UNIVERSITY OF TURKU

Power consumption of emerging cybersecurity technologies on network devices

Communication and Cyber Security Engineering
Master's Degree Programme in Information and Communication Technology
Department of Computing, Faculty of Technology
Master of Science in Technology Thesis

Author:
Vesa-Matti Antero Mäntysaari

Supervisors:
Dr. Jouni Isoaho
Dr. Tahir Mohammad

November 2025

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Communication and Cyber Security Engineering
Programme: Master's Degree Programme in Information and Communication Technology
Author: Vesa-Matti Antero Mäntysaari
Title: Power consumption of emerging cybersecurity technologies on network devices
Number of pages: 51 pages, 2 appendix pages
Date: November 2025

This thesis investigated the current matureness of IT systems in relation to flexibility support through application level controls with the aim of determining the future direction for emerging cybersecurity features. The research was driven by interest in investigating how flexibility principle could affect cybersecurity. This was accomplished through literature review of the current knowledge on IT systems and available controls and three power consumption experiments with each of them focusing on different solution.

In literature review part it was found that flexibility is not commonly available and enabling support for it may require moving workloads from dedicated hardware to virtualized environment. Comparatively in experiment portion it was found that the throughput penalty of cybersecurity complexity at the highest can be 50 percent in active network devices. This indicated that for organizations with known throughput needs at least one model above the matching throughput should be selected if maximum cybersecurity feature set is to be used.

Through literature review and experimentation, a grounded theory was established and assessed. Thesis concludes that current cybersecurity solutions do not support flexibility to the level flexibility principle needs to and as such there is clear need for adaptive cybersecurity solution that could automatically either downscale feature set complexity or change the workload from individual nodes to computationally more robust node. In literary review section some sources suggest data centre operators should choose the more efficient cybersecurity algorithms to curtail excess power consumption.

Keywords: power consumption, cybersecurity, network devices, machine learning, energy efficiency.

Table of contents

1 Introduction 1

1.1 Problem statement 1

1.2 Research questions 2

1.3 Research objectives 2

1.4 Research methodology 2

1.5 Thesis structure 3

2 Literature review 5

2.1 Smart electricity grid 7

2.1.1 Introduction to power system flexibility 7

2.2 Instability caused by renewable energy 14

2.3 IT power consumption 15

2.3.1 Power stability vs availability in IT 20

2.4 Cybersecurity power consumption 22

2.4.1 Effects on cybersecurity 24

2.4.2 Scalable cybersecurity as alternative 26

3 Cybersecurity power consumption experiments 29

3.1 TP-Link Archer AX55 30

3.2 Machine learning enabled next-generation firewalls 36

3.3 Open Source HIDS SECurity 38

3.4 Router and Next-Generation Firewall comparison 40

3.5 Results and analysis 41

3.5.1 Impact of TP-Link Archer AX55 42

3.5.2 Impact of Next-Generation Firewalls 43

3.5.3 Impact of Open Source HIDS SECurity 46

4 Conclusion 48

References 52

Appendices 58

Appendix 1 Maximum power generation in Satisfactory 58

List of figures

Figure 1. World electricity production in 2023 divided by source. [7] 6
Figure 2. Finland's electricity production in 2023 divided by source. [7] 6
Figure 3. Power system flexibility concept with the underlying components. [12: Fig. 4] 9
Figure 4. DR program divided into its individual components. [12: Fig. 9] 10
Figure 5. Available electricity reserves during September 2024 at Finland [15]. 12
Figure 6. Line graph of electricity consumption for A.1 and A.2. 32
Figure 7. Line graph of electricity consumption for A.3 and A.4. 33
Figure 8. Line graph comparing A.1 and A.3. 34
Figure 9. Line graph comparing A.2 and A.4. 35

List of tables

Table 1. Google data center and office electricity consumption by year. [33: p. 107] 18
Table 2. Microsoft electricity consumption by fiscal year. [34: p. 101] 19
Table 3. Telia Company electricity consumption by year. [35: p. 93] 19
Table 4. Archer AX55 scenario variables. 30
Table 5. Speed test results for experiments. 34
Table 6. Average power delta with reference experiment in vertical column. 35
Table 7. J/bps based on speed test results with maximum power. 36
Table 8. Device details derived from brochures. 36
Table 9. Devices and their respective J/bps values. 36
Table 10. NGFW throughput efficiency delta with PA-220 as the baseline. 37
Table 11. NGFW throughput efficiency delta in percentages with PA-220 as the baseline. 38
Table 12. OSSEC scenario variables. 39
Table 13. Table showing B.1 and B.2 results. 39
Table 14. Absolute delta between B.1 and B.2. 39
Table 15. Percentual delta between B.1 and B.2. 39
Table 16. Absolute delta between network devices. 40
Table 17. Percentual delta between network devices. 41
Table 18. Archer AX55 experiments with their respective kWh values. 42
Table 19. Calculation of Archer AX55 impact in 2023's Finland using Eurostat data. 42
Table 20. Calculation of Archer AX55 impact in 2023's Germany using Eurostat data. 43
Table 21. Calculation of Archer AX55 impact in 2023's Australia using AEMO data. 43
Table 22. NGFWs with their respective kWh values 43
Table 23. Calculation of NGFWs impact in 2023's Finland based on average wattage using Eurostat data. 44
Table 24. Calculation of NGFWs impact in 2023's Finland based on maximum wattage using Eurostat data. 44
Table 25. Calculation of NGFWs impact in 2023's Germany based on average wattage using Eurostat data. 45

Table 26. Calculation of NGFWs impact in 2023's Germany based on maximum wattage using Eurostat data. 45
Table 27. Calculation of NGFWs impact in 2023's Australia based on average wattage using AEMO data. 46
Table 28. Calculation of NGFWs impact in 2023's Australia based on maximum wattage using AEMO data. 46
Table 29. Calculation of OSSEC impact in 2023's Finland using Eurostat data. 46
Table 30. Calculation of OSSEC impact in 2023's Germany using Eurostat data. 47
Table 31. Calculation of OSSEC impact in 2023's Australia using AEMO data. 47
Table 32. Calculated power generation if somersloops are not utilised. 58
Table 33. Calculated power generation if all somersloops are used. 59

1 Introduction

For a while now the overall impact of our combined resource consumption has been a rising problem with projections of current climate policies and actions leading to 2.7°C of warming which is far from the pledged target of 2°C [1: Fig. 3] and almost double the 1.5°C goal in Paris agreement. With [2] concluding that while there are certain advances, they still are very small in only certain areas and as whole are not as big actions that are necessary.

Intergovernmental Panel on Climate Change (IPCC), Climate Action Tracker (CAT), and many other institutions conclude that the society at large will need to reduce the use of fossil fuels, with IPCC stating that the fossil fuel use should reach its maximum at the latest during 2025 after which it should start to fall cumulatively to reach the goal of 2°C [3: L. C.12.3]. To reach this goal each aspect of modern society may need to adapt to geographical and other aspects.

Some of the adaptations may be that in countries with electricity mix consisting of mainly solar energy during low-light time of day people will not use energy intensive devices at home or work simply because their energy grid does not have the capacity to supply power for such devices, in practice creating an inverse siesta only with electricity usage.

The research presumption is that countries with access to stable energy sources comparable to hydro, geothermal and nuclear can direct their electricity usage to more energy intensive cybersecurity solutions whereas countries where renewable is major part of energy mix the low-power alternatives are preferred.

1.1 Problem statement

Due to ever rising attack chain complexity the defences against them need to continuously become more complex and therefore require more CPU cycles than previous generation defensive tools have. Some defensive tools such as next-generation firewalls (NGFW) have included machine learning (ML) based monitoring capabilities on top of the pre-existing deep-packet inspection analysis capabilities.

Unfortunately, all these additional features incur some level of efficiency penalty, however due to the relevant knowledge on the matter being sparse there is no clear knowledge what level of efficiency penalty there is for emerging cybersecurity technologies on network devices such as NGFWs that include further additions similar to ML and how would the penalty be affecting in typical operational environments.

This thesis aims to determine how all of these will affect information security which is built on top of ever-increasing complexity of tools to identify malicious activity and stop them while also informing the cybersecurity team what has happened.

1.2 Research questions

This thesis aims to the problem statement by answering three research questions, which are:

RQ1: What level of flexibility in IT power consumption is available?

RQ2: How big is the power usage when cybersecurity solution complexity rises?

RQ3: In what kind of way would the seen power usage affect?

1.3 Research objectives

By answering the research questions the following objectives will be reached:

1. Investigate matureness of current IT system support flexibility in power consumption via hardware or software.
2. Investigate power draw difference between information security settings.
3. Determine difference in kWh and location-based metrics through operating cost and carbon footprint.

With these objectives completed the thesis furthers the current understanding of the real world cost of information security.

1.4 Research methodology

Hybrid methodology was used during literature review to establish grounded theory based on current state of flexibility in general IT and cybersecurity to inform the direction of quantitative experiment part. Quantitative methodology was used to map the energy use in each experiment and due to earlier literature on the field using Joules as the energy unit for comparisons between experiments it was used in this thesis as well. Majority of the experiments used primary data sources with one using secondary source in the form of product brochures.

In Chapter 3's first experiment the data was collected through 30 minutes of testing with the preliminary data processing occurring in a non-linear video editor allowing the playing of video

in absolute frame increments in accordance with the electricity monitor's fastest update cycle in frames with the resulting data collected into machine readable table. The second experiment with product brochures used secondary company provided data with them being converted to Joules/bps before doing comparisons between devices.

In the third experiment data was collected through 30 minutes of testing with data not being processed after. In subchapter 3.5 all the previously mentioned data was used together with additional secondary sources to get monetary and pollution cost metrics for each experiment. The pricing data from Australia required further processing to get $/kWh format and then conversion to €/kWh.

Using electricity monitoring device in experiment one caused a slight obstacle in that due to the LCD refresh cycle not staying constant further manual intervention in the form of counting how many frames the measurement was clearly visible was needed to determine the correct measurement for collection, if any, when complex measurements were seen on the LCD.

1.5 Thesis structure

The thesis is organized as follows:

- Chapter 2 literature review of current knowledge on flexibility via power controls in hardware or software
    - Subchapter 2.1 provides introduction to smart electricity grid and its individual components and its relation to following topics
    - Subchapter 2.2 investigates stability problems that arise when intermittent energy generation sources are used
    - Subchapter 2.3 investigates IT power consumption and its resilience when exposed to unstable electricity
    - Subchapter 2.4 investigates cybersecurity power consumption and possible auxiliary effects from previous subchapters
- Chapter 3 shows power usage experiments using electricity monitoring device, secondary brochures and *codecarbon*.

    - Subchapter 3.5 provides real world impact of previous experiments on monetary value and carbon equivalent emissions with comparisons provided for three countries.

- Chapter 4 concludes the thesis by discussing research questions and objectives while also providing further research pathways.

2 Literature review

In Finland during 2022 [4-5] companies doing manufacturing downscaled their power consumption together with consumers and therefore the estimates of electricity generation not being enough during winter due to the Olkiluoto not producing enough electricity for peak consumption was not reached. This was possible most of all because the relevant parties were proactively doing preparations for the worst-case scenario by getting additional supplies in the form of a new LNG terminal, delaying the decommissioning of old power plants and by launching a voluntary power system support scheme.

Nearing the winter 2022 there was considerable uncertainty about available power generation meeting demand if outside temperature were to cause significant need for house heating. This uncertainty was caused by many compounding aspects: due to nuclear power availability problems and the import restrictions from Russia causing problems in getting the required gas. [6]

According to Our World in Data [7] the electricity generation mix worldwide in 2023 was stable but highly atmosphere polluting sources such as coal were heavily exploited as shown in Figure 1. Waste, geothermal, wave and tidal power are included as other renewables in the figure. Figure 1's classifications out of all the electricity generated, 13,35% of it were from intermittent power sources. In Finland, the same year stable nuclear power was used to generate most of the required power as shown in Figure 2. Interestingly the other renewables were 0% for Finland. Correspondingly according to Figure 2's classifications out of all electricity generated, 19,13% of it were from intermittent power sources.

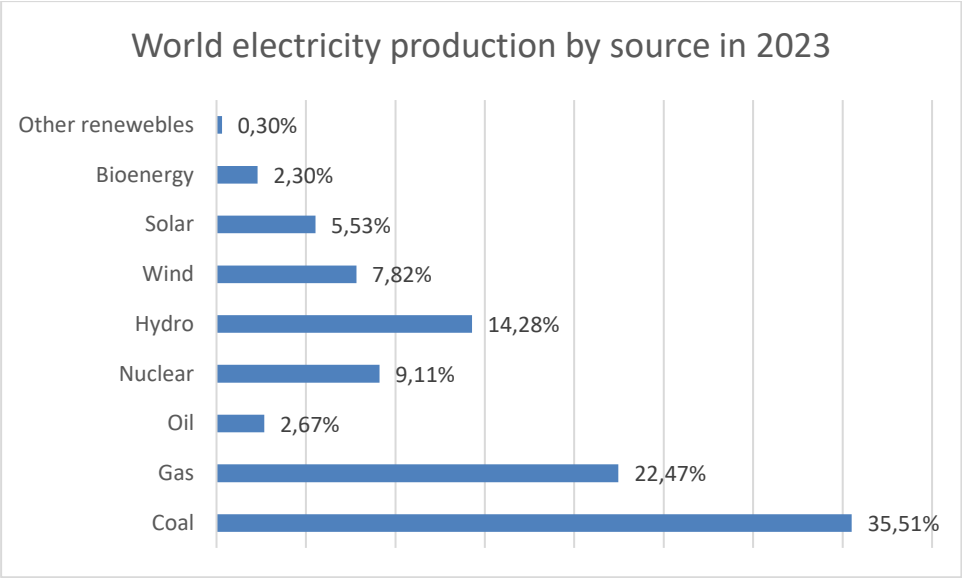

Figure 1. World electricity production in 2023 divided by source. [7]

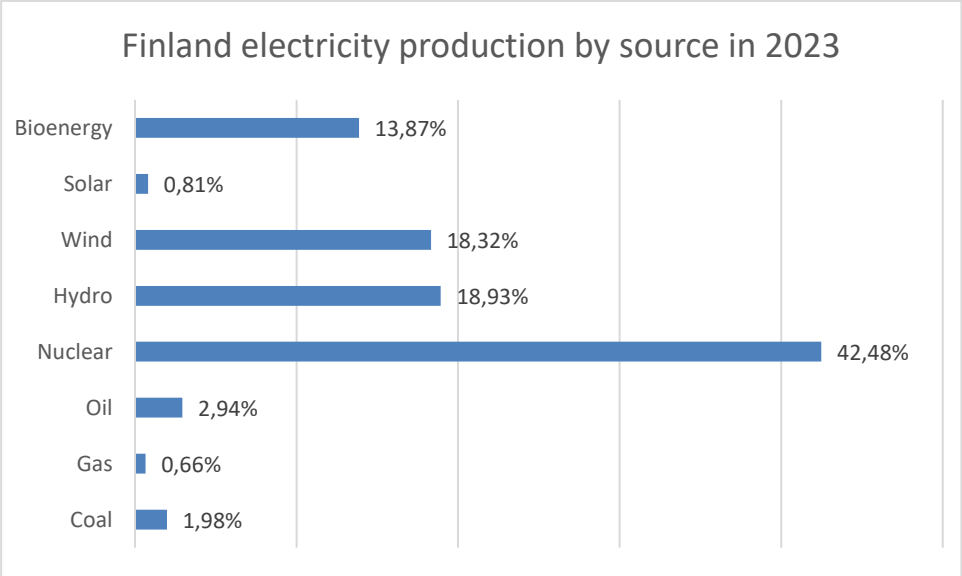

Figure 2. Finland's electricity production in 2023 divided by source. [7]

In [5] undergraduates were asked to group energy requirements of nearby appliances based on qualitative metrics such as relative & total energy consumption and volume in three different experiments. The study found that when it was asked to group items based on "general similarity and similarity in terms of energy consumed in an hour" the resulting grouping was similar in size and function of the device not energy consumption [8: Ch. Experiment 1: Free-Sorting Task]. Similarly, it was found that the smaller an item is the less it is perceived to consume energy [8: Ch. Experiment 2: Rank-Order Task].

