TECHNISCHE UNIVERSITÄT WIEN
Vienna | Austria

Modeling Cyber Attacks on Power Grid Consumers

A Comprehensive Threat Analysis and Risk Assessment Framework

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Embedded Systems

by

Alhasan Bondok, BSc
Registration Number 11770995

to the Faculty of Electrical Engineering and Information Technology

at the TU Wien

Advisor: Univ.Prof.in Dipl.-Ing. Dr.-Ing Tanja Zseby
Assistance: Projektass. Dipl.-Ing. Stefan Wilker, B.Eng.

Vienna, 16th April, 2025

Erklärung zur Verfassung der Arbeit

Alhasan Bondok, BSc

Hiermit erkläre ich, dass die vorliegende Arbeit gemäß dem Code of Conduct – Regeln zur Sicherung guter wissenschaftlicher Praxis (in der aktuellen Fassung des jeweiligen Mitteilungsblattes der TU Wien), insbesondere ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel, angefertigt wurde. Die aus anderen Quellen direkt oder indirekt übernommenen Daten und Konzepte sind unter Angabe der Quelle gekennzeichnet. Die Arbeit wurde bisher weder im In– noch im Ausland in gleicher oder in ähnlicher Form in anderen Prüfungsverfahren vorgelegt. Ich erkläre weiters, dass ich mich generativer KI-Tools lediglich als Hilfsmittel bedient habe und in der vorliegenden Arbeit mein gestalterischer Einfluss überwiegt. Im Anhang „Übersicht verwendeter Hilfsmittel“ habe ich alle generativen KI-Tools gelistet, die verwendet wurden, und angegeben, wo und wie sie verwendet wurden. Für Textpassagen, die ohne substantielle Änderungen übernommen wurden, haben ich jeweils die von mir formulierten Eingaben (Prompts) und die verwendete IT- Anwendung mit ihrem Produktnamen und Versionsnummer/Datum angegeben.

Wien, 16. April 2025

Acknowledgements

First and foremost, I would like to express my sincere gratitude to Professor Tanja Zseby for her invaluable guidance, support, and constructive feedback throughout the course of this thesis. Her expertise and encouragement were essential to the successful completion of this work.

I would also like to thank Stefan Wilker and Thomas Reisinger for their assistance and helpful insights during the development of this thesis. Their advice and input were greatly appreciated.

I am deeply grateful to my family, my fiancée, and my friends for their continuous support and encouragement. A special thank you goes to my brother, with whom I have shared many challenges and experiences, both in our personal lives and throughout our studies. Walking this path together has been a meaningful and unforgettable experience.

Kurzfassung

Diese Arbeit untersucht die Risiken koordinierter Cyberangriffe auf Smart-Home- und Internet of Things (IoT)-Geräte, insbesondere im Hinblick auf ihr Potenzial, durch verteilte Lastmanipulation die Stabilität von Stromnetzen zu gefährden. Simulationen von Angriffen auf leistungsintensive Verbraucher wie Elektrofahrzeuge, Elektroherde, Warmwasserboiler und Klimaanlagen zeigen, dass bereits ein moderater Anteil kompromittierter Geräte sowohl lokal begrenzte als auch weitreichende Stromausfälle verursachen kann. Die Schwere dieser Störungen wird maßgeblich von Faktoren wie dem Gerätetyp, der geografischen Verteilung, saisonalen Einflüssen sowie dem Grad der Koordination bestimmt.

Die Machbarkeit großflächiger IoT-Kompromittierungen ist durch historische Vorfälle, wie etwa den Mirai-Botnet-Angriff, hinreichend dokumentiert. Dabei wurden Hunderttausende von Geräten missbraucht, um Distributed Denial of Service (DDoS)-Attacken durchzuführen. Aktuell verdeutlicht die Entdeckung von Backdoors im weit verbreiteten ESP32-Wi-Fi/Bluetooth-Chip erneut die systemischen Schwachstellen innerhalb von IoT-Ökosystemen. Da dieser Chip in über einer Milliarde Geräte integriert ist, offenbaren derartige Sicherheitslücken nicht nur ein erhebliches Gefahrenpotenzial, sondern belegen auch die Realisierbarkeit hochgradig koordinierter Cyberangriffe.

Zur Minderung dieser Risiken wird in dieser Arbeit ein Sicherheitskonzept vorgeschlagen, das etablierte Methoden wie den ISO/Society of Automotive Engineers (SAE) 21434-Standard, MITRE ATT&CK sowie das STRIDE-Modell integriert. Durch die Anwendung zentraler Elemente dieser Ansätze wird eine strukturierte Methodik zur Bedrohungsmodellierung und Risikobewertung entwickelt, die eine systematische Identifizierung und Reduzierung von Schwachstellen in Smart-Home- und IoT-Umgebungen ermöglicht. Die Ergebnisse belegen eine signifikante Reduzierung der Risikostufen und unterstreichen die Wirksamkeit der entwickelten Sicherheitsstrategie.

Schlüsselwörter: Cybersecurity, Blackout, Smart Home, IoT, Threat Analysis and Risk Assessment (TARA)

Abstract

This thesis examines the risks associated with coordinated cyber-attacks on smart home and IoT devices, with a particular focus on their potential to disrupt power grids through distributed load manipulation. Simulations of attacks targeting high-wattage devices, such as Electric Vehicles (EVs), electric ovens, water heaters, and air conditioners, demonstrate that a moderate percentage of compromised devices can rapidly escalate into localized or widespread blackouts. The severity of these disruptions is influenced by factors such as device type, geographic distribution, seasonal aspects, and the level of coordination.

The feasibility of large-scale IoT compromises is well-documented, as evidenced by historical incidents such as the Mirai botnet attack, in which hundreds of thousands of devices were exploited to launch DDoS attacks. More recently, the discovery of backdoors in the widely used ESP32 Wi-Fi/Bluetooth chip has further underscored the systemic vulnerabilities within IoT ecosystems. Given that this chip is embedded in over a billion devices, these weaknesses not only expose critical security gaps but also reinforce the plausibility of highly coordinated cyber-attacks. Such findings highlight the significant risk of these threats, demonstrating that large-scale attacks of this nature are not just hypothetical but a realistic concern for power grid stability.

To mitigate these risks, this thesis proposes a security framework that integrates established methodologies, including the ISO/SAE 21434 standard, MITRE ATT&CK, and STRIDE models. By utilizing key elements from these approaches, the thesis introduces a structured methodology for threat modeling and risk assessment, significantly enhancing the identification and mitigation of vulnerabilities in smart home systems. The findings demonstrate a measurable reduction in risk levels, underscoring the effectiveness of the developed security strategy.

Keywords: Cybersecurity, Blackout, Smart Home, IoT, TARA

Contents

CHAPTER 1

Introduction

1.1 Motivation

The rising popularity of smart home devices, particularly in the areas of entertainment and energy management, is reflected in the increasing usage rates reported by Statista, as illustrated in fig. 1.1 [1]. Modern household appliances and systems are now commonly equipped with wireless communication capabilities, allowing for seamless remote control via the Internet. Devices such as smart thermostats, home assistants (e.g., Google Home and Amazon Echo), and smartphones enable users to manage various aspects of their homes effortlessly, significantly enhancing convenience and usability.

While these technological advancements in smart home systems offer numerous benefits, they also present significant challenges. The increased interconnectivity of smart home devices expands the potential attack surface, exposing households to a broad range of privacy threats and unauthorized control. This risk is further increased by the often overlooked security measures in IoT and smart home devices, as enhancing security requires additional resources and increases production costs, which are factors manufacturers may opt to minimize [2][3]. Although these vulnerabilities might initially appear limited to individual households, the potential consequences are far more alarming. In the event of a coordinated attack targeting multiple households and their high-wattage devices, the repercussions could extend far beyond private homes and establishments. This thesis explores how synchronized cyber-attacks on multiple homes could impact the power grid, one of modern society's most vital and complex infrastructures.

The power grid relies on a delicate balance between energy supply and demand, where unexpected shifts in consumption can disrupt this equilibrium, potentially leading to grid instability, equipment failures, or even widespread blackouts. These fluctuations in power demand can be deliberately induced through targeted and synchronized activation or deactivation of high-wattage devices, such as air conditioners, electric water heaters,

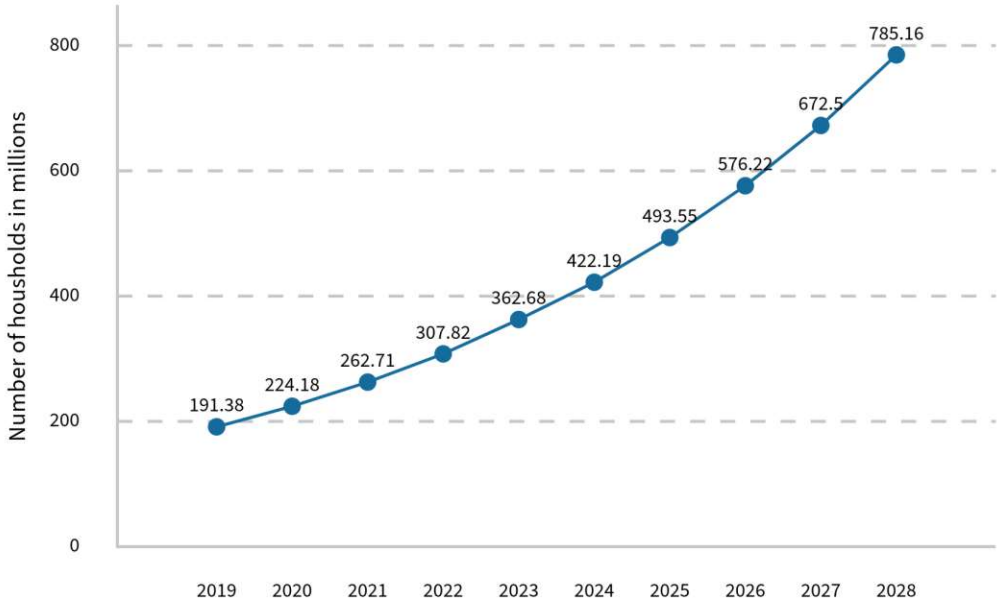


Figure 1.1: Global number of Smart Home users from 2019 to 2028 [in millions] (adapted from [1]).

ovens, and potentially EVs. The increasing prevalence of remote-control capabilities in smart home systems further facilitates such manipulations. What once seemed a far-fetched threat is now a plausible risk. The emergence of the Mirai botnet, which comprised over 600,000 compromised devices, primarily IoT devices, demonstrated the collective impact that IoT vulnerabilities can pose [4]. This scenario highlights a unique cyber-physical landscape where attacks on seemingly low-impact devices can trigger significant cascading effects, particularly affecting critical infrastructures like the power grid.

