the markets which have recently begun operation such as FCR-D downregulation as well as Balancing Capacity mFRR Upregulation market.

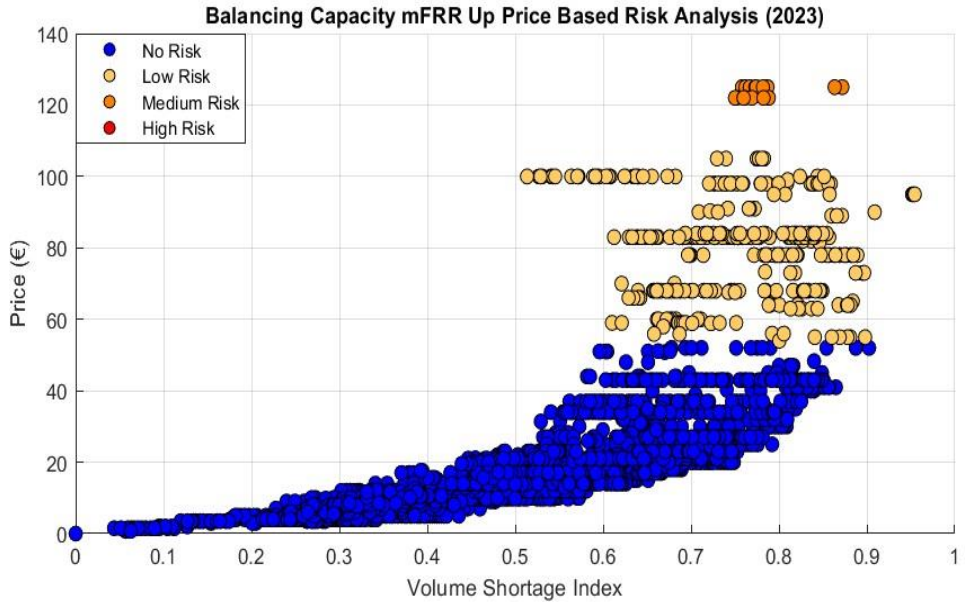


Figure 3.7 *Balancing Capacity mFRR Up Price based Risk Analysis (2023)*

For volume shortage-based risk analysis for this year, blue pointers represent no risk hours where volume shortage index was less than 0.8. Then, as the volume shortage index increases, scale of volume scarcity risk increases as well.

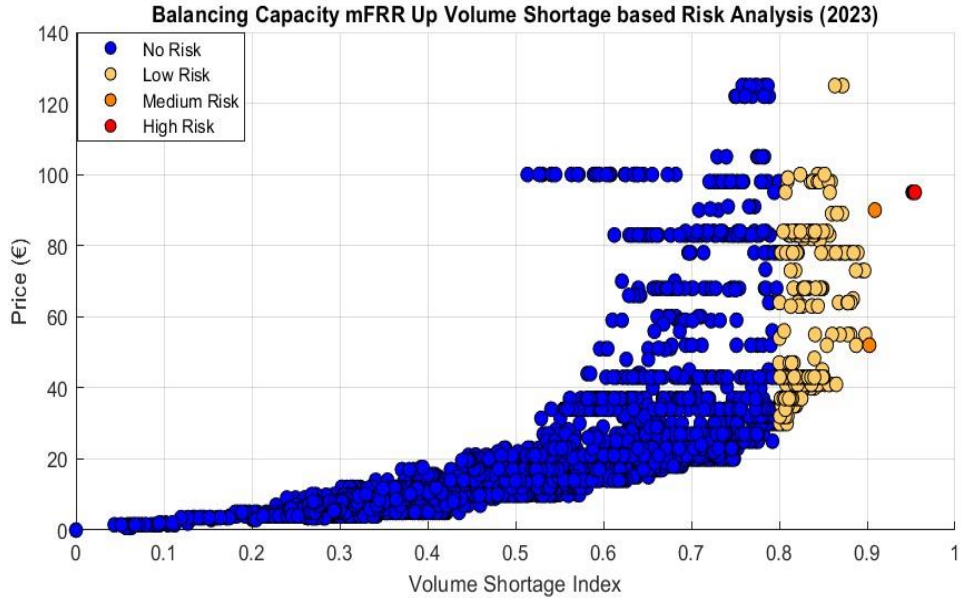


Figure 3.8 *Balancing Capacity mFRR Up Volume Shortage based Risk Anal ysis (2023)*

3.4.5 Balancing Capacity mFRR Downregulation

Procurement of Balancing Capacity mFRR downregulation is done through reserve power plants, weekly capacity market, and occasional import from neighboring countries. Balancing capacity mFRR Downregulation market was initiated by Fingrid in 2023. Available data is from January until September 2023 for which this analysis has been conducted. [26][30]

Table 3.14 shows that during the analysis time period, there were no price based high risk hours. Price volatility was also not significantly high as well. Furthermore, it can be observed from table 3.15 that volume based high and medium risk hours were more than balancing capacity mFRR upregulation. However, volume based low risk hours were lower as compared to balancing capacity mFRR upregulation market. This shows that market volume remains sufficient for most of the time. However, occurrences of insufficiency of volume are of more serious degree. In terms of volume availability, there is room for improvement in number of high and medium risk hours. [30]

Table 3.14 *Price based Risk Analysis of Balancing Capacity mFRR Downregulation Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2023	0	5	62

Table 3.15 *Volume Shortage based Risk Analysis of Balancing Capacity mFRR Downregulation Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2023	7	29	164

Load types and their use by hackers are same as Balancing Capacity mFRR Upregulation market. One major difference would be that instead of load increment, hackers would employ load decrement if attack is directed at Balancing Capacity mFRR Downregulation market. Moreover, fault conditions are also same for Balancing Capacity mFRR Up as well as Downregulation markets.

Table 3.16 *Fault Conditions for Risk creation through Balancing Capacity mFRR Downregulation Market*

Risk	Large Scale Fault Requirement
Price Manipulation Risk	No
Volume Shortage Risk	Yes/No

Figures 3.9 and 3.10 provide the visual representation of price based as well as volume shortage risk analysis for balancing capacity mFRR downregulation for the year 2023. In both these figures, volume shortage index on x-axis is the ratio of hourly procured volume to hourly offered volume in the weekly market. Moreover. price of this hourly procured volume is represented on y-axis.

For price-based risk analysis, it can be seen that prices below five times the overall average hourly price causes no risk. Then, as the price keeps on getting higher, level of risk keeps on increasing. Moreover, market trend of direct correlation between volume shortage index and price can also be seen.

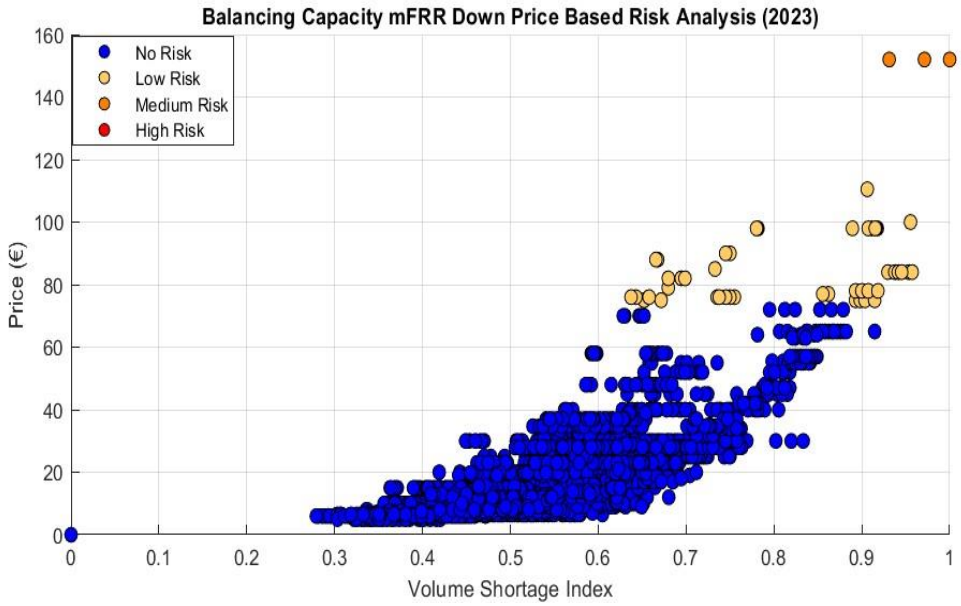


Figure 3.9 *Balancing Capacity mFRR Down Price based Risk Analysis (2023)*

For volume shortage-based risk analysis for this year, blue pointers represent no risk hours where volume shortage index was less than 0.8. Then, as the volume shortage index increases, scale of volume scarcity risk increases as well.

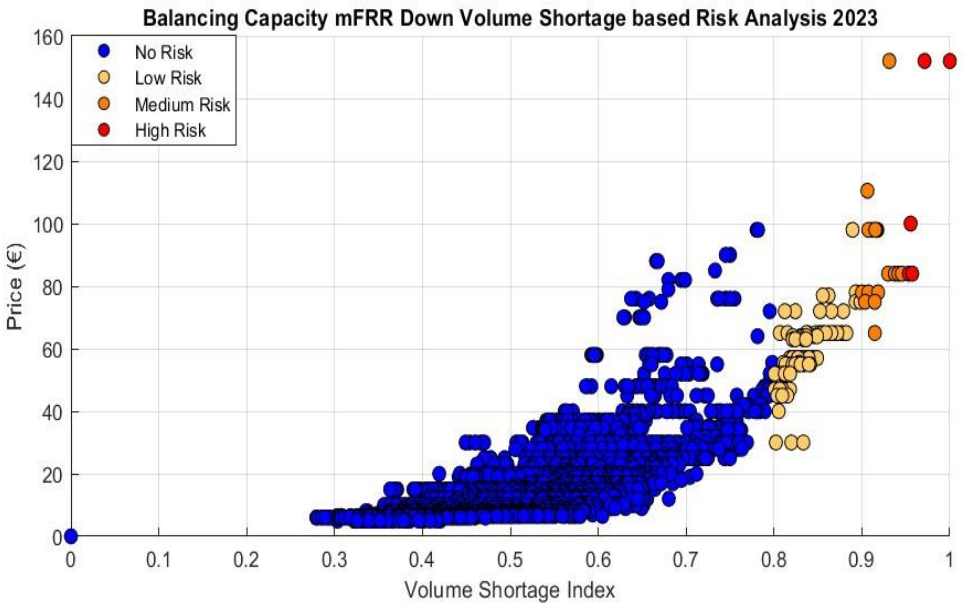


Figure 3.10 *Balancing Capacity mFRR Down Volume Shortage based Risk Analysis (2023)*

3.4.6 Balancing Energy mFRR Upregulation

Balancing Energy market mainly operates through reserves bids by reserve providers in Balancing Capacity market. Moreover, Balancing Energy mFRR Upregulation is procured through the hourly market where prices and bids are published with one hour delay. Analysis is conducted for each year from 1st January until 31st December. However, for year 2023, analysis is only conducted from January until May due to data availability and project timeline. [26][30]

For volume shortage analysis, '*' sign represents those years where the amount of ordered upregulation bids exceeded total number of bids offered by Finnish parties at least for one hour during the year. Those hours are categorized within the high-risk hour zone. It must be noted that this phenomenon is only present in Balancing Energy mFRR Up and Downregulation markets.

Table 3.18 shows that in terms of volume shortage, number of risk hours have remained low throughout the years. However, for the years 2008, 2010, 2012, 2013, 2015 and 2018, at least once the number of ordered bids have exceeded the total offered bids by Finnish parties in the market. It means that volume shortage index crosses the limit of 1. This type of situation is not preferrable at all because it shows that bids offered by Finnish parties in the market proved to be insufficient. Moreover, table 3.17 shows that in terms of price volatility, market performed worst in year 2022 as compared to all other years.

Table 3.17 *Price based Risk Analysis of Balancing Energy mFRR Upregulation Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2007	3	0	9
2008	4	1	4
2009	2	2	8
2010	3	10	52
2011	0	5	19
2012	9	11	37
2013	1	0	8
2014	0	0	14
2015	2	2	24
2016	1	2	12
2017	0	3	9
2018	1	5	12
2019	2	3	17
2020	4	1	25
2021	17	35	169
2022	15	197	1507
2023	2	3	24

Table 3.18 *Volume Shortage based Risk Analysis of Balancing Energy mFRR Upregulation Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2007	2	0	2
2008*	4	0	5
2009	0	2	0
2010*	3	1	7
2011	0	0	1
2012*	3	1	7
2013*	1	0	2
2014	0	0	1
2015*	3	0	4
2016	0	0	1
2017	0	0	0
2018*	1	0	0
2019	0	0	3
2020	0	1	5
2021	3	0	2
2022	1	1	4
2023	0	0	1

Furthermore, as of May 2023, between 15 and 470 MW of consumption sources were being utilized as demand response (classified as load type 2) within this market [33]. These consumption sources may include a certain proportion of domestic home automated loads, which are vulnerable to cyberattacks through strategies such as load manipulation and demand response blocking by hackers. In contrast, load type 1, which is not part of the allocated demand response, can only be exploited for load manipulation. Moreover, fault conditions remain same for both the Balancing Energy and Balancing Capacity markets.

Table 3.19 *Fault Conditions for Risk creation through Balancing Energy mFRR Upregulation Market*

Risk	Large Scale Fault Requirement
Price Manipulation Risk	No
Volume Shortage Risk	Yes/No

Figure 3.11 provides representation of price based risk analysis for Balancing Energy mFRR Upregulation market for year 2022. In this figure, volume shortage index on x-axis is the ratio of procured volume to offered volume in the hourly market. Moreover, price of this hourly procured volume is represented on y-axis. It can be seen from the figure that prices remained highly volatile throughout the year. Moreover, this market had the most number of medium and low risk hours in 2022 than any other year. Moreover, direct correlation between price and volume shortage index exists but it does not seem be very strong for Balancing Energy mFRR Upregulation market. (To further analyze such trends for other years, graphs can be found in attachment document of this thesis [32])

Figure 3.12 provides representation of volume shortage analysis for Balancing Energy mFRR Upregulation market for year 2008. It can be observed that although the number of instances of risk are not alot, the intensity of two high risk hours is very high. In fact, one high risk hour has more than 7 times the amount of ordered energy as compared to offered bids by Finnish parties. This is representation of very dire situation for the market during these hours.

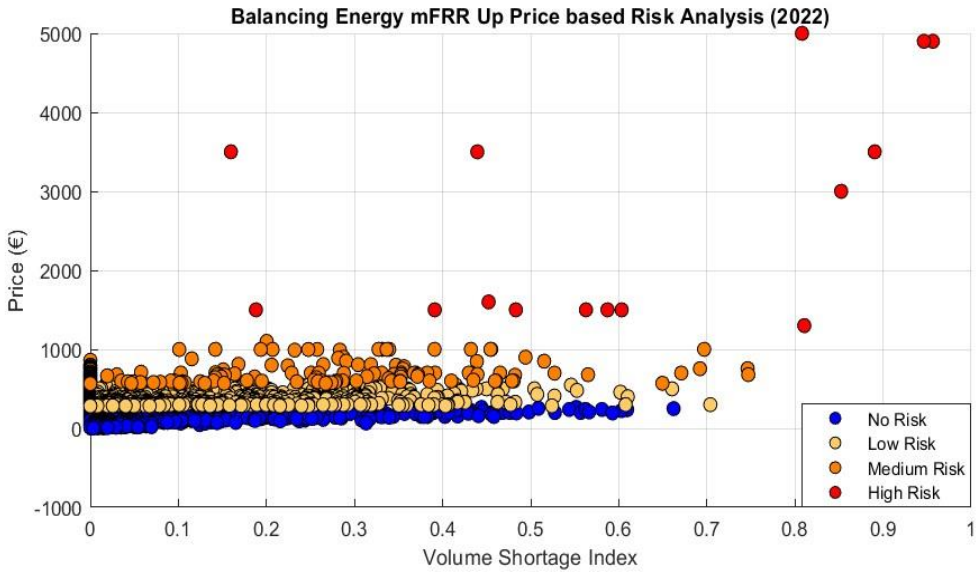


Figure 3.11 *Balancing Energy mFRR Up Price based Risk Analysis (2022)*

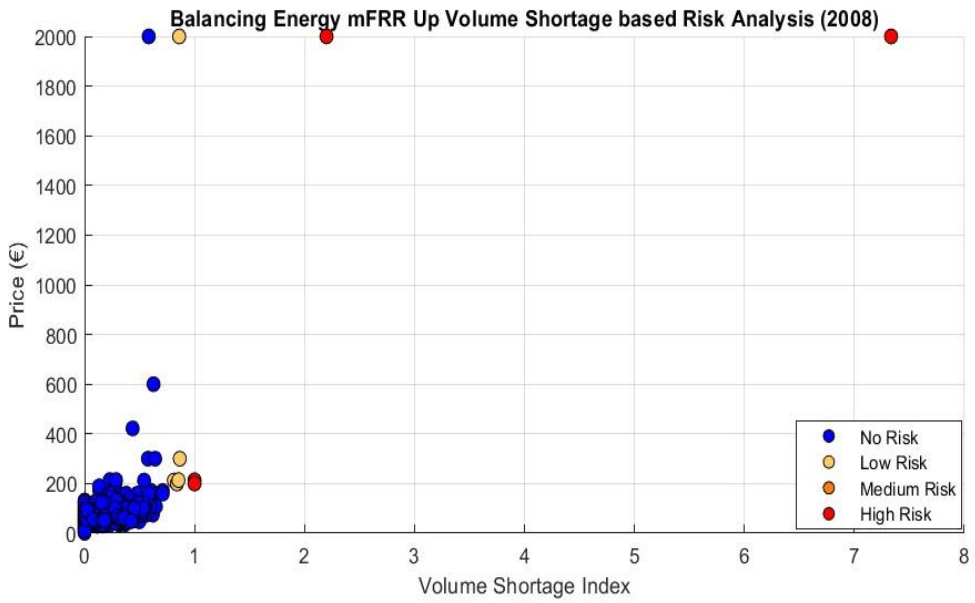


Figure 3.12 *Balancing Energy mFRR Up Volume Shortage based Risk Analysis (2008)*

3.4.7 Balancing Energy mFRR Downregulation

Balancing Energy mFRR Downregulation is procured through the hourly market where prices and bids are published with one hour delay. This market also operates through reserves bids by reserve providers in Balancing Capacity market. Analysis is conducted for each year from 1st January until 31st December. However, for year 2023, analysis is only conducted from January until May due to data availability and project timeline. [26][30]

For price-based risk analysis, high risk hours can occur for positive as well as negative prices. In the analysis for price-based risk, it is mentioned in the table 3.20 whether price volatility is in positive or negative direction. Moreover, trend shows that very high prices occur when no volume is ordered in the market. Moreover, prices usually go to extreme negative when most of the bids offered in the market are ordered.

Table 3.20 *Price based Risk Analysis of Balancing Energy mFRR Downregulation Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2007	0	0	0
2008	0	0	0
2009	0	0	1 (Positive)
2010	0	0	10 (All positive)
2011	0	0	0
2012	0	0	5 (All positive)
2013	0	0	0
2014	0	0	0
2015	0	0	0
2016	0	0	0
2017	4 (All Negative)	2 (All Negative)	0

2018	2 (All Negative)	0	1 (Positive)
2019	0	0	0
2020	0	0	1 (Positive)
2021	2 (All Positive)	35 (All Positive)	101 (All Positive)
2022	6 (All Positive)	346 (All Positive)	1213 (All Positive)
2023	2 (All negative)	0	7 (All negative)

For volume shortage analysis in table 3.21, '*' sign represents those years where the amount of ordered upregulation bids exceeded total number of bids offered by Finnish parties at least for one hour during the year. Moreover, price is not considered in volume shortage analysis for this market.

Table 3.21 *Volume Shortage based Risk Analysis of Balancing Energy mFRR Downregulation Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2007	0	0	10
2008	2	3	13
2009	20	2	15
2010	5	4	30
2011*	14	5	27
2012	4	0	3
2013	0	1	4
2014	0	0	0
2015	0	0	0
2016	0	0	0
2017	0	4	0
2018	1	0	0
2019	0	0	0
2020	0	0	0
2021	0	0	0
2022	0	0	0
2023	0	1	0

Furthermore, as of May 2023, until 140 MW of consumption sources were being utilized as demand response (classified as load type 2) within this market [33]. These consumption sources may include a certain proportion of domestic home automated loads, which are vulnerable to cyberattacks through strategies such as load manipulation and demand response blocking by hackers. In contrast, load type 1, which is not part of the allocated demand response, can only be exploited for load manipulation. Moreover, fault conditions remain same for both the Balancing Energy and Balancing Capacity markets.

Table 3.22 *Fault Conditions for Risk creation through Balancing Energy mFRR Downregulation Market*

Risk	Large Scale Fault Requirement
Price Manipulation Risk	No
Volume Shortage Risk	Yes/No

For representation of price-based risk analysis, years 2018 and 2022 are chosen. In the figure 3.13, it is evident that year 2018 has both risk hours in positive as well as negative price. Whereas figure 3.14 shows that year 2022 has the most amount of risk hours in total. In these figures, volume shortage index on x-axis is the ratio of procured volume to offered volume in the hourly market. Moreover, price of this hourly procured volume is represented on y-axis. Moreover, a common trend for price-based risk analysis in this market throughout the years is that positive priced risk hours occur when volume shortage index is zero or very close to zero, and negative priced risk hours occur when quite sufficient amount of offered bids by Finnish parties is ordered from the market. This trend can be seen from the graphs below as well. (To further analyze such trends for other years, graphs can be found in attachment document of this thesis [32])

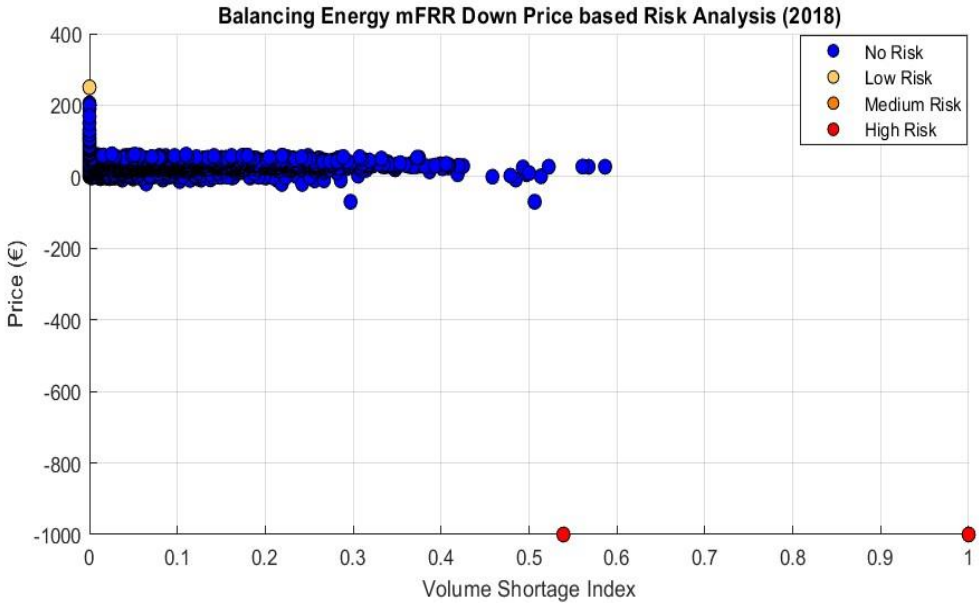


Figure 3.13 *Balancing Energy mFRR Down Price based Risk Analysis (2018)*

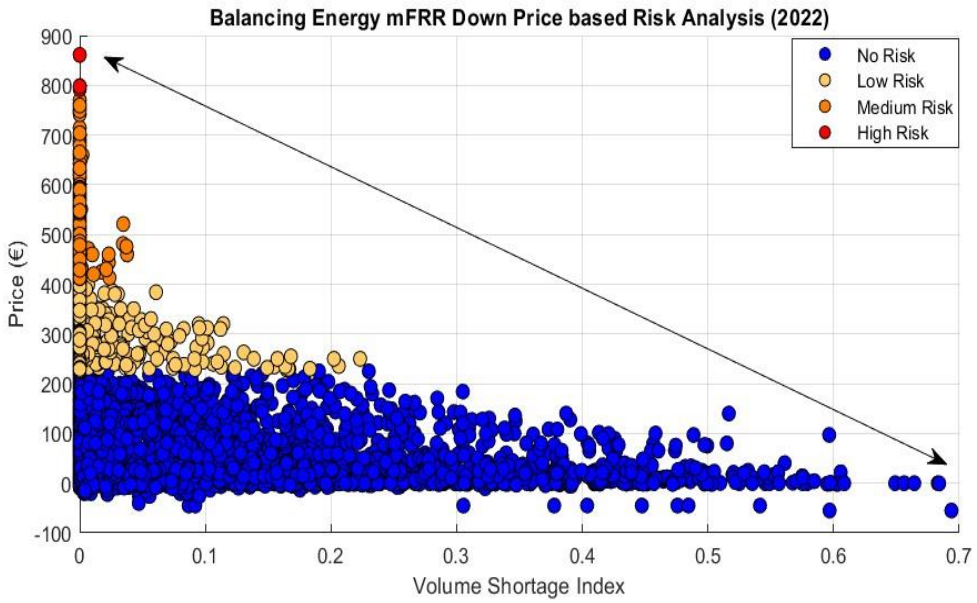


Figure 3.14 *Balancing Energy mFRR Down Price based Risk Analysis (2022)*

In the figure 3.15, representation of volume shortage analysis for year 2011 is provided for balancing energy mFRR downregulation market. It can be seen that in terms of volume shortage, the number of instances of risk alongwith the intensity of some of high risk hours is very high. (Graphs for remaining years can be found in attachment document of this thesis [32])

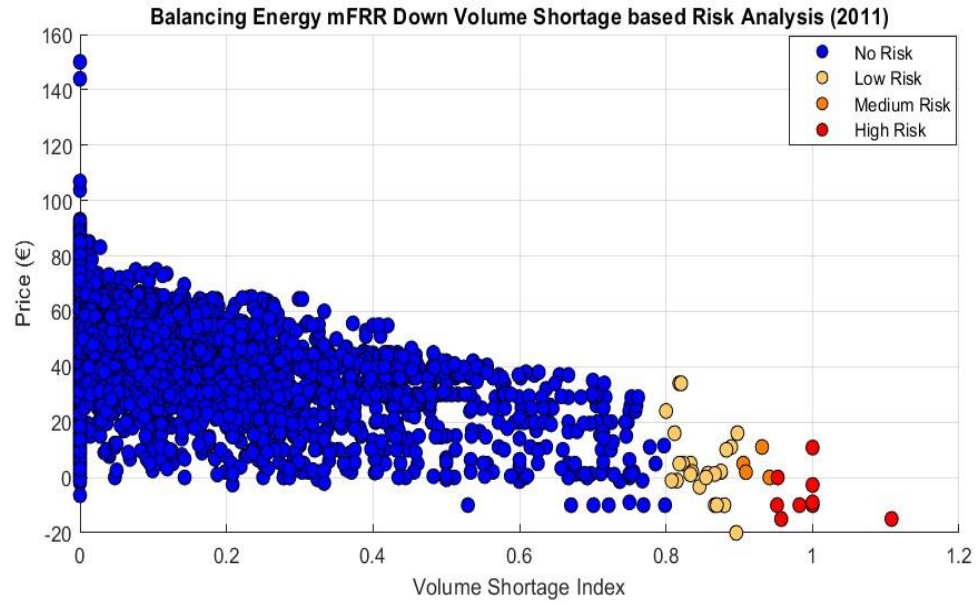


Figure 3.15 *Balancing Energy mFRR Down Volume Shortage based Risk Analysis (2011)*

3.4.8 FFR

Fast Frequency Reserves (FFR) were implemented in Nordic synchronous system in 2020. Currently, FFR is only utilized for upregulation and is the quickest activated reserve. Fingrid estimates the volume for FFR based on system inertia and reference incidence. Required volume is procured through day ahead hourly market. Analysis is conducted for each year from 1st January until 31st December. However, for year 2023, analysis is only conducted from January until May due to data availability and project timeline. [28][30]

It seems that throughout the years, maximum price of accepted bids for hourly FFR market never crosses the limit of 100 Euros [19]. Hence, price based risk analysis is not conducted for FFR market. In terms of volume availability, it can be seen from the table 3.23 that the initial years of the market had very high number of risk hours. However, throughout the years, market operation improved massively. [30]

Table 3.23 *Volume Shortage based Risk Analysis of FFR Market*

Year	High Risk Hours	Medium Risk Hours	Low Risk Hours
2020	534	4	18
2021	136	2	27
2022	77	1	11
2023	14	0	3

According to Fingrid data, 34.5% of sources utilized for FFR are consumption units which are categorized as load type 2 [28]. They can be utilized for load increment as well as demand response blocking by hackers. Hence, load type 2 is more dangerous for market and grid security perspective. Moreover, the share of such loads are quite huge for FFR market which makes it even more significant in terms of security of FFR market. However, load type 1 can only be utilized for load increment making it less effective for hackers, but it can also cause problems if it is hacked in large quantity.