2.1 Smart electricity grid

The concept of smart electricity grid or shortened to only smart grid (SG) has been proposed for the future electricity grids with the main aspect of it including the possibility of redistribution of electricity from available power storage facilities or even connected electric cars back into the grid when needed, therefore creating flexibility in electricity availability. Commonly the plans for building such a grid system involve including internet of things capabilities to the electricity grid itself. And depending on how each portion of SG would be designed these capabilities could allow one or more of the following capabilities: automatic switching, remote monitoring or control. [9, 10: p. 9]

Due to regulatory aim of implementing SG in India by 2027 the local regulators expect the renewable generation penetration to rise in delivery portion of the grid to comparable levels seen in production portion. It has already shifted the old paradigm of centralized power generation and the changes to the grid have made previously unidirectional grid to bidirectional. However, market penetration of digital appliances that cannot function without constant and correct grid voltage and frequency has changed the characteristics of the grid load to more vulnerable. [9: Ch. 3.3]

To control the electricity demand in grid the utility will need through forecasts in all available power generation in the grid be it located in delivery segment of grid or in production. With network enabled electricity monitors in households and grid the utility can determine real-time demand and depending on the connections to household owned power generation. [9] With the demand and forecast data the utility can control the demand for their electricity production via price or other demand-side management strategies. [11-12]

2.1.1 Introduction to power system flexibility

According to [12] the research on demand-side management strategies and their effectiveness on reaching stability in the power system has been expanding in late century and in this paper author's go through many of them in holistic manner detailing possible shortcomings in reference to eight research objectives such as "R4: Enhancement techniques for demand-side flexibility." The aim of the paper is to be reference point of previous research in power system flexibility (PSF) for other researchers or other interested parties that may even be in the field.

The review of the previous research found that due to the PSF concept in electricity grid being new there is very little information how it would be described which has caused the papers to adopt more general and less descriptive language. One way PSF can be described as is topmost level concept encompassing of all strategies and methodologies for implementing flexibility in the power system to support higher market penetration of renewable power sources in multiple parts of the grid. Due to the concept consisting of large concepts and differing research directions the full concept merged by paper author's is shown in Figure 3. [12]

Figure 3 shows that the PSF consists of five main areas: applications, characteristics, solutions, estimation & prediction approaches and finally quantification approaches. Applications contains the principles for the system while solutions detail the digi-physical implementation of it. Characteristics detail the specifics of the system such as operating timescale and how controllable individual aspects are. Estimation & prediction approaches detail the system for power usage and generation estimation while quantification approaches detail how previously mentioned estimates are quantified.

In [11] a demand response model (DSM) is proposed for smart grid and verified with real data, in Figure 3 DSM is classified under solutions. With the DSM the peak electricity demand in China commercial and residential decreased by 4,99% for commercial and 9,99% for residential with the utility gaining 7,13% and 2,37% respectively more profit from the same customer bases. The main component in its success was more through modelling of multifaceted variables such as electricity consumer satisfaction and lowest viable power generation during the specified period.

While there are other methods for controlling power in smart grid such as supply and network-side management and more standalone solution ESSs as shown in Figure 3 the DSM will be focused on, due to it being more viable in grids with greater usage of renewable energy in multiple sections of the grid. In [12: Fig. 8] DSM is further divided into five sections: policies, methods factors, techniques of load management, implementers and categories.

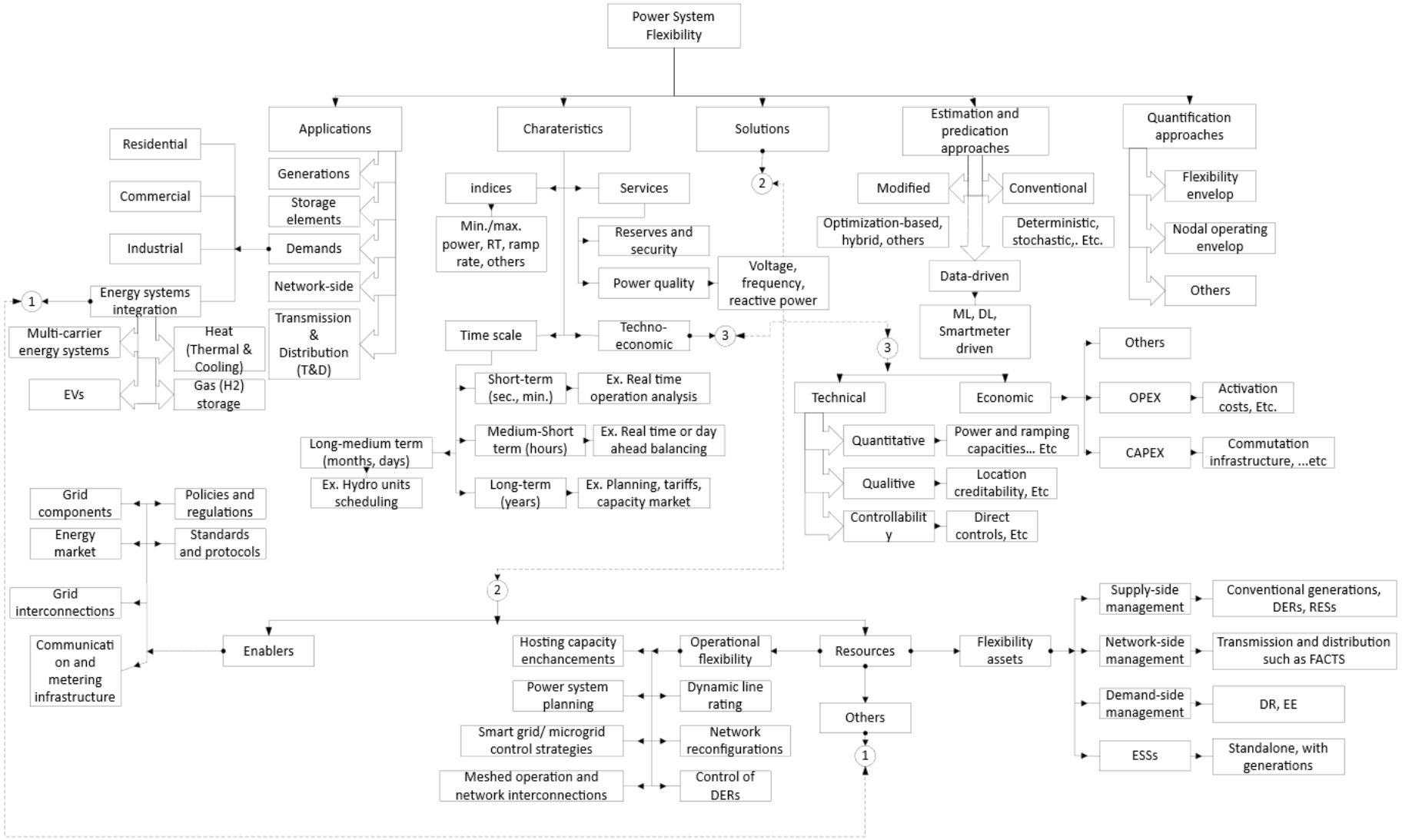

Figure 3. Power system flexibility concept with the underlying components. [12: Fig. 4]

Going through DSM's components figure in detail the policies include aspects such as regulations, standards and communication protocols while method factors include user's interaction, time scale and applied approaches. Techniques of load management details the power control style for example valley filling, load shifting and peak clipping. Implementing party can be among others an aggregator, customer and utility. Categories include on site back-up, strategic load growth and energy efficiency. [12: Fig. 8]

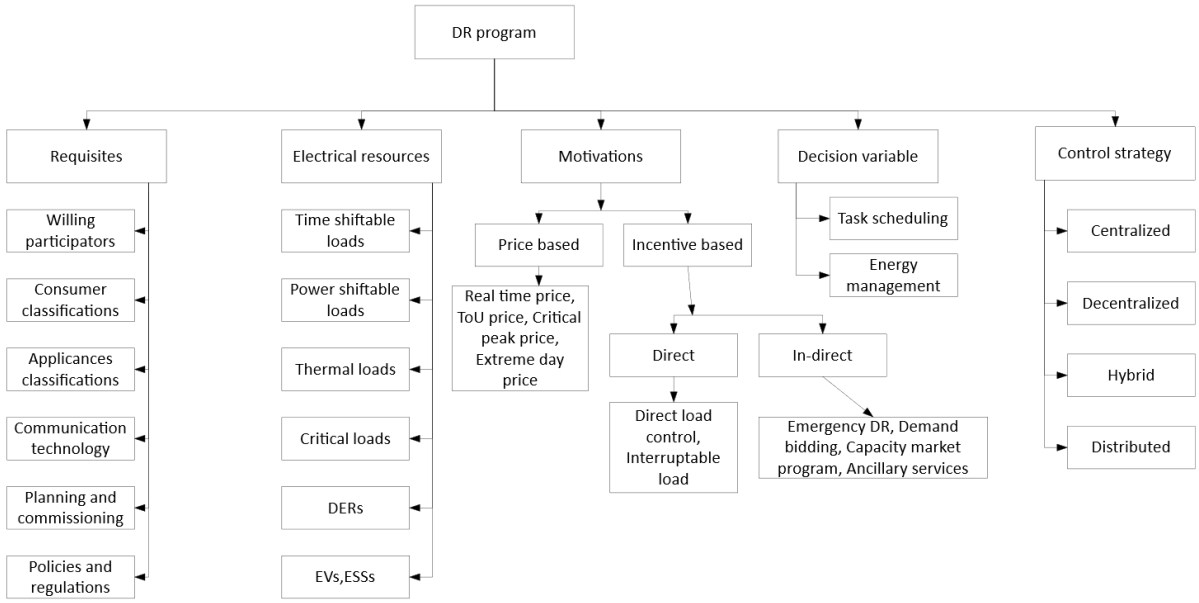

Figure 4. DR program divided into its individual components. [12: Fig. 9]

Additionally, in Figure 4 an individual DR program is divided into five areas: requisites, electrical resources, motivations, decision variable and control strategy. Through manipulation of these areas specialized DR programs can be built for multitude of implanting parties. Specifically, requisites detail possible regulations or how participant willingness to is part of DR program while electrical loads details available resources from EVs to critical loads that cannot be switched off. Motivation details the methodology for ensuring participants are active due to price or other incentives. Decision variable details possible variables leading to decision in DR while control strategy determines how program is managed ranging from centralized to hybrid solution.

In Finland market penetration for dynamic electricity contracts was ~33% in 2024 with the rest being fixed price contracts, however due to more than 99% electricity consumption places being equipped with smart meters there is possibility to grow its adoption. Based on Finland's Energy Authority's report there was significant volatility in dynamic electricity prices throughout the

2024 with the highest price of 12 cents/kWh happening in January. When January is not considered the dynamic price contract was cheaper as whole. [13: p. 38]

For dynamic contract the electricity consumption place such as apartment will require at least 1st generation smart meter. The smart meter generation can be determined on the measuring period of the device: one hour (1st generation) or 15 mins (2nd generation). While the former meter would function correctly the time precision loss would mean that user could be billed the wrong amount than with the latter meter generation due to the European dynamic price market called day-ahead market moves to 15 minute time unit during October 2025. [13: p. 39]

As of October 2024, Flow-based (FB) model underlined in CACM Guideline is used in Europe's day-ahead and intraday markets as capacity calculation method replacing the previously used Net Transmission Capacity (NTC) model [13: pp. 19–20, 14: Art. 20] with the change being done due to the need for more efficient use of existing power grid. It accomplishes this by making the grid congestion less of an issue and stabilizing prices.

According to [15] peak electricity consumption in the grid is controlled with an undisclosed demand response strategy alongside the FB model and during September 2024 at Finland the intraday flexibility was between 0-300 MW without taking into consideration the larger external market controlled reserve called Manual Frequency Restoration Reserve or mFRR (Figure 3). Figure 5 also depicts certified and non-certified demand-side flexibility with former being certified by Fingrid making obligations, however both are needed to make sure the electricity grid frequency stays around 50 Hz in all situations.

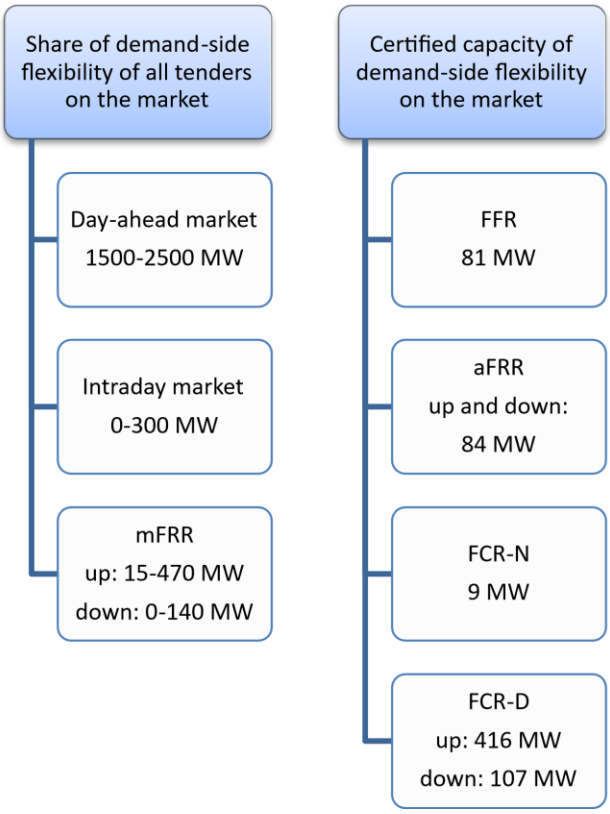

Figure 5. Available electricity reserves during September 2024 at Finland [15].

As previously stated, the demand response methodology in use with FB is undisclosed and therefore to further explore the inner workings of a demand response model the implementation from [10] is examined. The model considers high photovoltaic (PV) market penetration in district-level smart grid while its possible downsides and other implications are explored more in the next subchapter 2.2 through other sources. For electricity consumers (ECs) model (1) describes aspects such as the electricity consumer satisfaction (SF), subsidises for PV (RS) and "electricity consumption costs" (E) as components with all of them being used to get the overall utility.

$$\Phi_{ECs} = \sum_{t=1}^{T} RS^t - P^t \times E^t - SF^t \quad (1)\ [10]$$

Comparatively for energy service provider (ESP) a different set component selection is used to describe aspects such as revenue from electricity selling (E), cost of purchasing excess PV power from ECs (C), energy buying cost for ESP on wholesale market (μ), fluctuations in power systems (F) and its weight parameter (θ) which are then used to compile the overall utility model for ESP (2). [10] These two models together make a major part of the proposed demand response model; however, in the paper individual components are also shown in detail.

$$\Phi_{esp} = \sum_{t=1}^{T} \left[R^t - C^t - RS^t - \mu^t \times E_{esp}^t \right] - \theta \times F \quad (2)\ [10]$$

By setting the variables into the models the results give a viable range for price and viable load range from ECs. By comparing [10] and the figures from [11] it can be determined that the proposed model has load shifting as its focus which it aims to accomplish by motivating ECs with price which in turn would be accomplished through centralized control mechanism. According to Finland's Energy Authority [13: p. 26] there were 17 smart grid development projects ongoing during 2022 which consider all or some of the specified demands: smart metering, demand flexibility, flexibility solutions and storage solutions.