From the perspective of a power grid operator, such attacks can be especially stealthy, often going undetected because security measures tend to focus primarily on the production and distribution sides of the grid. This gap underscores the importance of understanding these vulnerabilities and the potential for cascading failures to ensure the security and resilience of our power systems.

1.2 Objective

The objective of this thesis is to explore the potential impacts of coordinated cyber-attacks on smart homes and their effects on power grid stability. This is achieved through a combination of literature-based analysis and simulations, with a focus on cyber-attack scenarios involving load manipulation. The literature will inform a high-level understanding of these threats, while simulations will specifically examine their impact on the low-voltage domain. This approach will provide deeper insights into the feasibility of such attacks.

In addition, this thesis will propose and carry out a comprehensive threat and risk assessment for a typical smart home/IoT system, focusing on analyzing specific scenarios in the context of load manipulation to identify and mitigate vulnerabilities. The assessment will leverage methodologies commonly used in the automotive and software development industries, which also target the analysis of cyber-physical systems. A thorough risk evaluation will be conducted to accurately assess vulnerabilities and their impacts, considering various dimensions such as safety, operational, and financial implications. The ultimate goal is to develop and apply a framework that addresses the security of smart home/IoT systems.

The scope of this thesis does not include the preparatory actions involved in conducting cyber-attacks or the specific procedures required to infiltrate a network of devices. It is assumed that a certain percentage of households are already compromised, which serves as the baseline scenario for this analysis. Additionally, the research will not cover cyber-attacks targeting grid control centers or Industrial Control Systems (ICS); the primary focus remains on the consumers and the role of smart home/IoT devices.

This research addresses a critical and emerging area of concern at the intersection of cybersecurity and power grid management. The findings provide valuable insights for grid operators, policymakers, and device manufacturers, emphasizing the necessity of proactive security measures and risk management at the consumer level. The proposed TARA framework offers a systematic approach to enhancing the resilience of modern power grids against evolving cyber threats originating from the consumer domain. Ultimately, this research seeks to contribute to developing more secure and robust energy systems in an increasingly interconnected world.

To achieve these objectives, this thesis will be guided by the following research questions:

- How do coordinated cyber-attacks on smart home/IoT devices affect the stability of low-voltage power grids, particularly through distributed load manipulation? What role do factors such as the number and type of devices, consumer location, and level of coordination play in these impacts?

- To what extent can methodologies from other domains, such as the automotive sector, which also address cyber-physical systems, be leveraged to improve the identification and mitigation of vulnerabilities in smart home systems through comprehensive threat and risk assessments?

1.3 Contributions

The contributions of this thesis are as follows:

- **Comprehensive State-of-the-Art Analysis:**This thesis conducts an in-depth review of existing research on load manipulation of high-wattage devices and their potential role in inducing blackout scenarios. Additionally, a systematic evaluation of existing TARA frameworks is performed. By identifying gaps in the current landscape, this work provides a structured overview of available frameworks and tools, highlighting their limitations in the context of IoT and smart home security.
- **Modeling of Cyber Attacks on Low-Voltage Grids:** This research models cyber-attacks targeting high-wattage devices within the context of low-voltage grids. The simulations evaluate various grid configurations and threat scenarios, including diverse household densities and the infiltration of different types of high-energy-consuming devices at distinct rates (e.g., 5%, 10%, 15% ... 60%). They also incorporate seasonal fluctuations, such as winter and summer, as well as variations in energy demand between morning and evening. These analyses offer critical insights into how compromised smart home devices can influence grid stability and potentially trigger large-scale disruptions.
- **Development of a Tailored Security Framework:** Furthermore, a security framework specifically designed for the IoT and smart home ecosystems is introduced. It integrates and adapts security standards from the automotive industry as well as established methodologies from the software and network security domains. The framework provides a structured set of guidelines, predefined Damage and Threat scenarios and evaluated attack and mitigation strategies, all of which can be directly applied to various security analyses. Additionally, it enables the creation of attack trees, offering deeper insights into attack strategies and system vulnerabilities. This enhances the ability to identify weaknesses and implement effective countermeasures, ultimately improving the resilience of smart home environments.

1.4 Structure

The background chapter provides foundational knowledge by defining key concepts and reviewing historical incidents relevant to power grid security. This section sets the context for understanding the complexities of protecting power grids in an increasingly digitalized world. The discussion then transitions into a comprehensive review of current research on cyber-attacks targeting IoT devices, specifically within the context of power grid disruption. It also examines the existing framework landscape for TARAs. This review establishes the basis for the subsequent presentation of the research methods, including the modeling approach, the choice of tools, and the simulation methodologies employed in this research. Following this, the thesis delves into the specifics of the power grid model, detailing its architecture and components, along with the integration of various attack scenarios. An in-depth examination of the simulation results is presented, focusing on the impact of these scenarios on grid performance and stability. The analysis of the simulation data evaluates the effects of cyber-attacks on grid reliability and resilience, highlighting key vulnerabilities and points of failure. The final stages of the thesis involve introducing a TARA framework and applying it to the findings, providing recommendations for mitigation strategies to enhance the security of power grids against cyber threats. The work concludes with a summary of the key findings, a reflection on the study's limitations, and suggestions for future research directions. This structured approach ensures a comprehensive exploration of the topic and offers valuable insights into strengthening power grid security in the face of evolving cyber threats.

CHAPTER 2

Background

2.1 Energy Consumption - Key Factors and Trends

2.1.1 Overview

Energy consumption in residential and commercial facilities is influenced by a range of factors, such as the efficiency of electronic devices, household behavior, and, most notably, external weather conditions. Furthermore, the ongoing shift toward electrification and sustainable technologies is significantly altering energy demand. Key drivers of this transformation include the increasing use of modern household appliances and consumer electronics, a growing need for temperature regulation systems to address fluctuating weather conditions (e.g., heat pumps and air conditioners), and the rising adoption of EVs. The integration of these large electrical loads into households leads to a significant increase in energy consumption, which would place more strain on the power grid. This section provides an overview of typical household energy consumption characteristics, highlighting key factors and emerging trends.

2.1.2 Household Energy Consumption

In 2023, the average household size in Germany was 2.03 people [5]. The annual electricity consumption of a two-person household in a multi-family apartment building typically ranges from 2000-2300 kWh without electric water heating and increases to 2600–3000 kWh when electric water heating is included. In comparison, a single-family home consumes between 2800 and 3100 kWh annually without electric water heating, rising to 3300–3800 kWh when hot water is included (see fig. 2.1).

Gebäudetyp	Warmwasser	Personen im Haushalt	Verbrauch in Kilowattstunden (kWh) pro Jahr						
			A	B	C	D	E	F	G
Haus	ohne Strom	1	bis 1.400	bis 1.800	bis 2.200	bis 2.600	bis 3.400	bis 4.500	über 4.500
		2	bis 2.000	bis 2.500	bis 2.800	bis 3.100	bis 3.500	bis 4.300	über 4.300
		3	bis 2.500	bis 3.000	bis 3.500	bis 3.900	bis 4.400	bis 5.200	über 5.200
		4	bis 2.800	bis 3.500	bis 3.900	bis 4.300	bis 5.000	bis 6.000	über 6.000
		5+	bis 3.200	bis 4.000	bis 4.500	bis 5.200	bis 6.000	bis 7.600	über 7.600
	mit Strom	1	bis 1.500	bis 2.000	bis 2.500	bis 3.000	bis 4.000	bis 5.500	über 5.500
		2	bis 2.400	bis 2.900	bis 3.300	bis 3.800	bis 4.500	bis 6.000	über 6.000
		3	bis 3.000	bis 3.600	bis 4.100	bis 5.000	bis 6.000	bis 7.500	über 7.500
		4	bis 3.500	bis 4.200	bis 5.000	bis 5.700	bis 7.000	bis 8.900	über 8.900
		5+	bis 4.000	bis 5.000	bis 6.000	bis 7.000	bis 8.200	bis 10.800	über 10.800
Wohnung	ohne Strom	1	bis 800	bis 1.000	bis 1.300	bis 1.500	bis 1.700	bis 2.100	über 2.100
		2	bis 1.400	bis 1.700	bis 2.000	bis 2.300	bis 2.500	bis 3.000	über 3.000
		3	bis 1.700	bis 2.100	bis 2.500	bis 2.900	bis 3.300	bis 3.800	über 3.800
		4	bis 1.800	bis 2.300	bis 2.600	bis 3.000	bis 3.600	bis 4.400	über 4.400
		5+	bis 1.500	bis 2.100	bis 2.700	bis 3.400	bis 4.100	bis 5.500	über 5.500
	mit Strom	1	bis 1.100	bis 1.400	bis 1.600	bis 1.900	bis 2.200	bis 2.800	über 2.800
		2	bis 1.900	bis 2.300	bis 2.600	bis 3.000	bis 3.500	bis 4.000	über 4.000
		3	bis 2.500	bis 3.000	bis 3.500	bis 4.000	bis 4.500	bis 5.500	über 5.500
		4	bis 2.500	bis 3.400	bis 4.000	bis 4.500	bis 5.000	bis 6.400	über 6.400
		5+	bis 2.000	bis 3.000	bis 4.000	bis 5.000	bis 6.000	bis 7.500	über 7.500

A = gering | B = niedrig | C und D = mittel | E und F = hoch | G = sehr hoch

Figure 2.1: Average annual power consumption in apartments and houses (in kWh/year) [6].

However, these figures do not account for the largest contributor to household energy demand: space heating [7]. In Germany, heating remains heavily reliant on fossil fuels. According to the German Association of Energy and Water Industries (Bundesverband der Energie- und Wasserwirtschaft), natural gas was the dominant heating source in 2023, supplying 48.3% of apartments, while oil accounted for 23.4%. District energy (Fernwärme), primarily used in urban areas, covered 15.2% of households. In contrast, electricity, mainly from electric resistance heating and heat pumps, comprised only 7.5%, with an additional 5.6% coming from alternative sources such as liquefied gas, biomass, and wood (categorized as "Other") [8] (see fig. 2.3). A similar distribution is observed in single-family homes.

Recent trends indicate a gradual shift toward electrification. Since 2019, the share of oil heating has declined, while gas usage has seen a slight uptick of 0.1%. Meanwhile, district heating and electric heating have gained momentum, driven by policy incentives and decarbonization efforts [8].