Form hacker's point of view, fault existence is not required for market price manipulation. However, in terms of grid instability, presence of fault in the system or sudden frequency dip is required during volume shortage hours as the activation threshold for FFR is usually either at 49.5, 49.6 or 49.7 Hz [23].

Table 3.24 *Fault Conditions for Risk creation through FFR Market*

Risk	Large Scale Fault Requirement
Price Manipulation Risk	No
Volume Shortage Risk	Yes

Figure 3.16 represents the visual representation of volume shortage-based risk analysis for FFR market for the year 2022. Volume shortage index on x-axis is the ratio of hourly procured volume to hourly offered volume in the day ahead market. Price of hourly procured volume is shown on y-axis. (Graphs for remaining years can be found in attachment document of this thesis [32])

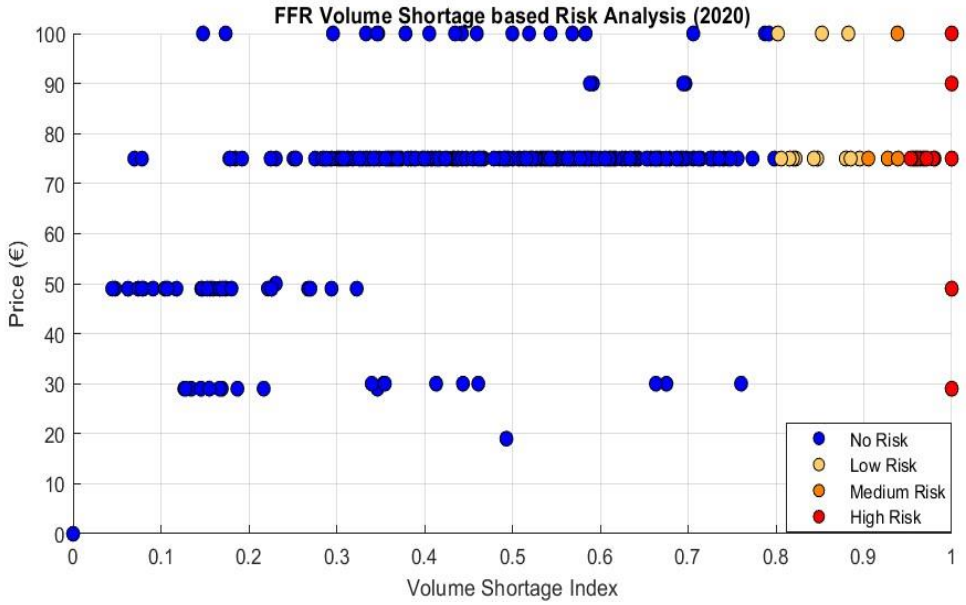


Figure 3.16 *FFR Volume Shortage based Risk Analysis (2020)*

4. LOAD MODELLING OF HEAT PUMPS AND ELECTRIC VEHICLES AS HOME AUTOMATED LOADS

In order to assess how cyberattack through home automation system would impact local grid network of South Savo, Finland, simulation of loads and their integration into service point data is done. Two loads are selected which are assumed to be controlled through home automation systems in future. First selected load is heat pumps which are already on increasing trend throughout Europe in general and Nordic countries in particular [34]. Second selected load is electric vehicles because electrification of energy sector is already underway at fast pace to achieve net zero emissions by 2050 as set out in Paris Climate Agreement [35][36]. Hence, it is assumed that all the houses in South Savo region of Finland will have heat pump and electric vehicle in future which would be controlled through home automation system. To simulate that scenario, each of these loads is first modelled for individual customers, and then added to existing customer consumption. It must be noted that load modelling is done for only houses/apartment buildings. In the last stage, a rationally selected cyberattack scenario is simulated for each customer for both of these loads to assess its effects on service points, conductors, and transformers of the whole network.

LV and MV network chosen to study the impacts of cyberattack through home automation loads is located in South Savo, Finland. The region under study can be viewed in figure 4.1 [37]:

Figure 4.1 *Visual representation of the under-study region of South Savo [37]*

This part of the project is done in collaboration with Rejlers Oy, Tietoevry and Suur-Savon Sähkö Group [38][39][40]. Network analysis results for service points, conductors, and transformers of South Savo was provided from Suur-Savon Sähkö Group through Rejlers Oy to Tampere University. Then the customer consumption data from service points (load profile and annual consumption) was reformed based on the simulations done in this thesis. This reformed data was then provided to Rejlers Oy where it was reconfigured and sent to Tietoevry. Afterwards, Tietoevry run the updated data and got network results which were sent back to Tampere University through Rejlers Oy for analysis and documentation. Four different simulations were designed in this thesis, and hence, this process was repeated four times as well.

4.1 Original Network Data

Initially, following data was provided to Tampere University:

4.1.1 Transformers

In total, there are 9442 transformers in the network. Provided data to Tampere University includes parameters for each transformer including transformer id, rated powers, primary voltage, secondary voltage, tertiary voltage, apparent power, real power, reactive power, loading level percentage, feeding substation, feeding substation output id, feeding main transformer, peak loading hour, and Well-known Text (WKT) Geometry.

4.1.2 Conductors

There are 243135 conductors in this network. Out of these, 219114 conductors belong to LV grid and 24021 conductors belong to MV grid network type. Provided data to Tampere University includes parameters for each conductor which includes conductor id, conductor type, maximum loading current, actual current level, apparent power, real power, reactive power, loading level, peak loading hour of the year, feeding main transformer, and Well-known Text (WKT) Geometry.

4.1.3. Service Points

There are 103607 user points, and 79627 service points in the network. Each user point supplies power to one or more service points. Provided data to Tampere University includes parameters for each service point which includes load curve, user group, voltage, apparent power, real power, reactive power, actual current, voltage drop, loading level, fuse size, total annual energy consumption, feeding secondary substation, feeding transformer, and Well-known Text (WKT) Geometry.

In the provided network data, 27228 service points belong to houses/apartments. These service points are categorized into load groups based on energy consumption values as well as load curves. Categorization of service points is as follows:

- Load Group 01: Single family houses with electric heating and heat storage capacity less than 300 l.
- Load Group 02: Single family houses with electric heating and heat storage capacity equal to 300 l.

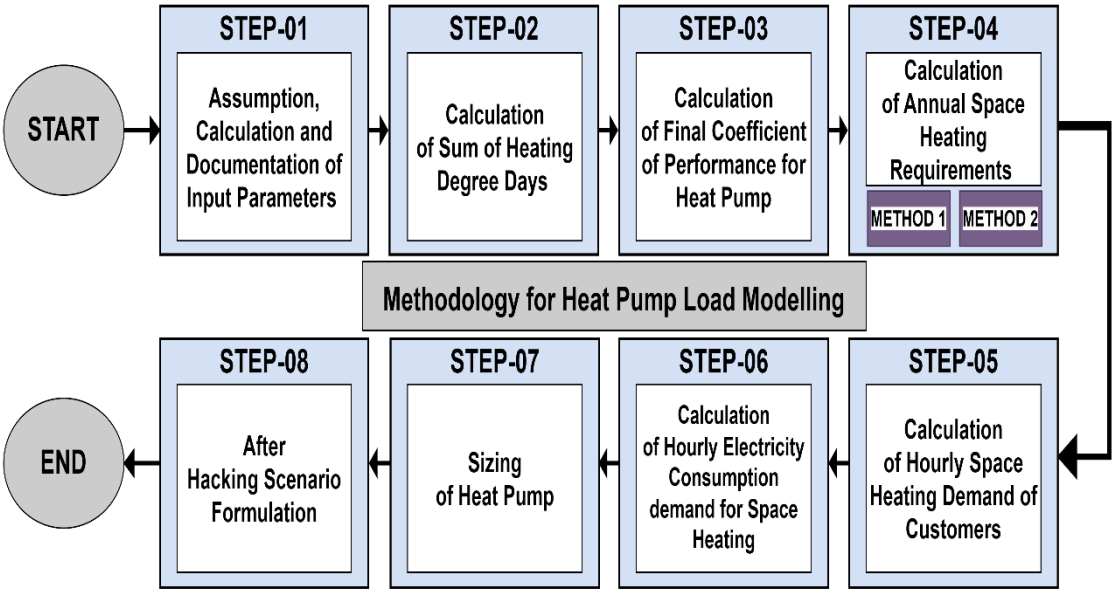
- Load Group 11: Single family houses with no electric heating and no electric sauna.
- Load Group 12: Single family houses with no electric heating but with electric sauna.
- Load Group 13: Row houses with no electric heating and no electric sauna.
- Load Group 14: Row houses with no electric heating but with electric sauna.
- Load Group 17: Row houses with electric heating.
- Load Group 18: Vacation houses.
- Load Group 23: Farming houses with no electric heating but with electric sauna.
- Load Group 24: Farming houses with electric heating and electric sauna.

4.2 Heat Pump Load Modelling

Heat pumps are devices which use electricity to transfer heat from source to sink. Depending upon the source of heat, it can be categorized into air, water, and geothermal heat pumps [41]. For Finland, almost 80 percent of overall installed heat pump output was provided by air-air heat pumps in 2021 [42]. Moreover, according to European Heat Pump Association, more than 81 % of new heat pumps sold in Finland were air-air heat pumps in 2022 [34]. Hence, only air-air heat pumps are modelled, and a generalization is made that these will be used by all houses in future. Moreover, it is also assumed that air-air heat pumps will only be used for heating purposes. This is done because of cold climate conditions of the area under study.

4.2.1 Methodology for Heat Pump Load Modelling

From here onwards, air-air heat pumps will often be referred as heat pumps for simplicity. For modelling of heat pump consumption for each customer, following steps are taken:



Step 01: Assumption, Calculation and Documentation of Input Parameters

1. Time resolution ($t_{\text{Time Resolution}}$)

Chosen time resolution is one hour for this simulation. Time resolution bigger than an hour would reduce accuracy whereas timestep smaller than an hour would increase complexity.

2. Simulation Timespan

Simulation timespan is chosen to be one year. It means that heat pump consumption is simulated on hourly basis for the period of one calendar year.

3. Outdoor Temperature Data ($T_{\text{Outdoor}}(t)$)

Outdoor temperature is the most important input parameter for heat pump simulation. In terms of Euclidean distance, Partala observation station of Finnish Meteorological Institute is located closest to South Savo [43]. Hence, outdoor temperature data is taken from that particular station. Ten years of hourly temperature data is taken from 2013 to 2022. Afterwards, this ten-year hourly temperature data is used to get hourly average temperature for a year which is then utilized as outdoor temperature input for this simulation. As hourly average temperature is being utilized, extreme temperatures are not utilized in the modelling. It is done to avoid oversizing the heat pumps for customers.

4. Indoor Temperature Representing Heating Degree Day (T_{HDD})

For Finland, indoor temperature representing heating degree day is chosen to be at 17 degrees Celsius [44]. This indoor temperature is utilized in calculation of difference of daily indoor and outdoor temperatures for the calculation of heating degree day. Heating degree day is simply a representation of how cold the weather is compared to a standard temperature.

5. Indoor Set Point Temperature

Indoor set point temperature is desired temperature of the house/apartment. According to National Building Code of Finland as well as multiple guidelines, indoor set point temperature should be between 20 to 22 degree Celsius [45][46]. For this simulation, this temperature is set at 20 degree Celsius. Lower limit is taken to keep in-blast temperature within realistic range.

6. In-blast Temperature (T_{ib})

For air-air heat pump, in-blast temperature is the temperature of heated-up air leaving the condenser. According to a combined study by VTT and Aalto University, if exact value of in-blast temperature is unknown, it can be taken as 15 degree Celsius above the indoor set point temperature [47]. Hence, Tib is set at constant 35 degree Celsius for the whole year for this simulation.

7. Nominal Coefficient of Power of Air-Air Heat Pump (COP_N)

Coefficient of Performance of heat pump is the ratio of heat output to electric energy input. So, COP is representation of the efficiency of heat pump, and it is usually quite high because heat is simply being transferred from source to sink. According to a report issued by Nordic Council of Ministers, nominal COP of air-air heat pump in Nordic climate at full capacity is approximately 3.5 [48]. This value is measured at standard 7 degree Celsius outdoor and 20-degree Celsius indoor set point temperature in accordance with SFS-EN 14511-2 [49].

8. Space Heating Requirement

Ideally, space heating demand of individual customers should be calculated through proper parameters such as insulation as well as area of the house where heating is required. However, that data is inaccessible for this study because there are tens of

thousands of household customers within South Savo region. Hence, annual energy consumption is used to estimate space heating requirement of each customer individually. Estimate for electrical and non-electric heated houses is done separately. A generalized model is made where each household is assigned certain amount of space heating demand based on the type of load group as well as the methodology being followed. On a large scale, this method should work fine. However, space heating requirements of individual customers may vary from this generalized model. Methodology of calculation of this parameter for each customer is explained in the later steps.

9. Seasonal Performance Factor

Seasonal Performance Factor (SPF) of a heat pump is the ratio of heating output to electricity consumption over a whole heating season throughout the year. For Nordic climates, SPF of air-air heat pump can be assumed to be at 2.75 [48].

Step 02: Calculation of Sum of Heating Degree Days

According to US Energy Information Administration, degree day is comparison of mean outdoor temperature to standard indoor temperature for daily basis [50]. However, this parameter is widely used for yearly time period as well. Degree Days can be further characterized into Heating Degree Days (HDD) and Cooling Degree Days (CDD). They are a measure of how hot or cold the weather is compared to a standard value. HDD is used for cold climates whereas CDD is used for regions with hot climates. For Nordic countries, calculation of HDD is more significant because of the intense cold weather for most of the time throughout the year.

Sum of HDD is assessment of overall heating demand in a particular region for an extended period of time. For this simulation, chosen timespan is one year with timestep of one hour. So, sum of HDD can be calculated through the following method [47]:

$$when\ T_{HDD} > T_{Outdoor}(t)$$

$$Sum\ of\ HDD = \sum (T_{HDD} - T_{Outdoor}(t)) \,.\, t_{Time\ Resolution}$$

$$when\ T_{HDD} \leq T_{Outdoor}(t)$$

$$Sum\ of\ HDD = 0$$

where

T_{HDD}= Indoor temperature representing Heating Degree Day.

$T_{Outdoor}(t) =$ Outdoor hourly average temperature data of past ten years.

$t_{Time\ Resolution}$= 1 hour.

Step 03: Calculation of Theoretical Hourly Coefficient of Performance (COPT(t)), Loss Factor, and Final Hourly Coefficient of Performance of Heat Pump (COPF(t))

To calculate COPT(t) of heat pump, following formula is utilized [47]:

$$COP_T(t) = \frac{T_{HSy}}{T_{HSy} - T_{HSo}(t)}$$

where

T_{HSy}= Building heating system temperature in Kelvin.

T_{HSo}(t)= Heating source temperature in Kelvin.

If these values are unknown, then in-blast temperature (Tib) can be used instead of building heating system temperature (THSy), and outdoor temperature (TOutdoor(t)) can be used instead of heating source temperature (THSo(t)) [47]. Hence, the aforementioned formula can be rearranged in the following way:

$$COP_T(t) = \frac{T_{ib}}{T_{ib} - T_{Outdoor}(t)}$$

where

$T_{ib} =$ In-blast temperature of heat pump.

$T_{Outdoor}(t) =$ Average hourly outdoor temperature.

Theoretical coefficient of performance (COPT) of heat pump is usually very high because any type of losses are not taken into account. In order to estimate losses associated with heat pump, loss factor is calculated. Loss factor is the ratio between nominal coefficient of performance (COPN) and theoretical coefficient of performance (COPT). Here, loss factor is considered to be constant throughout the year because is it measured at only one standard temperature. [47]

$$f = \frac{COP_N}{COP_T}$$

where

f = Loss Factor of heat pump.

COP_N= Nominal COP of heat pump measured at +7/+20-degree Celsius temperature standard according to Nordic Council of Ministers report [48].

COP_T= Theoretical COP of heat pump calculated at standard +7/+20-degree Celsius outdoor temperature.

To calculate final coefficient of performance of heat pump, following formula is utilized: [47]

$$COP_F(t) = COP_T(t) \times f$$

where

$COP_T(t)$= Theoretical coefficient of performance of heat pump.

f = Loss factor of heat pump.

Step 04: Calculation of Annual Space Heating Requirement (Q) vis-à-vis Changes in Annual Consumption of each Customer

Ideally, space heating requirement is calculated based on parameters of the house such as insulation and covered area. However, that data is not available for all customers. Hence, annual electricity consumption of each customer is used to get an estimate of how much space heating would be generally needed throughout the year. Then air-air heat pump is modelled to cover all space heating requirements of each customer. It is a model based on future scenario assumption that all houses will have their space heating requirements completely fulfilled through air-air heat pumps.

However, main problem is that it is not known which customers already have heat pumps. Moreover, it is also not known how much space heating is already being provided to each customer by those heat pumps. Hence, two different assumptions are made based on which two methods are formulated to design these simulations. In the first method, it is assumed that no customer has heat pump installed. It is assumed that each customer has their space heating requirement being fulfilled by combination of sources other than heat pumps. In second method, it is assumed that each customer already has a heat pump, but it covers certain percentage of their space heating requirements. This percentage is derived from Finland's national heat pump energy consumption data and is taken to be same for every customer.

Both aforementioned methods of simulation utilize key statistics of air-air heat pump consumption in Finland. Some of those important statistics are explained here. Accord-

ing to Finnish heat pump association SULPU, total annual output of heat pumps in Finland for year 2020 was 12 TWh [51]. Moreover, approximately 80 percent of heat pump output was from air-air heat pumps [42]. So, it can be estimated that air-air heat pumps produced around 9.6 TWh output during year 2020. At Seasonal Performance Factor (SPF) of 2.75 [48], annual heat pump electricity consumption can be calculated at 3.49 TWh.

According to Statistics Finland, 22 TWh of total electricity was consumed in Finnish households in 2020 [52]. Out of this, 9.9 TWh of electricity was consumed for space heating [52]. This includes consumption of electric heaters as well as heat pumps. As already discussed above, air-air heat pumps consumed 3.49 TWh of electricity. It means remaining 6.41 TWh of electricity is consumed by electric heating sources on annual basis. It must be noted that these statistics are for all households belonging to electric as well as non-electric heated load groups.

1. Method 01

In this method, core assumption is that no customer has any air-air heat pump installed initially. It is assumed that all of space heating requirements are being fulfilled through other sources. Then, it is simulated that all of those sources would get replaced by air-air heat pumps for each customer. Hence, all space heating requirement will be fulfilled by air-air heat pump for each customer.

a. Electric Heating Load Groups

For load groups which already have electric heating i.e. load groups 01, 02, 17 and 24, it is assumed that all of their space heating requirements are initially being fulfilled by electric heating. Then in future, it is simulated that electric heating would get completely replaced by air-air heat pumps for all these customers.

As already mentioned, 22 TWh of electricity was consumed by households in Finland in 2020. Out of this, 9.9 TWh of electricity was consumed for space heating [52]. Out of this, 3.49 TWh of electricity was consumed by air-air heat pumps. In this method, assumption is that all load groups have no heat pumps initially installed. So, this heat pump consumption can be replaced by electric heating for these customers. Moreover, according to US department of Energy, air-air heat pumps usually consume approximately half the amount of electricity in comparison to electric heaters while producing same amount of space heating [53]. Although this aforementioned statistic varies from region to region and is dependent upon the technology in use, approximate value is

taken here primarily due to credibility of the mentioned source. Moreover, As the initial average annual consumption of all households is 22 TWh; however, for households having electric heating, it is assumed that their average annual energy consumption would become 25.49 TWh as all their heat pump consumption is also being replaced by electric heating. Hence, electric heating consumption for these customers would become 13.39 TWh out of total 25.49 TWh. So, for these electric heated load groups, it is assumed that initially 52.53 % of their annual electricity consumption goes to electric heating based on the aforementioned extracted data.

In the next step, electric heating is replaced by air-air heat pumps which consume approximately half the amount of electricity in comparison to electric heaters according to US Department of Energy [53]. So, the overall consumption of these customers will be reduced from 25.49 TWh to 18.795 TWh after heat pumps replace electric heating. In other words, annual consumption of each customer would be reduced to 73.73 % of their original consumption. Furthermore, air-air heat pump would consume 6.695 TWh out of 18.795 TWh which is approximately 35.6 % of new annual consumption. These statistics are shown in table 4.1.

Table 4.1 *Changes in the Annual Electricity Consumption of Customers of Electric Heated Load Groups (Method 01)*

Actual Consumption	Consumption after Removal of Electric Heating	Consumption after Heat Pump Load Addition
100 %	47.47 %	73.73 %

b. Non-Electric Heating Load Groups

For load groups without electric heating i.e. load groups 11, 12, 13, 14, and 23, it is assumed that all their space heating requirements are initially being provided by non-electricity consuming sources. Hence, their annual average electricity consumption is assumed to be 12.1 TWh after removal of electric heating consumption from overall household consumption statistics. Afterwards, based on previous calculation of electric heating load groups following method 01, air-air heat pumps are installed which would consume approximately around 35.6 % of new annual consumption. Hence, new consumption of customers of these load groups after heat pumps load addition would increase to 18.795 TWh which equates to 155 % of the original consumption. These statistics are shown in table 4.2.

Table 4.2 *Changes in the Annual Electricity Consumption of Customers of non-Electric Heated Load Groups (Method 01)*

Actual Consumption	Consumption after Heat Pump Load Addition
100 %	155 %

c. Combined Row Houses

There are 938 service points which provide electricity to row houses belonging to electric as well as non-electric heated load groups. So, they cannot be taken in any of aforementioned category. For these, assumption is made that load is equally divided between rows houses belonging to electric as well as non-electric heated load groups. Thus, annual energy consumption after heat pump installation would also get changed as an average change between electric and non-electric heated load groups. Hence, if all customers of this category completely shift their space heating technology to air-air heat pumps, then their average annual energy consumption would increase by 114.36% as shown in table 4.3. Moreover, air-air heat pumps would consume same amount of 35.6% of overall customer consumption.

Table 4.3 *Changes in the Annual Electricity Consumption of Customers of Combined Row Houses (Method 01)*

Actual Consumption	Consumption after Heat Pump Installation and Replacement
100 %	114.36 %

2. Method 02

In this method, it is assumed that each customer already has air-air heat pump installed initially. Capacity of already installed heat pump for each customer is based on National air-air heat pump consumption of Finland. This would fulfill certain portion of required space heating of customers. Remaining space heating demand is being fulfilled by other heating sources. Then, other heating sources providing a certain portion of space heating would be replaced by air-air heat pumps as well. This way, all space heating requirement of all customers would be fulfilled by air-air heat pumps.

a. Electric Heating Load Groups

For Finland, consumption of air-air heat pumps was 3.49 TWh for year 2020 and the total annual household consumption was 22 TWh [34-52]. It means that 15.86 % of overall household consumption already goes to installed air-air heat pumps. Moreover, as calculated above, 6.41 TWh of electricity is consumed by electric heating. In this method, this electric heating consumption will be replaced by air-air heat pumps. Hence, 6.41 TWh of electric consumption would become 3.205 TWh of air-air heat pump consumption. It would mean that total space heating consumption through air-air heat pumps would become 6.695 TWh out of which 3.49 TWh capacity was already installed and remaining 3.205 TWh capacity has been attained by replacement of electric heating with air-air heat pumps. Overall consumption would also reduce from 22 TWh to 18.795 TWh. It means that overall consumption would decrease to 85.43 % of original consumption for electric heating load groups in this method as shown in table 4.4. Moreover, total air-air heat pump consumption would still be 35.6 percent of new annual consumption.

Table 4.4 *Changes in the Annual Electricity Consumption of Customers of Electric Heated Load Groups (Method 02)*

Actual Consumption	Consumption after Removal of Electric Heating	Consumption after Heat Pump Load Addition
100 %	70.86 %	85.43 %

b. Non-Electric Heating Load Groups

For those load groups which do not have electric heating, after removal of 6.41 TWh of electric heating consumption from 22 TWh total consumption, their average annual consumption would be 15.59 TWh [51][52]. Out of this, 3.49 TWh is already being consumed by heat pumps which equates to 22.38 % of overall consumption. To cover overall space heating requirements, additional heat pumps of 3.205 TWh are installed afterwards which would replace other space heating sources. Overall average customer consumption would increase from 15.59 TWh to 18.795 TWh equating to increase of 120.55 % which can also be observed from table 4.5. Moreover, total air-air heat pump consumption would still be 35.6 % of overall consumption of customers.

Table 4.5 *Changes in the Annual Electricity Consumption of Customers of non-Electric Heated Load Groups (Method 02)*

Actual Consumption	Consumption after Heat Pump Load Addition
100 %	120.55 %

c. Common Row Houses

For this method, existing load is equally divided between electric and non-electric heated load groups and then heat pump load is added based on method 2. Then, it is calculated that the annual energy increases just by approximately 2% after shifting of all space heating requirement to air-air heat pumps. Hence, this category has not been tested for two reasons:

- Annual energy change is too small.
- Time and resource limitation.

This way changes in annual energy consumption of each customer are assessed through both methods. Afterwards, 35.6 % of changed annual energy consumption is assigned to air-air heat pump annual consumption. Space heating requirement is assessed through following formula [54]:

$$Q = Annual\ Heat\ Pump\ Electricity\ Consumption\ \times SPF$$

where

Q is annual space heating demand.

SPF is Seasonal Performance Factor.

Step 05: Calculation of Hourly Space Heating Demand of Customers

After annual space heating requirement of each customer is estimated based on their category of load group and the method being used, hourly space heating requirement is calculated through the following formula [47]:

$$I_{Spaces\_demand}(t) = \frac{Q(T_{HDD} - T_{Outdoor}(t))}{Sum\ of\ HDD}$$

where

$I_{Spaces\_Demand}(t)$= Hourly space heating requirement.

T_{HDD}= Indoor temperature representing heating degree day.

$T_{Outdoor}(t) =$ Average hourly outdoor temperature of past ten years.

Step 06: Calculation of Hourly Electricity Consumption demand for Space Heating

Hourly electricity consumption of each customer is calculated based on their hourly space heating demand and coefficient of performance of heat pump [47].

$$e_{Spaces\_Demand}(t) = I_{Spaces\_Demand}(t) \times COP_F(t)$$

where

$e_{Spaces\_Demand}(t)$= Hourly electricity consumption demand of each customer.

$I_{Spaces\_Demand}(t)$= Hourly space heating demand of each customer.

$COP_F(t)$= Hourly coefficient of performance of heat pump.

Step 07: Sizing of Heat Pump

It is very important to size the air-air heat pump according to the space heating demand. This has to be done for tens of thousands of customers. To size heat pumps according to the demand of each customer, there is need of supposition of smallest sized heat pump theoretically. It is supposed that the customer with least amount of annual energy consumption has heat pump of size 0.25 kW output capacity. For that customer, maximum space heating output throughout all the hours of the year can be calculated as follows [47]:

$$I_{Spaces_{SingleHP}}(t) = \frac{0.25 \times COP_F(t)}{COP_N}$$

where

$I_{Spaces_{SingleHP}}(t)$= Hourly maximum heating output of smallest sized heat pump.

$COP_F(t)$= Final hourly coefficient of performance of heat pump.