The flexibility principle found in power systems is not limited to only power systems and can currently be seen in many areas of society. For example, in house engineering developments Earthship and passive house design, for the foremost flexibility is mostly on the inhabitants due to the design incorporating many off-grid principles whereas the latter design incorporates passive cooling and flexibility principles into a house connected to grid and therefore flexibility is shared between the house and inhabitants.

According to Swedish study on energy use differences between conventional and passive buildings [16] the flexibility of passive cooled houses comes from mainly the insulated and airtight environment within the passive house which in surveys showed colder floors than inhabitants were used to and internal heat sources will keep the house internal temperature higher than in the comparison conventional houses.

Eventually power system flexibility could encompass whole cities by becoming an interconnected and complex system commonly referred to as smart city where critical systems such as power system could dictate semi-autonomously individual city functions. In [17] the theoretical energy savings of such a system are assessed through mapping available support technologies and building a framework of it that can be used to find the synergy between key technologies that may have not been fully implemented whereas in [18] IoT based deep learning is used to control smart house functions based on current inhabitants.

Paper [17] concludes that their finished framework indicates greatest possibility within "intelligent operation and soft transformation of transport and heating of buildings" which enforces previous findings by other authors. Comparatively in [18] AC is controlled by camera based deep-learning algorithm which can turn AC off if no inhabitants are detected hence saving

on energy consumption however, the active camera monitoring can be considered limitation due to it introducing need for trust in camera being configured correctly.

Based on these findings there is clear pathway from power system flexibility to future systems that could surpass even the currently known complex systems by eventually integrating one or more of currently existing complex systems into one major complex system. However, currently by moving from the old paradigm of power generation in one sector of the grid to the new distributed one where power is generated in multiple sectors invariably the sectors will become more autonomous in power generation while also as side effect more vulnerable to issues arising from loosely planned or engineered grid infrastructure with the next subchapter detailing the issue more thoroughly.

2.2 Instability caused by renewable energy

Many research papers and assessments [19-23] have been published on the emerging problems when renewable energy sources are introduced to an electricity grid previously not designed to handle them or at the level of usage previously not designed for. In [19-21] the inverter-based renewable energy sources or IRESs have been identified as the primary contributor to the emerging problem because of them not being synchronized with other power sources by default and if the problem is not addressed by implementing flexible AC transmission system devices, then the power grid the IRESs is connected to could have reduced tolerance of direct or indirect faults.

While [19] was limited to researching solar and wind within strong and weak power grids it did show that when a power grid interconnect between IRESs and synchronous generators is not designed well or the grid as a whole is weak the grid may start to resist the electricity the IREs portion of the grid is trying to send when their electricity generation is varying too much which then requires the raising of the point of interconnection (POI) voltage before it is possible to receive it.

The faults that may hinder the efficiency of the power grid may be simple equipment failures, larger transmission line breakages or even power source failures but the difference between a strong power grid and a weak one is how well it can handle any of the above-mentioned problems without a complete shutdown as noted:

> “Power system stability is the ability of an electric power system, for a given initial operating condition, to regain a state of operating equilibrium after being subjected

> to a physical disturbance, with most system variables bounded so that practically the entire system remains intact." [21: p. 3]

In [22] theoretical modelling was done to determine how well Taiwan's renewable energy goals by 2030 fulfil the possible summer peak electricity consumption hour needs and the results were that if the current developments are completed on time, then Taiwan is expected to be at an hourly electricity capacity loss of 0,9 percent in 2024. Unfortunately, due to the nature of the modelling and it being done before previous sources it did not model what happens to the grid fault tolerance if current nuclear generation is not renewed but instead replaced by wind as the source is expecting.

In [23] P. Kivimaa and M.H. Sivonen analysed the governance side of the renewable energy transition and national security at Estonia, Finland and Scotland throughout 2006-2020 by going through the policy documentation related to them. Based on their analysis the holistic approach of both renewable energy transition and national security is not seen in the public documentation instead some energy related points are included in the national security policy documents. Finland for example has holistically named vision of energy and security however specific measures are not proposed that would make it possible.

With the previous paragraphs in mind power system stability affects external processes such as manufacturing, commerce, etc. directly in that if a breakage were to occur that would lower the overall grid capacity to a level that would not be possible to receive through other countries interlinks then quick response channels would need to be used to mitigate and control the available power in accordance with crisis management plans. For manufacturing using the continues production model the only feasible option may be cutting down on production numbers since a full stop of production could lead to throwing out of the output, some of the examples are chemical and food processes. The result could be for instance rolled out blackouts as seen in California.

2.3 IT power consumption

Every device or digi-physical device and software combination that can be used to control data through additional processing or by relaying it to other device can be construed as an IT system and therefore each of the systems will incur some level of energy and human resource cost to operate and maintain. However, due to the digitalisation efforts of recent years the full energy cost of such systems is not generally easily discernible in part due to the inherent distributed nature of their function as certain components can be in organisation controlled on-premises

while others are in public cloud and organisations are not able to easily link the energy consumption of both.

There have been many papers assessing how much IT clients and infrastructure consume electricity with the findings being sparse in detailing the whole consumption pattern of each individual client or system. However, due to papers from authors such as Ardito and Morisio [24] bringing relevant papers together the whole consumption pattern has been revealed. According to [24: Table 2] the networking devices used 6,05 TWh per year in 2010 while the datacentres [24: p. 26] consumed 330 TWh in 2009. In [24] it is estimated that networking devices' electricity consumption rises by 1 TWh per year with similar metric not available for datacentre.

According to Statista worldwide datacentre power consumption was 460 TWh in 2022 and the forecasts at the time indicated it would rise to 1,05 PWh by 2026 due to demands from AI, blockchain and hyperscale computing. Additionally in 2022 the AI power demand was determined to be 12 TWh. [25-26] Compared to 330 TWh in 2009 this means total power consumption rise from datacentre has been more than a quarter (28%) in 13 years. In [27: Fig. 2.3] IEA provides conflicting datacentre power consumption numbers for example that 400 TWh power consumption was reached in 2024 instead of 2022, in this instance the rise has been 21% in 15 years.

The reason for this data discrepancy is unknown but its causes can range from differences in data sources to calculation methods. Conversely, Statista reports their data coming from one entity Goldman Sachs which in turn has used data from various sources including IEA while IEA reports multiple entities for their data: IDC, OMDIA and Semi Analysis. Nevertheless, the reason for this difference in data is inconclusive because in IEA's report Goldman Sachs is attributed as data source in other areas which could mean they had access to the same data but either chose to discard it or did not include it into the same data set due to other unknown reasons.

Through [25, 27: Fig. 2.5] additionally estimation difference in future AI power consumption is found between Statista and IEA, between 94 TWh and nearly 300 TWh by 2026 respectively. Difference between these estimates is significant however, it may be explained with estimate age, Statista estimation is from 2023 whereas IEA is from 2024. This could mean that in one year the usage of AI technology has been so expansive that there has been need for significant estimate changes for the future.

One key point that IEA [27: pp. 60–62] highlights in relation to data centre power consumption estimations is the difference in them by source. Report states that all historical data about data centre power consumption is estimation based and even in recent high quality studies the estimation can vary greatly while direct company data gives narrow scope at the same time introducing reliance on company managed information releases. Furthermore, in this section IEA also shows they have chosen roughly the mid-point in studies while in company information the chosen point is slightly lower than reported.

Consumption driver variance is further emphasized in 2020 article where the datacentre energy use between 2010 and 2018 is assessed together with data on number of general compute instances. The article finds that compute instances have significantly increased while the total energy consumption has not hence leading authors to conclude that efficacy increases have allowed the compute instances to increase without causing similar levels of energy consumption and that based on the compute instance projections, they estimate the energy consumption to double from ~200 TWh in 3-4 years. [28] Interestingly article was released during the cusp of machine learning's (ML) incorporation to everyday devices which means that stated estimation was reached due to at the time unforeseen driver.

Due to the ML implementations of now being recent and constantly improving their power consumption is not fully up-to date or in some cases the information about the power consumption may be hidden due to business interests, however there are papers related to either energy saving implementation with IoT [29] or other energy raising implementations [30] such as image classifications that detail power usage while papers such as [31] provide empirical review of available power consumption setups and their best use cases with ML workloads in mind.

In [29] an energy saving IoT solution was built and used in smart house with the aim to determine the effect such a system can achieve when compared to previous energy management systems (EMS). According to the paper traditional EMS provides 5% energy savings and 3% cost reduction while it was between 12-30% and 10-28% respectively for the ML based implementation, depending on the ML model used. Based on this it can be determined that through correct application of ML in key systems energy consumption can also be minimized.

In [30] ML model is tasked with classification of different images and the power consumption is measured for three hardware configurations. Paper states that the most computationally and therefore resource intensive portion of ML is during the training portion of the models, this

could mean that if the system does not incorporate a continuous training module, then its power consumption is significantly lower than systems that do.

Furthermore, based on this it can be determined that if the system includes capability to do behavioural analysis with anomaly detection its constant learning component inclusion will not incur as significant power increase and therefore should be used when full training of the model is not needed for the specific use case. One mitigation technique for lowering the energy cost of behaviour analysis components would be to limit the time range, interval or other characteristics included in the determinisation.

Compared to previous ML papers in [32] a simplistic energy reduction system was proposed for LTE networks by combining Nash traffic entropy learning algorithm and a novel relay station (RS) overlapping model called "transmission area-based relay stations' deployment scheme" or TARSD. The algorithm is used to determine the maximum and minimum points for the network usage allowing the underlying base stations in two-way pattern to turn off when not needed while TARSD is used to determine the optimal distance between the RS. If ML can be used to the extent shown in [29] it could allow even bigger energy savings in the LTE network.

As part of environmental standards organizations keep statistics on their own consumption with the aim to cut down on excess consumption via using novel consumption reduction methodologies such as carbon credits. As part of this Google [33] and other organizations release their electricity, water and waste activities publicly in the reports hence Google's electricity consumption by year is shown in Table 1. Based on the Table 1 Google's datacentre business has continuously consumed more electricity and when years 2020 and 2024 are compared it can be determined that electricity use has almost doubled.

Table 1. Google data center and office electricity consumption by year. [33: p. 107]

Electricity consumption source	2020 (MWh)	2021 (MWh)	2022 (MWh)	2023 (MWh)	2024 (MWh)
Data centers	14 426 600	17 659 000	20 806 200	24 294 900	30 825 600
Office and other facilities	740 200	628 100	970 000	1 012 100	1 354 300
Total	15 166 800	18 287 100	21 776 200	25 307 000	32 179 900

Meanwhile, Microsoft has stopped reporting the full energy consumption breakdown for their operation as of 2022 with the later reporting choosing to use more general greenhouse gas (GHG) values to highlight their share of renewable energy use and energy consumption. The latest energy consumption breakdown from 2021 report [34: p. 101] is shown in Table 2. However, due to uncertainty in the meaning of 'within organization' the values may not contain electricity used by public cloud instances that Microsoft is not directly responsible for.

Table 2. Microsoft electricity consumption by fiscal year. [34: p. 101]

Electricity consumed within organization	FY17	FY18	FY19	FY20	FY21
Total (MWh)	6 344 700	7 357 636	8 744 834	10 244 377	12 969 393

Due to Telia being an ISP with both a backbone internet routing capabilities and datacentres their environmental reporting is very relevant to the thesis' subject matter. Similarly to Microsoft, Telia [35: p. 93] states total electricity consumption for the organisation, however in the text Telia clarifies that 95% of the consumption of electricity is caused by network operations and datacentre either directly or indirectly hence the results can be shown in Table 3. Report also highlights that the drop in electricity consumption from 2023 to 2024 was caused by Telia's divestment from Denmark.

When the metrics between Microsoft, Telia and Google (Tables 1-3) are compared it is easy to see that even with the bigger backbone networking side Telia is not nearly as big electricity consumer directly as multinational companies. And according to Table 2 Microsoft has had ~15% consumption rise through financial years 2017-2020 while from 2020 to 2021 it rose to 21%. Comparatively Telia has had ~2,6% rise in consumption whereas Google consumption rise stayed under quarter through years 2020-2023 but rose to ~27% from 2023 to 2024.

Table 3. Telia Company electricity consumption by year. [35: p. 93]

Electricity consumed by source	2022	2023	2024
Network and datacenter[1]	1 148 165,25	1 177 783,4	1 040 917,85
Office and others	60 429,75	61 988,6	54 785,15
Total (MWh)[2]	1 208 595	1 239 772	1 095 703

It is possible that Microsoft has determined that its competitors such as Google are too far ahead of them and therefore chosen to discard previously used metrics such as electricity use throughout organization and even power usage effectiveness (PUE) value while emphasizing GHG more than previously. One indicator that seems to support this assessment is that in 2024 report [36: p. 14] Microsoft states they have reached their datacentre design PUE of 1,12 while the competition Google [33: p. 108] for instance state being under 1,10. Comparatively Telia Helsinki datacentre, being the only datacentre entity from Telia that provides such an indicator state <1,12 is their target PUE.

According to [27] PUE value differentiates the ratio of power consumption through IT system and its auxiliary operation needs in datacentre in its usual operation. For example, PUE value of 1,12 indicates that the IT equipment consumes directly 1 kWh while its auxiliary operation requirements of cooling and air flow moderation systems consume 0,12 kWh. Being as near to PUE 1,00 as possible is therefore the optimal one.

Due to paradigm of information security measures not considered on the matter of energy use as widely as general IT and the inherent work required in determining the separated power usage details for IT system and its possible information security measures the IT power usage statistics have generally been used in place of a divided power usage details for both information security and IT.

2.3.1 Power stability vs availability in IT

As detailed in subchapter 2.2 the addition of IREs can incur a destabilizing effect between power grid generating and consuming segments and while modern IT systems cannot be used directly in generating segment it is possible that a specially constructed without reliance on x86

[1] Calculated electricity consumption with the assumption the stated network operations and datacentre consumption of 95% is constant through the years, even with divestment from Denmark.
[2] According to Telia Company the MWh value includes multitude of electricity consuming devices ranging from office lighting and datacentre cooling and heating systems to leased EVs.

is able to function, however even in such a case destabilizing effect could make the supporting IT system intermittent as well due to IREs voltage oscillation.

If IT system is behind a transformer or inverter and battery solution the effect of intermittent sources is not directly affecting it, instead the auxiliary effect of it taking more power than available may cause the battery solution to drain faster than intended inadvertently causing the stored energy to deplete hence leaving no energy available for other devices. These other devices can be anything from lighting to electrical heating systems and therefore can be critical to the inhabitant's wellbeing.