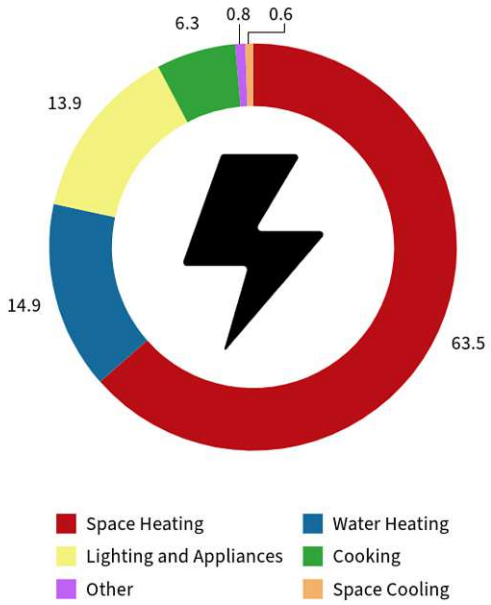


Figure 2.2: Breakdown of final energy consumption in EU households by end use in 2022 (in %) [7].

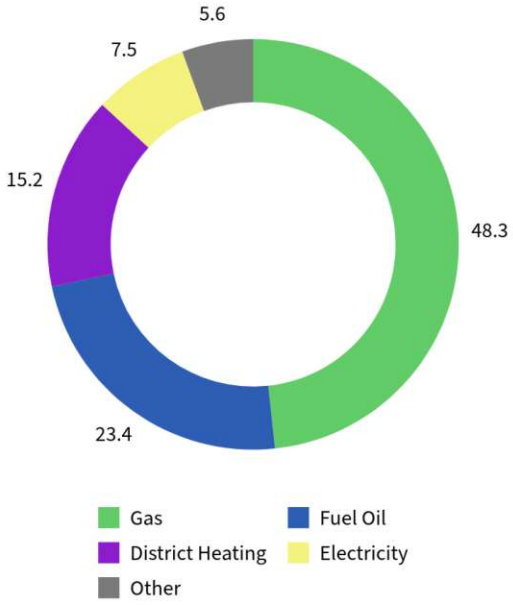


Figure 2.3: Share of energy sources used for residential heating in apartments in Germany, 2023 (in %) [8].

2.1.3 Growing Electricity Demand

The growing adoption of EVs, along with an increasing number of heat pumps and air conditioning units, is expected to raise household electricity demand in the coming years significantly. This trend is influenced by technological advancements, worsening climate conditions, and an evolving political landscape.

EVs

EVs are becoming increasingly popular in Europe, largely driven by growing concerns over climate change and the need to reduce carbon emissions. To facilitate this transition, the European Union (EU) offers financial incentives, such as subsidies, tax breaks, and the expansion of charging infrastructure. Additionally, advances in battery technology have improved the range and efficiency of EVs, making them more appealing to consumers. Figure 2.4 shows the projected rise in EV sales, with estimates surpassing 5.5 million units by 2029 [9].

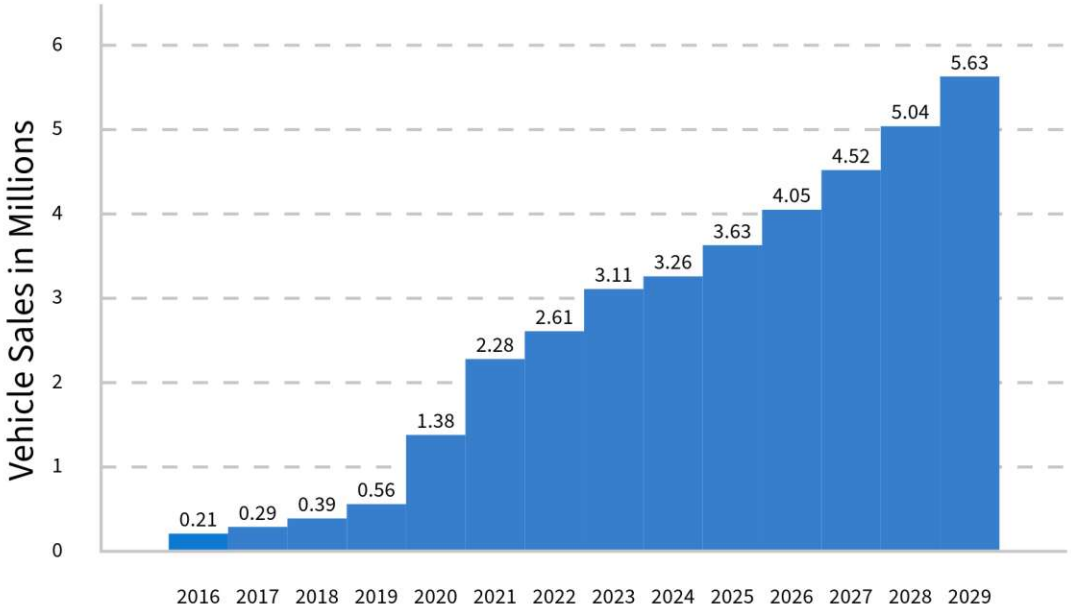


Figure 2.4: Forecasted expansion of EV sales across European markets.

Heat Pumps

Electric heat pumps are increasingly important as a sustainable and energy-efficient alternative to traditional heating systems. By harnessing heat from the air, ground, or water and converting it into usable energy, they significantly reduce carbon dioxide emissions compared to fossil fuel-based heating. The EU actively supports heat pump adoption through grants and regulations, encouraging the transition away from conventional heating systems. While sales saw a substantial rise until 2022, the past two years have witnessed a decline [10]. However, the European Heat Pump Association emphasizes that this downturn does not necessarily indicate a long-term slowdown, as more than 2 million units were sold in 2024 [10].

Space Cooling

The increasing demand for air conditioners and other cooling solutions across Europe is primarily driven by climate change and the increasing intensity of summer heat waves. Air conditioning has become essential for ensuring residents' well-being in many regions, as extreme temperatures have been linked to an estimated 175,000 deaths annually in Europe over the past three years [11]. While modern air conditioners are much more energy-efficient, environmentally friendly, and cost-effective, they still require substantial energy. Projections indicate that global demand for air conditioning will continue to grow, with Europe following this trend [12].

Despite this shift, a complete transition from fossil fuels to electricity remains a major challenge. Europe's current power generation capacity and grid infrastructure are insufficient to handle the increased load from widespread electrification. Seasonal fluctuations in heating demand, combined with the volatile nature of renewable energy sources, further complicate the transition. Without substantial upgrades to the grid and energy storage systems, the rising reliance on electricity for heating and mobility could lead to grid instability, especially during peak demand periods.

2.2 Power Grid

2.2.1 Overview

Our modern power grid is one of the largest and most intricate systems in operation today. It facilitates the transmission and distribution of electrical power from producers to end-users. Electricity generation is diversified, drawing from various sources such as nuclear, hydroelectric, coal, wind, solar plants, and many more.

The grid's operational frequency varies across the globe; most regions in Europe, Asia, and Africa use 50 Hz, while North America operates at 60 Hz. Transmission and distribution processes employ different voltage levels to ensure efficient and safe energy transfer (see fig. 2.5). By increasing the voltage level, the current is reduced, which in turn minimizes resistive losses in the transmission lines and enhances overall efficiency.

Dividing the grid into different voltage levels enables a secure and flexible power supply to various consumers and applications. Using the Austrian power grid [14] as an example, these voltage levels are classified into the following categories:

- **Extra-High Voltage (EHV):** The extra-high voltage level, also known as grid Level 1, primarily serves as the transmission network layer. It is used to transport large quantities of energy over long distances from power plants to the distribution network. Voltage levels in this category typically include 380 kV and 220 kV.
- **High Voltage (HV):** Known as Grid Level 3, the high voltage stage is typically considered part of the distribution network. It is primarily utilized for interregional power transmission and to supply electricity to large industrial consumers and railway systems. Additionally, medium-sized power plants connect to this grid level. Standard voltages at this stage are 110 kV.
- **Medium Voltage (MV):** The medium voltage level acts as the regional energy supply network, bridging the gap between substations and transformer stations that feed into the low voltage network. It caters to larger consumers, such as industrial facilities, as well as urban areas or small towns. This level typically operates at voltages ranging from 1 kV to 36 kV and is also known as grid Level 5.
- **Low Voltage (LV):** As the final stage in the power grid, grid Level 7 is responsible for distributing electricity to end-users, including individual households and small