COP_N= Nominal coefficient of performance of heat pump which is taken as 3.5 [46].

In the next step, maximum electricity consumption is calculated for this smallest sized heat pump for all hours of the year [47].

$$e_{Spaces_{SingleHP}}(t) = \frac{I_{Spaces_{SingleHP}}(t)}{COP_F(t)}$$

where

$e_{Spaces_{SingleHP}}(t)$= Maximum electricity consumption of smallest sized heat pump.

$I_{Spaces_{SingleHP}}(t)$= Hourly maximum heating output of smallest sized heat pump.

$COP_F(t)$= Final hourly coefficient of performance of heat pump.

This way, maximum space heating output and maximum electricity consumption of the smallest sized heat pump are calculated.

In the next step, the maximum hourly electricity consumption demand of each customer is taken from $e_{Spaces\_Demand}(t)$. It is then compared with $e_{Spaces_{SingleHP}}(t)$ which is maximum electricity consumption of lowest sized heat pump. [47]

$$when\ maximum\ of\ e_{Spaces\_Demand}(t) < e_{Spaces\_SingleHP}$$

$$I_{HPSpaces_{Max}}(t) = I_{Spaces_{SingleHP}}(t)$$

$$when\ maximum\ of\ e_{Spaces\_Demand}(t) > (n \times e_{Spaces_{SingleHP}})$$

$$I_{HPSpaces_{Max}}(t) = (n \times I_{Spaces_{SingleHP}}(t))$$

where

$e_{Spaces\_Demand}(t)$= Hourly electricity consumption demand of each customer.

$e_{Spaces_{SingleHP}}(t)$= Maximum electricity consumption of smallest sized heat pump.

$I_{HPSpaces_{Max}}(t)$= Maximum hourly heating output capacity of each heat pump.

$I_{Spaces_{SingleHP}}(t)$= Maximum hourly heating output of smallest sized heat pump.

n ranges from 1 to 3500.

Maximum range is kept at 3500 to save time as there are multiple load groups with tens of thousands of service points. Hence, in terms of heating output, heat pump sizes vary from 0.25 kW to 875 kW which is enough for almost all of households. This way, sizing on the basis of heating output is done for heat pumps of all customers. Then, actual hourly heat pump electricity consumption of each customer is calculated. The way heat pump is sized, for almost all the customers, heat pump does fulfill space heating requirement at all temperatures in this methodology. There might be some exceptions, but their sample size would be very small. [47]

$$\text{If } maximum\ of\ I_{Spaces\_Demand}(t) > maximum\ of\ I_{HP_{Spaces_{Max}}}(t)$$

$$I_{HP}(t) = I_{HP_{Spaces_{Max}}}(t)$$

$$else$$

$$I_{HP}(t) = I_{Spaces\_Demand}(t)$$

where

$I_{Spaces\_Demand}(t)$= Hourly space heating demand of each customer.

$I_{HPSpaces_{Max}}(t)$= Maximum hourly heating output capacity of each heat pump.

$I_{HP}(t)$= Actual hourly heating output of each heat pump.

Electricity Consumption under normal operation of heat pumps [47]:

$$e(t) = \frac{I_{HP}(t)}{COP_F(t)}$$

$e(t) =$ Actual electricity consumption of each heat pump.

$I_{HP}(t)$= Actual hourly heating output of each heat pump.

$COP_F(t)$= Final hourly coefficient of performance of heat pump.

Step 8: After Hacking Scenario Formulation

For the worse case after-hacking scenario, it is assumed that all heat pumps get hacked, and are operated at maximum capacity throughout the year irrespective of demand or weather conditions. This condition is simulated throughout the year to study the effects of such cyberattack on the network under all weather conditions, customer loads and grid configurations. Maximum size of each heat pump in terms of electricity consumption is calculated in the following way [47]:

$$e\_maximum = \frac{I_{HP\_Spaces\_Max}(t)}{COP_F(t)}$$

where

$e_{maximum} =$ Maximum size of each heat pump in terms of electricity consumption.

$I_{HP_{Spaces_{Max}}}(t) =$ Maximum hourly heating output capacity of each heat pump.

$COP_F(t) =$ Final hourly coefficient of performance of heat pump.

Additional electricity consumption after hacking:

$$e_{hacking}(t) = e_{maximum} - e(t)$$

where

$e_{hacking}(t) =$ Hourly hacking capacity of each heat pump in terms of electricity consumption.

$e_{maximum}$ = Size of each heat pump in terms of electricity consumption.

$e(t)$ = Actual electricity consumption of each heat pump.

4.2.2 Simulated Heat Pump Consumption Pattern

As the weather conditions and design methodology is same, heat pump load curve will be same for each customer group. However, energy consumption and size of heat pump will vary depending upon individual customer's annual electricity consumption. An example of mean hourly heat pump consumption pattern and remaining hacking capacity for customers of load group 01 is shown in figure 4.2. Blue curve in the figure shows the hourly consumption pattern of heat pump throughout the year.

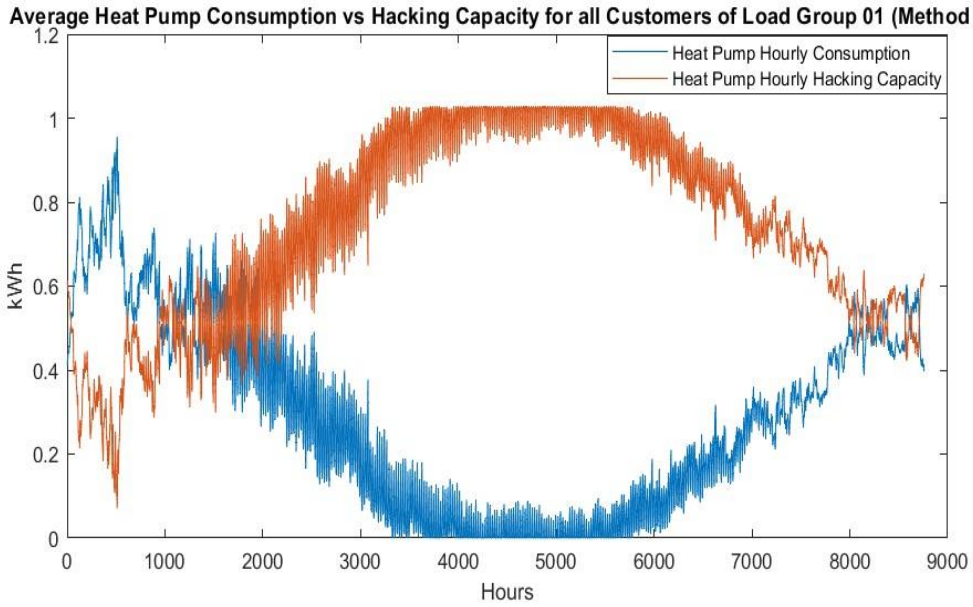


Figure 4.2 *Mean Consumption pattern of Heat Pumps for Customers of Load Group 01*

4.2.3 Example Cases of Modified Customer Load

It must be noted that actual hourly consumption of each customer is based on their individual annual energy consumption and average values of load profile of the load group to which they belong. Moreover, variance in the load profiles is not considered. Hence, heat pump load is added arithmetically to actual consumption of each customer.

a. Example of two Electric Heated Load Groups through both Methods of Simulation:

In the figures 4.3 and 4.4, average hourly consumption of load group 01 is shown for the whole year in three scenarios: actual consumption, consumption after heat pumps replace electric heating, and consumption after hacking of all heat pumps. It must be noted that these values represent the average hourly consumption for all customers belonging to this load group. This means that individual hourly consumption values are first recorded for each customer, and then these values are averaged to provide an overview of the entire load group. As it can be seen that through both methods, average consumption of customers decreases when heat pumps replace electric heating. However, this decrease is more evident in method 01 as compared to method 02. Moreover, in the after-hacking scenarios, average consumption of customers increases, and almost flat curve appears throughout the year because heat pumps operate at full capacity irrespective of heating demand.

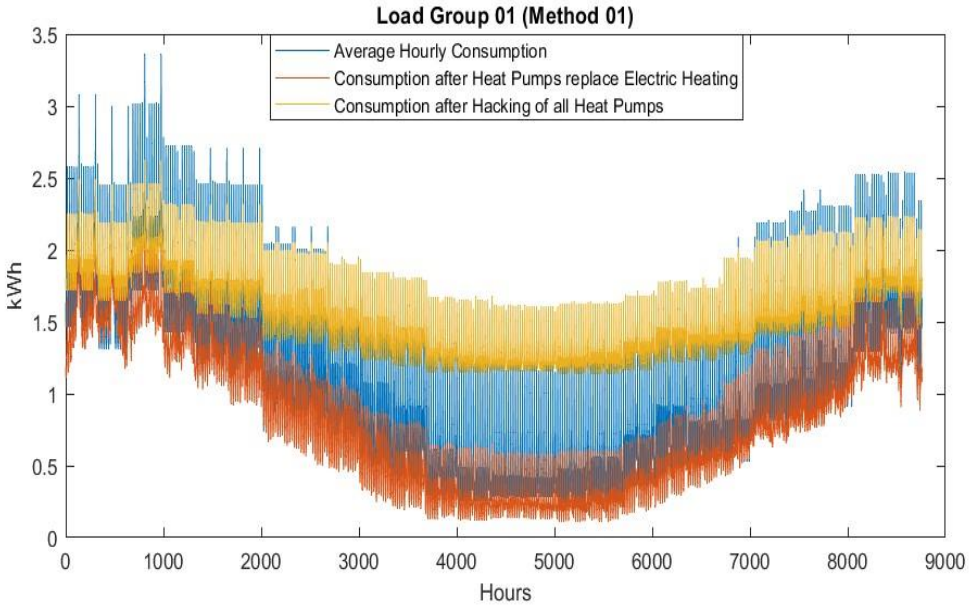


Figure 4.3 *Expected Mean Consumption comparison for Customers of Load Group 01(Method 01)*

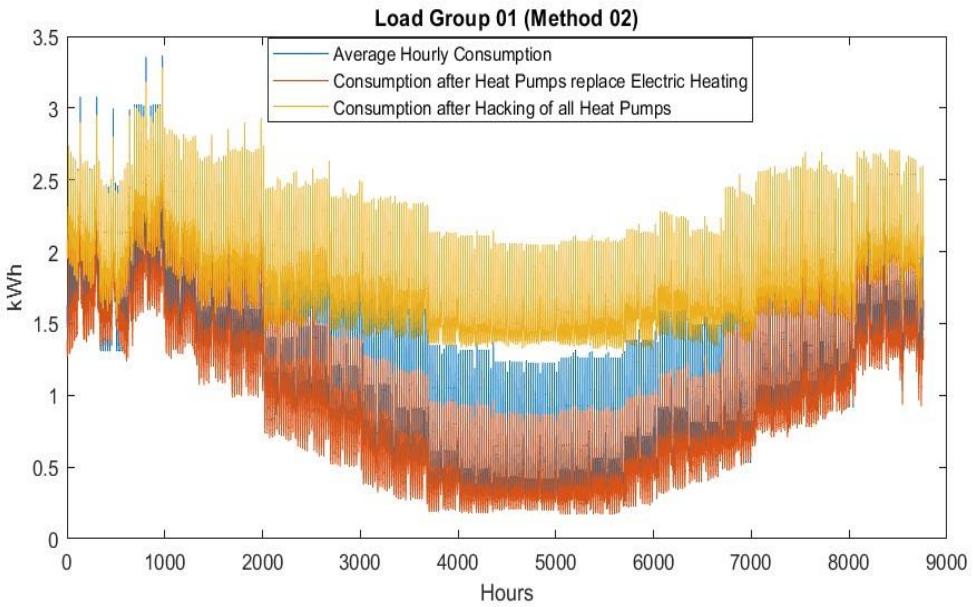


Figure 4.4 *Expected Mean Consumption comparison for Customers of Load Group 01(Method 02)*

In the figures 4.5 and 4.6, average hourly consumption of load group 17 is shown for the whole year in three scenarios: actual consumption, consumption after heat pumps replace electric heating, and consumption after hacking of all heat pumps. For this load group, the electricity consumption pattern is similar to that of load group 01, as both groups fall into the same category of electrically heated load groups. However, there is a significant difference in consumption values. Load group 17, which comprises row houses, has much higher annual electricity consumption compared to load group 01, which represents single-family houses. Graphs for all electric heated load groups can be found in the attachment document of this thesis [55].

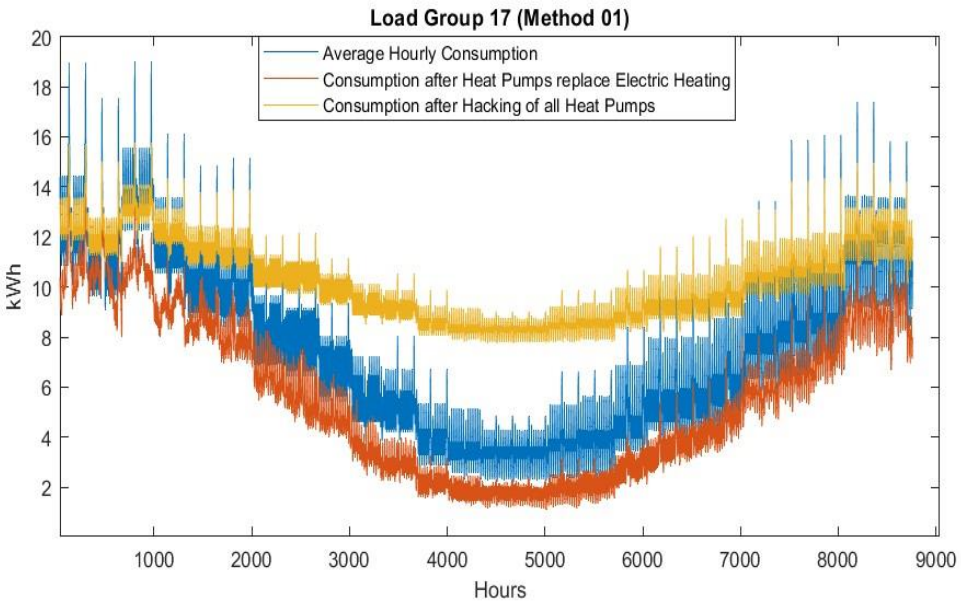


Figure 4.5 *Expected Mean Consumption comparison for Customers of Load Group 17(Method 01)*

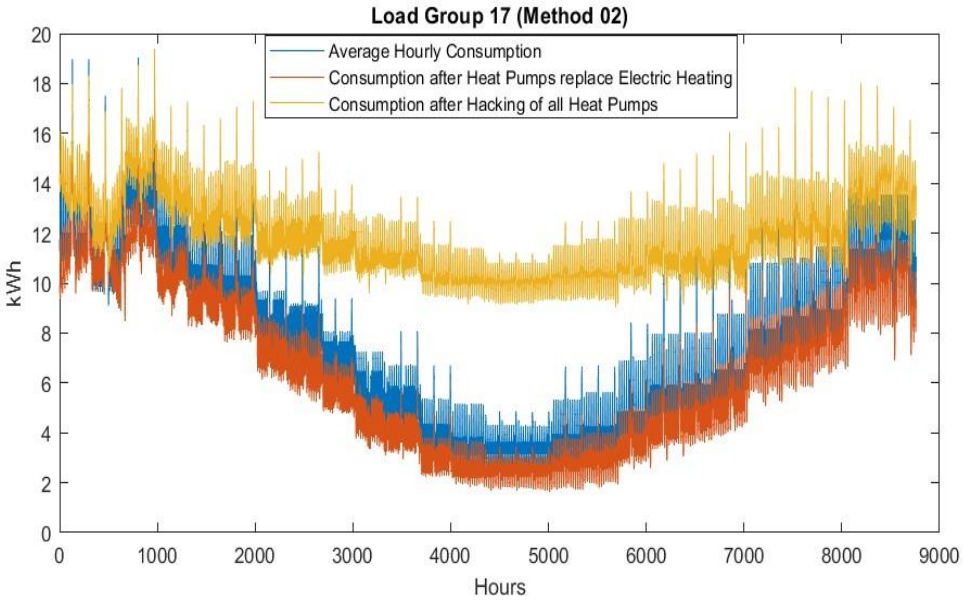


Figure 4.6 *Expected Mean Consumption comparison for Customers of Load Group 17(Method 02)*

b. Example of non-Electric Heated Load Group through both Methods of Simulation:

In the figures 4.7 and 4.8, average hourly consumption of load group 11 is shown for the whole year in three scenarios: actual consumption, consumption after addition of heat pumps, and consumption after hacking of all heat pumps. It can be seen that through both methods, average consumption of customers increases after heat pump

addition. However, this increase is more evident in method 01 as compared to method 02. Moreover, in the after-hacking scenarios, average consumption of customers increases, and almost flat curve appears throughout the year because heat pumps operate at full capacity irrespective of heating demand. Graphs for all non-electric heated load groups can be found in the attachment document of this thesis [55].

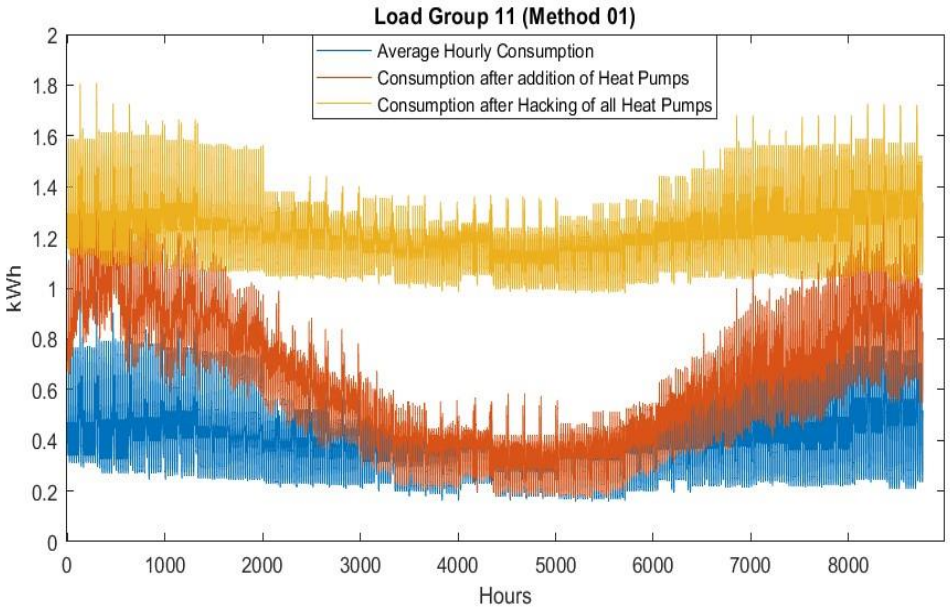


Figure 4.7 *Expected Mean Consumption comparison for Customers of Load Group 11(Method 01)*

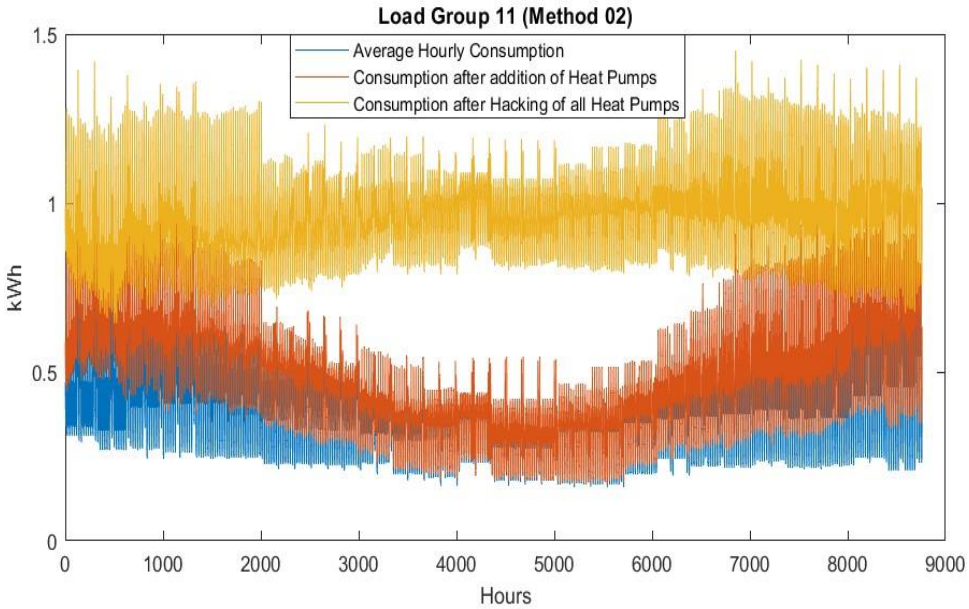


Figure 4.8 *Expected Mean Consumption comparison for Customers of Load Group 11(Method 02)*

4.2.4 Special Heat Pump Load Model for Load Group 18

Load group 18 has 1375 service points representing vacation houses which do not follow usual consumption pattern of households. These houses are mostly in use during weekends and public holidays. So, there should be a different pattern of consumption for heat pumps in vacation houses. This consumption pattern is based on season, day of the week, and average annual consumption of all customers of this load group.

Step 01: Sizing of Heat Pumps

In this methodology, single sized heat pump is assigned to each service point for whole load group to reduce complexity and save time. To find proper single sized heat pump for all customers, service point data for load group 18 is utilized. Initially, average annual energy consumption of all service points for load group 18 is calculated. That provides with the single value of annual energy consumption for the whole load group. This average annual energy consumption will then be used to calculate size of a heat pump through method 01 of non-electric heated load groups. This way, same sized heat pump is assigned all customers of load group 18.

Step 02: Categorization of Seasons

In step 02, three season categories are made: Winter, Autumn & Spring, and Summer. Winter season includes the months of November, December, January, February, and March. Summer season consists of months of May, June, July, August, and September. Autumn and Spring season comprises of April and October months. Moreover, calendar of year 2023 is used to assign weekends and public holidays during each of these seasons throughout the year.

Step 03: Assignment of Heat Pump Daily Consumption

It is assumed that heat pumps are only being used for heating purposes for this simulation. For such heat pumps in Nordic climate, it is estimated that consumption would be most during winter season, mediocre during spring and autumn seasons, and low during summer season. In this step, heat pump consumption is assigned based on seasons and days in the following way:

a. Winter Season

During winter season, it is assumed that heat pump consumption will remain highest in comparison to other seasons. Moreover, consumption is assigned based on day of the week during a particular season. This is how heat pump consumption is assigned to different days of the week during winter season:

- During weekdays, heat pumps consume 30 percent of their total capacity.
- During weekend holidays, heat pumps consume 80 percent of their total capacity.
- During public holidays, heat pumps consume 95 percent of their total capacity.

b. Summer Season

In this simulation, it is assumed that heat pumps are only being utilized for heating purposes. Hence, heat pump energy consumption during summer season would be lowest. Assignment of heat pump consumption for different days of the week during summer season is as follows:

- During weekdays, heat pumps consume 10 percent of their total capacity.
- During weekend holidays, heat pumps consume 30 percent of their total capacity.
- During public holidays, heat pumps consume 50 percent of their total capacity.

c. Spring and Autumn Seasons

During spring and autumn months, temperatures are usually quite similar. So, heat pump consumption for these months is considered to be similar as well. Moreover, consumption of heat pump during these seasons is considered to be in between winter and summer months consumption. Energy consumption assignment for heat pumps is done for different days of the week during spring and autumn season in the following way:

- During weekdays, heat pumps consume 20 percent of their total capacity.
- During weekend holidays, heat pumps consume 55 percent of their total capacity.
- During public holidays, heat pumps consume 72.5 percent of their total capacity.

Based on the energy consumption categorization, heat pump consumption pattern is designed which can be seen in figure 4.9.

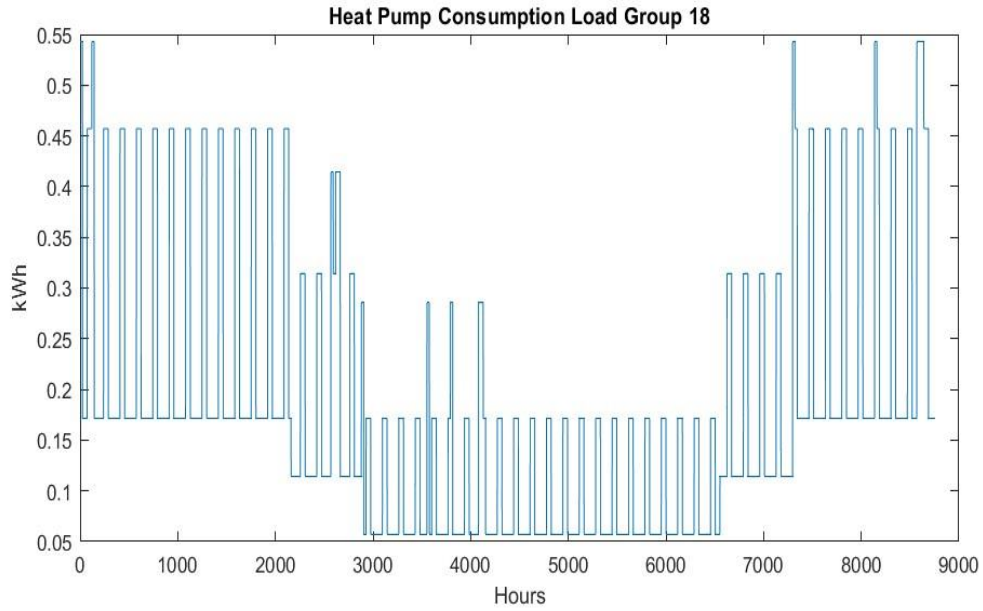


Figure 4.9 *Hourly Consumption of Heat Pump for all Customers of Load Group 18*

Step 04: Addition of Heat Pump Consumption to Customer Load

In the last step, hourly consumption of heat pump is added arithmetically to customer load for all service points of load group 18. It must be noted that customer load of each customer is based on their individual annual energy consumption and average values of load profile of the load group 18. Moreover, variance in the load profiles is not considered. Hence, heat pump load is added arithmetically to actual consumption of each customer. Moreover, it must be noted that although original load of each customer is different, heat pump hourly consumption remains the same. Furthermore, for the after hacking simulation, maximum capacity of heat pump is added to load of each customer throughout the year as a predicted worse-case scenario. Figure 4.10 compares the average hourly customer load for load group 18 under different scenarios.

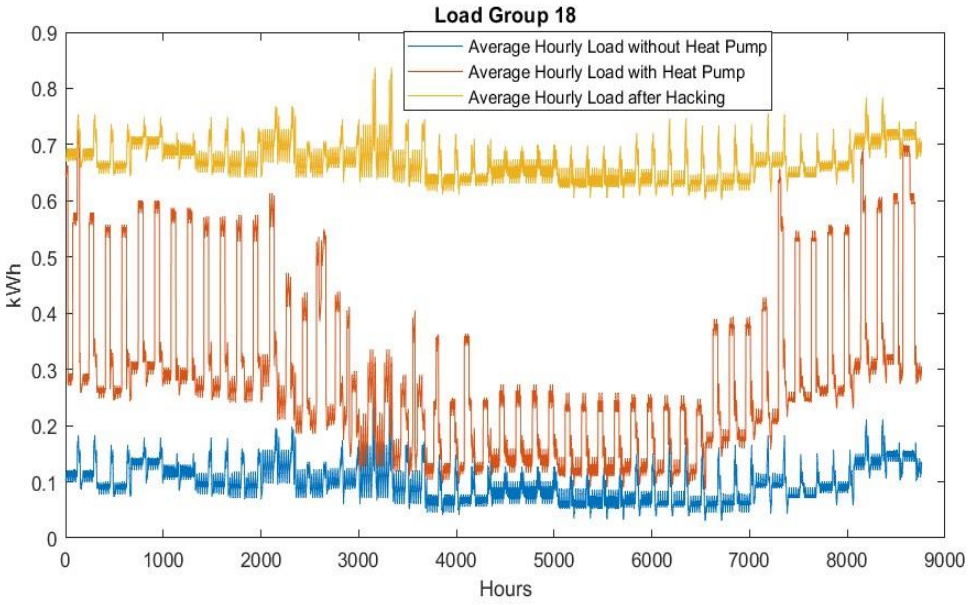


Figure 4.10 *Mean Consumption comparison for Customers of Load Group 18*

4.3 Electric Vehicle Load Modelling

In order to achieve the goal of Paris Climate Agreement to reach net zero emissions by 2050 [35], transformation from ICEVs to EVs is imperative as transportation sector is second biggest source of energy related CO2 emissions globally [36]. Hence, electric vehicles are the second type of home automated load chosen for simulation in this project. It is a future scenario prediction which will assist in understanding the impact of electric vehicles on the network under normal circumstances as well as after hacking scenarios.