At the moment the power stability is not taken into account in IT system operations due to modern systems using components that are not easily customizable by end user or organization and for example while modern x86 processors have some selection in their own operation for instance how resource intensively and quickly any received jobs are done with algorithms such as race to idle [37] it is not able to take any external variables such as voltage or frequency changes into account during its normal operations.

The primary reason is that there is no software or hardware linkage that could provide the required information in the required timeframe to the x86 processor. The only comparable feature is the automatic overclocking algorithms that work in junction in AMD Ryzen 2nd generation x86 processors are named Extended Frequency Range 2 (XFR 2) and Precision Boost 2 (PB2).

If enabled these algorithms will consider various variables such as CPU temperature and available cooling, CPU power and CPU maximum clock to set a custom overclocking target for more of the cores in the multi-core CPU and it constantly reexamines the variables to then modify the target values up or down in accordance with any variable changes with the primary goal of keeping the CPU running at the utmost maximum overclock setting at all times. [38]

XFR2 and PB2 are comparable because it constantly reexamines variables and, if necessary, readjusts the CPU power settings. However, the algorithms are limited to variables seen in CPU sensors and would need major redesign by AMD to take advantage of external electricity variable data from exchange electricity monitoring devices or something similar. The new design, however, could add a new attack vector.

As of now direct application level execution throttle controls on hardware itself are not ready for changing needs driven by PSF. In June 2025 documentation of major virtualization

platforms VMware ESX, Windows Hyper-V, Proxmox and Docker shows that organizations using virtualization and container technologies to separate hardware from workloads could use their respective execution throttle controls to downscale electricity consumption of each workload in organization periphery.

However, depending on the organization documentation maturity of each workload the thresholds could need further documentation to be use in downscaling the overall electricity consumption. Additionally, based on the documentation each of the considered virtualization platforms do not offer automated execution throttle capabilities hence using execution controls would require human resources during initial application and in any future monitoring and management activities. Thus, even with virtualization organizations cannot get the full benefits of a flexible power consumption within IT systems.

2.4 Cybersecurity power consumption

Cybersecurity technologies are built on top of existing IT systems or in some cases new technologies are built with cybersecurity in mind with the aim of replacing the older more vulnerable technologies such as the plain-text remote control protocol telnet which was introduced in early computing era and therefore cybersecurity was not taken into consideration during its inception like it was with its replacement SSH or Secure Shell.

Main proponent of why the old technologies was built that way is that cybersecurity was not as expansive field then as it is today and the paradigm shift of general computing connecting large sections of the world together into one worldwide network has made the threat map for organizations and users more complex where old technologies are not viable. Due to cybersecurity being built this way determining power consumption cost of different approaches can be problematic if there is no possibility to separate IT power consumption from cybersecurity.

In [10] it is stated that cybersecurity is an ongoing process for organizations and users because each of them needing to follow some level of information security practices to protect their systems or in case of users' digital identity information such as login credentials. For organizations cybersecurity program maturity determines the viable practices and how widely each of them is implemented. Meanwhile for users the familiarity with social engineering attacks such as phishing emails and malicious software install prompts on infected websites called Click Fix campaigns allow them to safeguard their credentials.

Typically, the nature of organization cybersecurity is in constant flux due to changing needs and everyone inside said organization having their own workflows that may require additional software or capabilities and as such cannot be easily changed without incurring a negative effect on their productiveness. If thorough application controls for example are not enforced users may use software that has not been classified as safe to use in certain regulatory areas. Malicious actors aim to use this and therefore the threats organizations face can be in the most simplistic term: anything the actors want.

To control holistically the organization cybersecurity threat map there are selection of administratively leaner and heavier types of cybersecurity frameworks and standards available that deal with high level disciplines such as organization type, endpoints and their protection levels & response and their individual controls. In [10], one of the leaner ones, NIST's Cybersecurity Framework (CSF) is highlighted as one fitting the sustainable cybersecurity ecosystem requirements. CSF's main principle is to assess risks before any control mechanisms are considered and this works well with Security-First Compliance approach. The approach is cyclical in nature and contains aspects such as risk, asset and threat map management before considering the industry specific aspects.

Through the above paragraphs it can be determined that cybersecurity is not limited to technical solutions or control mechanisms but instead contains also administrative aspects that can be used to dictate the technical solutions in use and the broader organizational information security policies. Policies that can be used to dictate the used software, messaging methods within organization & third parties and how data is controlled.

However, for smart grids to be resilient against cyber based threats all parties need to follow the best practices for securing their power system communication networks which may prove both problematic and resource intensive due to the relevant sections of standards being under constant revisions or extensions by the IEC TC57 working group 15 as detailed in [10: p. 10]. The constant changes can cause parties to select one of the available standards and then stay with it undetermined amount of time before assessing the new ones or parties following different standard revisions if proper communication channels between the parties are not established for this need.

2.4.1 Effects on cybersecurity

One direct effect of more industries needing cybersecurity professionals is human in nature. Cybersecurity professionals will need to familiarize themselves with the newly introduced industries, their respective standards and typical operating manner with also in the case of smart grid keeping their knowledge on the matters up-to-date constantly. This inadvertently can cause further specialisation within cybersecurity as well, similarly to current fields of information technology (IT) and operating technology (OT).

Evolution of smart grid is known as smart cities whereby technology supporting smart grid is also implemented through the whole city proper which in turn would allow precise control of each subset of city operation. The cybersecurity risks arising from the implementation could be controlled through the risk management system specifically crafted for such a case called Hybrid Smart City Cyber Security Architecture (HSCCA). [10: Ch. 9] However, due to the scale increase in smart city the citizens and separate organizations would also need to be empowered and provided with proper cybersecurity knowledge to get the most benefit out such a system.

Similarly to non-cybersecurity side of IT the AI technologies have been implemented across different cybersecurity systems to get further efficiency increases to individual workloads or better detection of anomalies in behavioural analytics. In [10] the Cybersecurity Autonomous Machine Learning Platform for Anomaly Detection or CAMLPAD is highlighted as one possible anomaly detection system, this system is a combination of five specialized ML algorithms that have been exposed to among others SNORT, PCAP and Cisco Meraki incidents. Similarly Network Detection and Response (NDR) manufacturers such as Vectra have trained their ML solution with network based attacks while allowing it to work on any network using just the basic TCP / IP stack.

Current ML implementations are relatively recent in cybersecurity solutions and the solutions they are part of usually are more of black boxes than in regular IT due to business interests, their power consumption information can be hidden. However, there are some papers about cybersecurity and ML implementations with IoT [39-40] that detail power consumption. Additionally, research on green cybersecurity [41] has been done, which aims to bridge the knowledge gap between static and dynamic cybersecurity in preparation for the cybersecurity of the future.

In [39] energy consumption of smart home based IoT by on-device ML model is examined while in [40] consumption is assessed for edge IoT within the realm of Software-Defined Networking (SDN). Due the difference in ML workload location both papers are worthwhile due to the approaches highlighting the difference between the two: edge computing generally is not as resource constraint as the IoT devices themselves and therefore the solution must be smaller in latter option.

In [41] the discipline of green cybersecurity as inclusion of environment into the equation of cybersecurity is explained and previous research on the matter is thoroughly detailed. Through previous research and background information it is shown that motivation for the new discipline comes primarily from green way of thinking rather than worries about power usage causing problems for other consumption targets. Furthermore, paper states that there is increasingly need for the development of "AI-driven adaptive systems" that would be able to control the cybersecurity complexity level in line with current needs, in real time.

However, so far such an adaptive system is only found as theoretical system but the paper underlines that at its most complex form such a system would need to be able to get real time electricity information similarly to a smart meter device and have integration to multitude of additional levels of the system with three major ones being cybersecurity complexity controls, overall usage level (network usage metric for active network devices, etc.) and Dynamic Resource Scaling (DRS) controls. Depending on the location of the workload the DRS could for example allow system to adaptively to wake up or hibernate additional nodes. [41]

While there have been research determining the energy cost of cybersecurity in encryption algorithms [42-43] and protocols [44] generally the cybersecurity energy cost has been rolled into the information systems energy costs which was in 2014: 830 TWh or 0.5% of total electricity consumption [24: Fig. 3]. And in further comparison the maximum generated power through nuclear, oil and coal in factory automation video game Satisfactory is between ~0,514% - 0,590% of it, depending on how much production chain boosting mechanics are used (Appendix 1).

In [42] the difference in power consumption with cryptographic algorithms is investigated using the variables of encryption key size and algorithm. The paper reaches a multifaceted conclusion that due to the observed behaviour being either constant or linear depending on the load suggestion of offloading or fragmenting of the load to additional nodes if possible and that datacentre operators could do runtime optimizations where a more efficient algorithm is

selected for the needed use case is highlighted. Furthermore, paper also states security mechanism energy use could even be used as marker for anomaly detection purposes.

In [43] the power consumption of IoT security algorithms and protocols are investigated and according to it the paper is the first that considers the transmission and computational parameters of the full activity from initial session establishment to closing session after sending data packets. This is achieved by collecting CPU cycle data from the devices hence using similar method to [42]. Paper concludes that transmission cost was not major contributor to power consumption during the session setup phase whereas during the session runtime phase this proved to be reverse.

In [44] the power consumption of various cryptographic algorithms is investigated before assessing the total power consumption of commonly used security protocol SSL. Paper states that their work is the first one that does this holistically first assessing the cryptographic algorithms that commonly used as security protocol building blocks and then separately assessing the complete security protocol SSL. To accomplish this a testbed consisting of real time-current monitoring, iPAQ PDA device and OpenSSL implementation was built. The found results indicate asymmetric algorithms are most expensive while also being the most effected by the used key sizes. These and SSL results lead the paper to the conclusion that dynamic security protocols could be able to be used when constant but, in some cases, excessive power consumption is not viable.

In the [42] paper investigating cryptographic algorithm's energy cost a combination of java and python application was built for data collection and processing purposes with the collection capability being included into the python side. The custom built data collection side follows the amount of CPU cycles used, however due to similar functionality included in pre-existing *codecarbon* python program while also including additional useful features for the thesis' experiment portion *codecarbon* will be used in experiments instead of building a custom solution for it.

2.4.2 Scalable cybersecurity as alternative

Because of the IoT market penetration surging its individual development areas have been given more resources which has resulted in many viable protocols for low-power systems. Protocols that have been built with certain concessions in level of confidentiality, integrity and availability

to reach the intended use case for the individual cybersecurity solution within IoT devices hence allowing better security between them.

Similarly, there have been advances in building distributed router solutions which is a further advancement in distributed computing discipline. Depending on the overall organization size they could see benefits in implementing distributed router solution due to it allowing easier upkeep. Cybersecurity measures could be shared in a comparable manner in network devices as part of the distributed router solution or as an extension of it.

In [41] a DRS capability for a next-generation adaptive cybersecurity solution is proposed with the capability allowing the system to down or upscale the workload complexity and scale or location. For example, in a hypothetical situation the system could move the cybersecurity workload from distributed nodes to dedicated hardware when it determines that the situation requires it due to network congestion or probable active attack. The nodes could be hardware constrained active network devices such as routers while the latter a dedicated firewall or IPS solution.

According to author topologically this kind of cybersecurity solution would be best in router on a stick or mesh networks due to other topologies adding further hops and therefore complexity while possibly routing traffic through network segments that are not aligned with the requirements for the source network segment. Through [42] the possible capability for the system to also change cryptographic algorithms to more efficient one temporarily is found, in this situation the supporting information security technologies would need to have some level of support for it as well, otherwise the system could generate false positive detections upon detecting cryptographic algorithm change.

According to [45] a similar functionality is found in IT power conserving technique proxying where an idling computationally robust network device would offload their presence in the network to other node or specific integrated low-power hardware in the network to curtail excess power consumption caused by unnecessarily keeping the more expensive device in idle state. Implementations of it are not new and have become part of pre-existing operating systems Mac and Windows however as stated by [45] the implementations have not dealt with cybersecurity feature sets and therefore expanding into cybersecurity will lead to additional engineering challenges in how cybersecurity features are moved from device to device without compromises to data integrity and confidentiality.

For automated driving a novel decision offloading mechanism is proposed in [46] which uses timing determinations as the mechanism for assessing which decisions are to be offloaded to edge and which are kept on the local decision computing hardware. The paper used simulation with latency variable to determine the viability of the solution within different distances between the vehicle and obstacle. Paper [46] concludes that proposed solution provides up to 54% energy consumption savings than constant local decision hardware usage. This proposed system is close to workload shifting capability need of still theoretical next-generation adaptive cybersecurity solution however, due to the paper [46] being limited to simulation the real-world viability of the system is unknown. Even with this limitation the proposal could prove useful in determining the implementation for adaptive cybersecurity solution.

3 Cybersecurity power consumption experiments

Through the application of qualitative and quantitative methods in literature review section it was determined that datacentre power consumption has somewhere between 400-460 TWh in 2024 with some forecasts indicating it's doubling in four years due to demand for AI technologies and other computationally expensive technologies. Similarly rising digitalization has increased the number of active endpoints and active network devices, with some of them including local AI technologies. This demand is happening simultaneously with global need for curtailing excess energy consumption and implementing flexibility throughout all facets of society without causing further pollution.

The driver for society flexibility is driven by PSF which is in turn driven by change in electricity generation location from the old, dedicated location system to the new distributed one where each section of the electricity grid may contain intermittent renewable energy sources that will not be able to generate stable electricity which requires ESPs to use precise controls throughout the electricity grid to keep the grid frequency stable. Otherwise, ESPs could risk electricity grid collapse resulting at their worst in sudden non-managed blackouts that could take enormous number of resources to solve.

Throughout the literature review current flexibility support in common network devices being not available and future implementation being far from becoming available in near-term became clearer. Due to these findings an experiment of currently available cybersecurity technologies was planned to determine the current impact of various cybersecurity feature sets. Two of the experiments focus on active network devices such as consumer level router and small-business to large business next-generation firewall (NGFW), these experiments share the ability to toggle more expansive cybersecurity feature on and off as the device operator wants to. Meanwhile, for the last experiment a host intrusion detection system (HIDS) with license based cybersecurity feature set was selected.

The router and NGFW were chosen as experiments due to both having the option to toggle additional cybersecurity features on-demand and there being a knowledge gap about the power consumption of these features. Meanwhile, the HIDS was selected due to it allowing only license based feature selection meaning that without changing licenses system operator cannot control its cybersecurity complexity and furthermore, there is also a knowledge gap how each feature set consumes power.

Therefore, this chapter is devoted to three experiments with the first one using electricity monitor to determine the delta between cybersecurity feature sets while the second investigates the NGFW brochures and based on them answers the research question with the last experiment looking into the Open Source HIDS SECurity (OSSEC) and how much its processing need changes when feature set changes. Experiments will be supported with statistical analysis and comparisons between similar device types found in experiment.

3.1 TP-Link Archer AX55

In this experiment the TP-Link Archer AX55, EU version 1.0.4 Build 20240521, is tested in four different scenarios, during which there will be two variables network load and the state of Home Shield service included in the device as shown in Table 4, for all these scenarios the power usage will be taken from the wall by using a wall electricity monitor installed between the router and the wall outlet. Home Shield is TP-Link's router integrated intrusion prevention system (IPS) solution.

Table 4. Archer AX55 scenario variables.