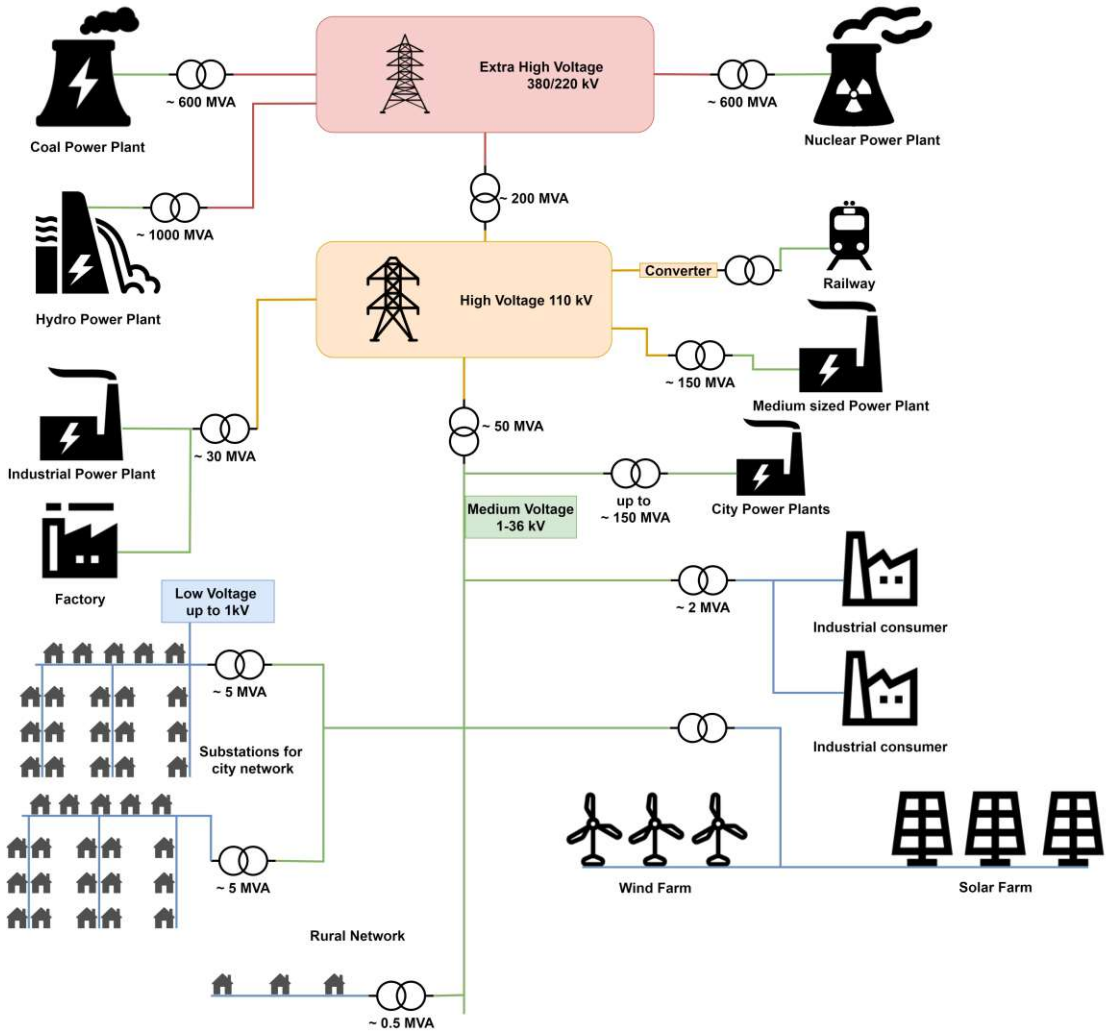


Figure 2.5: A exemplary power grid and its voltage levels (adapted from [13]).

businesses. This power grid segment supports single-phase and three-phase connections, operating at voltages up to 1 kV. It is the most direct interface between the power grid and the general public, ensuring safe and reliable delivery of electricity.

- **Intermediate Grid Levels (2, 4, and 6):** These levels consist of substations and transformer stations that facilitate the transition of voltages between the primary levels, ensuring a smooth flow of electricity throughout the grid.

In addition to the core components of a modern power grid, such as power plants, transmission and distribution networks, substations (responsible for voltage transformation, switching, protection, regulation, and redundancy), and transformer stations, a communication and control network also plays a crucial role. This network plays a key role in maintaining overall stability and reliability, as it is vital for monitoring and managing the grids' operations.

Grid operators depend on centralized control centers to oversee and regulate the flow of electricity in real-time. These control centers are crucial to the operation of power grids, as they ensure a continuous balance between energy production and consumption to maintain system stability and reliability. This real-time oversight is made possible through communication with distributed monitoring devices, such as Phasor Measurement Unit (PMU) and smart meters, that provide critical data on the grid's status. Additionally, the system is equipped with sensors that further enhance monitoring capabilities.

These components contribute to an increasingly complex communication infrastructure, supplying data to the Supervisory Control and Data Acquisition (SCADA) system to enable effective decision-making. It highlights the advanced control mechanisms that regulate the power grid and the strong security measures implemented. However, these expanding communication networks also increase the system's attack surface. Nevertheless, this is a separate topic and is not within the scope of this thesis.

A significant issue persists: despite these advances, a critical grid segment remains largely outside the direct control of grid operators, the end user, along with their connected IoT and smart home devices. This makes the low-voltage network particularly vulnerable, as coordinated and synchronized cyber-attacks at this level could severely disrupt the grid's balance, potentially leading to widespread instability.

2.2.2 Grid Stability and Operation

The stability of the power system is primarily supported by three interdependent pillars: voltage stability, frequency stability, and angle stability, as illustrated in the figure below. Each of these elements is crucial for maintaining a reliable and efficient power grid, ensuring that electricity is delivered safely and consistently to consumers.

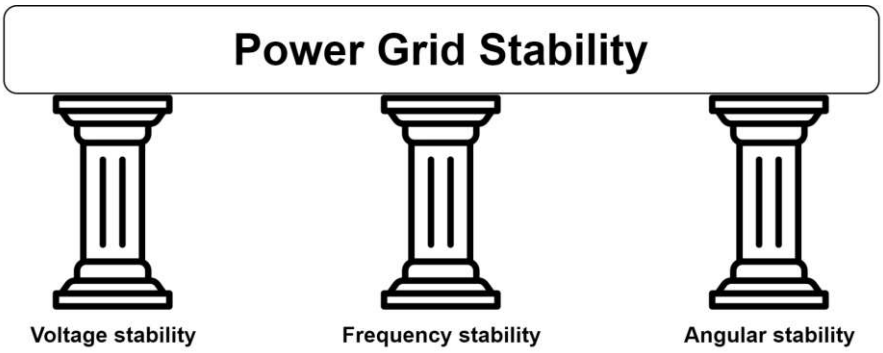


Figure 2.6: Pillars of Power Grid stability

Load Balancing

The most crucial aspect of grid stability is maintaining a continuous balance between energy production and consumption. At any given moment, the energy generated must precisely match the amount being consumed to ensure a stable and secure grid. Any disruption to this balance can lead to outages, resulting in substantial financial losses and various associated issues. This challenge arises mainly from the current limitations in storing large quantities of electrical energy.

To address this issue, grid operators utilize various strategies, including historical data analysis, weather forecasting, and societal behavior analysis, to predict daily consumption patterns and adjust production accordingly. These predictions vary based on the day of the week and season, enabling operators to plan for base load (continuous, minimal energy demand around the clock), mid-load (regular but intermittent additional demand), and peak load (short-term spikes in energy demand), as shown in fig. 2.7.

This process has become increasingly complex with the integration of renewable energy sources, which are inherently volatile due to natural fluctuations and factors like climate change. Balancing production and consumption is essential for maintaining stable grid frequency, voltage, and rotor angle, ensuring the smooth operation of both grid equipment and household appliances.

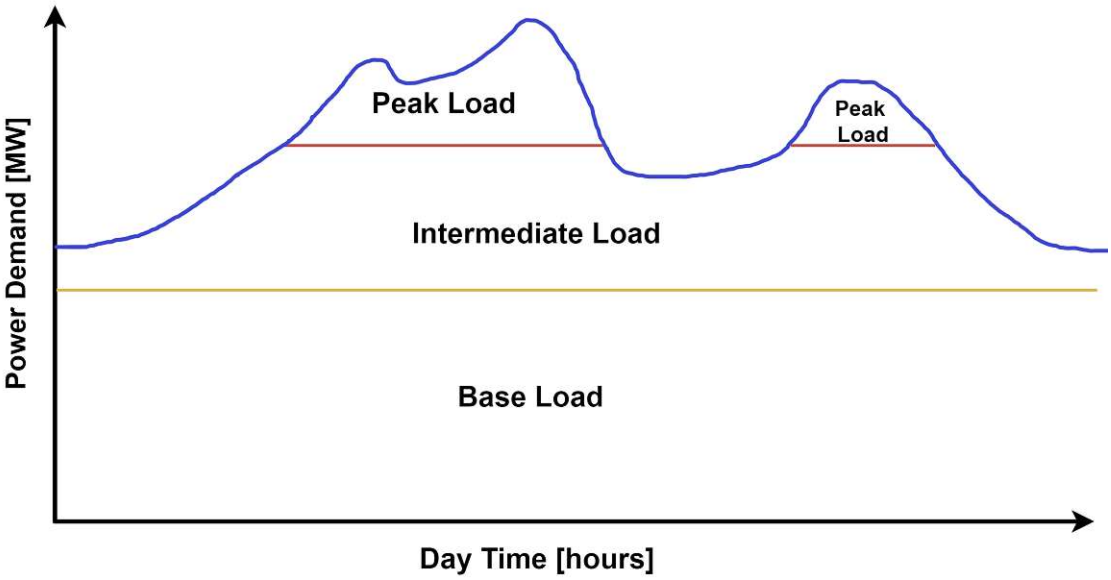


Figure 2.7: Load profile forecasting

Frequency Stability

The frequency of a synchronous system, such as the one used in Europe, is determined by the rotational speed of the generators. To maintain a stable grid, the frequency is regulated to a nominal value of 50 Hz by continuously balancing energy production and consumption. It is essential to keep deviations from this nominal frequency within 0.2 Hz, or 0.004%, to prevent instability [15]. When energy production exceeds consumption, the system frequency increases, resulting in a higher rotational speed, as the excess mechanical energy is not fully converted into electrical energy. Conversely, when consumption is greater than production, the system frequency drops, causing the generators to slow down as the demand for electrical energy surpasses the available mechanical energy.

Both scenarios are problematic, as they can cause significant damage to generators and connected equipment. In extreme cases, a prolonged deviation from the nominal frequency can lead to a grid collapse with severe consequences. To mitigate these risks, several integrated countermeasures are in place (see fig. 2.8):

- **Inertia Response:** This is the first line of defense against frequency fluctuations, leveraging the inertia of the rotating masses of synchronous generators. It provides an immediate response by either releasing kinetic energy during under-frequency or absorbing it during over-frequency, thus temporarily adjusting the rotation speed. This instant reaction is crucial for mitigating small fluctuations and providing time for further corrective measures to be deployed.

- **Primary Control:** Primary reserves comprise power plants (such as nuclear and pumped-storage plants), storage systems, and flexible commercial/industrial consumers that can quickly modulate their output. They can either supply additional energy to the system or absorb excess energy. This response must be fully activated within 30 seconds following a deviation of 200 mHz and should sustain the system for at least 30 minutes [15]. The process is automatic and aims to prevent further deviations, though the frequency may stabilize without returning exactly to the nominal 50 Hz.
- **Secondary Control:** The secondary control mechanism works to restore the frequency to its nominal value and relieve the primary control, allowing it to be ready for further immediate response if needed. The secondary reserve must be fully available within 5 minutes of detecting a deviation and is a regional control mechanism [15].
- **Tertiary Control:** Unlike the other reserves, tertiary control is manually triggered. It supports the secondary reserve in compensating for expected imbalances, aiming to correct these and provide long-term stability.