4.3.1 Major Assumptions for EV Load Modelling

- To reduce complexity, it is assumed that initially no household resident has any electric vehicle. Afterwards, each house/apartment is assigned one electric vehicle as a future scenario. It means that if a service point has one user point, one EV is assigned to it. However, if a service point has ‘x’ number of user points where ‘x’ is greater than 1, then ‘x’ number of electric vehicles are assigned to that service point.
- EV load is assigned only to houses/apartment buildings which belong to load groups 01, 02, 11, 12, 13, 14, 17, 18, 23 and 24.

- EV load is not dependent upon further categories with load groups. It means that EV load is assigned similarly to electric, non-electric, and combined load groups.
- Vacation houses belonging to load group 18 are assigned EV load in same way as other load groups. It is done to save time as well as to reduce the number of load curves as per demand of project partners.
- EV load is assumed to be constant throughout the charging time period [56][57].
- Self-discharge phenomenon of lithium-ion batteries is ignored.
- It is assumed that EV charging will be done at home by all customers and major commute of each customer is between home and work [58][59].
- EV simulations are designed first for dumb charging and then for after hacking scenarios.

4.3.2 Methodology for EV Dumb Charging Load Modelling

In dumb charging method, EV is plugged-in immediately at the time of arrival of the customer. Then it gets fully charged without any interruption or other control mechanism. Following process is followed for the simulation of dumb charging of electric vehicles for all customers of the network:

Step 01: Assumption, Calculation and Documentation of Input Parameters

1. Time Resolution

Time resolution for these simulations is chosen to be one hour. Time resolution bigger than an hour would reduce accuracy and smaller than an hour would increase complexity. Hence, time resolution of one hour is chosen as an optimal value.

2. Daily Driving Distance

It is assumed that driving behavior of customers will not be greatly impacted by high penetration of electric vehicles in the future [60]. Hence, current data of ICEVs is utilized under the assumption that customer driving behavior and pattern will remain same. According to Traficom, mean daily average driving distance in Finland is approx-

imately 46 kilometers [56]. Moreover, vehicle inspection data of Finland provides with standard deviation value of 20 kilometers [56].

3. Arrival Time

Daily arrival time of each customer is very difficult to predict accurately. Multiple articles were studied [56][61] after which a paper was selected as source for arrival time values. Method used by [56] involved fitting of Gaussian distribution to hourly measurements for roads of Southern Finland. Then, the original distribution was delayed by one hour to get arrival rate from traffic rate. Through this method, daily mean arrival time of 16.53h with standard deviation of 3.99h was obtained.

4. Charging Powers

For this simulation, charging powers of 1.84 kW and 11.1 kW are used. Following methods are realized for dumb charging simulation with these charging powers:

- All customers have a charging station providing output power of 1.84 kW.
- All customers have a charging station providing output power of 11.1 kW.

5. Charging Efficiency

It is not possible to estimate individual losses during charging of EV for each customer. Hence, efficiency of 90 percent is taken as a constant value for all customers. It is also assumed that charging power remains constant throughout the charging time period. [56][57]

6. Consumption per Kilometer

In reality, mileage of an EV is variable depending upon multiple factors such as technical performance of EV, terrain, weather, driving habits etc. However, such estimation is not possible for each EV because there are thousands of customers in the network. However, a study suggests that EV consumes 0.15 kWh/km during summer and 0.25 kWh/km during winter season in Nordic climate conditions [62]. Hence, it is assumed that each EV consumes 0.25 kW/km for all customers throughout the year to simulate maximum consumption scenario.

7. Connection Time

It is assumed that each EV is connected to the network for 16 hours each day since the start of arrival time. A generalization is made that each EV owner goes to work for eight hours every day. Afterwards, each EV is plugged into home charging station at individually pre-assigned time of arrival. Then the vehicle stays plugged in for the next 16 hours irrespective of charging time. To simplify the simulation, it is assumed that the connection time stays the same for a customer for all days of the week.

Step 02: Setting up Normal Random Distribution Pattern & Application of Limits to Daily Driving Distance

Normal random distribution function is used to assign daily driving distance to each customer. Mean value is set at 46 and standard deviation is set at 20 [56]. Moreover, lower limit of 0 km and upper limit of 115 km is set. Lower limit ensures that values do not go beyond zero. All the values that go beyond zero in this normal distribution are converted automatically to zero. Upper limit is set to ensure that it takes less than 16 hours to charge the vehicle at the lowest charging power as it is assumed that office working time of each individual is set at 8 hours. This way, unique driving distance is assigned to each customer of the network which can be observed from the figure 4.11.

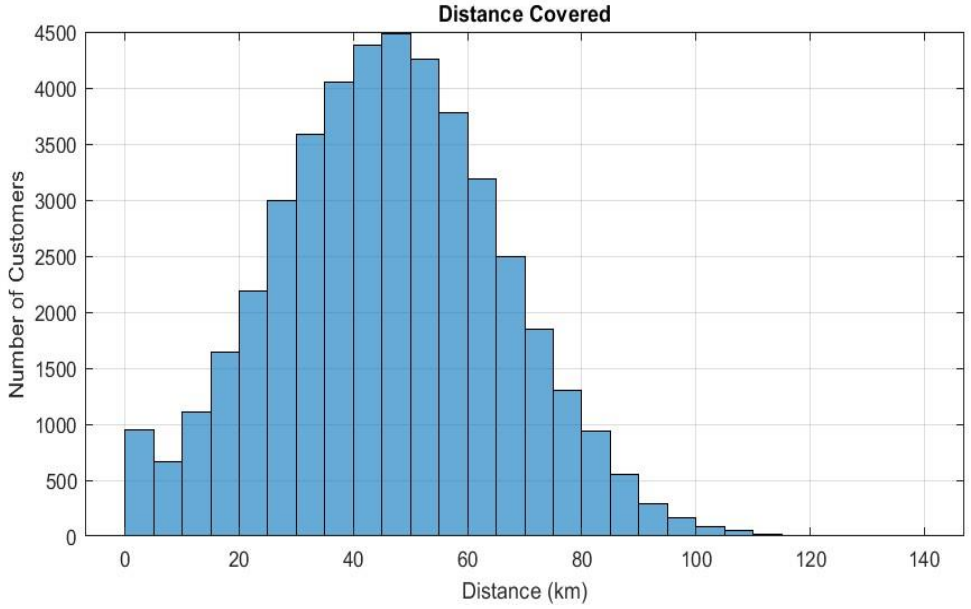


Figure 4.11 *Histogram of Distance Covered by Electric Vehicles*

Step 03: Setting up Normal Random Distribution Pattern to Arrival Time

Normal random distribution function is used to assign time of arrival to each customer with mean value of 16.53 h and standard deviation of 3.99 h [56]. No lower limit is set as if the value goes beyond zero, it would be considered for previous day. Moreover, no upper limit is set because next day starts after 24 hours. So, there is no need to set limits to distribution function of arrival time.

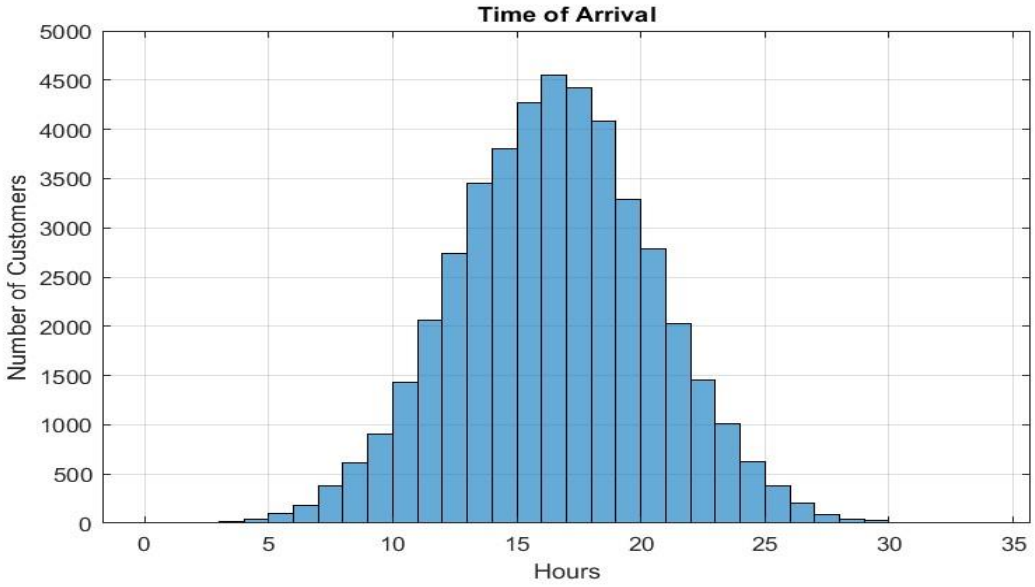


Figure 4.12 *Histogram of Time of Arrival of EV Owners*

Step 04: Calculation of Charging Timespan

To calculate timespan of charging for each electric vehicle, following formula is utilized [56]:

$$Timespan = \frac{Daily\ Driving\ Distance \times EV\ Consumption\ per\ Kilometer}{Charging\ Power \times Efficiency}$$

For the same amount of daily driving distance, consumption per kilometer and charging efficiency, EVs connected to 1.84kW chargers take most time whereas EVs connected to 11.1 kW take least amount of time to get charged.

Step 05: Allocation of EV Consumption to each Customer

Hourly EV charging consumption is allocated to each customer based on their individual time of arrival, timespan of charging, and charging power. In this simulation, it is assumed that EV charging consumption is linear [57]. Hence, EV consumption will be

maximum during middle hours of charging, and dependent upon timespan and time of arrival during first and last hour of charging cycle.

a. Individual EV Consumption Examples

Example 01: Figure 4.13 shows EV charging graph of a random customer with following parameters:

- Charging power of 1.84 kW.
- Time of arrival is 15.99 h.
- Daily driving distance is 48.85 km.
- Timespan of charging is 7.37 hours.

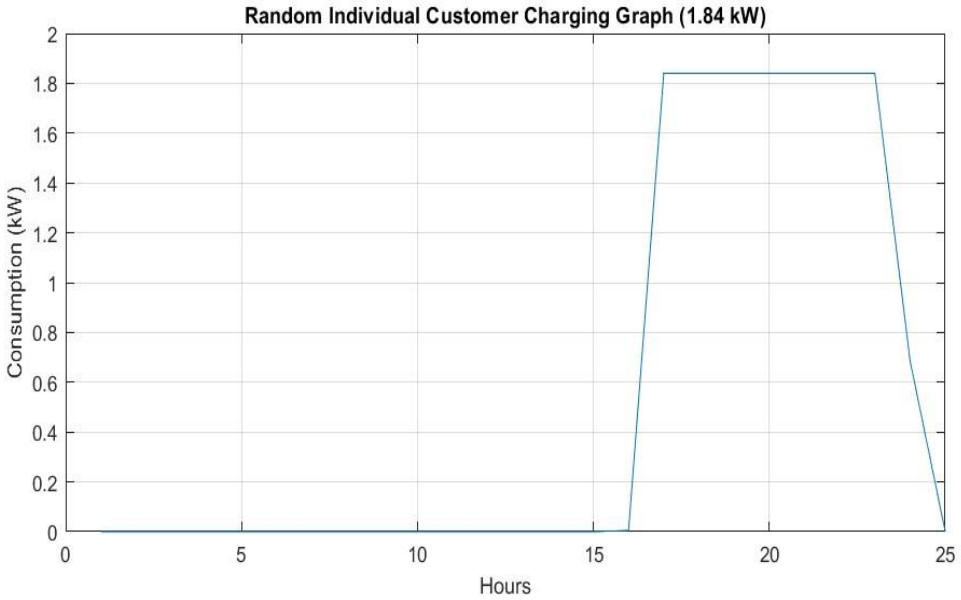


Figure 4.13 *Example of EV Charging at 1.84 kW Power for Individual Customer*

Example 02: Figure 4.14 shows EV charging graph of a random customer with following parameters:

- Charging power of 11.1 kW.
- Time of arrival is 15.99 h.
- Daily driving distance is 48.85 km.
- Timespan of charging is 1.24 hours.

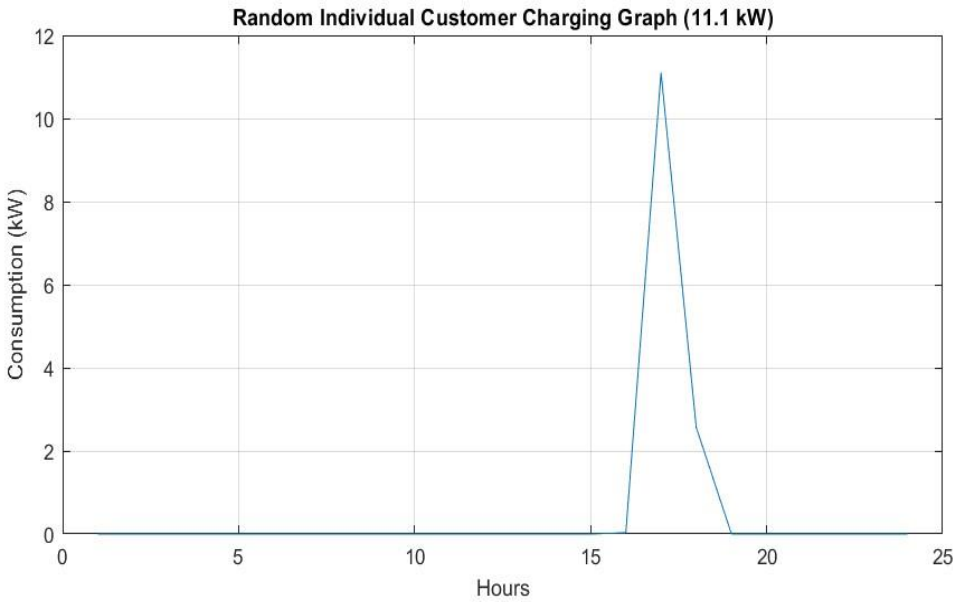


Figure 4.14 *Example of EV Charging at 11.1 kW Power for Individual Customer*

Step 06: Addition of EV charging Consumption to Customer Hourly Load

It must be noted that actual hourly consumption of each customer is based on their individual annual energy consumption and average values of load profile of the load group to which they belong. Moreover, variance in the load profiles is not considered. Furthermore, EV load pattern is assigned individually for each customer based on the aforementioned method. Thus, in the last step, hourly EV load is added arithmetically to actual hourly consumption of each customer for the whole year.

4.3.3 Choosing the after-Hacking Scenario for EV Charging

In the previous simulation, choosing the after-hacking scenario for heat pumps was quite easy because it was assumed that hackers will maximize consumption of heat pumps at all times i.e. each heat pump in the network will consume energy at its maximum capacity for the whole year. However, that scenario is not possible for electric vehicles. That is because electric vehicles can only consume limited amount of energy until they are fully charged. Afterwards, their consumption becomes minimal. In these simulations, EV consumption after full charge is assumed to be completely zero because self-discharging principle of batteries is neglected. Hence, a different after hacking scenario must be chosen which has the potential to create most damaging effects to the network.

Initially, reverse price-based after-hacking scenario was selected. This scenario was based on the day-ahead market price data of Finland from 1st January 2023 to 1st January 2024 [63]. In this method, hourly price for the whole year was used to get the average hourly price for one day. Then this price was set in descending order for 24 hours of the day. Then, based on this data, reverse price-based charging of all electric vehicles was simulated. It means that an electric vehicle connected to the network will most preferably start to charge at the highest priced hour. Then it will continue its charging during second highest price hour and so on until it is fully charged. Each electric vehicle connected to the network will follow the same pattern. Logic behind this scenario is that during the hours when prices are highest, net demand is usually highest as well, and vice versa. Hence, due to this direct correlation between load and electricity price, maximum EV load at those hours might cause most damaging affects to the grid.

However, one major factor became evident after the simulations which affected the output of aforementioned after-hacking scenario for electric vehicles. That factor was the number of electric vehicles connected to the network at certain point of time. It was found out that if a smaller number of EVs are connected to the network then cumulative effect of their charging at highest priced hours is not as damaging as initially thought out to be. In fact, if instead of following the reverse-price based hours, the order of number of electric vehicles connected to the network in descending order is followed by hackers, then effect on the network is more devastating especially if all customers have 11.1 kW charging stations. Hence, for the after-hacking scenario, descending order of hourly electricity prices is utilized for both charging powers.

Table 4.6 *Comparison of Descending Order of Hours based on Number of Electric Vehicles Connected to the Network to Descending Order of Hourly Electricity Prices.*

Descending order of hours based on number of electric vehicles connected to the network	**Descending order of hourly electricity prices**
01	07
24	08
02	17
23	09
22	18
03	06
21	10
04	16
05	11
20	19
06	15
19	12
07	13
18	14
08	20

17	05
09	21
16	22
10	04
15	23
11	24
14	03
12	01
13	02

If all customers have 11.1 kW charging stations, then EV consumption is usually the biggest load of the house. Even if EV charging peak does not converge with high load of customers, cumulative EV loads when the greatest number of EVs are connected to the network would become so high that it will form its own highest peak load which would be significantly higher than original peak load of the customers. Hence, for 11.1 kW charging, the strategy by hackers to charge all EVs based on number of EVs connected to the network proves to be more damaging for the network.

In case of 1.84 kW home charging stations, the difference between two after hacking strategies is comparatively small compared to 11.1 kW charging. Individually, EV peak load is slightly higher if hacker chooses the strategy of charging when most EVs are connected to the network. However, this difference is usually covered by the fact that original load of customers may usually converge with the reverse price-based after hacking technique. Hence, in case of 1.84 kW charging, the output from both strategies greatly depends upon the customers original load profiles.

Hence, for the after-hacking scenario, descending order of hourly electricity prices is utilized for both charging powers. Moreover, this methodology is chosen for its most adverse consequences on the local grid network. Worse after-hacking case scenarios for the individual house residents are mentioned in the last section of this thesis. It must also be noted that if the order of number of EVs connected to the network coincides with the order of highest prices hours, then the effects can be even most dangerous. However, based on price data from day-ahead market and vehicle data from Traficom, that is not the case for Finland [56][63].

a. Examples of Comparison of EV after-Hacking Charging Strategies

Example 01.

In the figures 4.15 and 4.16, 1.84 kW mean EV charging consumption for customers of load group 01 can be observed for both after-hacking strategies. For these graphs, individual EV daily charging consumption pattern at 1.84 kW for each customer of this load group is modelled through both strategies. Then, average is taken for all EV charging consumption of all customers to get an overview of as to which method pro-

vides with higher peak value. The strategy to follow descending order of number of vehicles connected to the network provides with higher consumption peak as compared to the reverse price-based strategy. However, this difference is not huge, and it depends upon the original customer load profile as to which method would provide higher peak load in overall consumption.

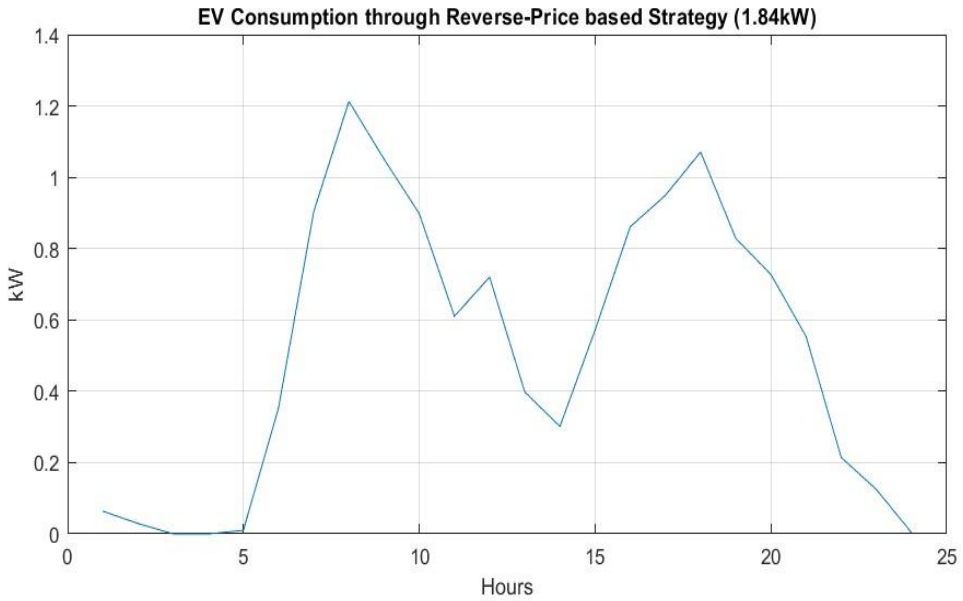


Figure 4.15 *Mean EV Consumption of Customers of Load Group 01 based on Reverse-Price based Strategy (1.84 kW)*

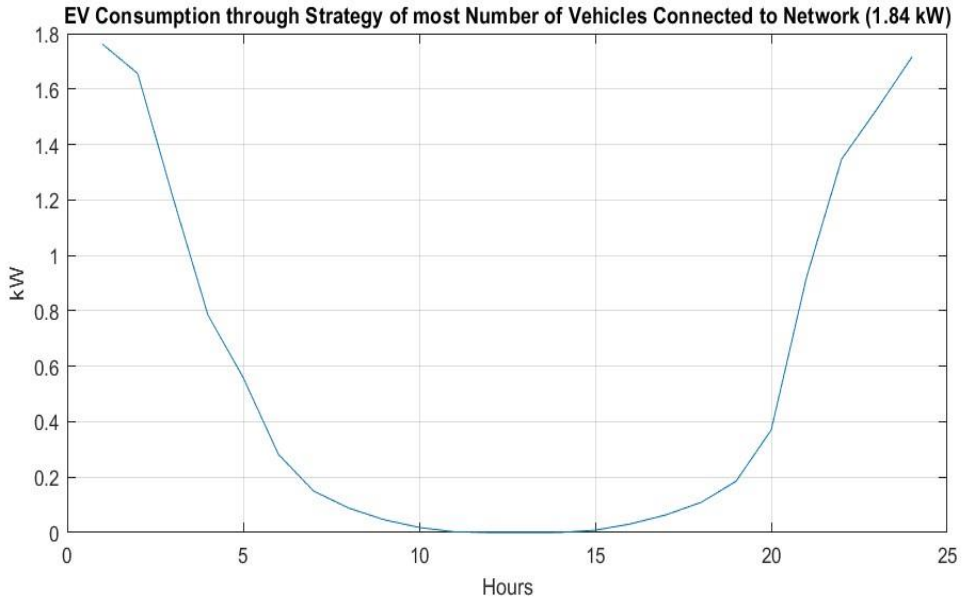


Figure 4.16 *Mean EV Consumption of Customers of Load Group 01 based on strategy of Descending Order of Number of Vehicles connected to the Network (1.84 kW)*

Example 02.

Similarly, in the figures 4.17 and 4.18, 11.1 kW mean EV charging consumption for customers of load group 01 can be observed for both after-hacking strategies. For these graphs, individual EV daily charging consumption pattern at 1.84 kW for each customer of this load group is modelled through both strategies. Then, average is taken for all EV charging consumption of all customers to get an overview of as to which method provides with higher peak value. It is evident that the strategy to follow descending order of number of vehicles connected to the network provides with much higher consumption peak as compared to the reverse price-based strategy. Moreover, as it can be seen from the graph that two different peaks are formed for reverse price based strategy because of lower driving distances, and half of the vehicles are connected at first prioritized hour of charging, and the other half are not connected to the grid at this time. This causes this strategy to cause much lower level of peak in comparison to the other strategy.

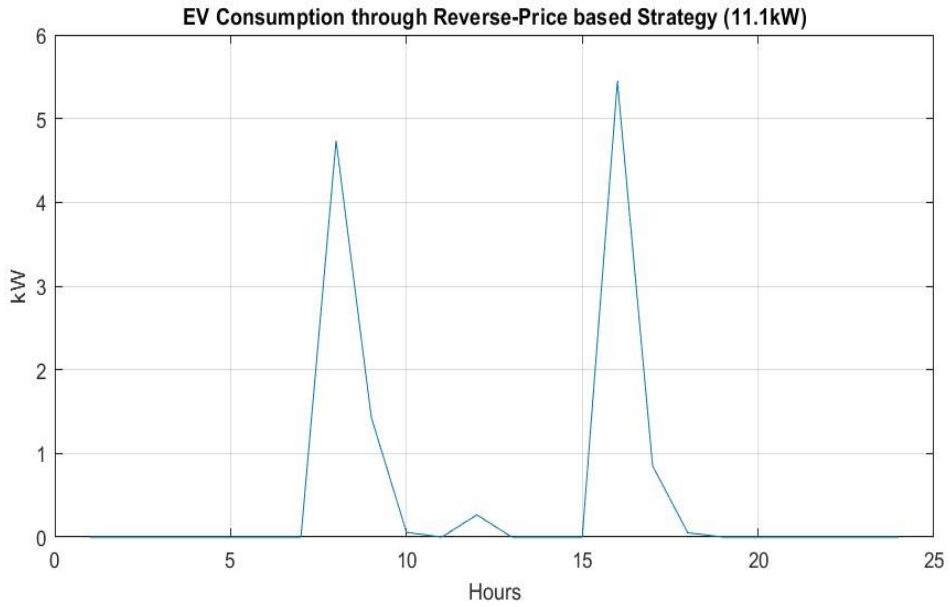


Figure 4.17 *Mean EV Consumption of Customers of Load Group 01 based on Reverse-Price based Strategy (11.1 kW)*

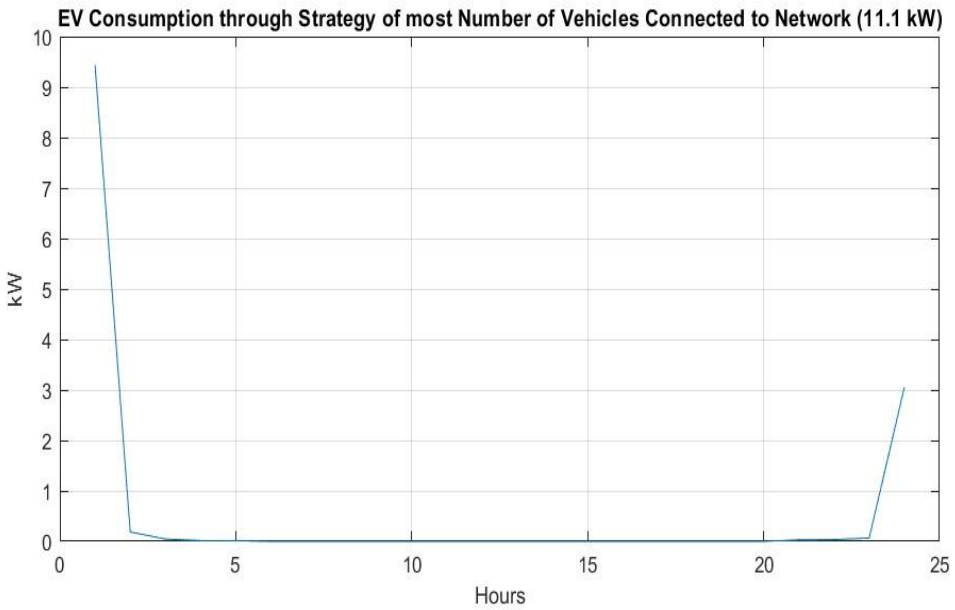


Figure 4.18 *Mean EV Consumption of Customers of Load Group 01 based on strategy of Descending Order of Number of Vehicles connected to the Network (11.1 kW)*

Hence, the after-hacking strategy is chosen based on number of vehicles connected to the network irrespective of electricity hourly price or original customer load curve.