Experiment number	Network load	Home Shield
A.1	Two devices, some activity	Off
A.2	Two devices, all streaming high-quality content	Off
A.3	Two devices, some activity	On
A.4	Two devices, all streaming high-quality content	On

To get modellable electricity usage data the Axel 8050 electricity monitoring device, which will incur ± 2% inaccuracy in the measurements, will be watched by a continuously rolling 60FPS video camera. This will be done because the possibility of small fluctuations in the power drawing is more easily seen from a video without creating further deviations on power usage by raising the monitoring setup complexity.

To make sure that the measurements are not affected by any of the individual devices, internet browsers or DNS caches, these will be purged right before doing one of the scenarios, the same measure will also be done when scenario is switched. Furthermore, the documentation for Home Shield does not clearly state it can be toggled on or off once the subscription it is part of is enabled. Due to these reasons the A.1 and A.2 will be grouped together, similar grouping will be done also to A.3 and A.4.

Through setup experiments it was determined that with an intermittent load the Axel 8050 can update every ~33,333 milliseconds or 2 frames of 60 FPS video however when the LCD refresh cycle was complex changes took double the amount of time to show clearly, hence the following figures will use foremost as the basic divider between measurements and when complex measurements are seen the measurement will be collected only if it stays clear after the full 4 frames.

The highest peak was done by running a speed test through wireless connection to Cinia Oy's Helsinki endpoint while other machine was used to browse websites with some embedded images, however the other portions with slight peaks were from browsing websites with some embedded images on one machine while the other browsed to sites with auto playing media embedded as well. The first two figures will detail the full 30 minutes of recorded data modelled into a line graph, with the comparisons between groupings being shown only as half of it due to clarity reasons.

In the first grouping (Figure 6) Home Shield feature was set to off which showed that idle wattage for TP-Link Archer AX55 with two LAN devices was between 5,2-5,3 W during A.1 while in A.2 it rose to between 5,4-5,5 W. Furthermore, during active website loadings, the wattage peaked at 5,4-5,7 W for A.1 depending on how heavily multimedia objects were used on the page while for A2 it peaked between 5,7-5,9 W. However, the peak during speed test segment stayed the same 8,8 W in both A.1 and A.2.

In the second grouping (Figure 7) Home Shield feature was set to on which showed that idle wattage for TP-Link Archer AX55 with two LAN devices became sporadic between 5,2-5,9 W during A.3 while in A.4 it was more stable between 5,5-5,6 W. Furthermore, during active website loadings, the wattage peaked at 6,1 W with rare occurrence of 6,8 W peak for A.3 depending on how heavily multimedia objects were used on the page while for A.4 it peaked 6 W with rare occurrences of 6,8 W. However, the peak during speed test segment lowered from A.3's 8,8 W to 6,9 W in A.4 with analysis of collated speed test results in Table 5 indicating the cause being the lowering of the total device throughput when both Home Shield is on and multiple devices are streaming high quality video streams.

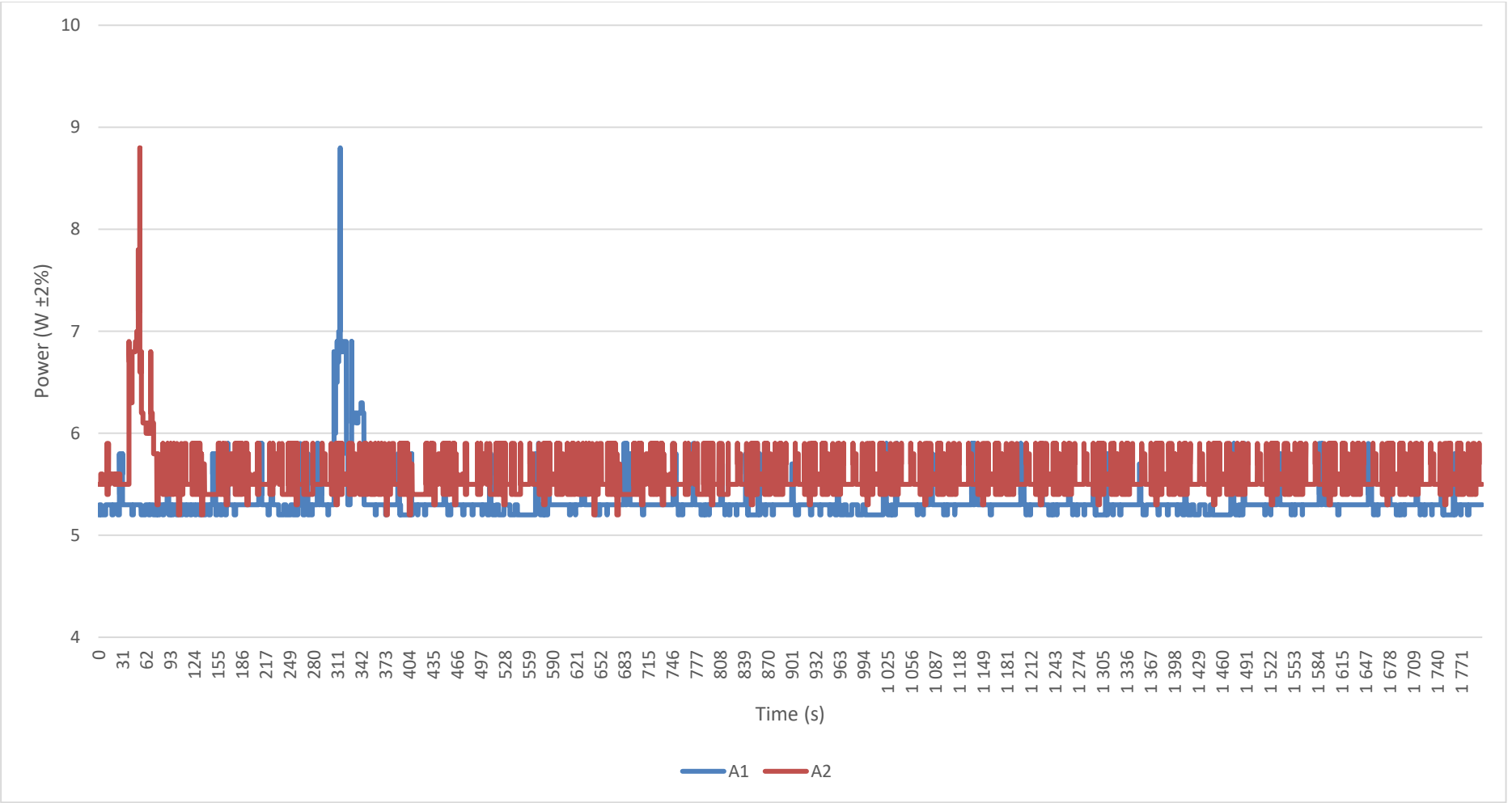

Figure 6. Line graph of electricity consumption for A.1 and A.2.

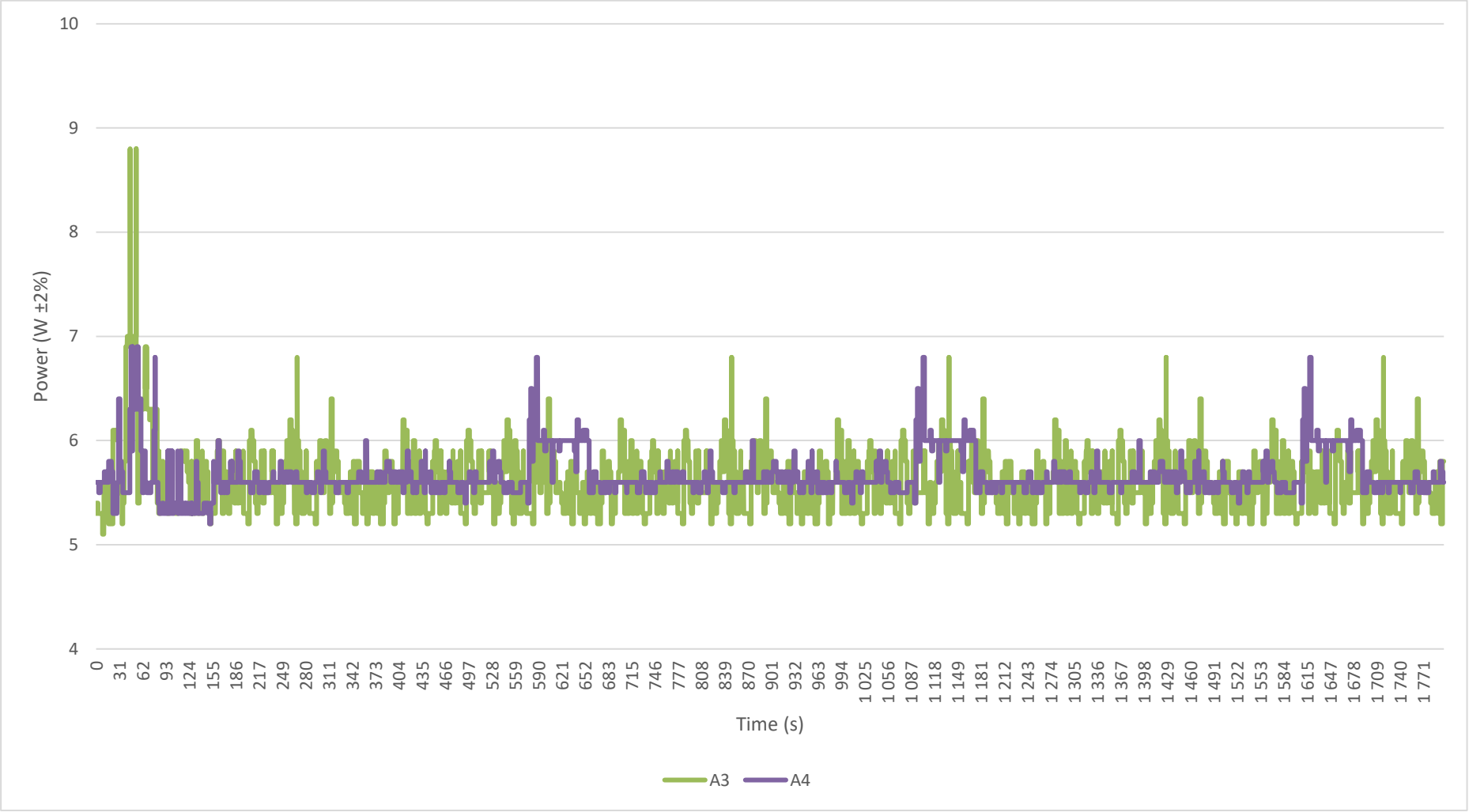

Figure 7. Line graph of electricity consumption for A.3 and A.4.

Table 5. Speed test results for experiments.

Experiment	Ping (ms)	Download (Mbps)	Upload (Mbps)
A1	7	74,60	79,59
A2	4	91,60	83,04
A3	11	82,52	59,74
A4	11	48,39	18,70

By taking only half of the total runtime of the experiments in the following comparisons, it can be clearly seen that the electricity consumption pattern from A.1 changes to more sporadic one in A.3 (Figure 8). Furthermore, when the A.1 and A.3 values are analysed via Excel's variance function the results of 0,033618913 and 0,088612001 are found for each experiment, respectively. These indicate that even in a normal browsing the addition of Home Shield will make the electricity needs more sporadic by 62%.

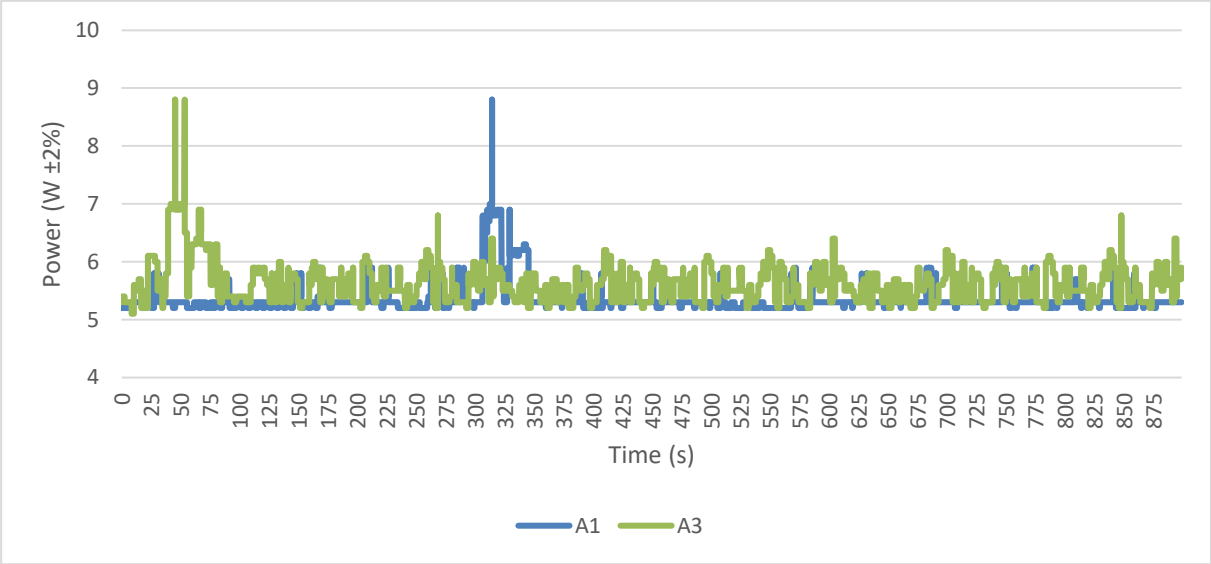

Figure 8. Line graph comparing A.1 and A.3.

When A.2 is compared to A.4 (Figure 9) it can be clearly seen that the same level of electricity consumption variance is not happening as in Figure 9. Instead, the variance between A2 (σ^2 = 0,031744492) and A4 (σ^2 = 0,040907689) drops to 22% when in previous comparison between A.1 and A.3 it was 62%. This could indicate that due to the high quality video streams active constantly on multiple devices the router does not need to vary its electricity consumption to the same level as in experiment where it did not have similar workload active at the time.

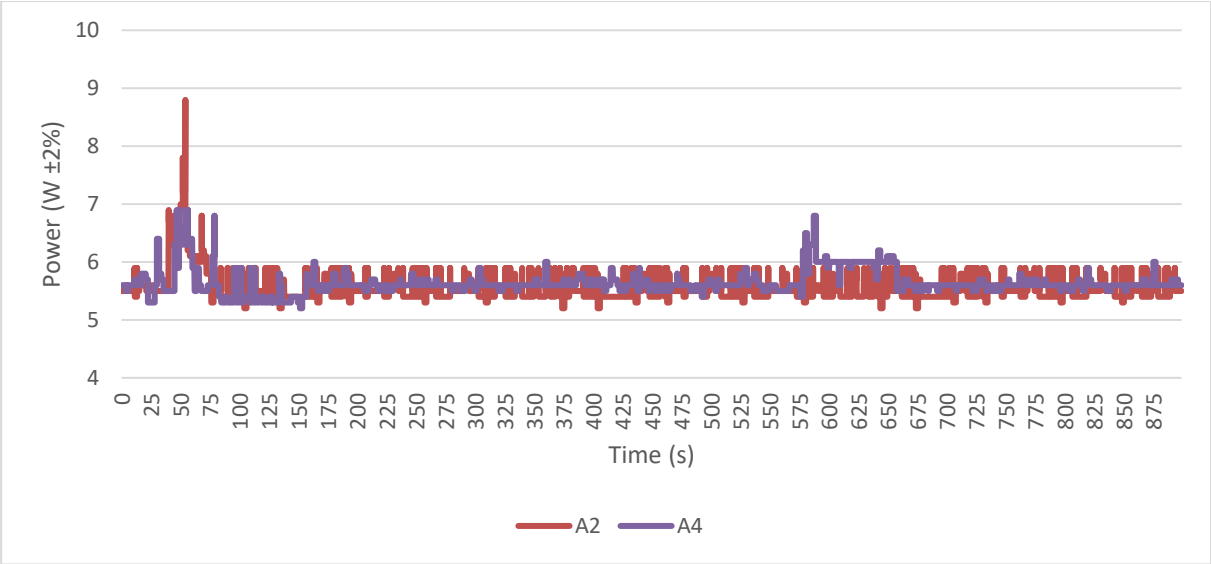

Figure 9. Line graph comparing A.2 and A.4.