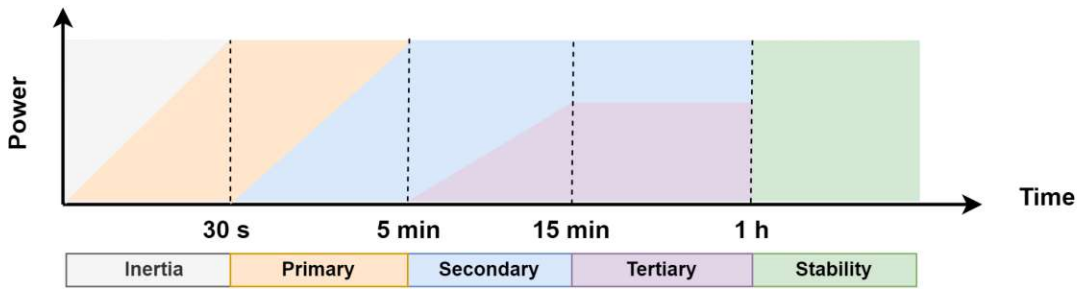


Figure 2.8: Reserve controls and their timing constraints (adapted from [16])

These measures are integral to maintaining grid stability, preventing equipment damage, and ensuring the reliable operation of the power system.

Voltage Stability

Under normal operating conditions, the voltage must remain within a defined range to ensure stability. Regulatory bodies establish permissible terminal and bus voltage levels to guarantee the safe operation of grid infrastructure and devices connected to the network. Significant deviations from these specified levels can lead to serious complications that may threaten the stability of the entire grid.

Sudden changes in demand primarily cause voltage fluctuations. Additionally, faults or failures in system components such as transformers or generators can lead to voltage drops or even complete power loss in certain parts of the grid. The voltage at various nodes in the system is regulated through reactive power management. Voltage stability is compromised if insufficient reactive power is produced, leading to potential grid instability.

Voltage stability is intrinsically tied to the reactance between the voltage source and the load, which is influenced by the inductive and capacitive components within the system, such as motors, generators, transformers, and transmission lines. The load impedance decreases as the load demand increases, resulting in higher current flow. This, in turn, causes greater voltage losses during transmission, leading to a voltage drop on the receiving side.

To assess voltage stability, P-V (active power-voltage) and Q-V (reactive power-voltage) curves are commonly used to depict the relationship between voltage and power flow (see fig. 2.9). These curves offer crucial insights into system stability and its proximity to potential collapse. The P-V curve, often called the "nose curve," illustrates the relationship between active power and voltage at a specific node or bus. It demonstrates the system's capacity to handle increasing loads until it reaches a critical threshold, the 'point of no return,' where voltage drops irreversibly, leading to a collapse. This curve is vital for evaluating system performance under varying load conditions. The Q-V curve, on the other hand, analyzes the amount of reactive power a system must absorb or supply to maintain stable voltage at a specific node or bus. This curve is essential for understanding how variations in reactive power affect voltage stability and helps ensure the system operates within safe voltage limits.

Moreover, a phase shift between the voltage at the transmitting and receiving sides further exacerbates the risk of collapse, as the misalignment impacts the effective transfer of power. The system may become unstable beyond a particular phase difference, contributing to widespread failure. This highlights the importance of managing reactive power and closely monitoring voltage levels across the network to prevent cascading failures that could lead to a grid-wide collapse.

To mitigate voltage instability, both under normal operating conditions and in extreme scenarios, a range of countermeasures are implemented. Specialized devices are deployed across the grid to regulate and maintain voltage stability by controlling reactive power flow into and out of the system. These devices ensure that voltage remains within acceptable limits, thus preserving grid stability.

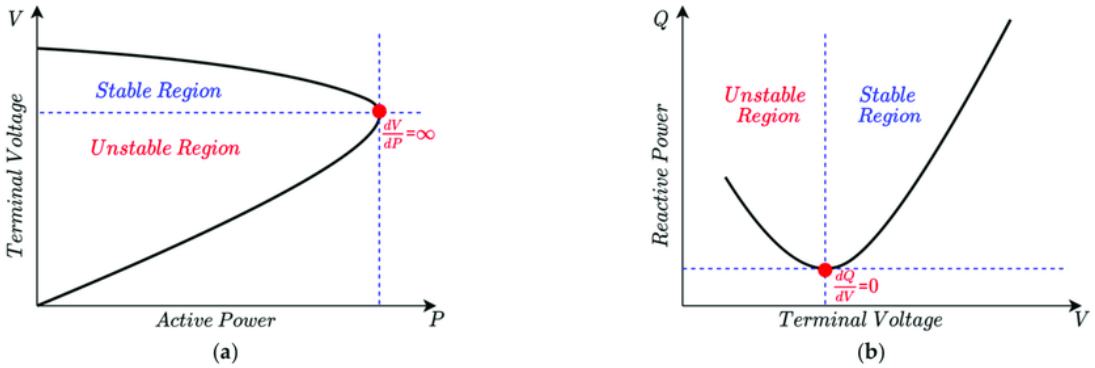


Figure 2.9: P-V and Q-V curves [17]

In addition to these regulatory mechanisms, protective relays are utilized to quickly isolate faults within a network, preventing them from cascading to other grid sections. This fast response helps minimize the risk of widespread outages.

When other methods prove insufficient, a strategy known as 'load shedding' is employed as a last resort. This involves selectively disconnecting specific loads from the grid to reduce overall demand, thereby relieving stress on the system and preventing a complete collapse. Load shedding, while disruptive, is an essential safety measure that can protect the grid from catastrophic failure during severe instability.

Angle Stability

Rotor angle stability is a key factor in maintaining grid stability. It ensures that generators remain synchronized with the rest of the system after disturbances or load changes. This stability depends on keeping the rotational speed and phase angle between generators aligned, with deviations typically limited to no more than 30 degrees.

Disturbances, such as transformer failures, transmission line faults, or sudden load shifts, can cause generators to speed up or slow down, altering their phase angle relative to other units. When this happens, the generator may disconnect from the grid to avoid damage, or it could lead to broader system instability. This desynchronization can disrupt the power flow, causing voltage and current fluctuations across the grid.

As a result, the grid may experience overloaded lines, equipment failures, and even cascading failures, where one issue leads to a series of breakdowns throughout the system. Therefore, ensuring rotor angle stability is crucial for preventing widespread outages and maintaining reliable grid operation.

2.2.3 Blackout

Power grids are engineered to ensure continued functionality even in the event of a failure of one critical component, such as a generator, transmission line, or transformer. This principle, known as the N-1 criterion, is fundamental to maintaining grid reliability and highlights the built-in redundancy of such complex systems. To assess and prepare for potential failures, grid operators conduct contingency analyses, simulating fault scenarios to test the system's resilience and ensure it can remain operational under such component failures.

Despite these safety measures, large-scale power outages still occur globally, as seen in fig. 2.10. A notable example in recent history is the 2021 Texas winter blackout, which left more than 10 million people without electricity and resulted in an estimated $130 billion in economic damages [18]. One mitigating factor during this crisis was that Texas operates its independent power grid, meaning the damage was contained within the state's borders, preventing the outage from cascading across the broader U.S. grid.

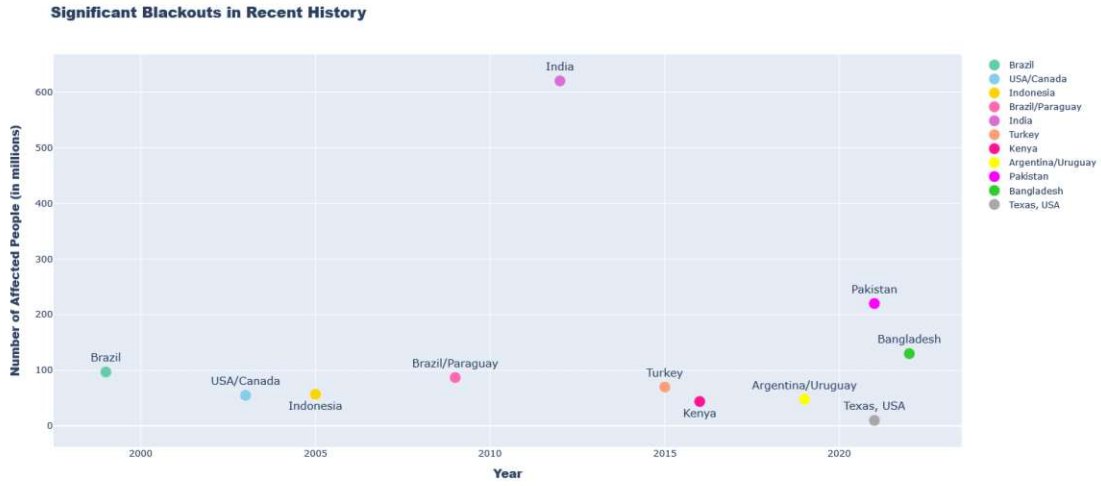


Figure 2.10: Major Blackouts in recent history relative to population impact [19] [20] [18] [21][22] [23] [24] [25] [26] [27] [28]

This level of isolation is not typical in other regions. In Europe, for instance, the interconnected nature of its power grid, one of the largest in the world, means that failures in one area can propagate and affect neighboring countries. The Texas event serves as a reminder of the vulnerabilities that exist even in highly sophisticated power systems and how regional isolation or interconnectivity can drastically impact the scope of an outage.

A 'blackout' refers to a large-scale power outage during which electricity is completely lost for a significant number of consumers over an extended period. Although the exact number of affected users and the duration may vary, a blackout generally implies a widespread and prolonged disruption in energy supply. Another interpretation involves the creation of 'islands,' where, after the failure of key transmission lines, a once unified grid fragments into two or more isolated networks.

2.2.4 Power Flow

Power flow calculations are essential numerical tools for analyzing and understanding electrical power transmission from the generation source to the loads within a power system. These calculations consider currents, voltages, and other electrical parameters at critical nodes, enabling operators to assess key factors such as equipment capacity in relation to the current grid configuration and load demands. The ultimate goal is to ensure that the system operates with maximum safety, efficiency, and reliability. They are typically conducted under the assumption of a steady-state operation, meaning that system parameters remain stable over time, even in the presence of disturbances like sudden load changes. Key outputs from power flow analysis include the active and reactive power flowing through transmission lines, as well as voltage characteristics such as magnitude and phase angle at various buses. These power flow equations are based on Kirchhoff's laws and the power balance between generation and the consuming end, i.e., loads.

Such analyses must consider several critical constraints, including the balance between power generation and consumption, voltage limits to ensure stable operation, and phase angle restrictions at buses to maintain synchronization across the system. Additionally, the thermal limits of transmission lines must be accounted for to prevent overheating and ensure safe energy transfer. Equipment capacities, such as the maximum output of generators and the operational limits of transformers, are also key factors that influence the system's performance and stability. Addressing these constraints is essential for optimizing grid reliability and preventing system overloads or failures.