4.3.4 Changes in the EV Simulation Design

After designing the EV simulations, they were sent to Rejlers to be integrated into the NIS to obtain results. However, it was found that each load curve has to be entered in the system manually which takes hours. Hence, due to time limitation, only limited number of load curves (20-30) could be handled. For EV simulations, each customer had a unique random sampled time series making it seemingly impossible to run those through the existing software for tens of thousands of customers. Hence, there was requirement to re-design the EV simulations to limit the number of unique load curves.

a. 1.84 kW Simulation Changes

1.84 kW EV simulations were redesigned in the following way:

1. Daily Driving Distance

To reduce the number of individual load curves, 4 different driving distances are assigned to customers. Those distances are chosen based on standard distribution data from Traficom and vehicle inspection data of Finland [56]. From the already formulated standard deviation data for daily driving distances, customers are divided into 4 different groups. Groups are based on range of driving distances from 0 to 26 km, 26 to 46 km, 46 to 66 km, and 66 km until maximum distance. Then median value is taken as

constant driving distance for each group which would give four distance values of 16, 36, 56 and 76. Then each customer is assigned one of these 4 values as their daily driving distance depending upon which group they belong to. Due to the normal distribution curve, over 70 percent of customers are assigned driving distances of either 36 km or 56 km. The remaining customers are assigned distances of either 16 km or 76 km. Specifically, 36 km and 56 km distances are each assigned to 11538 customers. Additionally, 16 km and 76 km distances are each assigned to 4945 customers. This is done to reduce the number of individual load curves as efficiently as possible. Visual representation of assigned driving distances can be observed in figure 4.19.

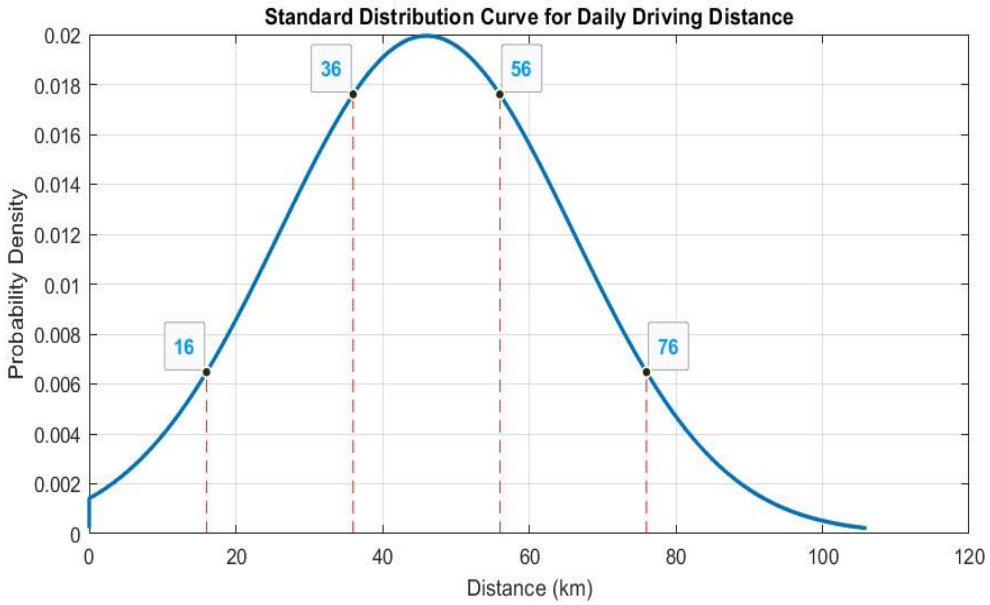


Figure 4.19 *Chosen Daily Driving Distances based on Standard Distribution Curve*

2. Arrival Time

Initially, arrival time was also set based on normal distribution with mean value of 16.53 h and standard deviation of 3.99 h. However, some kind of grouping of already assigned arrival time was needed to limit to number of unique EV load curves. So, four different customer groups were made based on pre-assigned arrival times. First group had arrival time from 00 to 06, second group had arrival time from 06 to 12, third group had arrival time from 12 to 18, and fourth group had arrival time from 18 to 24. It must be mentioned that most number of customers usually would lie in the groups 3 and 4 because of pattern of normal distribution.

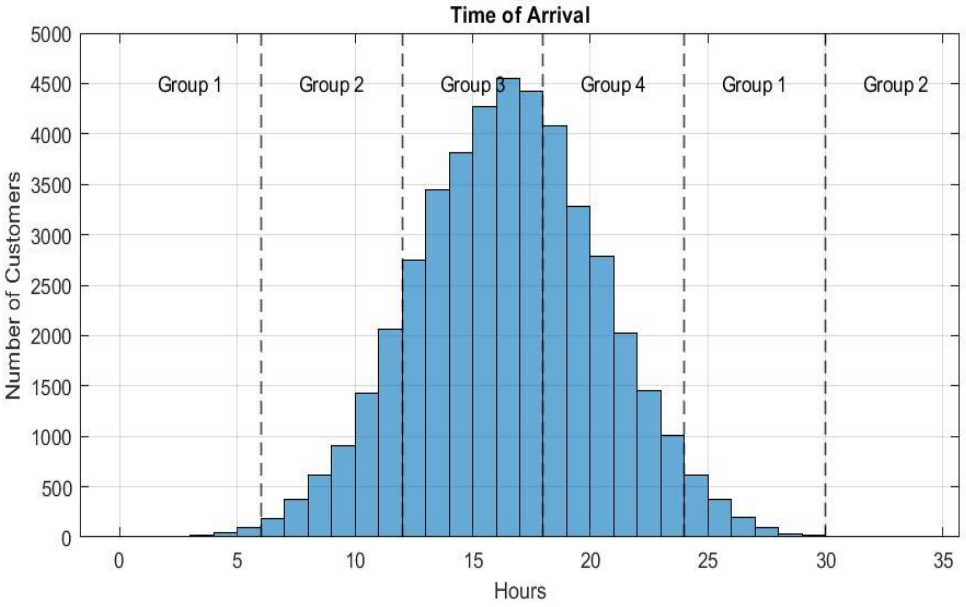


Figure 4.20 *Grouping Methodology for pre-assigned Time of Arrival*

3. Customer Grouping for before Hacking Scenario

For before hacking scenario, customer grouping is done in a way that customers which have same driving distance and same group of arrival time will have same load curve. This similar load curve will be formulated by taking the average value of hourly EV charging consumption of all customers in a group. There are 4 driving distance values and 4 groups of arrival time. Thus, there will be 16 load curves for EV charging before hacking scenario. This grouping is illustrated in the table 4.7.

Table 4.7 *Customer Grouping for EV Load Modelling at 1.84 kW Charging Power*

Load Curve	Daily Driving Distance	Arrival Time
Load Curve 01	16 km	00-06
Load Curve 02	16 km	06-12
Load Curve 03	16 km	12-18
Load Curve 04	16 km	18-24
Load Curve 05	36 km	00-06
Load Curve 06	36 km	06-12
Load Curve 07	36 km	12-18
Load Curve 08	36 km	18-24
Load Curve 09	56 km	00-06
Load Curve 10	56 km	06-12
Load Curve 11	56 km	12-18
Load Curve 12	56 km	18-24
Load Curve 13	76 km	00-06
Load Curve 14	76 km	06-12
Load Curve 15	76 km	12-18
Load Curve 16	76 km	18-24

In the figure 4.21, a screenshot from MATLAB software is presented to elaborate the process of load curve formulation. It shows consumption pattern of customers belong-

ing to load curve 6 category. All customers in this group have 36 km driving distance which assigns them similar daily energy consumption for EV charging. Moreover, arrival time of all customers of this group is from 6-12. Once the charging pattern of each customer is formulated in this customer group, average value for EV charging consumption is taken of the whole group. This way, similar load curve is assigned to all the customers of this group. Single driving distance value coupled with similar group of arrival time allows for this type of simplification as high level of accuracy is maintained.

tt2 extcons

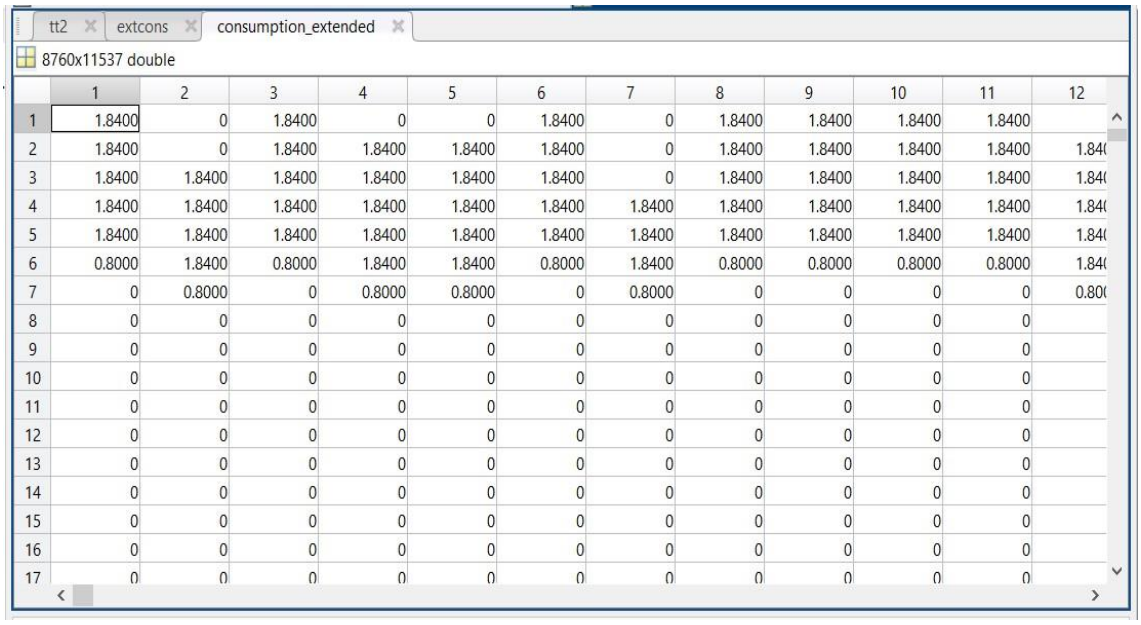
8760x1455 double

	1	2	3	4	5	6	7	8	9	10	11	12
4	0	0	0	0	0	0	0	0	0	0	0	
5	0	0	0	0	0	0	0	0	0	0	0	
6	0	0	0	0	0	0	0	0	0	0	0	
7	0	0	0	0	0	0	0	0	0	0	0	
8	0	0	0	0	0	0	0	0	0	0	0	
9	0	0	0	0	0	0	0	0	0	0	0	0.01
10	0	0	0	0	0	0	1.5609	0	0	0	0	1.84
11	1.6494	1.1318	0	0	1.0622	0	1.8400	0	0	0	0	1.84
12	1.8400	1.8400	1.5244	1.7763	1.8400	1.8394	1.8400	0.0313	1.2745	1.7899	1.2539	1.84
13	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.84
14	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.84
15	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.0791	1.8400	1.8400	1.8400	1.8400	0.78
16	0.9906	1.5082	1.8400	1.8400	1.5778	1.8400	0	1.8400	1.8400	1.8400	1.8400	
17	0	0	1.1156	0.8637	0	0.8006	0	1.8400	1.3655	0.8501	1.3861	
18	0	0	0	0	0	0	0	0.7687	0	0	0	
19	0	0	0	0	0	0	0	0	0	0	0	
20	0	0	0	0	0	0	0	0	0	0	0	

Figure 4.21 *Grouping of EV Dumb Charging (1.84 kW) Customers for Load Curve 6*

4. Customer Grouping for after Hacking Scenario

Grouping of arrival time is not required because hackers will employ charging pattern based on descending order of number of vehicles connected to the network. It is simply assumed that each vehicle will stay connected to the grid for 16 hours since arrival time of each customer which is pre-assigned through normal distribution pattern as explained in the initial simulation. The only grouping done is this category is based on four different driving distances assigned to customers. For example, for the customers belonging to 36 km distance group, their after hacking charging consumption pattern will be quite similar as it can be seen from figure 4.22. Although some variations would exist. Nevertheless, once the charging pattern of each customer is formulated, average value for EV charging consumption is taken of the whole group. This way, similar load curve is assigned to all the customers of this group. As four different driving distances are assigned, four different unique load curves are formulated for after hacking scenario.



	1	2	3	4	5	6	7	8	9	10	11	12
1	1.8400	0	1.8400	0	0	1.8400	0	1.8400	1.8400	1.8400	1.8400	
2	1.8400	0	1.8400	1.8400	1.8400	1.8400	0	1.8400	1.8400	1.8400	1.8400	1.84(
3	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	0	1.8400	1.8400	1.8400	1.8400	1.84(
4	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.84(
5	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.8400	1.84(
6	0.8000	1.8400	0.8000	1.8400	1.8400	0.8000	1.8400	0.8000	0.8000	0.8000	0.8000	1.84(
7	0	0.8000	0	0.8000	0.8000	0	0.8000	0	0	0	0	0.80(
8	0	0	0	0	0	0	0	0	0	0	0	
9	0	0	0	0	0	0	0	0	0	0	0	
10	0	0	0	0	0	0	0	0	0	0	0	
11	0	0	0	0	0	0	0	0	0	0	0	
12	0	0	0	0	0	0	0	0	0	0	0	
13	0	0	0	0	0	0	0	0	0	0	0	
14	0	0	0	0	0	0	0	0	0	0	0	
15	0	0	0	0	0	0	0	0	0	0	0	
16	0	0	0	0	0	0	0	0	0	0	0	
17	0	0	0	0	0	0	0	0	0	0	0	

Figure 4.22 *Grouping of EV after-Hacking Customers assigned with 36 km Daily Driving Distance*

b. 11.1 kW Simulation Changes

Ideally, 11.1 kW simulations should also have been redesigned the same way as 1.84 kW simulations. However, number of load curves was further needed to be reduced because of demand of our project partners. Hence, 11.1 kW simulations are redesigned in the following way:

1. Daily Driving Distance

Daily driving distance of all customers is assumed to be 46 km. It is the mean value of daily driving distance in Finland according to Traficom. Only one driving distance value is assigned to all customers to reduce number of unique load curves even further.

2. Arrival Time

For 11.1 kW simulations, 8 different customer groups are formulated based on standard distribution of arrival times. These customer groups are based on 3-hour timespan instead of 6 hours. This is done because for 11.1 kW charging power, it takes comparatively less time to completely charge the vehicle. If customer grouping is done for bigger span of arrival time, then mean value for charging consumption of all customers of that load group would become less precise. This would result in inaccurate load curve. Hence, 3-hour window is selected for customer grouping for 11.1 kW charging power.

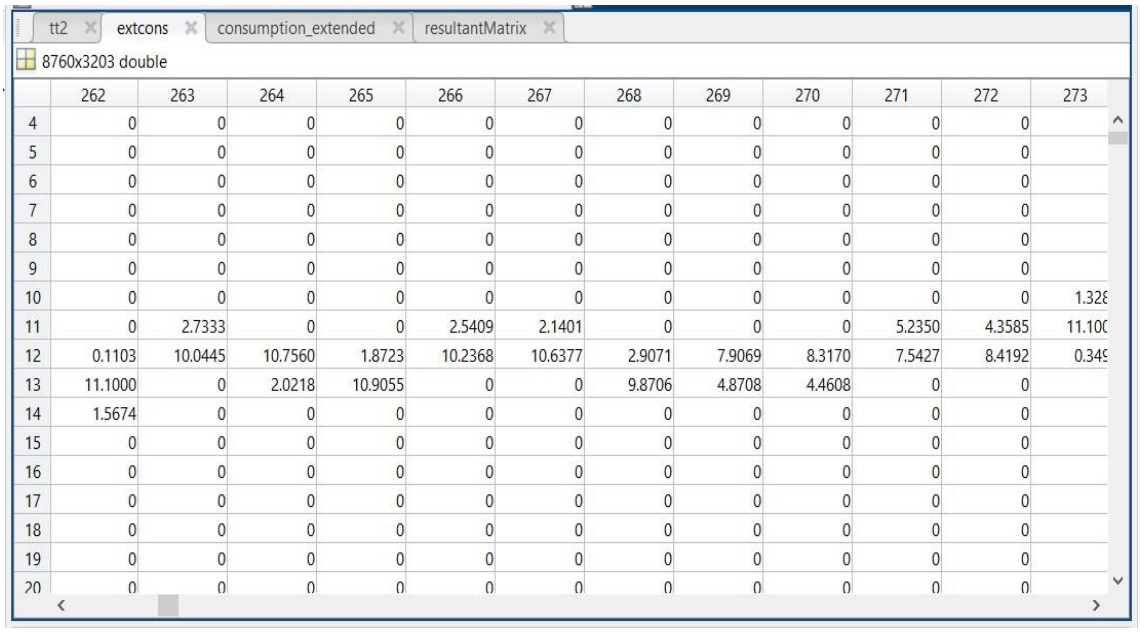
3. Customer Grouping for before Hacking Scenario

In total, there will be 8 unique load curves for customer groups. These are formulated in the following way:

Table 4.8 *Customer Grouping for EV Load Modelling at 11.1 kW Charging Power*

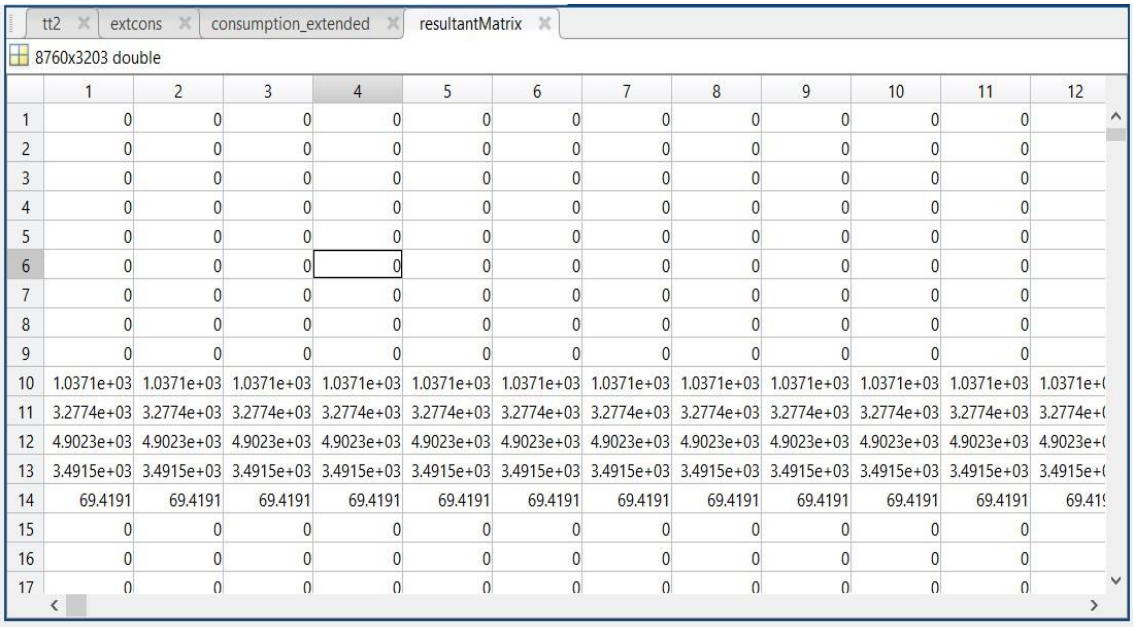
Load Curve	Daily Driving Distance	Arrival Time
Load Curve 01	46	00-03
Load Curve 02	46	03-06
Load Curve 03	46	06-09
Load Curve 04	46	09-12
Load Curve 05	46	12-15
Load Curve 06	46	15-18
Load Curve 07	46	18-21
Load Curve 08	46	21-24

The example of EV consumption for customers with arrival time between 9 to 12 is shown in the figure 4.23. To formulate single load curve for all these customers, average value for EV hourly consumption is taken. The, a uniform value of EV consumption will be assigned to all customers belonging to this group as evident from the figure 4.24.



	262	263	264	265	266	267	268	269	270	271	272	273
4	0	0	0	0	0	0	0	0	0	0	0	
5	0	0	0	0	0	0	0	0	0	0	0	
6	0	0	0	0	0	0	0	0	0	0	0	
7	0	0	0	0	0	0	0	0	0	0	0	
8	0	0	0	0	0	0	0	0	0	0	0	
9	0	0	0	0	0	0	0	0	0	0	0	
10	0	0	0	0	0	0	0	0	0	0	0	1.328
11	0	2.7333	0	0	2.5409	2.1401	0	0	0	5.2350	4.3585	11.100
12	0.1103	10.0445	10.7560	1.8723	10.2368	10.6377	2.9071	7.9069	8.3170	7.5427	8.4192	0.349
13	11.1000	0	2.0218	10.9055	0	0	9.8706	4.8708	4.4608	0	0	
14	1.5674	0	0	0	0	0	0	0	0	0	0	
15	0	0	0	0	0	0	0	0	0	0	0	
16	0	0	0	0	0	0	0	0	0	0	0	
17	0	0	0	0	0	0	0	0	0	0	0	
18	0	0	0	0	0	0	0	0	0	0	0	
19	0	0	0	0	0	0	0	0	0	0	0	
20	0	0	0	0	0	0	0	0	0	0	0	

Figure 4.23 *Grouping of EV Dumb Charging (11.1 kW) Customers for Load Curve 4*



tt2 | extcons | consumption_extended | resultantMatrix

8760x3203 double

	1	2	3	4	5	6	7	8	9	10	11	12
1	0	0	0	0	0	0	0	0	0	0	0	
2	0	0	0	0	0	0	0	0	0	0	0	
3	0	0	0	0	0	0	0	0	0	0	0	
4	0	0	0	0	0	0	0	0	0	0	0	
5	0	0	0	0	0	0	0	0	0	0	0	
6	0	0	0	0	0	0	0	0	0	0	0	
7	0	0	0	0	0	0	0	0	0	0	0	
8	0	0	0	0	0	0	0	0	0	0	0	
9	0	0	0	0	0	0	0	0	0	0	0	
10	1.0371e+03	1.0371e+03	1.0371e+03	1.0371e+03	1.0371e+03	1.0371e+03	1.0371e+03	1.0371e+03	1.0371e+03	1.0371e+03	1.0371e+03	1.0371e+(
11	3.2774e+03	3.2774e+03	3.2774e+03	3.2774e+03	3.2774e+03	3.2774e+03	3.2774e+03	3.2774e+03	3.2774e+03	3.2774e+03	3.2774e+03	3.2774e+(
12	4.9023e+03	4.9023e+03	4.9023e+03	4.9023e+03	4.9023e+03	4.9023e+03	4.9023e+03	4.9023e+03	4.9023e+03	4.9023e+03	4.9023e+03	4.9023e+(
13	3.4915e+03	3.4915e+03	3.4915e+03	3.4915e+03	3.4915e+03	3.4915e+03	3.4915e+03	3.4915e+03	3.4915e+03	3.4915e+03	3.4915e+03	3.4915e+(
14	69.4191	69.4191	69.4191	69.4191	69.4191	69.4191	69.4191	69.4191	69.4191	69.4191	69.4191	69.41
15	0	0	0	0	0	0	0	0	0	0	0	
16	0	0	0	0	0	0	0	0	0	0	0	
17	0	0	0	0	0	0	0	0	0	0	0	

Figure 4.24 *Assignment of 11.1 kW Dumb Charging Load Curve 4 to Customers*

4. Customer Grouping for after Hacking Scenario

After hacking scenario is based on descending order of number of vehicles connected to the network at any given time. There is just one load curve for after hacking scenario of 11.1 kW charging power EV simulation. This is because driving distance is assumed to be same for each customer and arrival time becomes irrelevant except for when choosing the order of number of vehicles connected to the network. This is because it is assumed that each vehicle stays connected to the network for 16 hours after arrival time. Hence, there will be one load curve for after hacking scenario for 11.1 kW charging power.

5. RESULTS OF IMPACTS OF CYBERATTACK ON LOCAL GRID IN SOUTH SAVO, FINLAND

In terms of impacts of cyberattack on local grid, there are three components on which the effects usually occur: transformers, conductors, and service points. Most common impacts can be non-compliance of voltage quality standards and overloading. Voltage quality can be impacted especially in already stressed LV and MV network by synchronized load increment especially during peak loading hours. This may cause non-compliance of voltage quality vis-à-vis power quality standards. Undervoltage, overvoltage, supply voltage variations, voltage dips, transient overvoltage, harmonic and inter-harmonic voltage are some of the standards which may become non-compliant due to cyberattack on home automation systems. This would result in excessive customer complains along with creation of artificial grid reinforcement needs. In situations of local overloading, there exists the potential for the existing capacities network components, particularly when the grid is already operating under conditions of high loading or alternative topology. Excessive amount of current drawn due to load increment of multiple automated loads may result in overloading of service points, conductors as well as transformers. If network protection system works properly, such overloading incidents may cause outages. If network protection system fails, then thermal damage to the equipment may be caused. More serious consequences can occur as well. For instance, if a distribution transformer does not have unit protection, and feeder protection does not detect overloading of this transformer, fire may erupt posing threat to environment as well as human beings.

In this section, results of impacts of heat pump and electric vehicle addition to the customer load in both before and after-hacking scenarios are presented. HP (Method 01) refers to heat pump method 01 simulation. HP (Method 02) refers to heat pump method 02 simulation. EV (1.84 kW) refers to electric vehicle charging simulation with charging power of 1.84 kW. Similarly, EV (11.1 kW) refers to electric vehicle charging simulation with charging power of 11.1 kW.

5.1 Impacts on Service Points

Total number of service points in the network for base case are 79488. It must be noted that only unique Tunnus id service points are considered. Moreover, service points which have loading level above 1000 % are omitted as it is assumed to be erroneous data. In total, 8 different simulations are modelled for which results are calculated to compare them to base case. As each case of simulation is run individually at different times, there may be some minor changes in the network data. Most common aspect of data change is service points missing from the network. However, if base case is set as standard, missing data comprises of less than 0.5 percent of overall number of service points. Hence, these changes are small and should not affect the integrity of the results.

However, for the case of EV 1.84 kW normal operation simulations, data for 10536 service points is missing. This accounts for around 15 percent of the total available data. It may have happened due to any error during processing of the simulation. However, due to shortage of time, this simulation was not repeated. Hence, for EV 1.84 kW simulation both operation scenarios, number of service points considered are 68952. Moreover, same number of service points are considered for base case comparison for this simulation to enable clarity in the results. However, for all other cases, and their base case comparisons, number of service points are considered to be 79488. Hence, each simulation should be compared to its own base case value.

It must also be noted that after heat pump simulation method 01, NIS version as well as data base was updated. Moreover, base loads were recalculated and changed during this update. Hence, there may be some disparities in results for HP (method 01) in comparison to other cases.

5.1.1 Average Loading Level

As it can be seen from the table 5.1, for both heat pump simulations, average loading level under normal operation of heat pumps decreases in comparison to base case. This decrease is understandable because loading level deceases for electric heated load groups and increases for non-electric heated load groups. This shows that decrease in loading level in electric heated load groups causes more effect on the network in comparison to load increase in non-electric heated load groups. Moreover, in the after hacking scenario, loading level does not increase massively for heat pump simulations. This is because heat pumps already operating near full capacity during

winters under normal operation. Hence, the remaining capacity for load increment for after hacking scenario is not substantial.

For 1.84 kW EV simulations, there isn't any significant change in either operation scenario because of the lower power level. Moreover, for the after hacking scenario, instead of load increment, load shifting is done. This load shifting is done based on the descending order of number of electric vehicles connected to the network. However, those hours correspond to low peak hours, and EV consumption is not high enough to formulate its own peak. Hence, there does not seem to be any significant change in loading level of service points in after hacking scenario of this case. Moreover, it must be noted that these are results for all service points in the network. The simulated loads, however, are only added on service points belonging to houses/apartments which constitute for less than 40 of overall service points in the network. Consequently, the impact of low-power electric vehicle charging loads (1.84 kW) on the overall loading levels of the network's service points may be minimal. Moreover, as explained in the methodology for EV (1.84 kW simulations), grouping of customers was done and average value of individual consumption was taken which does affect the simulation as well.