Moving to analyse the electricity consumption delta when information security complexity is raised it is found that average power delta between A.1 and A.3 is -0,2672 while for A.2 and A.4 it is -0,1508 (Table 6). This indicates that in the first grouping enabling Home Shield will increase the average power consumption by 4,789 % while in the second grouping it increases only by 2,665 %. If power measurement inaccuracy is considered during calculations, then in both groupings the delta is -0,2674 and -0,1509 respectively which is 4,792 % and 2,668 % hence still being statistically significant.

Table 6. Average power delta with reference experiment in vertical column.

Experiment	**A.1**	**A.2**	**A.3**	**A.4**
A1	0	-0.1922	-0.2672	-0.3430
A2	0.1922	0	-0.0751	-0.1508
A3	0.2672	0.0751	0	-0.0757
A4	0.3430	0.1508	0.0757	0

By comparing the download and upload J/bps shown in Table 7 the download difference of ~11% from A.1 to A.3 and ~ -33% from A.2 to A.4 is found. With the upload difference being ~ -25% from A.1 to A.3 and -71% from A.2 to A.4. While the decrease in both download and upload in the latter comparison group was significant it must be that noted author was not able to control the WAN performance during any of these tests meaning that it is possible that when the experiment or verifications were run the WAN was congested or otherwise performing worse than expected.

Table 7. J/bps based on speed test results with maximum power.

Experiment	Download J/bps	Upload J/bps
A.1	1.1796e-07	1.1057e-07
A.2	9.6070e-08	1.0597e-07
A.3	1.0664e-07	1.4730e-07
A.4	1.4259e-07	3.6898e-07

3.2 Machine learning enabled next-generation firewalls

This experiment is devoted to comparisons of machine learning enabled NGFWs with the technical details being derived from each device's brochures from two companies Palo Alto Networks and Fortinet (Table 8). In the first section a baseline throughput with and without protection is established, afterwards the baseline is used to scale each device's power usage values: average and maximum. With this the result will show the range the scaled power usage would be.

Table 8. Device details derived from brochures.

Device	Throughput with App-ID	Throughput with threat detection	Operating wattage
PA-200 [47]	100 Mbps	50 Mbps	20 W avg, 30 W max
PA-220 [48]	535 Mbps	320 Mbps	21 W avg, 25 W max
FG-30E [49]	200 Mbps	150 Mbps	13 W avg, 15 W max
FG-40F [50]	800 Mbps	600 Mbps	7,74 W avg, 9,46 W max

First step was to find the absolute Joules per bits per second values for both App-ID and threat detection modes. Due to the brochures having both average and maximum operating wattage shown the values under both are shown in Table 9.

Table 9. Devices and their respective J/bps values.

Device	J/bps with App-ID using average wattage	J/bps with App-ID using maximum wattage	J/bps with threat detection using average wattage	J/bps with threat detection using maximum wattage
PA-200 [9]	2.0000e-07	3.0000e-07	4.0000e-07	6.0000e-07
PA-220 [10]	3.9252e-08	4.6729e-08	6.5625e-08	7.8125e-08
FG-30E [11]	6.5000e-08	7.5000e-08	8.6667e-08	1.0000e-07

Device	J/bps with App-ID using average wattage	J/bps with App-ID using maximum wattage	J/bps with threat detection using average wattage	J/bps with threat detection using maximum wattage
FG-40F [12]	9.6750e-09	1.1825e-08	1.2900e-08	1.5767e-08

By selecting the newest Palo Alto firewall, PA-220, as the one comparison is done against the equations 4.2.1T-4.2.3T are found for throughput with threat detection when using the maximum indicated wattage.

$$J/bps\ \Delta_{PA-200} = (7.8125e-08) - (6.0000e-07) = -5.2188e-07 \quad (4.2.1T)$$

$$J/bps\ \Delta_{FG-30E} = (7.8125e-08) - (1.0000\mathrm{e}-07) = -2.1875e-08 \quad (4.2.2T)$$

$$J/bps\ \Delta_{FG-40F} = (7.8125e-08) - (1.5767\mathrm{e}-08) = 6.2358e-08 \quad (4.2.3T)$$

Consequently 4.2.1D-4.2.3D are found for throughput with only App-ID enabled when using maximum indicated wattage.

$$J/bps\ \Delta_{PA-200} = (4.6729e-08) - (3.0000e-07) = -2.5327e-07 \quad (4.2.1D)$$

$$J/bps\ \Delta_{FG-30E} = (4.6729e-08) - (7.5000e-08) = -2.8271e-08 \quad (4.2.2D)$$

$$J/bps\ \Delta_{FG-40F} = (4.6729e-08) - (1.1825e-08) = 3.4904e-08 \quad (4.2.3D)$$

With the maximum wattage numbers gathered the same equations were made for the average wattage values, thereby giving the data detailed in Table 10.

Table 10. NGFW throughput efficiency delta with PA-220 as the baseline.

Device	Threat detection Δ versus PA-220 at average wattage	App-ID Δ versus PA-220 at average wattage	Threat detection Δ versus PA-220 at maximum wattage	App-ID Δ versus PA-220 at maximum wattage
PA-200	-3.3438e-07	-1.6075e-07	-5.2188e-07	-2.5327e-07
FG-30E	-2.1042e-08	-2.5748e-08	-2.1875e-08	-2.8271e-08
FG-40F	5.2725e-08	2.9577e-08	6.2358e-08	3.4904e-08

For easier reading Table 4 with its absolute values has been converted to show only percentages and included as Table 11, with PA-220 average and maximum wattage being used as the reference point.

Table 11. NGFW throughput efficiency delta in percentages with PA-220 as the baseline.

Device	Threat detection Δ % versus PA-220 at average wattage	App-ID Δ % versus PA-220 at average wattage	Threat detection Δ % versus PA-220 at maximum wattage	App-ID Δ % versus PA-220 at maximum wattage
PA-200	-83.5938	-80.3738	-86.9792	-84.4237
FG-30E	-5.2604	-12.8738	-3.6458	-9.4237
FG-40F	13.1812	14.7887	10.3931	11.6347

Based on results shown in Tables 10 & 11 it can be surmised that PA-220 is between 83-86% more efficient than its predecessor in threat detection meanwhile the efficiency distance to the benefit of Palo Alto between the older FG-30E and PA-220 shrink to 3-5%. However, when the new models from Fortinet and Palo Alto are compared the more efficient one switches to Fortinet FG-40F with a lead between 10-13%. Meanwhile when FG-40F is compared to its predecessor the newer model is more efficient by 84-85%.

Similarly, when App-ID efficiency is compared (Tables 10 & 11) it can be surmised that PA-220 is between 80-84% more efficient than its predecessor meanwhile the efficiency distance to the benefit of Palo Alto between the older FG-30E and PA-220 shrink to 9-12%. However, when the new models from Fortinet and Palo Alto are compared the more efficient one switches to Fortinet FG-40F with a lead between 11-14%. Meanwhile when FG-40F is compared to its predecessor the newer model is more efficient by 84-85%.

3.3 Open Source HIDS SECurity

The final experiment in this chapter is used to compare Open Source HIDS SECurity or OSSEC (available from ossec.net) power usage in normal mode and in machine learning mode as shown in Table 12, latter option being available in OSSEC+ which requires user registration. Two systems will be used: Ubuntu 24.04.1 with OSSEC manager and Windows 10 22H2 with OSSEC agent. Furthermore, because in this setup OSSEC does correlations and other related activity in the OSSEC manager it will be installed to the laptop HP Notebook 15-ba074no which will be used as the measurement point.

In this experiment two measurements will be taken via python package *codecarbon* version 2.8.2 (available from github.com/mlco2/codecarbon) which will be used in non-integrated mode to measure the overall power consumption of hardware package with the laptop connected to a power outlet since this will allow it to raise electricity consumption if the workload needs it.

Table 12. OSSEC scenario variables.

Experiment number	**OSSEC mode**
B.1	Normal mode
B.2	ML mode

With the system ready both scenarios were run with the measurements collected into Table 13. However, it needs to be noted that due to the *codecarbon* not being able to measure the consumption for integrated GPU separately in this experiment scenario that value is already contained in the CPU results and hence there is minor uncertainty in how significant portion of the consumption is due to the display. However, since there was no significant graphical workload.

Table 13. Table showing B.1 and B.2 results.

Component	**B.1 (kWh)**	**B.2 (kWh)**
RAM	0,001270808	0,001273650
CPU	0,003751475	0,003758006
Total	0,005022283	0,005031655

Moving on to compare the values with B.1 as the reference point the following delta values are found (Table 14).

Table 14. Absolute delta between B.1 and B.2.

B.1	**B.2** Δ
RAM	2,84158E-06
CPU	6,53077E-06
Total	9,37235E-06

For easier comparison between the results found in Table 14 an additional Table 15 with the percentual delta between experiments is shown, with B.1 being used as the reference point.

Table 15. Percentual delta between B.1 and B.2.

B.1	B.2 Δ %
RAM	0,22310545
CPU	0,17378293
Total	0,18626781

Based on the Tables 14 & 15 the delta is less than half percent in an environment consisting of only one client and OSSEC manager. Due to the one client limitation, it is likely it would increase in an environment consisting of more clients however, determining the level of it is not in the scope of this thesis hence discovering it and its possible implications for information security will be left to other authors.

3.4 Router and Next-Generation Firewall comparison

Due to the difference in variables that were measured, only the first two electricity consumption experiments are comparable directly hence these will be compared in this part. Both TP-Link Archer AX55 and NGFW's share the rudimentary technologies of a firewall, however the casing is the easiest differentiator. NGFW is a specially built firewall device which does not generally include wireless connectivity support and as such is aimed at more demanding use cases whereas AX55 is an all-in-one solution to regular home customers. With these differences noted when results from previous experiments are collated the resulting Table 16. While the workload is not directly comparable between AX55 and the NGFW it is worthwhile considering it.

Table 16. Absolute delta between network devices.

Device	Threat detection Δ versus AX55 at maximum wattage in A.3	App-ID Δ versus AX55 at maximum wattage in A.3	Threat detection Δ versus AX55 at maximum wattage in A.4	App-ID Δ versus AX55 at maximum wattage in A.4
PA-200	-4.9336e-07	-1.9336e-07	4.5741e-07	-1.5741e-07
PA-220	2.8516e-08	5.9912e-08	6.4466e-08	9.5862e-08
FG-30E	6.6408e-09	3.1641e-08	4.2591e-08	6.7591e-08
FG-40F	9.0874e-08	9.4816e-08	1.2682e-07	1.3077e-07

For easier comparison between the results found in Table 16 an additional Table 17 with the percentual delta between experiments is shown, with Archer AX55 maximum wattage during A.3 and A.4 respectively being used as the reference points.

Table 17. Percentual delta between network devices.

Device	Threat detection Δ % versus AX55 at maximum wattage in A.3	App-ID Δ % versus AX55 at maximum wattage in A.3	Threat detection Δ % versus AX55 at maximum wattage in A.4	App-ID Δ % versus AX55 at maximum wattage in A.4
PA-200	-86.9792	-181.3182	-320.7826	-110.3913
PA-220	26.7401	56.1810	45.2106	67.2288
FG-30E	6.2273	29.6705	29.8696	47.4022
FG-40F	85.2152	88.9114	88.9428	91.7071

These findings indicate that the oldest Palo Alto NGFW PA-200 is the most efficient while the other models can be anywhere from 6-88 % less efficient in the full threat detection or 29-91 % in App-ID detection. With above findings on resource consumption throughout different devices and cybersecurity feature sets it can be determined that the level of additional resource consumption that arises from cybersecurity complexity is determined by the device or technology class in that consumer pointed routers with IPS are generally not near the resource consumption level as business pointed dedicated NGFWs.

3.5 Results and analysis

This subchapter is designed to show the impact of rising information security complexity in quantitative metrics for instance money in different countries and the resulting carbon dioxide pollution due to the electricity grid renewable energy exposure. For these reasons, the experiment data from Chapter 3 will be used to get the total kWh values for all scenarios and then the results will be used to calculate the monetary and CO2/kg pollution impact values. To allow accurate calculations to kWh all experiments have been 30 minutes in total length.

Three countries Finland, Germany and Australia were selected for this section based on following metrics: on their share of renewable energy in use, total electricity prices and total electricity grid pollution. These selections highlight the strengths and weaknesses of each country's electricity grid in relation to consumer footprint. Finland can be seen as the mid-point in electricity price with lowest pollution whereas Australia is the lowest electricity price

location with highest pollution. Germany has highest electricity price while being mid-point in pollution.

This division is the result of differing electricity grid policies – some short-term while others long-term. For example, due to long-term investments to nuclear energy in Finland the price is not the highest among the selection while being the least polluting whereas due to Australia's investment to more polluting but cheaper energy sources their prices are not at the level of either Finland or Germany.

The carbon intensity data from *codecarbon* 2.8.2 version (defined as CO2-equivalents) will be used with the pricing data for Finland and Germany being sourced from Eurostat [51] and Australia's pricing data will be from Australian Energy Market Operator (AEMO) [52]. Due to AEMO providing local currency pricing data only in $/MWh format the data will be converted to $/kWh before comparisons. Furthermore, Australian dollar (AUD) prices will be shown next to Euros (EUR) in Australia segments to make comparisons between markets possible. To allow this the 2023's currency exchange rates between AUD and EUR from Bank of Finland [53] are used.

3.5.1 Impact of TP-Link Archer AX55

Doing the kWh conversion for each experiment the resulting Table 18 is found.

Table 18. Archer AX55 experiments with their respective kWh values.

Experiment	kWh
A.1	0,002658162
A.2	0,002754247
A.3	0,0027917754
A.4	0,0028296489

At Finland, the monetary cost increase from A1 to A3 is 0,000024358 € with pollution increasing by 0,010576601 CO2/kg. Similarly monetary increase from A2 to A4 is 0,000013746 € with pollution increase by 0,005968688 CO2/kg (Table 19).

Table 19. Calculation of Archer AX55 impact in 2023's Finland using Eurostat data.

Experiment	EUR (€)	CO2/kg
A.1	0,000484583	0,210414756
A.2	0,000502099	0,21802066

Experiment	EUR (€)	CO2/kg
A.3	0,000508941	0,220991357
A.4	0,000515845	0,223989348

At Germany, the monetary cost increase from A1 to A3 is 0,000039115 € with pollution increasing by 0,050900177 CO2/kg. Similarly monetary increase from A2 to A4 is 0,000022074 € with pollution increase by 0,028724468 CO2/kg (Table 20).

Table 20. Calculation of Archer AX55 impact in 2023's Germany using Eurostat data.