Most open-source and commercial power flow software tools utilize the 'single-line diagram' (see fig. 2.11), a simplified graphical representation of the power system that allows for easier visualization and understanding of complex grid configurations. This diagram helps operators to quickly assess system components and relationships, facilitating more efficient analysis and decision-making. Additionally, these tools often employ the per-unit system, which normalizes electrical quantities relative to a common base value. This helps avoid working with large values; for instance, instead of using 110 kV, it would be expressed as 1.1 p.u if the base value is 100 kV. Essentially, it is a percentage-based approach.

This method not only enhances consistency across calculations but also improves scalability and computational efficiency, making it easier to compare different systems and scenarios under a unified framework.

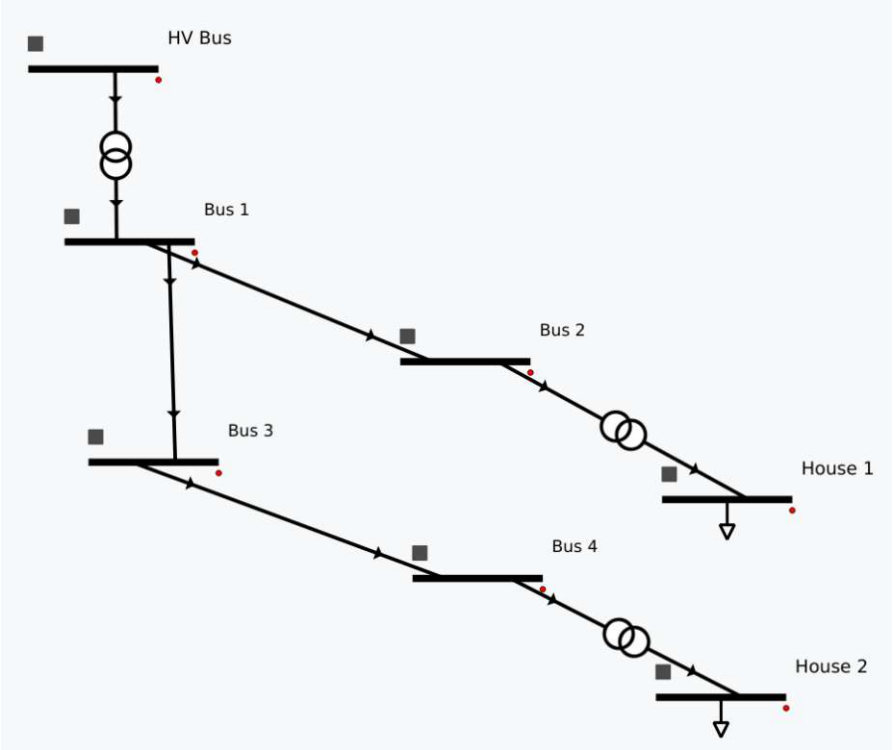


Figure 2.11: Single-line diagram example

Depending on the software's capabilities, various analyses, such as short-circuit, stability, contingency, and other advanced types, can be performed. These tools provide comprehensive insights into the grid's performance under varying conditions and help operators proactively develop strategies for potential issues, therefore increasing grid resilience and reliability.

2.2.5 Distribution Transformers

Distribution transformers are the final stage of the electrical distribution network and play a vital role in ensuring a stable and reliable power supply. Their main function is to step down medium voltages to low voltages, making electricity accessible to homes, businesses, hospitals, and industrial facilities. In addition to voltage transformation, they help maintain grid stability by acting as a buffer against power fluctuations and disturbances. These transformers typically operate at 20–80%[29][30] of their rated capacity, depending on the region, weather conditions, and the specific applications. This operating range is designed to balance efficiency and lifespan while ensuring they can handle peak loads when necessary. However, prolonged overload conditions can lead to overheating, insulation degradation, and damage to internal components, ultimately reducing their lifespan and increasing the risk of failure.

The efficiency of distribution transformers generally falls between 85% and 95%[31], depending on factors like design, age, and cooling mechanisms. With the rise of smart grids and the integration of Decentralized Energy Resourcess (DERs) such as solar panels, new challenges have emerged, including bidirectional power flows, voltage regulation issues, and grid stability concerns. To protect transformers and ensure reliable operation, they are equipped with various safety mechanisms, including:

- **Thermal Protection:** Sensors monitor temperature levels and disconnect the transformer if it overheats to prevent damage.
- **Overcurrent Protection:** Circuit breakers and fuses disconnect the transformer in response to excessive current from short circuits or sustained overloads.
- **Overvoltage Protection:** Help prevent damage from voltage spikes, such as those caused by lightning strikes.
- **Ground Fault Protection:** Fault current detection mechanisms prevent dangerous voltage shifts that could impact safety and system stability.

While these protections are essential for preventing transformer failures, they also create a potential point of disruption. If triggered, they may disconnect the transformer, cutting power to consumers. These mechanisms are central to the simulation conducted in this thesis, which examines how cyber-attacks could disrupt electricity supply. Rather than physically damaging transformers, attackers could manipulate the system to force disconnections, demonstrating the real-world risks of cybersecurity threats in modern energy infrastructure.

2.3 SMART Homes

2.3.1 Overview

Smart homes refer to an integrated network of intelligent household devices with advanced capabilities that enable remote control. These systems provide user convenience, improved comfort, and greater energy efficiency by leveraging modern technological advancements, thus contributing to their growing popularity. Typical smart devices include appliances like refrigerators, lighting systems, security cameras, heating systems, water heaters, and air conditioning units. Many of these devices can be automated to perform specific tasks and are able to adapt to individual user preferences. Control is managed typically through smartphone or tablet applications, often via a cloud server provided by the service provider, as well as a central hub that facilitates communication between the user and the devices. Some Smart-Hubs like Amazon Echo and Google Home offer direct interaction with connected devices via voice commands. However, some smart home appliances can be accessed directly through the internet without the need to route through the central hub, which is a key consideration in the context of this thesis. The most commonly used communication standards in smart homes include Wi-Fi, Bluetooth, ZigBee, and Z-Wave, each chosen based on factors such as range, data transfer speed, and energy consumption.

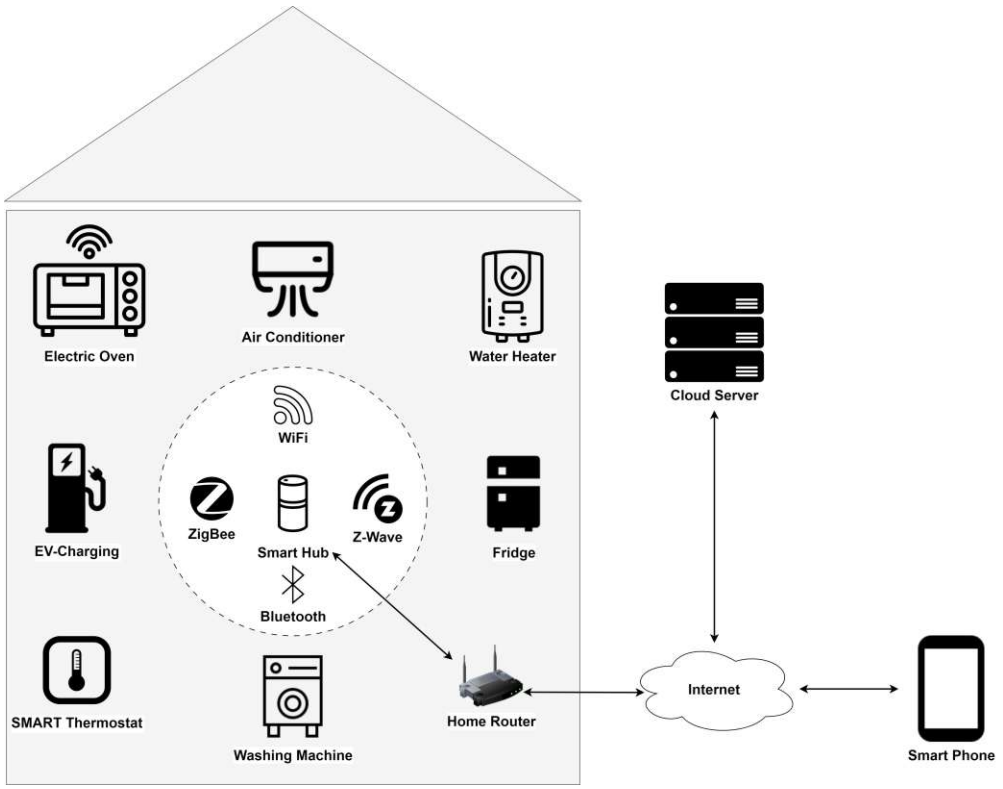


Figure 2.12: Exemplary Smart Home system architecture.

Although these systems provide greater convenience, user comfort, and energy efficiency, they also introduce challenges. Increased connectivity and communication expand the attack surface, leading to a heightened risk of cyber threats in this domain.

2.3.2 IoT/Smart Homes Device Architecture

IoT/Smart Home devices are embedded systems consisting of both hardware and software components. Over time, various layered models and architectures have been developed to cater to different applications. These models range from 3 to 7 layers, with the 3- and 4-layer architectures being the most commonly implemented [32]. The standard architecture is typically composed of the following layers (see fig. 2.13):

1. **Perception Layer:** The perception layer, also called the device or edge layer, is the foundation of the architecture. It consists of sensors, actuators, and other hardware components directly interacting with the physical environment. This layer is responsible for gathering data such as temperature, humidity, motion, and other environmental variables. The perception layer acts as the system's eyes and ears, enabling devices to monitor and respond to their surroundings. Being the most essential and widely used layer in all models [33], it forwards the collected data to the next layer for further processing.

2. **Network Layer:** The network layer, also known as the transmission layer, facilitates device communication and connectivity. It incorporates various communication technologies and protocols, enabling devices to interact with one another and external networks. Common standards such as Wi-Fi, Bluetooth, ZigBee, and cellular networks (e.g., 4G and 5G) are used to transfer data between devices and across networks. This layer plays a critical role in maintaining the flow of information, allowing devices to function in a coordinated manner.

3. **Processing Layer (only part of the 4-layer model):** The processing layer is responsible for analyzing, storing, and managing the raw data collected by the perception layer. This layer processes the data to extract meaningful insights, which can then be used for decision-making and system control. Additionally, it oversees device management, including software updates and system monitoring, to ensure proper functionality. In some models, it is referred to as the management layer, as it helps maintain the overall integrity and efficiency of the system.