For, 11.1 kW EV simulations, it is evident that loading level increases significantly for normal operation. Furthermore, in the after hacking scenario, loading level increases more than two-folds while following the same load shifting technique as used in 1.84 kW charging simulation. Hence, this case has the most affect in terms of average loading level.

Table 5.1 *Average Loading Level Percentage of all Service Points*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	24.93 %	22.59 %	23.67 %
HP (Method 02)	24.93 %	16.51 %	18.51 %
EV (1.84 kW)	24.7914 %	24.7914 %	24.7917 %
EV (11.1 kW)	24.93 %	34.43 %	53 %

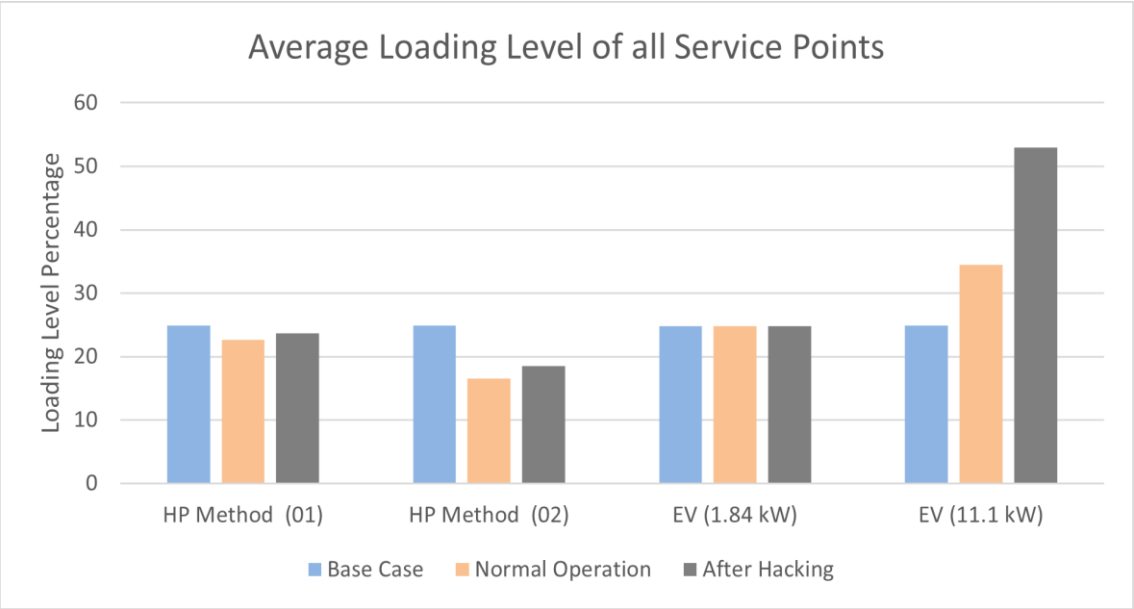


Figure 5.1 *Comparison of Average Loading Level of Service Points*

5.1.2 Overloading

In this section, overloading analysis is conducted for all scenarios of all cases. Initially, number of overloaded service points, and then average loading level of overloaded service points is calculated. This provides with complete overview of scale as well as degree of overloading of service points throughout the network.

a. Number of Overloaded Service Points

Results of number of overloaded service points beyond 100 % are shown in the table 5.2. For both methods of heat pump simulations under normal operation as well as after hacking scenario, the number of overloaded service points remain lower than base case. For 1.84 kW EV simulations under both operation scenarios, number of overloaded service points remain same. Meanwhile, for 11.1 kW EV simulation, the greatest number of service points get overloaded beyond 100 %. For this case, under normal operation, number of overloaded service points increase more than two-folds. Moreover, in the after hacking-scenario of this case, almost 20 percent of service points of the whole network get overloaded. Graphical representation can be observed from figure 5.2.

Table 5.2 *Number of Service Points Overloaded beyond 100 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	903	517	545
HP (Method 02)	903	575	693
EV (1.84 kW)	776	776	776
EV (11.1 kW)	903	1864	15639

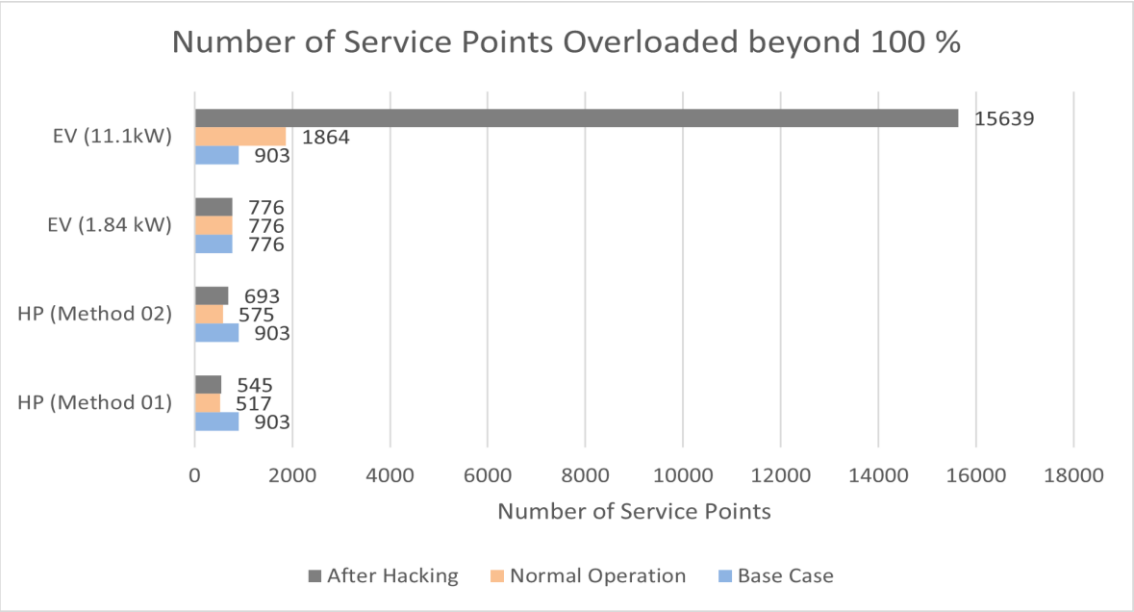


Figure 5.2 *Comparison of Number of Service Points Overloaded beyond 100 %*

Moreover, it is evident from the table 5.3 that the number of service points overloaded beyond 130 percent follow the same pattern as explained above for each case.

Table 5.3 *Number of Service Points Overloaded beyond 130 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	368	242	252
HP (Method 02)	368	243	288
EV (1.84 kW)	309	309	309
EV (11.1 kW)	368	639	5672

b. Average Loading Level of Overloaded Service Points

In this section, average loading level of overloaded service points is presented in the tables 5.4, and 5.5. It gives the idea of severity of overloading problem for each scenario.

Table 5.4 *Average Loading Level of Service Points Overloaded beyond 100 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	132.14 %	136.95 %	137.03 %
HP (Method 02)	132.14 %	132.67 %	134.07 %
EV (1.84 kW)	132.14 %	132.19 %	132.13 %
EV (11.1 kW)	132.14 %	134.18 %	135.54 %

Table 5.5 *Average Loading Level of Service Points Overloaded beyond 130 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	161.08 %	163.61 %	164.45 %
HP (Method 02)	161.08 %	159.60 %	162.75 %
EV (1.84 kW)	161.08 %	162.04 %	161.04 %
EV (11.1 kW)	161.08 %	178.10 %	174.69 %

5.1.3 Undervoltage

In this section, undervoltage analysis is conducted for all scenarios of all cases. Initially, number of service points experiencing undervoltage, and then average loading level of those service points is calculated. This provides with complete overview of scale as well as degree of issue of undervoltage throughout the network.

a. Number of Service Points experiencing Undervoltage

The issue of service points experiencing undervoltage below 95 % is most prevalent in the network as compared to the issues of overloading and overvoltage. In HP method 01, number of service points experiencing undervoltage below 95 % increase slightly for normal operation as well as after hacking scenario. For HP method 02, this number decreases for both operation scenarios. For 1.84 kW EV simulation, number of service points experiencing undervoltage below 95 % fluctuate slightly for both operational scenarios in comparison to base case. This fluctuation might be accredited to different time periods at which the simulation is being conducted along with update of NIS. Finally, in 11.1 kW EV simulation, number of service points experiencing undervoltage below 95 % almost double during normal operation scenario. However, in the after-hacking scenario for this case, this number increases massively. In fact, more than 66 % of all the service points in the network experience undervoltage below 95 %. This case represents very alarming situation for the network. Figure 5.3 presents graphical comparison for number of service points experiencing undervoltage below 95 % for all cases under multiple operating conditions.

Table 5.6 *Number of Service Points experiencing Undervoltage below 95 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	9845	10029	12064
HP (Method 02)	9845	5905	8050
EV (1.84 kW)	8770	8771	8759
EV (11.1 kW)	9845	17762	52474

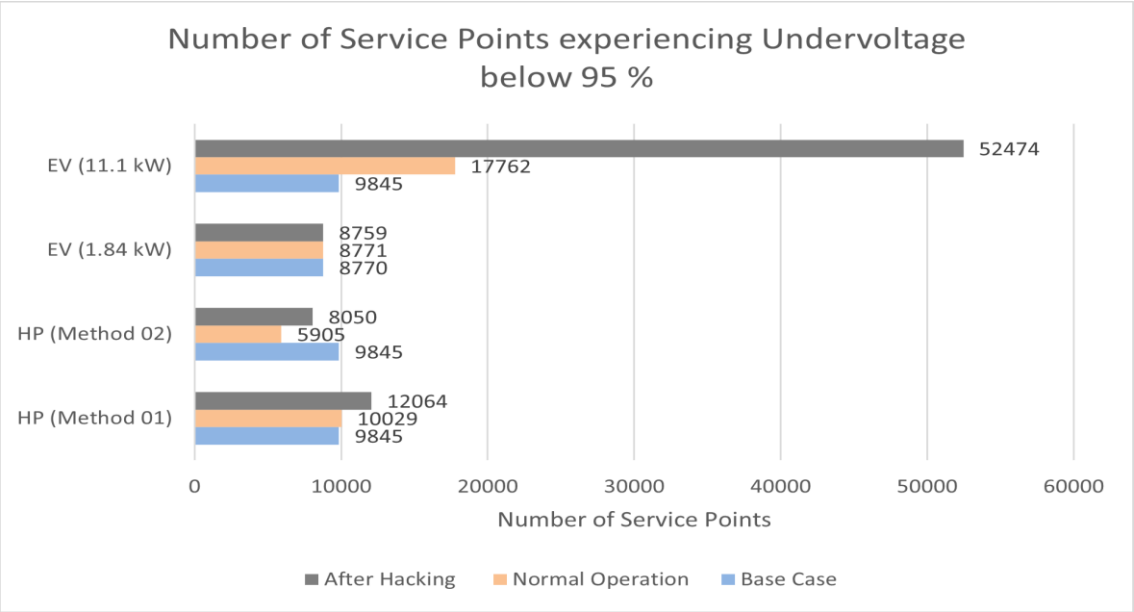


Figure 5.3 *Number of Service Points experiencing Undervoltage below 95 %*

However, in the tables 5.7 and 5.8, sharp decline can be seen for number of service points experiencing undervoltage below 90 % and 85 % especially for HP (Method 02) and EV (1.84 kW). However, 11.1 kW EV case, especially in the after hacking operation scenario, has lots of service points experiencing undervoltage below 90 % and 85 %.

Table 5.7 *Number of Service Points experiencing Undervoltage below 90 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	1008	949	1249
HP (Method 02)	1008	520	838
EV (1.84 kW)	1008	822	950
EV (11.1 kW)	1008	2566	27987

Table 5.8 *Number of Service Points experiencing Undervoltage below 85 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	68	55	84
HP (Method 02)	68	30	58
EV (1.84 kW)	68	52	68
EV (11.1 kW)	68	292	13130

b. Average Voltage Level of Service Points experiencing Undervoltage

Average voltage level of service points experiencing undervoltage depict severity of the problem. As evident from the tables 5.9, 5.10 and 5.11, 11.1 kW EV after hacking has the most severe undervoltage problem. This operation scenario not only has the highest number of service points experiencing undervoltage but also has the lowest average voltage for those service points.

Table 5.9 *Average Voltage Level of Service Points experiencing Undervoltage below 95 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	213.31 V	213.52 V	213.29 V
HP (Method 02)	213.31 V	213.41 V	213.28 V
EV (1.84 kW)	213.31 V	213.48 V	213.36 V
EV (11.1 kW)	213.31 V	212.44 V	200.93 V

Table 5.10 *Average Voltage Level of Service Points experiencing Undervoltage below 90 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	202.53 V	202.88 V	202.57 V
HP (Method 02)	202.53 V	202.71 V	202.74 V
EV (1.84 kW)	202.53 V	202.49 V	202.36 V
EV (11.1 kW)	202.53 V	201.70 V	190.24 V

Table 5.11 *Average Voltage Level of Service Points experiencing Undervoltage below 85 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	187.20 V	190.23 V	190.57 V
HP (Method 02)	187.20 V	186.98 V	188.62 V
EV (1.84 kW)	187.20 V	185.44 V	187.21 V
EV (11.1 kW)	187.20 V	190.18 V	177.10 V

5.2 Impacts on Transformers

Total number of transformers in the network is 9465 for all cases except EV (1.84 kW). For that, number of transformers analyzed are 4742. Such low number is because of the missing data due to some error while running the simulation. Hence, for this case, 4742 transformers are analyzed for both operational scenarios as well as their base case. Moreover, those transformers which have loading level beyond 1000 % are not considered in calculation as they are assumed to be erroneous data.

5.2.1 Average Loading Level

In this section, average loading level of all transformers for all operation scenarios of all cases are compared. As it can be seen from the table 5.12, average loading level does not change much in any case except 11.1 kW EV simulation. In that case, average loading level increases to 42.32 % for normal operation, and 73.36 % for after hacking scenario.

Table 5.12 *Average Loading Level Percentage of all Transformers*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	33.83 %	33.89 %	35.72 %
HP (Method 02)	33.83 %	25.58 %	29.04 %
EV (1.84 kW)	34.89 %	34.90 %	34.90 %
EV (11.1 kW)	33.83 %	42.32 %	73.36 %

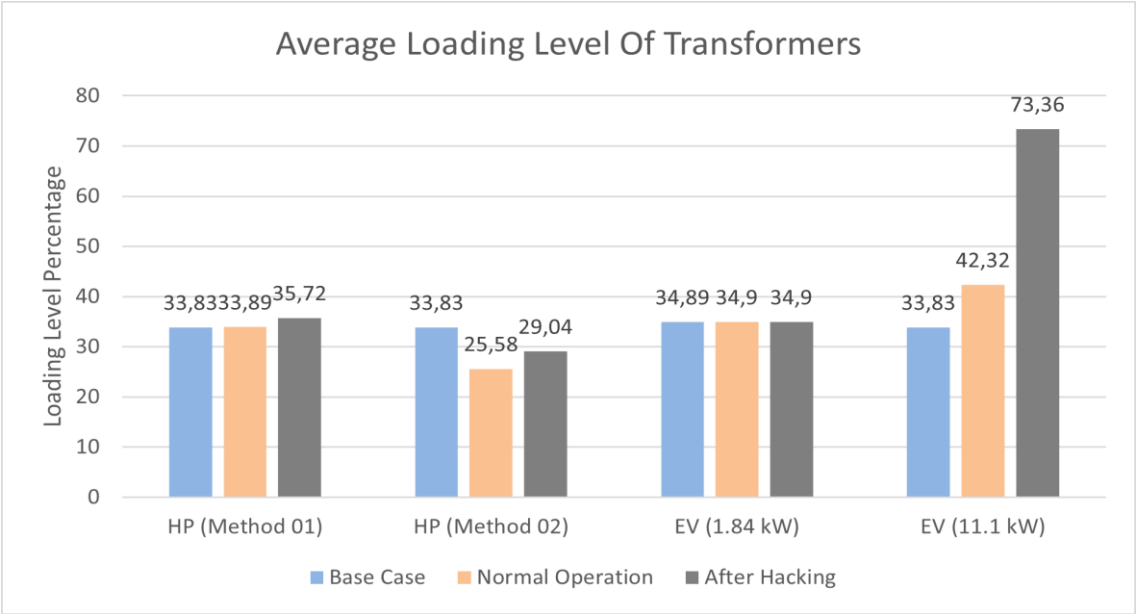
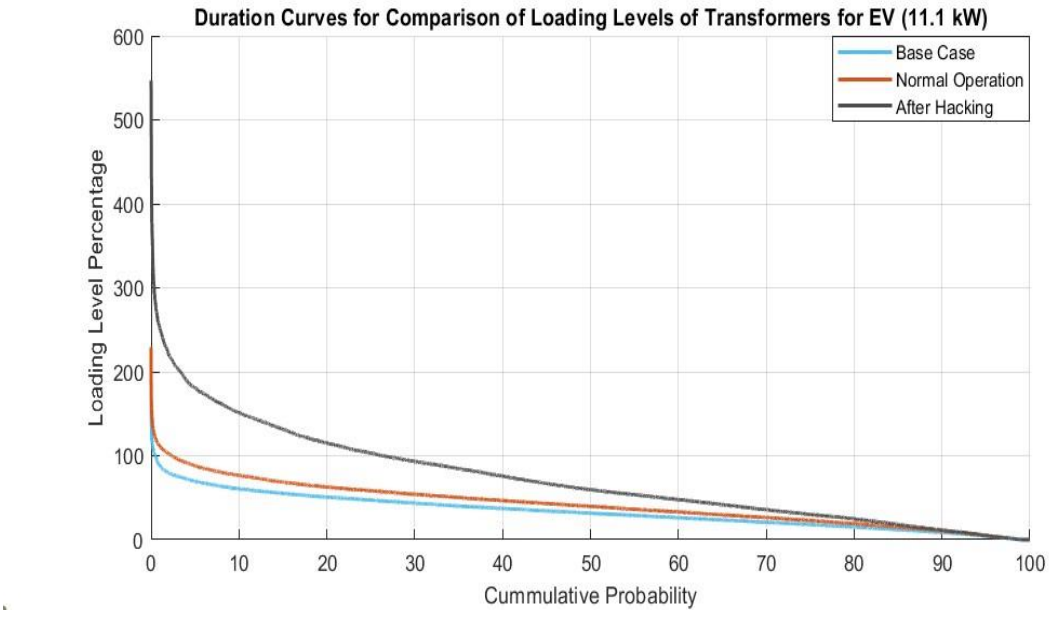


Figure 5.4 *Comparison of Average Loading Level of Transformers*

The figure below shoes duration curve for comparison of loading level of transformers for 11.1 kW EV case. It can be seen from the figure that with the addition of EV loads (11.1 kW), the loading level of transformers as well as number of overloaded transformers increase under both operation scenarios. However, this increase is much more evident in the after hacking scenario.



5.2.2 Overloading

In this section, overloading analysis is conducted for all scenarios of all cases. Initially, number of overloaded transformers, and then average loading level of overloaded

transformers is calculated. This provides with complete overview of scale as well as degree of overloading of transformers throughout the network.

a. Number of Overloaded Transformers

While analysing the number of transformers overloaded beyond 100 % from table 5.13, multiple observations are made. For HP method 01, number of overloaded transformers increase for both operation scenarios. However, this increase is greater in the after hacking scenario as number of overloaded transformers increase by 150 %. In contrast, for HP method 02, number of overloaded transformers decrease in both operation scenarios. This decrease might be accredited to reduction of load for service points belonging to electric heated load group as well as change in the network base load data in the NIS system. Moreover, for EV (1.84 kW) normal operation, number of overloaded transformers remain exactly same for both operation scenarios in comparison to base case. However, 11.1 kW EV simulations show major overloading concern for transformers in the network. Here, number of overloaded transformers increase more than four-folds in the normal operation scenario. Furthermore, in the after-hacking scenario of this case, more than one-fourth transformers of the whole network get overloaded causing major problem for the whole network.

Table 5.13 *Number of Transformers Overloaded beyond 100 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	48	52	72
HP (Method 02)	48	27	37
EV (1.84 kW)	23	23	23
EV (11.1 kW)	48	226	2491

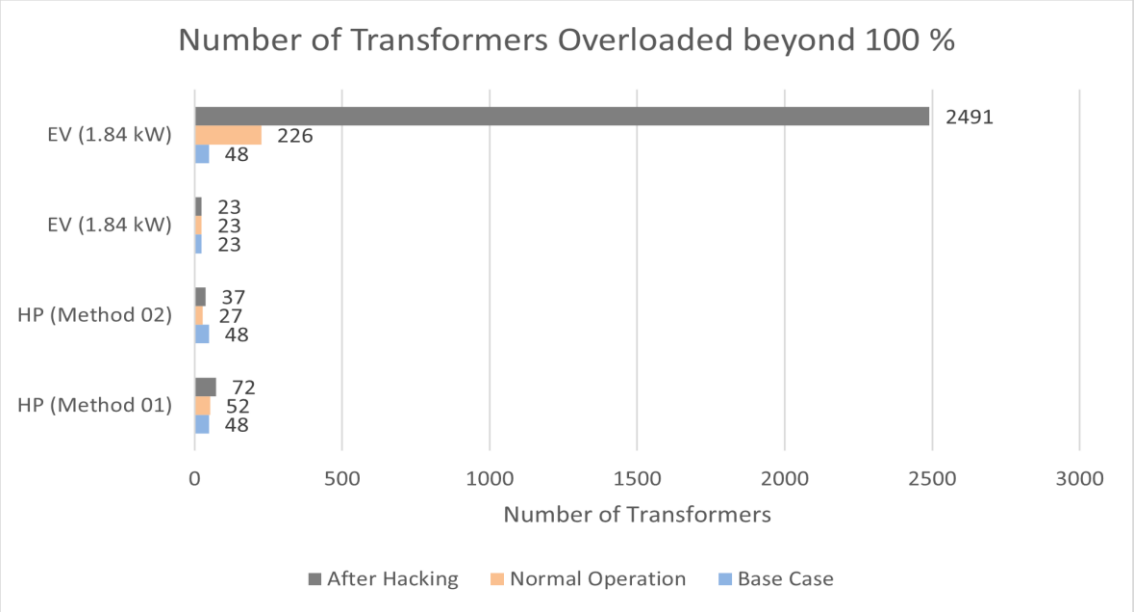


Figure 5.5 *Comparison of Number of Transformers Overloaded beyond 100 %*

To further going into detail, number of transformers overloaded beyond 130 % are calculated. As it can be seen from the table 5.14, more than one half of overloaded transformers are loaded beyond 130 % for 11.1 kW EV after hacking scenario.

Table 5.14 *Number of Transformers Overloaded beyond 130 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	9	10	10
HP (Method 02)	9	8	8
EV (1.84 kW)	3	3	3
EV (11.1 kW)	9	32	1460

b. Average Loading Level of Overloaded Transformers

In this section, average loading level of overloaded transformers is analysed from tables 5.15 and 5.16. Data for each case scenario should be observed separately while keeping sample size in mind.

Table 5.15 *Average Loading Level of Transformers Overloaded beyond 100 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	139.82 %	136.71 %	129.63 %
HP (Method 02)	139.82 %	161.65 %	147.36 %
EV (1.84 kW)	117.36 %	117.36 %	117.36 %
EV (11.1 kW)	139.82 %	119.34 %	151 %

Table 5.16 *Average Loading Level of Transformers Overloaded beyond 130 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	270.78 %	249.64 %	251.56 %
HP (Method 02)	270.78 %	281.73 %	284.44 %
EV (1.84 kW)	182.22 %	182.22 %	182.22 %
EV (11.1 kW)	270.78 %	179.07 %	177.52 %

5.3 Impacts on Conductors

Total number of conductors in the network is 244284 for all cases except 1.84 kW EV both operation scenarios as well as its base case. For that, number of conductors in the network are 227308. Moreover, those conductors which have loading level beyond 1000 % are not considered in calculation as they are assumed to be erroneous data.

5.3.1 Average Loading Level

In the table 5.17, average loading level of all conductors is presented for all operation scenarios of all cases. Most increase can be observed for 11.1 kW EV after hacking scenario where average loading level increases more than twice.

Table 5.17 *Average Loading Level Percentage of all Conductors*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	8.20 %	7.70 %	8.10 %
HP (Method 02)	8.20 %	5.60 %	6.34 %
EV (1.84 kW)	8.4828 %	8.4832 %	8.4838 %
EV (11.1 kW)	8.20 %	11.11 %	18.90 %

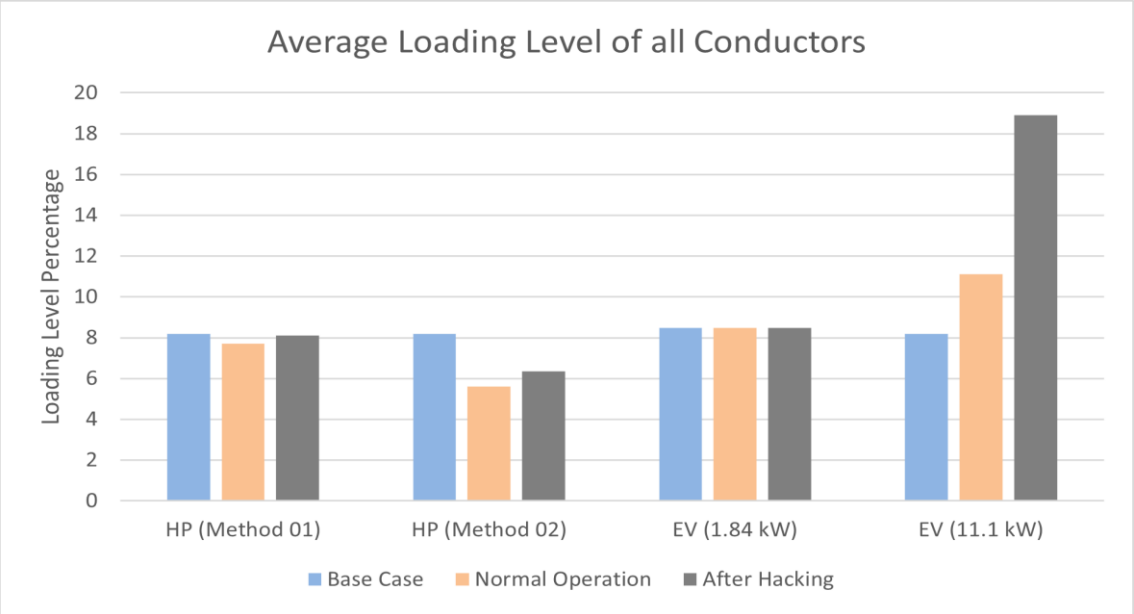


Figure 5.6 *Comparison of Average Loading Level of Conductors*

To further analyse the network, loading levels of MV and LV conductors are examined separately. There are 24016 MV and 220178 LV conductors in the network. However, for EV 1.84 kW both scenarios and its base case standard, 23185 MV and 204123 LV conductors analyzed as remaining data was missing. In the tables 5.18 and 5.19, loading level for MV and LV conductors can be analyzed separately. General trend is that MV conductors have lower loading level on average as compared to LV conductors throughout the network in all the cases.

Table 5.18 *Average Loading Level Percentage of MV Conductors*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	4.65 %	4.69 %	4.97 %
HP (Method 02)	4.65 %	3.58 %	4.03 %
EV (1.84 kW)	4.71 %	4.71 %	4.71 %
EV (11.1 kW)	4.65 %	5.50 %	10.15 %

Table 5.19 *Average Loading Level Percentage of LV Conductors*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	8.59 %	8.03 %	8.44 %
HP (Method 02)	8.59 %	5.82 %	6.59 %
EV (1.84 kW)	8.61 %	8.61 %	8.62 %
EV (11.1 kW)	8.59 %	11.72 %	19.86 %

5.3.2 Overloading

In this section, overloading analysis is conducted for all scenarios of all cases. Initially, number of overloaded conductors, and then average loading level of overloaded conductors is calculated. This provides with complete overview of scale as well as degree of overloading of conductors throughout the network.

a. Number of Overloaded Conductors

While analysing the number of overloaded conductors in the network from table 5.20, significant increase can only be observed in 11.1 kW EV case for both scenarios. For its normal operation, number of overloaded conductors almost double as compared to base case. For after hacking scenario, number of overloaded conductors increase more than 17 times. However, it still only accounts for 1.59 % of total number of conductors in the network. So, the effect of 11.1 kW EV after hacking scenario in terms of overloading scale is least on conductors as compared to service points and transformers.