Experiment	EUR (€)	CO2/kg
A.1	0,000778177	1,012626662
A.2	0,000806306	1,04923028
A.3	0,000817292	1,063526839
A.4	0,00082838	1,077954748

In Australia, the monetary cost increase from A1 to A3 is 0,000010262 € with pollution increasing by 0,073312604 CO2/kg. Similarly monetary increase from A2 to A4 is 0,000005792 € with pollution increase by 0,041372419 CO2/kg (Table 21).

Table 21. Calculation of Archer AX55 impact in 2023's Australia using AEMO data.

Experiment	AUD ($)	EUR (€)	CO2/kg
A.1	0,000332462	0,000204155	1,458512224
A.2	0,000344479	0,000211534	1,511233295
A.3	0,000349173	0,000214417	1,531824828
A.4	0,00035391	0,000217326	1,552605714

3.5.2 Impact of Next-Generation Firewalls

Doing the kWh conversion for each device the resulting Table 22 is found. In Chapter 3 it was found that PA-220 is more efficient when compared to its predecessor (83-86 %) or the FG-30E (3-5 %) in threat detection while the lead goes to FG-40F (10-13 %) when the newest models are compared. Meanwhile FG-40F was 84-85 % more efficient than its predecessor. Hence the comparisons will be done in equivalent manner in this part.

Table 22. NGFWs with their respective kWh values

Device	kWh from average operating wattage	kWh from maximum operating wattage
PA-200	0,01	0,015
PA-220	0,0105	0,0125
FG-30E	0,0065	0,0075
FG-40F	0,00387	0,00473

For Finland using the average wattage from manufacturer brochure the Table 23 results are found. In real world impact PA-220 monetary cost is more by 0,00009115 € while polluting 0,039579 CO2/kg more than its predecessor. FG-30E requires 0,0007292 € less to run than PA-220 while also polluting 0,316632 CO2/kg less. PA-220 costs 0,001208649 € more to run than FG-40F while also 0,52481754 CO2/kg more. Meanwhile FG-40F requires 0,000479449 € and 0,20818554 CO2/kg less to run than its predecessor.

Table 23. Calculation of NGFWs impact in 2023's Finland based on average wattage using Eurostat data.

Device	EUR (€)	CO2/kg
PA-200	0,001823	0,79158
PA-220	0,00191415	0,831159
FG-30E	0,00118495	0,514527
FG-40F	0,000705501	0,30634146

Using the maximum wattage from manufacturer brochure the Table 24 results are found. In real world impact PA-220 monetary cost is 0,00045575 € less while polluting 0,197895 CO2/kg less than its predecessor. FG-30E requires 0,0009115 € less to run than PA-220 while also polluting 0,39579 CO2/kg less. PA-220 costs 0,001416471 € more to run than FG-40F while also 0,61505766 CO2/kg more. Meanwhile FG-40F requires 0,000504971 € and 0,21926766 CO2/kg less to run than its predecessor.

Table 24. Calculation of NGFWs impact in 2023's Finland based on maximum wattage using Eurostat data.

Device	EUR (€)	CO2/kg
PA-200	0,0027345	1,18737
PA-220	0,00227875	0,989475
FG-30E	0,00136725	0,593685
FG-40F	0,000862279	0,37441734

For Germany using the average wattage from manufacturer brochure the Table 25 results are found. In real world impact PA-220 monetary cost is more by 0,000146375 € while polluting 0,190475 CO2/kg more than its predecessor. FG-30E requires 0,001171 € less to run than PA-220 while also polluting 1,5238 CO2/kg less. PA-220 costs 0,001940932 € more to run than FG-40F while also 2,5256985 CO2/kg more. Meanwhile FG-40F requires 0,000769932 € and 1,0018985 CO2/kg less to run than its predecessor.

Table 25. Calculation of NGFWs impact in 2023's Germany based on average wattage using Eurostat data.

Device	EUR (€)	CO2/kg
PA-200	0,0029275	3,8095
PA-220	0,003073875	3,999975
FG-30E	0,001902875	2,476175
FG-40F	0,001132943	1,4742765

Using the maximum wattage from manufacturer brochure the Table 26 results are found. In real world impact PA-220 monetary cost is 0,000731875 € less while polluting 0,952375 CO2/kg less than its predecessor. FG-30E requires 0,00146375 € less to run than PA-220 while also polluting 1,90475 CO2/kg less. PA-220 costs 0,002274667 € more to run than FG-40F while also generating 2,9599815 CO2/kg more pollution. Meanwhile FG-40F requires 0,000810917 € and 1,0552315 CO2/kg less to run than its predecessor.

Table 26. Calculation of NGFWs impact in 2023's Germany based on maximum wattage using Eurostat data.

Device	EUR (€)	CO2/kg
PA-200	0,00439125	5,71425
PA-220	0,003659375	4,761875
FG-30E	0,002195625	2,857125
FG-40F	0,001384708	1,8018935

For Australia using the average wattage from manufacturer brochure the Table 27 results are found. In real world impact PA-220 monetary cost is more by 0,000038402 € while polluting 0,274346 CO2/kg more than its predecessor. FG-30E requires 0,000307212 € less to run than PA-220 while also polluting 2,194768 CO2/kg less. PA-220 costs 0,000509204 € more to run than FG-40F while also 3,63782796 CO2/kg more. Meanwhile FG-40F requires 0,000201992 € and 1,44305996 CO2/kg less to run than its predecessor.

Table 27. Calculation of NGFWs impact in 2023's Australia based on average wattage using AEMO data.

Device	AUD ($)	EUR (€)	CO2/kg
PA-200	0,00125072	0,00076803	5,48692
PA-220	0,001313256	0,000806432	5,761266
FG-30E	0,000812968	0,00049922	3,566498
FG-40F	0,000484029	0,000297228	2,12343804

Using the maximum wattage from manufacturer brochure the Table 28 results are found. In real world impact PA-220 monetary cost is less by 0,000192008 € while polluting 1,37173 CO2/kg less than its predecessor. FG-30E requires 0,000384015 € less to run than PA-220 while also polluting 2,74346 CO2/kg less. PA-220 costs 0,000596759 € more to run than FG-40F while also generating 4,26333684 CO2/kg more pollution. Meanwhile FG-40F requires 0,000212744 € and 1,51987684 CO2/kg less to run than its predecessor.

Table 28. Calculation of NGFWs impact in 2023's Australia based on maximum wattage using AEMO data.

Device	AUD ($)	EUR (€)	CO2/kg
PA-200	0,00187608	0,001152046	8,23038
PA-220	0,0015634	0,000960038	6,85865
FG-30E	0,00093804	0,000576023	4,11519
FG-40F	0,000591591	0,000363279	2,59531316

3.5.3 Impact of Open Source HIDS SECurity

Due to *codecarbon* already providing the kWh values for the experiments the conversion is not needed for OSSEC. These absolute values can be found in subchapter 3.3. At Finland, the monetary cost increase from B.1 to B.2 is 0,0000017085 € with pollution increasing by 0,000000742 CO2/kg (Table 29).

Table 29. Calculation of OSSEC impact in 2023's Finland using Eurostat data.

Experiment	EUR (€)	CO2/kg
B.1	0,000915562	0,000397554
B.2	0,0009172705	0,000398296

At Germany, the monetary cost increase from B1 to B2 is 0,0000027435 € with pollution increasing by 0,0035702634 CO2/kg (Table 30).

Table 30. Calculation of OSSEC impact in 2023's Germany using Eurostat data.

Experiment	EUR (€)	CO2/kg
B.1	0,0014702735	1,91323870885
B.2	0,001473017	1,91680897225

In Australia, the monetary cost increase from B1 to B2 is 0,000000719 € with pollution increasing by 0,005142341 CO2/kg (Table 31).

Table 31. Calculation of OSSEC impact in 2023's Australia using AEMO data.

Experiment	AUD ($)	EUR (€)	CO2/kg
B.1	0,000628147	0,000385727	2,755686504
B.2	0,000629319	0,000386446	2,760828845

Based on findings on impact, it can be determined that even with one active client in OSSEC experiment the differences in resource consumption are measurable throughout the benchmark locations and the emphasises in resource consumption differs as expected on the benchmark location characteristics. This can be confirmed by assessing OSSEC's cost difference in all three locations within Finland emphasis is on less pollution while in Australia it is reversed and in Germany centre between these characteristics is seen.

4 Conclusion

As the power system flexibility (PSF) is increasingly incorporated into various areas of the society and each area of the society becomes more flexible information systems will need to be adapted to the new flexibility paradigm through further advances in integrating various systems or by exposing application level power consumption controls to users as support for flexibility. When PSF is successfully incorporated throughout society it could allow society to became more robust in answering to various environmental changes.

In this thesis research questions 1-3 were presented with the aim of determining the level of support for flexibility in IT and how significant delta is between cybersecurity feature sets in different solutions through literature review and experiments, respectively. While there were measurable differences in each completed experiment the answer to RQs was multifaceted and therefore the answers will be provided in detail in sections below. Through RQs the thesis objectives in investigating matureness of current IT system support flexibility, investigation of power draw difference between information security settings and determining difference in location-based metrics were successfully completed.

RQ answers were gained through combination of quantitative and qualitative research methodologies. In literature review section selected material consisted of various documents and interviews which directed author to select grounded theory as data analysis type while in practical experiment and impact assessment portion statistical analysis was used as support to determine theory impact.

Two primary and one secondary data collection methods were used during experiment. For TP-Link Archer AX55 data was collected by externally monitoring an electricity monitoring device with variables of network load and the operation state of its integrated IPS solution tested in four different scenarios. For tracking resource consumption of Open Source HIDS SECurity (OSSEC) a novel resource consumption tracker *codecarbon* was used with variable of machine learning (ML) status in OSSEC manager on a laptop in two scenarios. Whereas for next-generation firewalls (NGFW) manufacturer's brochures were used to calculate efficiency in four scenarios with variables of operating wattage and cybersecurity complexity.

By answering these questions this thesis furthers the current understanding of power consumption in IT and cybersecurity in preparation for the next-generation smart cybersecurity solutions that will adopt the flexibility characteristics from smart grid and distributed

computing. Upon reflection about the overall progress on the thesis the initial plan of incorporating experiments and literature section together through qualitative and quantitative methods can be highlighted as important due to it informing the direction and structure of the work.

5.1. Answer to RQ1

RQ1: What level of flexibility in IT power consumption is available?

During the literature review part, it was found that currently flexibility with electricity consumption is not currently feasible with workloads that are running directly on dedicated hardware. When the workload is moved from dedicated hardware to virtualized environment or to public cloud the electricity consumption flexibility becomes easier due to execution throttle controls on the platform of choice.

However, depending on the platform of choice the controls may not allow automated flexibility which is one of the requirements for the next-generation adaptive cybersecurity solution. This currently theoretical solution will need to interface with multiple different systems and the fully realised solutions could for example move workload from computationally constrained nodes to dedicated endpoint.

To conclude the literature part this investigation highlights the current knowledge and trajectory of IT power consumption reduction technologies. This part informs the experiment part by highlighting the knowledge gap.

5.2. Answer to RQ2

RQ2: How big is the power usage when cybersecurity solution complexity rises?

In the experiment running part the absolute and percentual delta were found for all included experiments and afterwards router-based experiments were compared between each other in the additional subchapter. During the first experiment the results indicated that increasing information security complexity on customer market TP-Link Archer AX55 could increase power consumption by 2,66-4,79 %.

Second experiment results of NGFW showed that enabling the ML based threat detection mode could incur a up to 50% throughput penalty in Palo Alto devices while it could be 25% for Fortinet devices. When efficiency between manufacturers was compared the results showed

that PA-220 is 3-5% more efficient than the older Fortinet while newer model takes the lead of 10-13%. Interestingly when older PA-200 is compared the lead stays with Fortinet with results of 67,5 % and 95,16 % respectively.

In the last experiment where the complexity increase of OSSEC without and with ML functionality enabled was assessed using *codecarbon* python library. The results of it indicate that in environments with few consumer devices the increase is ~0,19 % for the whole laptop hosting OSSEC with RAM and CPU power usage increasing by 0,22 % and 0,17 % respectively.

To conclude the research part the findings were consistent with the research presumption that increasing the information security complexity on devices or software that offer options for it will increase electricity consumption by measurable levels. This part furthers the current understanding of power consumption in cybersecurity by highlighting the delta between feature sets.

5.3. Answer to RQ3

RQ3: In what kind of way would the seen power usage affect?

According to firewall vendors the suggested installation topology is that there is constantly one backup in the inline to mitigate the risk of one device becoming faulty. The implications of the this and experiment results are that in a business environment with modern NGFW installed the increase of electricity consumption can increase by factor of 2 if the recommended topology with threat detection is used by inadvertently decreasing the total throughput between network segments.

Furthermore, depending on the usage location of these systems the resulting pollution can vary greatly for example the newest and most efficient NGFW according to the calculations FG-40F has pollution cost of between ~2,123 - ~2,595 CO2/kg in Australia depending on the load level. Comparatively its pollution cost at Finland is not even one quarter (~14%) of it in its highest instead keeping between ~0,306 - ~0,374 CO2/kg. Meanwhile direct monetary operating cost is ~42% higher in Finland at maximum load.

To conclude the impact part for experiment results based on the metrics the direct resource and pollution cost can differ considerably between regions, especially if manufacturer

recommendations are followed. This part furthers the current understanding of the real world cost of different cybersecurity feature sets.

5.4. Limitations and future work

As was written in experiment chapter the observed power consumption delta in OSSEC experiment was not as significant as in other experiments which could be caused by the workload of one log source not being as equivalent to workloads in other experiments. Hence the significance of more log sources could be used as a further research premise in other relevant papers.

It also needs to be noted that the additional throughput data taken from speed test during experiment one was not verified after the experiments and as such it is possible due to network congestion or other problems that the values are not constant. The speed test data was used to determine the Joules per bit moved for experiment one. A workaround for this could have been to host the different speed test workloads in local network.

References

[1] Climate Action Tracker (CAT), “Warming Projections Global Update - November 2022. Massive gas expansion risks overtaking positive climate policies,” COP27, Nov. 2022. [Online]. Available: https://climateactiontracker.org/publications/massive-gas-expansion-risks-overtaking-positive-climate-policies/

[2] S. Boehm *et al.*, “State of Climate Action 2023,” *World Resources Institute*, Nov. 2023, doi: 10.46830/wrirpt.23.00010.

[3] P. R. Shukla, J. Skea, and R. Slade, “Climate Change 2022: Mitigation of Climate Change. Contribution of Working Group III to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change,” IPCC, 6, 2022.

[4] ENTSO-E, “Winter Outlook Report 2022-2023 and Summer 2022 Review: Country Comments,” ENTSO-E, Dec. 2022.

[5] ENTSO-E, “Summer Outlook Report 2023 and Winter Review 2022-2023: Country Comments,” ENTSO-E, Jun. 2023.

[6] ENTSO-E, “Winter Outlook Report 2022-2023 and Summer Review 2022,” ENTSO-E, Dec. 2022. Accessed: Mar. 09, 2025. [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/sdc-documents/seasonal/WOR2022/Winter%20Outlook%202022-2023_Report.pdf

[7] H. Ritchie and P. Rosado, “Energy Mix,” Our World in Data. Accessed: Nov. 29, 2023. [Online]. Available: https://ourworldindata.org/energy-mix

[8] J. C. Baird and J. M. Brier, “Perceptual awareness of energy requirements of familiar objects,” *Journal of Applied Psychology*, vol. 66, no. 1, pp. 90–96, Feb. 1981, doi: 10.1037/0021-9010.66.1.90.