4. **Application Layer:** The application layer is the interface between the smart device and the end user. It allows users to visualize data and make informed decisions based on the insights provided by the system. This layer also supports automation, enabling users to customize device behavior according to their preferences, such as automating lighting or heating based on time or environmental conditions. The application layer enhances user experience by delivering convenience, control, and personalization.

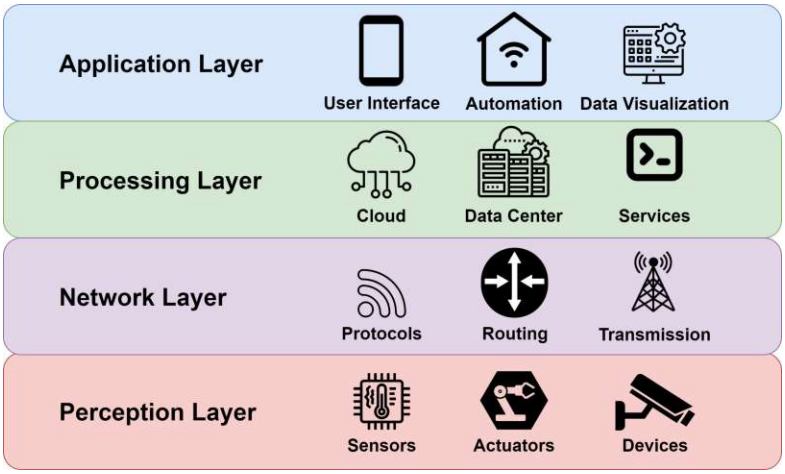


Figure 2.13: IoT Architecture layers [34]

An equally important aspect critical to the functionality of IoT devices is the operating system (OS). Most IoT devices rely on operating systems to provide an abstraction layer, efficiently manage resources, enforce security protocols, coordinate processes, and facilitate communication across networks. A robust OS with a well-designed kernel and strong networking capabilities enables IoT devices to achieve greater flexibility and interoperability within the diverse ecosystem of devices typically found in smart homes.

In recent years, a wide range of operating systems explicitly tailored for IoT devices have emerged [35]. Some of these operating systems are based on Linux distributions or the Berkeley Software Distribution (BSD), both of which are derived from Uniplexed Information Computing System (UNIX). These systems are designed to operate with minimal resource consumption, optimizing memory usage and processing power while still delivering the necessary functionality. Additionally, energy efficiency is a top priority, ensuring that tasks are executed at the scheduled time and accurately without excessive power consumption.

However, the complexity introduced by this architecture also comes with certain drawbacks. One of the most critical issues is that, despite the integration of robust security measures, vulnerabilities can still emerge, and exploits may surface, particularly when essential practices like regular updates are neglected, a common occurrence in the IoT space. The vast diversity of devices within a Smart Home/IoT ecosystem, along with the growing number of connected devices, significantly expand the attack surface, providing more opportunities for attackers to exploit weaknesses in software, firmware, and network configurations. This topic is explored further in section 2.4.

2.4 Cyber Security

Security in the context of power grids is a critical concern, as these networks form the backbone of modern infrastructure, essential for the functioning of society. Power grids are attractive targets for cyber attacks designed to cause significant economic and social disruption. Attacks on this critical infrastructure, particularly on the systems responsible for monitoring and control, are not new but are becoming increasingly sophisticated and more frequent, making it crucial to detect and defend against them.

Typically, attackers focus on control centers, local utility companies, Regional Transmission Organizations (RTOs), Independent System Operators (ISOs), and power plants. Some prominent examples from recent years include:

- **Generation:** The Triton malware attack on a Saudi oil and gas plant in 2017 [36] and the INCONTROLLER/PIPEDREAM [37] malware targeting ICSs.
- **Transmission:** Attacks by groups like RedEcho [38] and TAG-38 [39], which specifically targeted the Indian power grid.
- **Distribution:** The BlackEnergy [40] and Industroyer (including Industroyer2) [41] malware, which was used in the attacks on Ukraine's critical infrastructure.

While many countermeasures are in place and substantial efforts are being made to mitigate cyber-attacks on power grids, one critical aspect is often overlooked: the role of connected consumers. Although this may not seem immediately significant, it can strongly impact grid stability. Specifically, attacks targeting the manipulation of electrical loads with the intent of disrupting grid stability are not yet widely acknowledged. This thesis aims to investigate this largely unexplored threat.

2.4.1 Cyber Security Properties

Cybersecurity involves several fundamental properties critical for protecting systems, data, and communications [42]. These core properties are:

- **Confidentiality:** Ensures that only authorized users/components can access sensitive information, both in memory and during transmission, preventing unauthorized disclosure or data leaks.
- **Integrity:** Protects data from unauthorized modification, ensuring it remains accurate, complete, and unaltered.
- **Availability:** Guarantees that systems, services, and data are accessible to authorized users whenever needed, ensuring uninterrupted operation and the timely execution of processes.

- **Authenticity:** Confirms the identity of users to ensure that only legitimate individuals or entities can access and interact with the system.
- **Authorization:** Defines and enforces user permissions, determining who is allowed to access specific resources and perform certain actions within the system.
- **Non-repudiation:** Ensures that actions or transactions performed can be traced back to a specific individual or entity, preventing users from denying their involvement or responsibility.

These cybersecurity properties form the foundation for designing robust security strategies and ensuring systems are secure, reliable, and resilient against potential threats.

2.4.2 Cyber Attacks on Smart Home/IoT Systems

The categorization of attacks based on specific IoT layers has been extensively researched and discussed [43][44]. The following subsections highlight some possible attacks, detailing their characteristics and implications for the security of such smart home systems.

2.4.3 Attacks on Perception Layer [43]

Compromised/Malicious Node Insertion

An attacker can infiltrate a smart home system by introducing a malicious, compromised node to gain unauthorized access and control. This can be achieved through malicious code injection, which involves the insertion of harmful software or firmware into smart home devices. Once the attacker gains control over a device, they can manipulate its operations and issue commands to other interconnected devices. This type of attack can result in unauthorized control over various processes within the smart home, including the arbitrary activation or deactivation of devices, thereby potentially disrupting the entire network. Furthermore, such an attack can serve as a starting point for the creation of botnets, where compromised devices are co-opted into a network of bots used to execute large-scale cyber-attacks.

Signal Jamming

In smart home systems, signal jamming is the deliberate act of disrupting communication between devices by emitting signals at the same frequencies being used. Attackers typically target Wi-Fi and Bluetooth frequencies, resulting in communication failures.

Eavesdropping and Replay Attacks

In the perception layer of IoT architecture, eavesdropping involves the interception of sensor data by an attacker who is in close proximity to the devices. This intercepted data can subsequently be replayed to the system, inducing unintended behaviors.

2.4.4 Attacks on Network Layer [43][44]

Denial of Service (DoS) Attacks

A DoS attack overwhelms a system or network, such as the control system of a smart home, by flooding it with a large volume of data or requests. This overload causes the system to become unresponsive, resulting in service disruption or complete unavailability for legitimate users. Such attacks target the system's ability to handle requests, rendering it incapable of processing legitimate operations.

Man-in-the-Middle (MiM) Attacks

Here, an attacker intercepts the communication between devices exchanging data within the network. This interception allows the attacker to eavesdrop on sensitive information, manipulate the transmitted data, or alter the communication entirely. MiM attacks pose significant risks as they can compromise data integrity and confidentiality.

Spoofing

Spoofing occurs when attackers impersonate legitimate system components or communication partners to gain unauthorized access to the network. By presenting themselves as trusted entities, attackers can infiltrate the system.

Blackhole Attacks

A black hole attack in ad-hoc networks involves a malicious node falsely advertising the optimal route to reroute data traffic. Once the traffic is directed to this node/IoT device, it drops all packets, preventing data from reaching its intended destination and leading to data loss or interception.

Gateway Attacks

In a gateway attack, the adversary targets the communication link between smart home devices and the internet, disrupting the connection to interfere with the system's operations. This type of attack often involves manipulating routing protocols, causing either incorrect or no data to be transmitted between devices and the internet.

2.4.5 Attacks on Application Layer [43]

Social Engineering

Social engineering is one of the most prevalent forms of cyber attacks, as humans often represent the weakest link in the security chain. In these attacks, users are psychologically manipulated, often through emotional tactics, into giving up sensitive information such as access credentials or other private data.

Data Breaches

Through data breaches, attackers are able to exploit known or public vulnerabilities in applications to gain unauthorized access to systems. Once inside, they can extract sensitive data or assume control over the targeted network, often leading to significant privacy and security violations.

Default Configurations

The use of default configurations, such as factory-set usernames and passwords, poses a considerable security risk. Many users fail to change these default settings, leaving their devices susceptible to brute-force attacks. This common oversight underlines the importance of proper configuration and user diligence in securing smart home devices.

As cyber-physical entities connected to the Internet, smart home systems present numerous potential vectors for cyberattacks. This thesis explores a critical scenario in which a large number of smart home devices, often produced by the same vendors or using similar frameworks and hardware, can be exploited due to shared vulnerabilities. These devices can be manipulated to abruptly alter their power consumption, thereby impacting the electrical grid's stability. Such manipulation is facilitated through the deployment of a botnet that capitalizes on these common weaknesses to coordinate actions across multiple devices.

In this context, the subsequent section provides a comprehensive analysis of the Mirai botnet, which has demonstrated the capability to infect hundreds of thousands of devices. Understanding Mirai's operations and impact is crucial for grasping how coordinated attacks on smart home systems can affect grid stability.

2.4.6 Mirai - The Future

The Mirai botnet (Japanese for "future") first gained widespread attention in mid-2016 after executing highly disruptive DDoS attacks on prominent targets such as Krebs on Security [45], OVH [46], and the DNS provider Dyn [47]. This worm-like malware orchestrated large-scale attacks by infecting approximately 600,000 IoT devices connected to the internet. Since its emergence, numerous enhanced and more sophisticated variants of the Mirai botnet have been developed, each with unique features and capabilities [48]. The following section explains the steps that enabled the infection of such a vast number of devices, and fig. 2.14 represents the sequence diagram of the attack process.

1. **Rapid Scanning Phase:** Mirai's initial spread began with an aggressive scanning phase, in which the botnet scoured the internet for publicly accessible IP addresses. The malware sent a high volume of TCP SYN packets to pseudo-randomly generated IP addresses. The scanning process was asynchronous, meaning each scan was independent and stateless, i.e., Mirai did not maintain ongoing connections. To avoid premature detection, specific IP addresses, such as those belonging to large corporations and government entities, were hardcoded into a blacklist and excluded from the scanning.