Table 5.20 *Number of Conductors Overloaded beyond 100 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	226	172	179
HP (Method 02)	226	148	172
EV (1.84 kW)	205	205	205
EV (11.1 kW)	226	421	3905

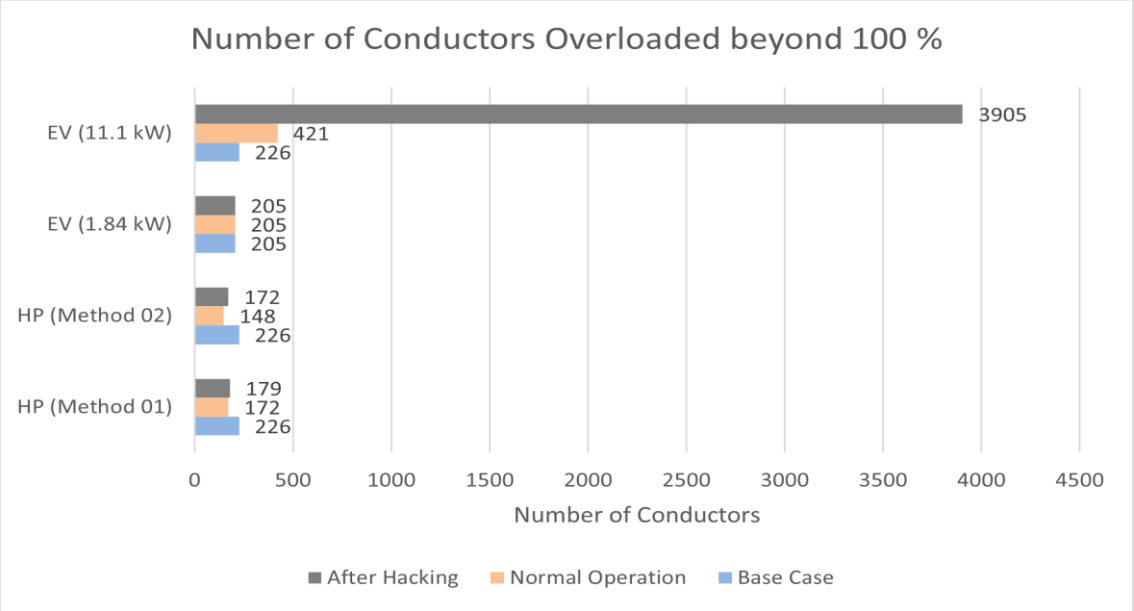


Figure 5.7 *Comparison of Number of Conductors Overloaded beyond 100 %*

Furthermore, tables 5.21 and 5.22 show that most of the conductors overloaded beyond 100 % belong to LV conductors for all cases.

Table 5.21 *Number of MV Conductors Overloaded beyond 100 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	19	19	19
HP (Method 02)	19	5	5
EV (1.84 kW)	19	19	19
EV (11.1 kW)	19	19	74

Table 5.22 *Number of LV Conductors Overloaded beyond 100 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	207	153	160
HP (Method 02)	207	143	167
EV (1.84 kW)	186	186	186
EV (11.1 kW)	207	402	3831

To further go into detail, number of conductors overloaded beyond 130 % are calculated for the whole network. As it can be seen from the table 5.23, more than one half of overloaded conductors are loaded beyond 130 % for 11.1 kW EV after hacking scenario.

Table 5.23 *Number of Conductors Overloaded beyond 130 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	128	116	119
HP (Method 02)	128	87	93
EV (1.84 kW)	117	117	117
EV (11.1 kW)	128	200	2057

In the tables 5.24 and 5.25, further categorization is done to analyse number of MV and LV conductors overloaded beyond 130 %.

Table 5.24 *Number of MV Conductors Overloaded beyond 130 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	18	18	18
HP (Method 02)	18	4	4
EV (1.84 kW)	18	18	18
EV (11.1 kW)	18	18	57

Table 5.25 *Number of LV Conductors Overloaded beyond 130 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	110	98	101
HP (Method 02)	110	83	89
EV (1.84 kW)	99	99	99
EV (11.1 kW)	110	182	2000

b. Average Loading Level of Overloaded Conductors

In this section, average loading level of overloaded conductors is analyzed from tables 5.26 and 5.27. It must be noted that data of each case scenario should be viewed separately while keeping sample size in mind. Furthermore, average loaded level of overloaded conductors is not analysed independently for MV and LV conductors.

Table 5.26 *Average Loading Level of Conductors Overloaded beyond 100 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	252.4 %	289.5 %	285.0 %
HP (Method 02)	252.4 %	255 %	242.3 %
EV (1.84 kW)	262.6 %	262.6 %	262.6 %
EV (11.1 kW)	252.4 %	199.2 %	177.1 %

Table 5.27 *Average Loading Level of Conductors Overloaded beyond 130 %*

Simulation Type	Base Case	Normal Operation	After Hacking
HP (Method 01)	360.4 %	374.5 %	371.5 %
HP (Method 02)	360.4 %	356 %	351.5 %
EV (1.84 kW)	376.3 %	376.3 %	376.3 %
EV (11.1 kW)	360.4 %	296.5 %	235.2 %

6. IMPACTS OF CYBERATTCACK ON INDIVIDUAL CUSTOMERS

Individual impacts of cyberattack on home automation system can be of quantitative as well as qualitative in nature. In terms of quantitative impacts, financial loss incurred to the customer is the main parameter. This monetary loss can occur due to multiple reasons ranging from theft to maximum load operation at most priced hours instead of least priced hours. In terms of qualitative analysis, main impact on customer is in terms of physical discomfort and mental distress which can be caused by range of multiple reasons including heating system shutdown, uncharged electric vehicle, malfunctioning of devices. This way, individual customers are also highly susceptible to cyberattack through their poorly secured home automation systems.

Cyberattack on home automation systems can be in various forms resulting in multiple possibilities of impacts on individuals. In the research [64], two main categories of cyberattacks are identified: non-targeted and targeted attacks on individual houses. Non-targeted attacks are usually broader and more random but their impact on individual customers is comparatively less damaging. Targeted cyberattacks on the other hand can be much more damaging to customer as they are usually based on some prior information. Moreover, targeted cyberattacks usually display higher degree of sophistication and complexity [64].

In the research done in [65], it is found out that there cyberattacks on home automation can further be characterized into two different categories: passive and active cyberattacks. In passive cyberattack, hackers gain access to communication and information channels of customer. However, in active cyberattack, direct control of home automation devices is accessed along with communication and information channels. In this assessment of impacts of cyberattacks on individual customers, it is assumed that these customers are being subjected to an active cyberattack. Hence, there can be wide range of impacts which can be categorized into different categories:

6.1 Threats to Safety, Security, Property, Privacy, and Data Security

A simple command by hackers to unlock doors may render residents of the house in acute physical danger. This may cause threat to life or physical injuries which is the most dangerous outcome for customer in case of cyberattack on home automation system. Such threat may exist if hackers target an individual beforehand with the intention of causation of harm, robbery or any other such reason. Hence, under any circumstances, hacking of home automation systems may prove to be detrimental for residents in the worse-case scenario.

Theft of physical property of house residents can also occur if home automated loads get hacked. This scenario can occur if main target of hackers is monetary profit. It is also important to note that hackers may target one specific house based on prior information with the intention of stealing. Furthermore, electricity theft is also possible by manipulation of smart meter data.

Threat to privacy is another major threat posed to residents because of hacked home automated loads. Malicious software can be installed not only on home automation devices but also on users' cell phones via automation control applications. This allows hackers to access data from both the home automation devices and the users' cell phones. Furthermore, energy consumption data of households can be accessed as well. This way, privacy of residents of automated house may seriously be breached. Hence, acute privacy threat exists especially for customers who have poorly secured and cheaply designed home automation software systems.

Apart from privacy threat, data of multiple sorts may be accessed by hackers. For instance, business related confidential files may be accessed through malicious or compromised software within the applications in use for home automation. Moreover, other types of data such as electricity consumption, EV charging habits, household appliance usage pattern may be accessed and sold to third parties by the hackers. Hence, data security threat also exists for users of home automation systems.

6.2 Discomfort

Discomfort is another effect which may be caused by hacking of home automation systems. Discomfort can be of multiple sorts and may range from major to minor in nature. However, discomfort is a subjective terminology, and its degree may vary from user to user. However, hacker actions which may usually cause discomfort are as follows:

1. Manifestation of any of aforementioned threats which includes threat to safety, security, property, privacy, and data. If any of these is compromised, at the very least, it would cause extreme discomfort to the user. Degree of discomfort would vary depending upon the extremity in nature of cyberattack and its consequences.
2. Hackers may shut down heating system of automated house during winters. Nordics have extreme cold weather during winters and if heating system stops working suddenly during such weather, it may cause extreme distress or even illness depending upon insulation of the house. Additionally, it may cause damage to household appliances. For instance, water pipes may burst due to frozen water.
3. Another method could be changing of thermostat settings. This may be done during any time of the year as it can cause discomfort to residents. Even during summer, thermostat setting shift from cooling to heating would cause distress. However, its discomfort effect may not be as extreme as during winter season.
4. Uncharged electric vehicle in the morning would cause discomfort to many users especially if their house is not close to public transport. Moreover, effects of such cyberattack would increase exponentially if it's an important day for the user such as an early morning meeting with a client or an important exam.
5. Hackers may trigger false warning alarm causing distress to residents. Another way might be blocking of alarm signal which would have even more dangerous consequences.
6. Malfunctioning of automated electricity consumption devices such as heating, refrigerator, television, and sauna may cause electricity bills to increase manifolds which would cause distress to users.
7. Malfunctioning of indoor lights as well as reduced ventilation for longer periods of time may cause headaches and severe distress to residents of the house.

7. DISCUSSION

7.1 Analysis

In primary part of this thesis, detailed analysis of frequency markets of Fingrid is done to recognize those risk hours which might be exploited by hacked home automated loads to cause power system instability and affect market functioning. It is vital to recognize past risk instances within frequency markets so that their rate of occurrence can be minimized in future. With minimization of occurrence of volume shortage and price volatile risk hours, chances of hacked home automated loads affecting National grid stability, and frequency market operation can also be minimized.

Let's discuss operation of different frequency markets of Fingrid through the lens of volume shortage-based analysis. Balancing Energy mFRR Up and downregulation markets, and FCR-N market has had lower occurrence rate of risk hours in comparison to other markets. Moreover, the occurrence rate of risk hours in FCR-D upregulation market has increased over time but for FFR market, this rate has decreased massively. Furthermore, Balancing Capacity markets and FCR-D Downregulation market analysis is only done for very small period of time due to which any conclusive statement can't be given for their trend or trajectory. However, volume shortage years do exist for these markets, and their operation should be improved as well.

In terms of price volatility in frequency markets of Fingrid, 2022 proved to have very high number of risk hours for Balancing Energy mFRR Up and Downregulation, FCR-D Up and Downregulation, and FCR-N markets. However, it must be kept in mind that 2022 was the year of energy crisis as well as high market price volatility throughout Europe. Moreover, for Balancing Capacity Up and Downregulation markets, analysis was only conducted for some months of 2023 in which price volatility existed, but its degree was not very serious as no high risk hours were identified. For FFR market, price based risk analysis was not conducted because of market operational differences.

In the secondary part of this thesis, comprehensive load modelling analysis of home automation systems, specifically heat pumps and electric vehicles, is conducted for residential buildings in the South Savo region of Finland. This analysis encompasses normal operational conditions as well as after hacking scenarios for both these loads. Main objective of this analysis is to evaluate the effects of these home automated loads

under different operational conditions on network infrastructure, including transformers, conductors, and service points.

Two different simulations are conducted for load modelling of heat pumps. In the first simulation, it is assumed that no residential buildings in the region are equipped with heat pumps initially. Alternatively, in the second simulation, it is assumed that certain space heating requirements of households are already being met by heat pumps, based on national statistics for Finland. Both simulations are carried out under two conditions: normal operation and after hacking scenario.

The results of both heat pump simulations indicate no significant adverse effects to the network. In fact, network health improves based on most of the key performance indicators. This improvement is likely attributable to the replacement of electric heating with heat pumps for customers belonging to electric heated load groups, thereby reducing their overall consumption However, some issues do arise for the network as well. For first simulation, two KPI's reveal negative impacts on the network: increase in the number of service points experiencing undervoltage and rise in the number of overloaded transformers. Specifically, the percentage of service points experiencing undervoltage below 95% rose by 1.8% during normal operation and by 22% in the after hacking scenario as compared to base case. Additionally, the number of transformers operating beyond 100% capacity increased from 48 in base case to 52 under normal operation, and further to 72 under the after hacking scenario.

For EV simulations, two different load models are made. In the first load model it is assumed that all households in the network have an EV home charging station with 1.84 kW charging power. In the second simulation, maximum EV charging power assigned to each household is 11.1 kW.

In the first load model of EV charging at 1.84 kW, no significant effect on any network element can be observed either in normal operation or in after hacking scneario. This shows that 1.84 kW charging power is too small to cause major problems for the network. It also shows that the after hacking strategy chosen for this level of charging power might not have been the ideal choice as this amount of EV load cannot formulate separate peak load on its own.

In the second load model of electric vehicle (EV) charging at 11.1 kW, significant adverse effects are evident across all network elements. Under normal operation, in comparison to base case, the number of service points overloaded beyond 100% increases more than twofold. Additionally, the number of service points experiencing undervoltage below 95% nearly doubles as well. Furthermore, the number of overloaded trans-

formers also increases more than fourfold, and the number of overloaded conductors nearly double as well. However, extremely serious situation arises for after hacking scenario where almost 20% of all service points become overloaded beyond 100%, and more than 66% of all service points experience undervoltage below 95%. Furthermore, more than one-fourth of the transformers in the entire network become overloaded beyond 100 %. The number of overloaded conductors increases more than seventeen times compared to the base case, although this accounts for only 1.59% of the total number of conductors in the network. Hence, after hacking scenario of EV simulation at 11.1 kW proves to be most detrimental to the network.

For future direction in terms of heat pump and EV simulations, one option can be is the assumption that hackers have access to both these loads simultaneously. Simulation methodology of this thesis can be utilized for combination of these load types. Moreover, different after hacking strategies can be formulated with different combination schemes of EV and heat pump loads. Then, the local grid service points, transformers and conductors can be tested under normal operation as well these after hacking schemes.

7.2 Limitations

This section highlights main limitations of this thesis and offers directions for further research on this topic. The primary limitations of this thesis are as follows:

- Data availability from frequency markets of Fingrid proved to be one of the main limitations in terms of volume shortage and price based risk analysis. Main reason for this data limitation is security of market operation. Moreover, some frequency markets are relatively new for which detailed trends could not be identified.
- It could not be determined as to how much amount of home automated load would create how much impact on National Grid stability and frequency market operation. It is a very broad field of research which also requires additional data from Fingrid. It can also be a gateway for further research in this topic.
- General assumptions were made for most of the input parameters of heat pump especially for annual space heating requirements. In ideal circumstances, more customer specific data would have been utilized. However, that could not be done due to lack of data as well as enormity of number of service points within the whole network.

- Initial design of EV simulations assigned unique distance, start time of charging, and load curve to each customer. However, it had to be simplified to much simpler and generic version where average values had to be utilized for EV consumption. This has to be done because of the limitations of the available software tool.
- Data storage and analysis techniques by grid companies is outdated. All measurements of network elements and customer loads should be stored for all hours of the year. This would pave way for better analysis as well as monitoring of the grid health.
- Due to time shortage, detailed quantification analysis of impacts of cyberattack on individual customers could not be done.

8. CONCLUSION

This thesis identifies the profound implications of potential cyberattacks through home automation systems on stability of national grid, functioning of frequency markets, operation of LV and MV networks, and wellbeing of household residents. In primary section of this thesis, frequency markets of Fingrid are chosen for analysis of volume shortage and price volatile risk hours during which power system stability and frequency market functioning might be affected by large amount of hacked home automated loads. This vulnerability analysis is aimed to identify deficiencies within reserve markets, with the objective of improving reserve volume procurement and ensuring stable prices to prevent any future exploitation.

In the secondary part of the thesis, simulations of selected home automation loads are conducted under normal and after hacking scenarios to assess their impact on the local grid in the South Savo region of Finland. This analysis is crucial for local grid management authorities to understand how different scenarios involving home automation loads might affect various parts of the network. It enables local grid managers to anticipate, prepare for, and mitigate any potential impacts on the grid. Additionally, this thesis includes a qualitative analysis of the impacts of cyberattacks through home automation systems on household residents. This analysis aims to raise awareness about the possible implications of such cyberattacks on individuals, emphasizing the need for enhanced cybersecurity measures.

In essence, it is determined that vulnerable instances in terms of volume shortage as well as price volatility do exist across all frequency markets in Finland. Higher amount of these vulnerable instances represents a greater number of opportunities for hackers to exploit. However, the degree of volume shortage and price volatility represent the level of impact that can be caused through cyberattack. Furthermore, existence of large-scale fault or major frequency dip during vulnerable instance would further exacerbate the situation in these risk hours. However, such fault existence is not necessary to create adverse effects on all frequency markets. Moreover, customer loads which are designated part of demand response for any market can prove to be more dangerous if they get hacked as they can be utilized for load manipulation as well as demand response blockage. Furthermore, if large amount of home automated loads gets hacked, and high risk hours get coupled with major frequency dip in the system, then effects such as extreme price volatility, outage, or even blackout may happen. However, exact outcome depends on multitude of factors which need to be studied individual-

ly depending upon all the factors. It is also gateway for further research to formulate case scenarios with predetermined factors to simulate outage or blackout situation to test system limits. In terms of impacts of cyberattack through home automation system on local grid, it was found that low powered EV charging (1.84 kW) and heat pump loads do not cause major problems for the network. However, EV charging (11.1 kW) especially in the after hacking scenario would create extremely dangerous situation for the whole network as it would cause overloading of service points and transformers on major scale. In fact, for after hacking scenario of this case, more than one-fourth of network's total service points as well as transformers get overloaded beyond 100 %. Moreover, more than 65 % of all service points experience undervoltage beyond 95 %. On top of that, number of conductors overloaded beyond 100 % also increase more than twice in comparison to base case. In specific case of this network, major grid reinforcement needs are required in the EV (11.1 kW) after-hacking scenario especially for transformers and service points. Moreover, this thesis discusses how cyberattacks on home automation systems can pose serious threats to the safety, security, property, privacy, and data security of residents, as well as cause various cases of significant discomfort for them.

To conclude, this thesis underscores the need for more proactive approach by National grid authorities to enhance security, efficiency, and reliability of power systems. It also emphasizes the importance of improving frequency market operations to ensure stable and secure volume procurement. Moreover, it calls for local grid authorities to improve the resilience of electricity networks. Furthermore, it advocates for measures to ensure well-being of individuals in automated homes. It also urges policymakers to implement stricter standards for home automation companies. In essence, collective and comprehensive efforts from all stakeholders are essential for mitigating the multifaceted cybersecurity risks associated with home automation systems.

REFERENCES

[1] Manshreck, Titus. Software Engineering at Google: Lessons Learned from Programming over Time. Oreilly & Associates Inc, 2020, abseil.io/resources/swe-book/html/ch21.html.

[2] Georgescu, Elena. “Software Rot and Cybersecurity.” Heimdal Security Blog, Oct. 2020, heimdalsecurity.com/blog/software-rot/.

[3] L. Jiang, D-Y. Liu and B. Yang, "Smart home research", IEEE Proceedings of the Third International Conference on Machine Learning and Cybernetics, pp. 659-663, 26–29 August 2004.

[4] Z. Wei, S. Qin, D. Jia and Y. Yang, "Research and design of cloud architecture for smart home", 2010 IEEE International Conference on Software Engineering and Service Sciences (ICSESS), pp. 86-89, July 2010.

[5] Fensel, Anna, Vikash Kumar, and Slobodanka Dana Kathrin Tomic. "End-user interfaces for energy-efficient semantically enabled smart homes." Energy Efficiency 7 (2014): 655-675.

[6] Next-Gen Living: The Future of Smart Homes Powered by AI and Automation. Grand View Research, Inc, 2023, www.linkedin.com/pulse/next-gen-living-future-smart-homes-powered-ai-automation/.

[7] Global: Smart Home Number of Users 2019-2028. Statista Research Development, 2023, www.statista.com/forecasts/887613/.

[8] Smart Home - Finland. Statista, 2023, www.statista.com/outlook/dmo/smart-home/finland.

[9] Mihai Tomescu (EEA), Victor Juarez (Ramboll), Søren Møller Thomsen (Ramboll), Ils Moorkens (ETC-CM, VITO), Marco Ortiz Sanchez (ETC-CM, VITO. Flexibility Solutions to Support a Decarbonised and Secure EU Electricity System. European Environment Agency, 2023.

[10] Kirkham, Tom, et al. “Risk Driven Smart Home Resource Management Using Cloud Services.” Future Generation Computer Systems, vol. 38, Sept. 2014, pp. 13–22, https://doi.org/10.1016/j.future.2013.08.006.

[11] Rambus, “Smart Home: Threats and Countermeasures - Rambus.” [Online]. Available: https://www.rambus.com/iot/smart-home/. [Accessed: 23- Aug-2019].

[12] Hammi, Badis & Zeadally, Sherali & Khatoun, Rida & Jamel, Nebhen. (2022). Survey on Smart Homes: Vulnerabilities, Risks, and Countermeasures. Computers & Security. 117.102677. 10.1016/j.cose.2022.102677.

[13] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh, “Security vulnerabilities in bluetooth technology as used in IoT,” J. Sens. Actuator Networks, vol. 7, no. 3, pp. 1–26, 2018.

[14] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, “Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms,” pp. 83–92, 2016.

[15] A. Jacobsson, M. Boldt, and B. Carlsson, “A risk analysis of a smart home automation system,” Futur. Gener. Comput. Syst., vol. 56, pp. 719–733, 2016.

[16] Ahmed, A.A. and Ahmed, W.A. An Effective Multifactor Authentication Mechanism Based on Combiners of Hash Function over Internet of Things. Sensors, 19(17), 2019, p.3663.

[17] Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2015.09.003

[18] Law of demand. Oxford Reference. (2009.). https://www.oxfordreference.com/display/10.1093/acref/9780199237043.001.0001/acref-9780199237043-e-3739.

[19] Denning, Tamara, et al. “Computer Security and the Modern Home.” Communications of the ACM, vol. 56, no. 1, 2013, pp. 94–103.

[20] Adrian Dabrowski, Johanna Ullrich, and Edgar R. Weippl. 2017. Grid Shock: Coordinated Load-Changing Attacks on Power Grids: The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well. In 2017 Annual Computer Security Applications Conference. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3134600.3134639.

[21] Amini, Sajjad, et al. Dynamic Load Altering Attacks against Power System Stability: Attack Models and Protection Schemes. July 2018.

[22] Simpson, Robert. Assessment of the Impact of Cyberattacks on Power System Stability - Manipulation of Controllable Loads in Smart Homes. 2021.

[23] Modig, N., Eriksson, R., Ruokolainen, P., Ødegård, J., Weizenegger, S. and Fechtenburg, T. (2022). Overview of Frequency Control in the Nordic Power System. [online] Available at: https://www.epressi.com/media/userfiles/107305/1648196866/overview-of-frequency-control-in-the-nordic-power-system.pdf.

[24] TSO Report on Balancing in Accordance with Article 60 of Commission Regulation (EU) 2017/2195 of 23 November 2017 Establishing a Guideline on Electricity Balancing. FINGRID, Feb. 2022, www.fingrid.fi/globalassets/dokumentit/fi/sahkomarkkinat/reservit/ebgl60-tso-report-on-balancing-2022.pdf.

[25] “Frequency Containment Reserves (FCR Products).” Fingrid, www.fingrid.fi/en/electricity-market/reserves_and_balancing/frequency-containment-reserves/#procurement.

[26] “Balancing Energy and Balancing Capacity Markets (MFRR).” Fingrid, Feb. 2018, www.fingrid.fi/en/electricity-market/reserves_and_balancing/balancing-energy-and-balancing-capacity-markets/.

[27] “Automatic Frequency Restoration Reserve (AFRR).” Fingrid, Feb. 2018, www.fingrid.fi/en/electricity-market/reserves_and_balancing/automatic-frequency-restoration-reserve/.

[28] “Fast Frequency Reserve (FFR).” Fingrid, Feb. 2020, www.fingrid.fi/en/electricity-market/reserves_and_balancing/fast-frequency-reserve/#technical-requirements.

[29] Electricity Market Needs Fixing - What Can We Do? FINGRID, 2016, www.fingrid.fi/globalassets/dokumentit/en/electricity-market/development-projects/fingrid-electricity-market-needs-fixing-2016-web.pdf.

[30] “Datasets.” Data.fingrid.fi, FINGRID, data.fingrid.fi/en/data?datasets=290&datasets=286&datasets=289.

[31] 2022 NORDIC and BALTIC GRID DISTURBANCE STATISTICS. Ensto-e, Oct. 2023.

[32] Thesis Attachment Documents-Fingrid Frequency Market Analysis-All Graphs.

[33] “Demand Response” Fingrid, www.fingrid.fi/sahkomarkkinat/markkinoiden-yhtenaisyys/sahkomarkkinoiden-kehityshankkeet/kysyntajousto/#kulutusjouston-projektit.

[34] “Almost 200,000 Heat Pumps Were Sold Last Year. An Increase of 50%.” SULPU, 16 Jan. 2023, www.sulpu.fi/almost-200000-heat-pumps-were-sold-last-year-an-increase-of-50/.

[35] “For a Livable Climate: Net-Zero Commitments Must Be Backed by Credible Action.” United Nations, www.un.org/en/climatechange/net-zero-coalition.

[36] Emissions Gap Report . United Nations Environment Programme (UNEP), 2022, www.unep.org/resources/emissions-gap-report-2022.

[37] “Location Southern Savonia Region on Map Finland. 3d Location Sign Similar to the Flag of South Savo Stock Vector - Illustration of Borders, Border: 204928461.” Dreamstime, www.dreamstime.com/print-location-southern-savonia-region-map-finland-d-sign-similar-to-flag-south-savo-quality-regions-your-image204928461.

[38] Rejlers Finland, www.rejlers.fi/.

[39] *Tietoevry,* www.tietoevry.com/.

[40] *Suur-Savon Sähkö,* www.sssoy.fi/.

[41] U.S. Department of Energy. Heat Pump Systems. 2023, www.energy.gov/energysaver/heat-pump-systems.

[42] Myydyt Lämpöpumput Vuosittain, Kappaletta (Heat Pumps Annual Units Sold). SULPU, 2021, www.sulpu.fi/wp-content/uploads/2022/01/SULPU-lampopumpputilasto-2021-kuvaajat.pdf.

[43] “Weather and Sea-Observations in Finland.” Finnish Meteorological Institute, en.ilmatieteenlaitos.fi/download-observations.

[44] “Services and Products-Heating Degree Days” Finnish Meteorological Institute, en.ilmatieteenlaitos.fi/heating-degree-days.

[45] Indoor Air Quality and Ventilation at Home. The Organization for Respiratory Health in Finland, 2021, www.hengitysliitto.fi/wp-content/uploads/2021/10/IlmanvaihtoOpas_2021_englanti_saavuttettava.pdf.

[46] Indoor Climate and Ventilation for Buildings-Regulations and Guidelines. Ministry of the Environment, Department of Built Environment, 2012, www.puntofocal.gov.ar/notific_otros_miembros/fin41_t.pdf.

[47] Laitinen A, Tuominen P, Holopainen R, Tuomaala P, Jokisalo J, Eskola L, Sirén K. Renewable energy production of Finnish heat pumps. VTT. https://publications.vtt.fi/pdf/technology/2014/T164.pdf.