[9] M. Kathiresh, A. M. Subahani, and G. R. Kanagachidambaresan, *Integration of renewable energy sources with smart grid*. in Next-Generation Computing and Communication Engineering. Hoboken, NJ: Wiley, 2021. [Online]. Available: https://app.knovel.com/kn/resources/kpIRESSG0A/toc

[10] S. Sadik, A. Mohiuddin, L. F. Sikos, and A. K. M. N. Islam, “Toward a Sustainable Cybersecurity Ecosystem,” *Computers*, vol. 9, no. 3, p. 74, 2020, doi: 10.3390/computers9030074.

[11] L. Wen, K. Zhou, W. Feng, and S. Yang, “Demand Side Management in Smart Grid: A Dynamic-Price-Based Demand Response Model,” *IEEE Transactions on*

Engineering Management, vol. 71, pp. 1439–1451, 2024, doi: 10.1109/TEM.2022.3158390.

[12] H. H. H. Mousa, K. Mahmoud, and M. Lehtonen, "Recent developments of demand-side management towards flexible DER-rich power systems: A systematic review," *IET Generation, Transmission & Distribution*, vol. 18, no. 13, pp. 2259–2300, 2024, doi: 10.1049/gtd2.13204.

[13] Energy Authority, "National Report on electricity and gas markets in 2024 in Finland," Ref: 2735/040800/2025 8.7.2025. Accessed: Jul. 19, 2025. [Online]. Available: https://energiavirasto.fi/documents/11120570/13026619/National%20Report%20on%20electricity%20and%20gas%20markets%20in%202024%20in%20Finland.pdf/17892681-3825-663f-1efa-4328022653fa/National%20Report%20on%20electricity%20and%20gas%20markets%20in%202024%20in%20Finland.pdf?t=1752124732404

[14] *Commission Regulation (EU) 2015/1222 of 24 July 2015 establishing a guideline on capacity allocation and congestion management (Text with EEA relevance)*, vol. 197. 2015. Accessed: Jul. 19, 2025. [Online]. Available: http://data.europa.eu/eli/reg/2015/1222/oj/eng

[15] Fingrid, "Demand-side flexibility," Fingrid. Accessed: Jul. 22, 2025. [Online]. Available: https://www.fingrid.fi/en/electricity-market/market-integration/electricity-market-development-projects/demand-side-management/

[16] P. Rohdin, A. Molin, and B. Moshfegh, "Experiences from nine passive houses in Sweden – Indoor thermal environment and energy use," *Building and Environment*, vol. 71, pp. 176–185, Jan. 2014, doi: 10.1016/j.buildenv.2013.09.017.

[17] A. Kramers, M. Höjer, N. Lövehagen, and J. Wangel, "Smart sustainable cities – Exploring ICT solutions for reduced energy use in cities," *Environmental Modelling & Software*, vol. 56, pp. 52–62, Jun. 2014, doi: 10.1016/j.envsoft.2013.12.019.

[18] M. Elsisi, M.-Q. Tran, K. Mahmoud, M. Lehtonen, and M. M. F. Darwish, "Deep Learning-Based Industry 4.0 and Internet of Things towards Effective Energy Management for Smart Buildings," *Sensors*, vol. 21, no. 4, Art. no. 4, Jan. 2021, doi: 10.3390/s21041038.

[19] M. I. Saleem, S. Saha, U. Izhar, and L. Ang, "Stability assessment of inverter-based renewable energy sources integrated to weak grids," *IET Energy Systems Integration*, vol. n/a, no. n/a, doi: 10.1049/esi2.12151.

[20] D. Huang, H. Sun, J. Zhang, S. Zhao, and Q. Zhou, “A data mining-based method for mining key factors affecting transient voltage stability for power systems with renewable energy sources,” *IET Generation, Transmission & Distribution*, vol. 16, no. 4, pp. 617–628, 2022, doi: 10.1049/gtd2.12314.

[21] N. Hatziargyriou *et al.*, “Definition and Classification of Power System Stability – Revisited & Extended,” *IEEE Transactions on Power Systems*, vol. 36, no. 4, pp. 3271–3281, Jul. 2021, doi: 10.1109/TPWRS.2020.3041774.

[22] M.-T. Chuang, S.-Y. Chang, T.-C. Hsiao, Y.-R. Lu, and T.-Y. Yang, “Analyzing major renewable energy sources and power stability in Taiwan by 2030,” *Energy Policy*, vol. 125, pp. 293–306, Feb. 2019, doi: 10.1016/j.enpol.2018.10.036.

[23] P. Kivimaa and M. H. Sivonen, “Interplay between low-carbon energy transitions and national security: An analysis of policy integration and coherence in Estonia, Finland and Scotland,” *Energy Research & Social Science*, vol. 75, p. 102024, May 2021, doi: 10.1016/j.erss.2021.102024.

[24] L. Ardito and M. Morisio, “Green IT – Available data and guidelines for reducing energy consumption in IT systems,” *Sustainable Computing: Informatics and Systems*, vol. 4, no. 1, pp. 24–32, Mar. 2014, doi: 10.1016/j.suscom.2013.09.001.

[25] Goldman Sachs, “Data center power demand worldwide from 2015 to 2023, with a forecast to 2030, by major region (in terawatt-hours) [Graph],” Statista. Accessed: Sep. 08, 2025. [Online]. Available: https://www.statista.com/statistics/1546348/data-center-global-power-demand

[26] IEA, “Electricity demand from data centers, artificial intelligence, and cryptocurrencies worldwide in 2022, with a forecast for 2026, by scenario (in terawatt-hours) [Graph],” Statista. Accessed: Sep. 08, 2025. [Online]. Available: https://www.statista.com/statistics/1462540/global-electricity-demand-from-data-centers-artificial-intelligence-crypto-forecast/

[27] IEA, “World Energy Outlook Special Report: Energy and AI,” Jun. 2025. Accessed: Sep. 30, 2025. [Online]. Available: https://iea.blob.core.windows.net/assets/601eaec9-ba91-4623-819b-4ded331ec9e8/EnergyandAI.pdf

[28] E. Masanet, A. Shehabi, N. Lei, S. Smith, and J. Koomey, “Recalibrating global data center energy-use estimates,” *Science*, vol. 367, no. 6481, pp. 984–986, Feb. 2020, doi: 10.1126/science.aba3758.

[29] A. Swetha Priya, S. Kamatchi, and E. Lakshmi Prasad, “Optimized Power Consumption for Intelligent Architecture with AI/ML and IoT Integration,” *E3S Web of Conferences*, vol. 591, p. 08006, Jan. 2024, doi: 10.1051/e3sconf/202459108006.

[30] I. Mavromatis, K. Katsaros, and A. Khan, “Computing Within Limits: An Empirical Study of Energy Consumption in ML Training and Inference,” in *1st International Workshop on Artificial Intelligence for Sustainable Development*, in ARISDE ‘24. July 2024.

[31] E. García-Martín, C. F. Rodrigues, G. Riley, and H. Grahn, “Estimation of energy consumption in machine learning,” *Journal of Parallel and Distributed Computing*, vol. 134, pp. 75–88, Dec. 2019, doi: 10.1016/j.jpdc.2019.07.007.

[32] R. Ratheesh, M. S. Nair, M. Edwin, and N. V. S. S. R. Lakshmi, “Traffic based power consumption and node deployment in green LTE-A cellular networks,” *Ad Hoc Networks*, vol. 149, p. 103248, Oct. 2023, doi: 10.1016/j.adhoc.2023.103248.

[33] Google, “Google Environmental Report 2025,” Jun. 2025. Accessed: Jul. 22, 2025. [Online]. Available: https://www.gstatic.com/gumdrop/sustainability/google-2025-environmental-report.pdf

[34] Microsoft, “2021 Environmental Sustainability Report,” Mar. 2022. Accessed: Jul. 22, 2025. [Online]. Available: https://www.microsoft.com/en-us/corporate-responsibility/reports-hub#sustainability

[35] Telia Company, “Telia Annual Report 2024,” Apr. 2025. Accessed: Jul. 22, 2025. [Online]. Available: https://www.teliacompany.com/assets/u5c1v3pt22v8/4LVJsLuOlr3SbbnB7DT3X/73beb42e5e541b858eb05957247fcb83/Telia_Annual_Report_2024_.pdf#page=65

[36] Microsoft, “2024 Environmental Sustainability Report,” May 2024. Accessed: Jul. 22, 2025. [Online]. Available: https://www.microsoft.com/en-us/corporate-responsibility/reports-hub#sustainability

[37] H. Hoffmann, “Racing and pacing to idle: an evaluation of heuristics for energy-aware resource allocation,” in *Proceedings of the Workshop on Power-Aware Computing and Systems*, in HotPower ’13. New York, NY, USA: Association for Computing Machinery, Nov. 2013, pp. 1–5. doi: 10.1145/2525526.2525854.

[38] AMD, *2nd Gen AMD Ryzen™ Processors: XFR 2 and Precision Boost 2*, (Apr. 24, 2018). Accessed: Dec. 21, 2024. [Online Video]. Available: https://www.youtube.com/watch?v=426hLGoXDbM

[39] N. Tekin, A. Acar, A. Aris, A. S. Uluagac, and V. C. Gungor, “Energy consumption of on-device machine learning models for IoT intrusion detection,” *Internet of Things*, vol. 21, p. 100670, Apr. 2023, doi: 10.1016/j.iot.2022.100670.

[40] S. Jamshidi, K. W. Nafi, A. Nikanjam, and F. Khomh, “Evaluating machine learning-driven intrusion detection systems in IoT: Performance and energy consumption,” *Computers & Industrial Engineering*, vol. 204, p. 111103, Jun. 2025, doi: 10.1016/j.cie.2025.111103.

[41] Y. Usman, C. J. Ihejirika, S. N. Offor, A. Robert, and R. Chataut, “Green Cybersecurity: Leveraging AI, ML, and LLMs to Optimize Energy, Threat Detection, and Sustainability Frameworks,” *IEEE Access*, pp. 1–1, 2025, doi: 10.1109/ACCESS.2025.3602451.

[42] L. Caviglione, M. Gaggero, E. Cambiaso, and M. Aiello, “Measuring the Energy Consumption of Cyber Security,” *IEEE Communications Magazine*, vol. 55, pp. 58–63, Jan. 2017, doi: 10.1109/MCOM.2017.1600955.

[43] J. Winderickx, A. Braeken, D. Singelée, and N. Mentens, “In-depth energy analysis of security algorithms and protocols for the Internet of Things,” *Journal of Cryptographic Engineering*, vol. 12, no. 2, pp. 137–149, Jun. 2022, doi: 10.1007/s13389-021-00274-7.

[44] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, “Analyzing the energy consumption of security protocols,” in *Proceedings of the 2003 International Symposium on Low Power Electronics and Design, 2003. ISLPED ’03.*, Aug. 2003, pp. 30–35. doi: 10.1109/LPE.2003.1231830.

[45] B. Nordman and K. Christensen, “Proxying: The Next Step in Reducing IT Energy Use,” *Computer*, vol. 43, no. 1, pp. 91–93, Jan. 2010, doi: 10.1109/MC.2010.21.

[46] M. Odema, J. Ferlez, G. Vaisi, Y. Shoukry, and M. A. Al Faruque, “EnergyShield: Provably-Safe Offloading of Neural Network Controllers for Energy Efficiency,” in *Proceedings of the ACM/IEEE 14th International Conference on Cyber-Physical Systems (with CPS-IoT Week 2023)*, in ICCPS ’23. New York, NY, USA: Association for Computing Machinery, May 2023, pp. 187–198. doi: 10.1145/3576841.3585935.

[47] Palo Alto Networks, “PA-200 datasheet.” 2014. Accessed: Nov. 29, 2023. [Online]. Available: https://www.paloguard.com/datasheets/pa-200.pdf

[48] Palo Alto Networks, “PA-220 datasheet.” Mar. 24, 2022. Accessed: Nov. 29, 2023. [Online]. Available: https://www.paloaltonetworks.com/resources/datasheets/pa-220-specsheet

[49] Fortinet, “FortiGate/FortiWiFi 30E datasheet.” 2017. Accessed: Apr. 01, 2024. [Online]. Available: https://www.avfirewalls.com/datasheets/FortiGate/FortiGate_FortiWiFi_30E.pdf

[50] Fortinet, “FortiGate/FortiWiFi 40F Series datasheet.” Jan. 30, 2024. Accessed: Apr. 01, 2024. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-40f-series.pdf

[51] Eurostat, *Electricity prices for household consumers - bi-annual data (from 2007 onwards)*. (Dec. 20, 2024) Distributed by Eurostat. doi: https://doi.org/10.2908/NRG_PC_204

[52] AEMO, *Average price*. (Mar. 22, 2025) Distributed by Australian Energy Market Operator (AEMO). Accessed: Mar. 22, 2025. [Online]. Available: https://aemo.com.au/energy-systems/electricity/national-electricity-market-nem/data-nem/data-dashboard-nem

[53] Suomen Pankki, *Valuuttakurssit, kuukauden keskiarvo*. (Mar. 22, 2025) Distributed by Suomen Pankki. Accessed: Mar. 22, 2025. [Online]. Available: https://www.suomenpankki.fi/fi/tilastot/taulukot-ja-kuviot/valuuttakurssit/taulukot/valuuttakurssit_taulukot_fi/valuuttakurssit_short_fi

Appendices

Appendix 1 Maximum power generation in Satisfactory

In this factory building game the player is tasked with the completion of project assembly by doing automation of continuously more complex parts while maintaining one important aspect: player is not allowed to dump excess resources automatically to the environment. Instead, player is encouraged to use any excess resources in other processes or storing it indefinitely.

To accomplish project assembly task player is given access to two production chain efficiency management mechanisms: managing individual production building clock hence allowing under or overclocking which can linearly use to control how much input and output it requires and lastly somersloopingwhich exponentially increases the required power with the benefit of doubling the output. Both mechanics were used in these calculations.

Some of the calculations and modelling of the production chain were done with satisfactorytools.com website. In the first calculation somersloops were not used to increase output of any fuel sources in Table 32 and in Table 33 calculations were done by using all available somersloops in the game to produce the maximum amount of plutonium fuel rods and rocket fuel with plutonium being the higher priority one due to its production being done in assemblers that require only two somersloops to double whereas rocket fuel that is produced in blender requires four.

Table 32. Calculated power generation if somersloops are not utilised.

Fuel Source	**Production (per/min)**	**Burn rate (per/min)**	**Power generated (MW)**
Uranium Fuel Rod	50,4	0,2	630 000
Plutonium Fuel Rod	22,4	0,1	560 000
Rocket Fuel	48904	4,16667	2 934 237,65
Coal	28346,2	15	141 731

Fuel Source	**Production (per/min)**	**Burn rate (per/min)**	**Power generated (MW)**
Total power generated (TW)			4,265968653

Table 33. Calculated power generation if all somersloops are used.

Fuel Source	**Production (per/min)**	**Burn rate (per/min)**	**Power generated (MW)**
Uranium Fuel Rod	50,4	0,2	630 000
Plutonium Fuel Rod	44,8	0,1	1 120 000
Rocket Fuel	50104	4,16667	3 006 237,60
Coal	28346,2	15	141 731
Total power generated (TW)			4,897968595

Based on Tables 32 and 33 the usage of all available somersloops adds ~0,632 TW of power.