[48] Stignor, Caroline, and Tommy Walfridson. Nordsyn Study on Air-To-Air Heat Pumps in Humid Nordic Climate. Nordic Council of Ministers, 2019, norden.diva-portal.org/smash/get/diva2:1313699/FULLTEXT01.pdf.

[49] SFS-EN 14511-2. sales.sfs.fi/fi/index/tuotteet/SFS/CEN/ID6/1/236688.html.stx.

[50] Degree-Days - U.S. Energy Information Administration (EIA). 2023, www.eia.gov/energyexplained/units-and-calculators/degree-days.php.

[51] In Finland Another Peak Year for Heat Pumps. More than 100,000 Pumps Were Sold. SULPU, 2021, www.sulpu.fi/wp-content/uploads/2021/05/Pressrelease-in-English-SULPU-1.20212.pdf.

[52] Rouhiainen, Virve. Energy Consumption in Households. Statistics Finland, 2021, stat.fi/til/asen/2020/asen_2020_2021-12-16_tie_001_en.html.

[53] Electric Resistance Heating. US Department of Energy, www.energy.gov/energysaver/electric-resistance-heating.

[54] SPF of Heat Pumps, www.wolf.eu/en-de/advisor/spf-heat-pumps.

[55] Thesis Attachment Documents-Heat Pump Figures.

[56] O. Lehtinen, S. Pitkäniemi, A. Weckman, M. Aikio, M. Mabano and M. Lehtonen, "Electric Vehicle Charging Loads in Residential Areas of Apartment Houses," 2020 21st International Scientific Conference on Electric Power Engineering (EPE), Prague, Czech Republic, 2020, pp. 1-6, doi: 10.1109/EPE51172.2020.9269191.

[57] M. Kurfirt and J. Hlavnicka, "E-mobility impact on supply in distribution grid", 2019 20th International Scientific Conference on Electric Power Engineering (EPE), May 2019.

[58] F. Yi, P. Zeng, S. Yu, C. Gu, J. Li, C. Yuan, et al., "Impacts of classified electric vehicle charging derived from driving patterns to the lv distribution network", 2014 IEEE PES General Meeting - Conference Exposition, pp. 1-5, July 2014.

[59] F. Rassaei, W. Soh and K. Chua, "A statistical modelling and analysis of residential electric vehicles' charging demand in smart grids", 2015 IEEE Power

Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1-5, Feb 2015.

[60] D. Fischer, A. Harbrecht, A. Surmann and R. McKenna, "Electric vehicles' impacts on residential electric local profiles-a stochastic modelling approach considering socio-economic behavioural and spatial factors", Applied Energy, vol. 233, pp. 644-658, 2019.

[61] T. Lee, Z. Bareket, T. Gordon and Z. S. Filipi, "Stochastic modeling for studies of real-world phev usage: Driving schedule and daily temporal distributions", IEEE Transactions on Vehicular Technology, vol. 61, no. 4, pp. 1493-1502, May 2012.

[62] A. Lajunen, "Evaluation of energy consumption and carbon dioxide emissions for electric vehicles in nordic climate conditions", 2018 Thirteenth International Conference on Ecological Vehicles and Renewable Energies (EVER), pp. 1-7, April 2018.

[63] *ENTSO-E Transparency Platform*. 2024, transparency.entsoe.eu/.

[64] I. G. Seissa, J. Ibrahim, and N. Yahaya, “Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review,” Int. J. Sci. Res., vol. 6, no. 1, pp. 180–186, 2017.

[65] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, “Security and privacy issues for an IoT based smart home,” 2017 40th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2017 - Proc., pp. 1292–1297, 2017.

APPENDIX A: SIMULATION PROGRAMS

Program 1: The following simulation program is for price based risk analysis of FCR-D Up & Downregulation, Balancing Capacity mFRR Up & Downregulation, FCR-N, FFR, and Balancing Energy mFRR Upregulation Market.

```
xData = Risk;                %Risk is Volume Shortage Index
yData = Price;               %Price is the hourly price of market
meanPrice = x;               %x is mean market price
markerSize = 50;             %Setting up marker size for plot

% Scatter plot for all data
scatter(xData, yData, markerSize, 'filled', 'MarkerFaceColor', 'blue', 'MarkerEdgeColor',
'black');
hold on

% Setting up limits for low, medium, and high risk hours
limit1 = 5 * meanPrice;
limit2 = 10 * meanPrice;
limit3 = 20 * meanPrice;

% Finding maximum y-axis data point
maxY = max(yData);

% Identifying data points that fall within different risk categories
areaIndicesTop2 = find(yData > limit1 & yData <= limit2);
yDataTop2 = yData(areaIndicesTop2);

areaIndicesTop1 = find(yData > limit2 & yData <=limit3);
yDataTop1 = yData(areaIndicesTop1);

areaIndicesTop = find(yData > limit3);
yDataTop = yData(areaIndicesTop);
```

```
% Scatter plot for different risk levels
scatter(xData(areaIndicesTop2), yDataTop2, markerSize, 'filled', 'MarkerFaceColor', [1, 0.8, 0.4], 'MarkerEdgeColor', 'black');

scatter(xData(areaIndicesTop1), yDataTop1, markerSize, 'filled', 'MarkerFaceColor', [1, 0.5, 0], 'MarkerEdgeColor', 'black');

scatter(xData(areaIndicesTop), yDataTop, markerSize, 'filled', 'MarkerFaceColor', 'red', 'MarkerEdgeColor', 'black');

% Adding labels and legend to the plot
grid on;
xlabel('Risk');
ylabel('Price');
legend('No Risk', 'Low Risk', 'Medium Risk', 'High Risk');
```

Program 2: The following simulation program is for volume shortage based risk analysis of FCR-D Up & Downregulation, Balancing Capacity mFRR Up & Downregulation, FCR-N, FFR, and Balancing Energy mFRR Upregulation Market.

```
xData = Risk;                % Risk is Volume Shortage Index
yData = Price;               % Price is the hourly price of market
limit = x;                   % x is two times mean market price
markerSize = 50;             % Setting up marker size for plot

% Scatter plot for all data
scatter(xData, yData, markerSize, 'filled', 'MarkerFaceColor', 'blue', 'MarkerEdgeColor', 'black');
hold on

% Identifying and plotting low risk hours
indices_low_risk = Risk >= 0.80 & Risk < 0.90 & Price > limit;
scatter(Risk(indices_low_risk), Price(indices_low_risk), markerSize, 'Marker', 'o', 'MarkerFaceColor', [1 0.8 0.4], 'MarkerEdgeColor', 'k');
low=yData(indices_low_risk);
hold on;
```

```
% Identifying and plotting medium risk hours
indices_medium_risk = Risk >= 0.90 & Risk < 0.95 & Price > limit;
scatter(Risk(indices_medium_risk), Price(indices_medium_risk), markerSize, 'Marker',
'o', 'MarkerFaceColor', [1 0.5 0], 'MarkerEdgeColor', 'k');
medium = yData(indices_medium_risk);

% Identifying and plotting high risk hours
indices_high_risk = Risk >= 0.95 & Price > limit;
scatter(Risk(indices_high_risk), Price(indices_high_risk), markerSize, 'Marker', 'o',
'MarkerFaceColor', [1 0 0], 'MarkerEdgeColor', 'k');
high = yData(indices_high_risk);

% Adding labels and legend to the plot
xlabel('Volume Shortage Index');
ylabel('Price');
legend('No Risk', 'Low Risk', 'Medium Risk', 'High Risk');
grid on;
```

Program 3: The following simulation program is for price based risk analysis of Balancing Energy mFRR Downregulation market.

```
xData = Risk;                % Risk is Volume Shortage Index
yData = Price;               % Price is the hourly price of market
markerSize = 50;             % Setting up marker size for plot

% Scatter plot for all data
scatter(xData, yData, markerSize, 'filled', 'MarkerFaceColor', 'blue', 'MarkerEdgeColor',
'black');
hold on

% Setting up limits for low, medium, and high risk hours based on market statistics
limit1 = 226.45;
limit2 = 410.53;
limit3 = 778.69;
limit4 = -141.71;
limit5 = -326.16;
```

```
limit6 = -693.95;

% Finding maximum y-axis data point
maxY = max(yData);

% Identifying data points that fall within different risk categories
areaIndicesTop2 = find(yData > limit1 & yData <= limit2 | yData < limit4 & yData >= lim-
it5);
yDataTop2 = yData(areaIndicesTop2);

areaIndicesTop1 = find(yData > limit2 & yData <=limit3 | yData < limit5 & yData >= lim-
it6);
yDataTop1 = yData(areaIndicesTop1);

areaIndicesTop = find(yData > limit3 | yData < limit6);
yDataTop = yData(areaIndicesTop);

% Scatter plot for different risk levels with distinct colors
scatter(xData(areaIndicesTop2), yDataTop2, markerSize, 'filled', 'MarkerFaceColor', [1,
0.8, 0.4], 'MarkerEdgeColor', 'black');

scatter(xData(areaIndicesTop1), yDataTop1, markerSize, 'filled', 'MarkerFaceColor', [1,
0.5, 0], 'MarkerEdgeColor', 'black');

scatter(xData(areaIndicesTop), yDataTop, markerSize, 'filled', 'MarkerFaceColor', 'red',
'MarkerEdgeColor', 'black');

% Adding labels and legend to the plot
grid on;
xlabel('Risk');
ylabel('Price');
legend('No Risk', 'Low Risk', 'Medium Risk', 'High Risk');
```

Program 4: The following simulation program is for volume shortage based risk analysis of Balancing Energy mFRR Downregulation market.

```
xData = Risk;                    % Risk is Volume Shortage Index
```

```
yData = Price;                % Price is the hourly price of market
markerSize = 50;              % Setting up marker size for plot

% Scatter plot for all data
scatter(xData, yData, markerSize, 'filled', 'MarkerFaceColor', 'blue', 'MarkerEdgeColor',
'black');
hold on

% Identifying and plotting low risk hours
indices_low_risk = Risk >= 0.80 & Risk < 0.90;
scatter(Risk(indices_low_risk), Price(indices_low_risk), markerSize, 'Marker', 'o',
'MarkerFaceColor', [1 0.8 0.4], 'MarkerEdgeColor', 'k');
low=yData(indices_low_risk);
hold on;

% Identifying and plotting medium risk hours
indices_medium_risk = Risk >= 0.90 & Risk < 0.95;
scatter(Risk(indices_medium_risk), Price(indices_medium_risk), markerSize, 'Marker',
'o', 'MarkerFaceColor', [1 0.5 0], 'MarkerEdgeColor', 'k');
medium = yData(indices_medium_risk);

% Identifying and plotting high risk hours
indices_high_risk = Risk >= 0.95;
scatter(Risk(indices_high_risk), Price(indices_high_risk), markerSize, 'Marker', 'o',
'MarkerFaceColor', [1 0 0], 'MarkerEdgeColor', 'k');
high = yData(indices_high_risk);

% Adding labels and legend to the plot
xlabel('Volume Shortage Index');
ylabel('Price');
legend('No Risk', 'Low Risk', 'Medium Risk', 'High Risk');
grid on;
```

Program 5: The following simulation program is for load modelling of heat pumps for customers of all load groups except load group 18.

```
% Calculating resultantMatrix based on TotalAnnualEnergyMWh and Load Profiles
resultantMatrix = zeros(numel(NISlaskennankuormituskyrt.KuormaWh), size(LG, 1));
for i = 1:size(LG, 1)
    resultantMatrix(:, i) = (LG.TotalAnnualEnergyMWh(i) .*
    NISlaskennankuormituskyrt.KuormaWh) / 10000;
end

THdd = 17;              % Setting up HDD temperature (THdd) to 17°C
Ttimestep = 1;          % Setting up time step (Ttimestep) to 1 hour

% Initializing a variable to store the hourly heating degree hours (Hdd)
Hdd = zeros(size(AirTemperaturedegC));

% Calculating Hdd for each hour based on hourly outdoor temperature
for t = 1:length(AirTemperaturedegC)
    Hdd(t) = max(0, THdd - AirTemperaturedegC(t));
end
SumHdd = sum(Hdd) * Ttimestep;

% Setting the fixed value for Thsy in Kelvin
Thsy = 308.5;

% Calculating COP for each hour
COP = zeros(size(AirTemperatureK));
for t = 1:length(AirTemperatureK)
    COP(t) = Thsy / (Thsy - AirTemperatureK(t));
end
f = 3.5/11.01;
COP_Final= COP*f;

% Assigning hourly COP values to all customers of the load group
numColumns = 4613;      % Number of customers
COP_Final_expanded = repmat(COP_Final, 1, numColumns);
COP_e = repmat(COP, 1, numColumns);
COP_Final_expanded = COP_Final_expanded(2:end, :);
COP_Final_expanded1 = COP_Final_expanded(1:end-25, :);
SHdd = SumHdd;
```

```
% k is the percentage of heat pump consumption of customer dependent upon method
and load gouup.
Qheating_spaces_data = (LG1.TotalAnnualEnergyMWh) .* (k); % Extract the data

% Calculating Ispaces (Space heating demand for each customer)
Ispaces = zeros(length(AirTemperaturedegC), length(Qheating_spaces_data));
for q = 1:length(Qheating_spaces_data)
    for t = 1:length(AirTemperaturedegC)
        if THdd > AirTemperaturedegC(t)
            Ispaces(t, q) = ((Qheating_spaces_data(q) * (THdd - AirTempera-
turedegC(t))) /
            SHdd);
        else
            Ispaces(t, q) = 0;
         end
    end
end
Ispaces = Ispaces(2:end, :);
Ispaces_trimmed = Ispaces(1:end-25, :);
AirTemperaturedegC= AirTemperaturedegC(2:end, :);
AirTemperaturedegC1= AirTemperaturedegC(1:end-25, :);

% Assigning electricity consumption demand for space heating of all customers
e_spaces = Ispaces_trimmed ./ COP_Final_expanded1;

% Assigning the size of smallest sized single heat pump
Ihp_spaces_max = (0.25 .* COP_Final_expanded1) / 3.5;

% Assigning electricity consumption of smallest sized single heat pump
e_maximum = Ihp_spaces_max ./ COP_Final_expanded1;

%Calculating size and hourly output of heat pump assigned to each customer
x = 0.07142;
checktable = e_spaces;
max_checktable = max(checktable);
for row = 1:size(Ihp_spaces_max, 1)
```

```
    for colu = 1:size(mean_checktable, 2)
        currentValue = max_checktable(1, colu);
        numConditions = 3500;
        multipliers = 1:numConditions;
        maxnumConditions = 3500;
        conditionBoundaries = (1:numConditions) * x;
        for condition = 1:numConditions
            if currentValue > conditionBoundaries(condition) && currentValue <
                conditionBoundaries(condition + 1)
                Ihp_spaces_max1(row, colu) = Ihp_spaces_max(row, colu) *
                multipliers(condition + 1);
                break;
            elseif currentValue > maxnumConditions * x
                Ihp_spaces_max1(row, colu) = Ihp_spaces_max(row, colu) * maxnumCon-
ditions;
            else
                Ihp_spaces_max1(row, colu) = Ihp_spaces_max(row, colu);
            end
        end
    end
end
I_hp = zeros(size(Ihp_spaces_max1));
for col = 1:size(Ihp_spaces_max1, 2)
    for t = 1:size(Ihp_spaces_max1, 1)
        if Ispaces_trimmed(t, col) > Ihp_spaces_max1(t, col)
            I_hp(t, col) = Ihp_spaces_max1(t, col);
        else
            I_hp(t, col) = Ispaces_trimmed(t, col);
        end
    end
end

%Calculating maximum size, hourly electricity consumption, and hacking capacity of
each heat pump
e = I_hp ./ COP_Final_expanded1;
e_max1 = Ihp_spaces_max1 ./ COP_Final_expanded1;
e_hacking = e_max1 - e;
```

```
%Modifying customer load in normal as well as after hacking operation
modified = resultantMatrix_other + e;
final = modified + e_hacking + e_hacking_original;
```

Program 6: The following simulation program is for load modelling of heat pumps for customers of load group 18.

```
% Assigning heat pump size based on average annual consumption of load group 18
maxConsumption = 0.5714;

% Initializing an array to store daily consumption
consumptionPattern = zeros(size(Number, 1), 1);

% Loop through each day
for col = 1:size(Number, 1)
    day = Day(col, 1);        % Extract the day for the current row
    season = Season(col, 1);  % Extract the month for the current row
    holiday = Holiday{col};   % Extract the Holiday status for the current day
    month = Month(col, 1);

    % Checking if it's a "Summer" month
    if ismember(season, 'Summer')
        if ~isempty(holiday) && strcmp(holiday, 'Yes')
            consumptionPattern(col) = 0.5 * maxConsumption;
        elseif ismember(day, {'Sa', 'Su'})
            consumptionPattern(col) = 0.3 * maxConsumption;
        else
            consumptionPattern(col) = 0.10 * maxConsumption;
        end

    % Checking if it's a "Winter" month
    elseif ismember(season, 'Winter')
        if ~isempty(holiday) && strcmp(holiday, 'Yes')
            consumptionPattern(col) = 0.95 * maxConsumption;
        elseif ismember(day, {'Sa', 'Su'})
```

```
            consumptionPattern(col) = 0.80 * maxConsumption;
        else
            consumptionPattern(col) = 0.30 * maxConsumption;
        end
    % Checking if it's April or October
    elseif ismember(month, {'April', 'October'})
        if ~isempty(holiday) && strcmp(holiday, 'Yes')
            consumptionPattern(col) = 0.725 * maxConsumption;
        elseif ismember(day, {'Sa', 'Su'})
            consumptionPattern(col) = 0.55 * maxConsumption;
        else
            consumptionPattern(col) = 0.20 * maxConsumption;
        end
    end
end

% Adding the consumption pattern to the table
calendarTable.Consumption = consumptionPattern;
originalPattern = consumptionPattern;

% Creating a new array to store the hourly pattern (8760x1 table)
hourlyPattern = zeros(8760, 1);

% Counter for the hourly pattern
hourlyCounter = 1;

% Loop through each day in the original pattern
for day = 1:365
    for hour = 1:24
        hourlyPattern(hourlyCounter) = originalPattern(day);
        hourlyCounter = hourlyCounter + 1;
    end
end

% Number of times to repeat each column
numRepeats = 1375;
```

```
% Getting the number of rows in the original array
numRows = size(hourlyPattern, 1);

% Formulating hourly consumption pattern of heat pump for each customer
hourlyPattern1 = repmat(hourlyPattern, 1, numRepeats);

% Calculating resultantMatrix based on TotalAnnualEnergyMWh and Load Profiles
resultantMatrix = zeros(numel(NISlaskennankuormituskyrt.KuormaWh), size(LG18, 1));
for i = 1:size(LG18, 1)
    resultantMatrix(:, i) = (LG18.TotalAnnualEnergyMWh(i) .*
    NISlaskennankuormituskyrt.KuormaWh) / 10000;
end

% Assigning heat pump hourly consumption to each customer's load
m2 = resultantMatrix + hourlyPattern1;

% Calculating remaining hacking capacity and customer load after heat pump hacking
m3  = 0.5714-hourlyPattern1;
m4 = m3 + m2;
```

Program 7: The following simulation program is for load modelling of dumb charging of electric vehicles for all customers of the network at 11.1 kW charging power.

```
% Mean and standard deviation values
mu = 16.53;
sigma = 3.99;
num_customers = 45000;        % Replace with the actual size of customer list

% Generating start time from the Gaussian distribution
start_time = normrnd(mu, sigma, [num_customers, 1]);


% Assigning distance covered for each customer
Distance_Avg = 46;
Distance_Deviationstd = 20;
```

```
Distance_covered = normrnd(Distance_Avg, Distance_Deviationstd,[num_customers,
1]);
Distance_covered = max(Distance_covered, 0);

%Assigning time span of charging to each customer
timespan = (Distance_covered * 0.25) / (9.9);
s = start_time + timespan;

% Assigning time of charging from start time to ceiling of start time
cil_strt = ceil(start_time);
flr_strt = floor(start_time);
time_first_hour = zeros(num_customers, 1);
for i = 1:num_customers
    if s(i) > cil_strt(i)
        time_first_hour(i) = cil_strt(i) - start_time(i);
    else
        time_first_hour(i) = timespan(i);
    end
end

% Assigning EV charging consumption from start time to ceiling of start time
consumption_first_hour = 11.1*time_first_hour;
consumption_first_hour_tsp = transpose(consumption_first_hour);

% Assigning time of charging from floor of ending time to ending time
ending_time= start_time+timespan;
cil_end = ceil(ending_time);
flr_end = floor(ending_time);
time_last_hour= ending_time-flr_end;

% Assigning EV charging consumption from floor of ending time to ending time
consumption_last_hour = 11.1*time_last_hour;
consumption_last_hour_tsp = transpose(consumption_last_hour);

% Transpose variables for matrix operations
flr_strt_tsp = transpose(flr_strt);
cil_end_tsp = transpose(cil_end);
```

```
flr_end_tsp = transpose(flr_end);

% Formulation of matrix for each customer for 48 hours charging assignment
f= combine(flr_strt_tsp+1,flr_end_tsp+1);
newMatrix = zeros(48, 45000);
for col = 1:size(f, 2)
    row_ind = f(:, col);
    valid_rows = row_ind >= 1 & row_ind <= size(newMatrix, 1);
    row_ind = row_ind(valid_rows);
    linear_ind = sub2ind(size(newMatrix), row_ind, col * ones(size(row_ind)));
    newMatrix(linear_ind) = row_ind;
end
for col = 1:size(newMatrix, 2)
    uniqueValues = unique(newMatrix(:, col));
    uniqueValues = uniqueValues(uniqueValues ~= 0);

    if numel(uniqueValues) == 2
        idx1 = find(newMatrix(:, col) == uniqueValues(1));
        idx2 = find(newMatrix(:, col) == uniqueValues(2));
        newMatrix(idx1(1):idx2(1), col) = linspace(uniqueValues(1), uniqueValues(2),
        numel(idx1:idx2));
    end
end

% Formulation of matrix for each customer for the whole year charging assignment
extMatrix = zeros(8760, 45000);
extMatrix(1:48, :) = newMatrix;
desired_rows = 8760;
for col = 1:size(extMatrix, 2)
    uniqueValues = unique(extMatrix(:, col));
    uniqueValues = uniqueValues(uniqueValues ~= 0);

    while max(uniqueValues) + 24 < desired_rows
            newIndices = uniqueValues + 24;
            newIndices = min(newIndices, desired_rows);
            extMatrix(newIndices, col) = newIndices;
            uniqueValues = newIndices;
```

```
        end
    end

    % Assigning EV charging consumption pattern to each customer for 48 hours
    for idx = 1:length(newIndices)
        extMatrix = [extMatrix; zeros(1, size(extMatrix, 2))];
        extMatrix(end, col) = newIndices(idx);
    end
    extMatrix = extMatrix(1:8760,:);
    consu = zeros(48, 45000);
    consumption_middle = 11.1;
    for col = 1:size(newMatrix, 2)
        [~, first_non_zero_row] = max(newMatrix(:, col) ~= 0);
        unique_values = unique(newMatrix(:, col));
        unique_values = unique_values(unique_values ~= 0);

        consu(first_non_zero_row, col) = consumption_first_hour_tsp(col);
        if numel(unique_values) > 2
          last_unique_value = unique_values(end);
          medium_values = unique_values(2:end-1);
          consu(newMatrix(:, col) == last_unique_value, col) = consump-
    tion_last_hour_tsp(col);
          consu(ismember(newMatrix(:, col), medium_values), col) = consumption_middle;
          elseif numel(unique_values) == 2
                last_value = unique_values(end);
                consu(newMatrix(:, col) == last_value, col) = consump-
    tion_last_hour_tsp(col);
        end
    end

    % Assigning EV charging consumption pattern to each customer for the whole year
    extcons = zeros(8760, size(consu, 2));
    for col = 1:size(consu, 2)
        nonZeroIndices = find(consu(:, col) ~= 0);
        for val = 1:length(nonZeroIndices)
            currentVal = consu(nonZeroIndices(val), col);
            indicesToFill = nonZeroIndices(val):24:8760;
```

```
        indicesToFill = indicesToFill(indicesToFill <= 8760);
        extcons(indicesToFill, col) = currentVal;
    end
end

% Calculating resultantMatrix based on TotalAnnualEnergyMWh and Load Profiles
resultantMatrix = zeros(numel(NISlaskennankuormituskyrt.KuormaWh), size(LG, 1));
for i = 1:size(LG, 1)
    resultantMatrix(:, i) = (LG.TotalAnnualEnergyMWh(i) .*
    NISlaskennankuormituskyrt.KuormaWh) / 10000;
end

%Adding EV load to customer consumption
resultantMatrix2 = resultantMatrix + extcons;
```

Program 8: The following simulation program is for after-hacking load modelling of electric vehicles for all customers of the network at 11.1 kW charging power. This code can be based on after hacking strategy of reverse price based as well as descending order of number of vehicles connected to the network.

```
% Assigning distance covered for each customer
Distance_Avg = 46;
Distance_Deviationstd = 20;
Distance_covered = normrnd(Distance_Avg, Distance_Deviationstd,[num_customers,
1]);
Distance_covered = max(Distance_covered, 0);

% Mean and standard deviation values
mu = 16.53;
sigma = 3.99;
num_customers = 363;        % Replace with the actual size of customer list

% Generating start time from the Gaussian distribution
start_time = normrnd(mu, sigma, [num_customers, 1]);

%Assigning time span of charging to each customer
```

```
timespan = (Distance_covered * 0.25) / (9.99);

% order is either based on hourly price or number of vehicles connected to the network
[~, order] = sort(HourlyPrice);

%Assigning vehicle connection to the grid times
t1 = (start_time + 16).';
t2 = (start_time + 24).';
timespan= (timespan).';
t_choose = t1;
indices = timespan >= 15;
t_choose(indices) = t2(indices);
order_ext = zeros(48, 1);
for i = 1:24
    order_ext((i-1)*2 + 1) = order(i);
    order_ext((i-1)*2 + 2) = order(i) + 24;
end
n = zeros(48,363);
start_time = (start_time).';
t_choose = (t_choose).';
ceil_timespan = ceil(timespan);
ceil_t_choose = ceil(t_choose)';
ceil_start_time = ceil(start_time);
flr_timespan = floor(timespan);
time_last_hour= timespan-flr_timespan;

%Assigning charging powers for charging times
c2 = 11.1 * time_last_hour;
c1 = 11.1;

% Formulation of matrices for for daily charging assignment each customer
E = zeros(24, 363);
for col = 1:size(ceil_timespan, 2)
    numValues = ceil_timespan(1, col);
    minValue = ceil_start_time(1, col);
    maxValue = ceil_t_choose(1, col);
    minValue = max(minValue, min(order_ext));
```

```
    maxValue = min(maxValue, max(order_ext));
    selectedValues = order_ext(order_ext >= minValue & order_ext <= maxValue);
    numRowsToFill = min(numValues, numel(selectedValues));
    E(1:numRowsToFill, col) = selectedValues(1:numRowsToFill);
end
above_24 = E > 24;
E(above_24) = E(above_24) - 24;
consumption = zeros(24,363);
for col = 1:size(E, 2)
    values = E(:, col);
    nonZeroIndices = values ~= 0;
    if any(nonZeroIndices)
        lastNonZeroIndex = find(nonZeroIndices, 1, 'last');
        consumption(values(nonZeroIndices), col) = consump-
tion(values(nonZeroIndices), col)
       + 1;
    if ~isempty(lastNonZeroIndex)
         consumption(values(lastNonZeroIndex), col) =
         consumption(values(lastNonZeroIndex), col) + 1;
         end
   end
end

% Assigning EV charging consumption to each customer for whole year
for col = 1:size(consumption, 2)
    consumption(consumption(:, col) == 2, col) = c2(col);
end
hours_in_a_day = 24;
total_hours = 8760;
consumption_extended = zeros(total_hours, size(consumption, 2));
for i = 1:size(consumption, 2)
    consumption_extended(:, i) = repmat(consumption(:, i), total_hours /
hours_in_a_day, 1);
end

%Adding EV load to customer consumption
R2 = resultantMatrix+consumption_extended;
```