2. **Targeting of Telnet Ports:** The primary target ports were Telnet TCP ports 23 and 2323. Telnet is a widely used network protocol for remote management and control of embedded systems. However, its lack of encryption poses a significant security risk, as communications are transmitted in plaintext. After sending TCP SYN packets, Mirai waited for a response. If a SYN-ACK was received, it indicated that the port was open and accessible, signaling that a connection to the device was possible. If a TCP RST packet was returned, the port was closed, and no further action was taken. This method ensured an efficient use of resources.

3. **Brute Force Login Phase:** Upon identifying open ports, Mirai transitioned into a brute force login phase. It attempted to log in using default username/password combinations from a predefined list of 62 credential pairs, exploiting the widespread issue of unchanged factory default settings in IoT devices.

4. **Report Server:** Once a successful login was achieved, Mirai transmitted the IP address and corresponding credentials to a hardcoded report server, a critical component of its architecture. This server acted as a central hub, storing information about compromised devices, coordinating the distribution of malware, and maintaining control over the expanding botnet.

5. **Deployment of the Loader Program:** Following the reporting stage, an independent loader program was deployed, which operated asynchronously. The loader retrieved the necessary login data from the report server and logged into the compromised device to gather system information, including details about the operating system and hardware architecture. Based on this information, the

loader downloaded the appropriate malware version and configuration, successfully infecting the device and incorporating it into the botnet.

6. **Obfuscation and Self-Defense Mechanisms:** In the final stage of the infection process, Mirai employed obfuscation techniques to erase traces of its presence. The loader program deleted the downloaded binary file and altered the process name to evade detection. Additionally, the malware terminated any other processes occupying the targeted ports, including those from competing malware, ensuring full control over the infected device and preventing further exploitation.

7. **Expanding Botnet:** At this point, the attacker gained control of a vast botnet, which could be directed for coordinated and synchronized attacks through the Command and Control (C2) server. Simultaneously, the botnet continued its propagation, seeking out and infecting new devices to expand its reach.

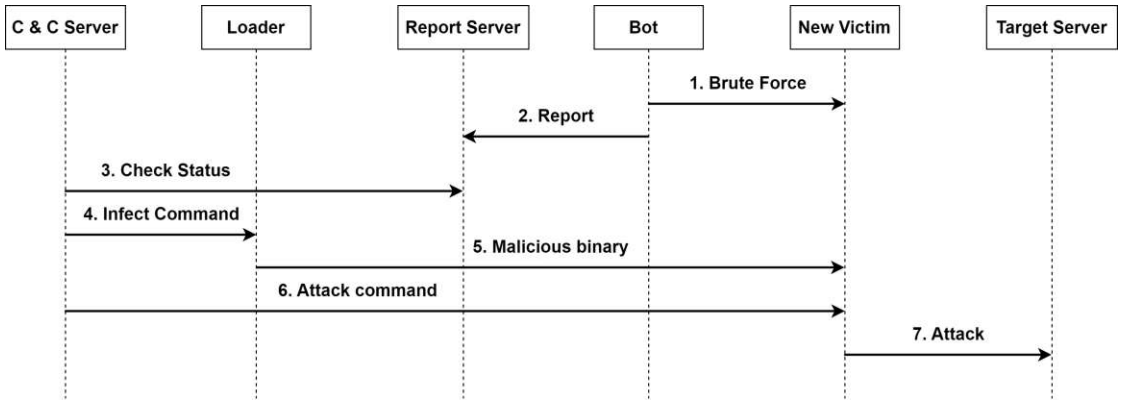


Figure 2.14: Mirai Attack Sequence

2.5 Threat Analysis and Risk Assessment

A threat analysis is a critical process used to identify and evaluate potential threats that could compromise the security and functionality of the system under consideration. This involves a detailed examination of possible threat scenarios, including the motivations, capabilities, and methods attackers might use. The goal is to determine which of these threats are technically feasible based on the system's characteristics and predefined assumptions.

Building upon the threat analysis, a risk assessment evaluates the identified threats by considering their potential impact and the likelihood of occurrence. The overall risk is derived from the combination of these two factors, thus providing a framework for prioritizing threats and informing the necessary mitigation strategies. Technical feasibility and cost considerations are central to determining the most effective response.

These two processes, threat analysis and risk assessment, help create robust and secure systems. Together, they enable proactive security strategies that effectively mitigate risks before they lead to serious vulnerabilities. Various frameworks have been developed for these processes, each tailored to different domains. However, these frameworks share many commonalities despite their domain-specific differences and may offer distinct perspectives that can prove advantageous depending on the context. In the State of the Art chapter 3, the frameworks relevant to this thesis will be thoroughly examined and described.

CHAPTER 3

State of the Art

3.1 Load Manipulation Attacks

The increasing adoption of smart home technologies, particularly high-power devices, presents both opportunities and challenges for the stability of power grids. Recent research has highlighted various attack scenarios and potential risks posed by IoT-based manipulations, which will be explored in detail. A significant focus of this research involves the growing interconnectivity of high-power devices, which, if compromised, could severely threaten grid stability.

Dabrowski et al. [49] examine the susceptibility of power grids to load-switching attacks, which can be triggered by IoT devices or home office setups, such as PCs, monitors, and laser printers. Their study combines theoretical analysis with simulations to evaluate the potential impact of such attacks. Both static and dynamic load changes are considered, i.e., single, one-time load changes and repeated cyclical load changes. The simulations account for factors such as grid reserve responses and other operational conditions. The results reveal that under specific conditions, such as low overall grid demand and a high share of renewable energy, an additional load of 4500 MW could destabilize the system and lead to load shedding. To launch such an attack, an adversary would need a botnet comprising between 2.5 and 9.8 million bots. In a highly technological region like Europe, this scale of attack is considered feasible and becomes increasingly plausible with the growing number of IoT devices.

Soltan et al. [50] also explore this critical issue in their research. Their study investigates not only frequency drops and rises but also a range of other scenarios, such as the disruption of black starts, line failures and the resulting cascading effects, tie-line failures, and attacks aimed at increasing operational costs. The insights are primarily obtained through simulations and power flow analyses, which are used to identify the botnet size required to execute these attacks. These analyses are demonstrated using Institute

of Electrical and Electronics Engineers (IEEE) grid models as well as models of a historical Polish power grid. The study concludes that, under specific conditions, even a relatively small number of compromised devices can significantly disrupt grid stability. It demonstrates that a 30% surge in demand could trigger a complete system blackout by tripping all generators in the US Western Interconnection. Similarly, a mere 1% increase in demand on the Polish grid can cause a cascading failure of 263 transmission lines, affecting 86% of the system's load.

Huang et al. [51] provide a more detailed analysis and highlight why the findings of Soltan et al. and Dabrowski et al. may not fully reflect realistic conditions. Their study addresses gaps in both prior works by incorporating existing protective mechanisms into the simulations, elements that were not considered in Soltan et al.'s research, and by accounting for the fact that not all generators connected to the grid will respond simultaneously, which was a key assumption in Dabrowski et al.'s study. Additionally, Huang et al. performed both transient and steady-state analyses within a closed-loop simulation, where the results from the transient analysis informed the steady-state analysis and vice versa, iterating until the solver could no longer generate a solution. Their simulations modeled attacks that increased demand by 1%, 10%, and 30%, as well as load-decrease attacks following load-shedding events. The results revealed that neither the 1% nor the 10% demand increase led to system failure, although load shedding was necessary. At 30%, generators began to disconnect, leading to islanding within the grid; however, even at this level, a full system collapse did not occur immediately.

Shekari et al. [52] go a step further by incorporating additional protective mechanisms, as well as both static and dynamic loads, into their simulations. They argue that, although Huang et al. employed accurate simulations, the analyzed attacks were more generalized, targeting the entire grid randomly rather than representing a coordinated and sophisticated attack. Shekari et al. demonstrate that the grid remains vulnerable to coordinated and strategic attacks even with protective mechanisms in place. In their methodology, rather than targeting all nodes equally, the attack focuses on the three weakest or most overloaded nodes, identified through a systematic analysis. The attack process is divided into three phases. The first phase involves gathering detailed information about the target grid and its structure. The authors suggest that this could be accomplished using publicly available resources, such as Google Maps or OpenStreetMap, as a one-time reconnaissance effort. In the second phase, the actual attack is launched using publicly accessible data from ISOs, along with stock-trading tools that provide real-time information on the loads at specific nodes. Updated every five minutes, this data allows attackers to pinpoint the grid's weakest nodes using voltage stability indices. Based on this information, they evaluate the feasibility of the attack and calculate its projected success rate, which is also influenced by the availability of the botnet at that time. Their method, termed MaDIoT 2.0, demonstrated a significantly higher success rate, ranging from 67% to 91%, compared to earlier attack models. In simulations, MaDIoT 2.0 not only outperformed previous approaches but also did so with a smaller and more realistic botnet size.

Goerke et al. [53] expand on the research by Dabrowski et al., examining this threat through the lens of projected device numbers in Germany for 2030 and 2040. They highlight how the increasing integration of DERs, such as EVs, heat pumps, photovoltaic inverters, and battery storage systems, creates new opportunities for attackers to compromise grid stability. By combining a comprehensive literature review with detailed calculations, the authors quantify the extent of DER control necessary for an attacker to destabilize the European power grid or a typical distribution network while considering specific conditions. Conservative estimates of device growth and adoption rates are used to inform their analysis. Their findings suggest that an attacker would only need to control a small percentage of devices in Germany to destabilize the European grid. In contrast, attacks on distribution networks are considered less feasible or more challenging to execute, as the number of compromised devices connected to a single low-voltage transformer would need to be significantly higher than current projections.

Lakshminarayana et al. [54] explore the impact of static and dynamic Load-Altering Attacks through the application of second-order dynamic system theory. Their study employs Eigenvalue sensitivity analysis to identify the most vulnerable nodes within the power grid and to determine the minimum load alteration necessary to induce unsafe frequency deviations.

In a separate study, Lakshminarayana et al. [55] and Ospina et al. [56] examine the increased vulnerability of power grids under low-inertia conditions, which were worsened by the COVID-19 pandemic. Lakshminarayana et al. analyze how lockdown measures led to reduced electricity demand and increased integration of renewable energy sources, creating conditions characterized by low inertia. Ospina et al., on the other hand, utilize Dynamic Mode Decomposition to assess the impact of load-altering attacks on frequency stability under low-demand conditions. Both studies highlight that attacks carried out in such conditions can result in significantly more severe consequences.

Building on the findings of previous studies that demonstrate the feasibility of such attacks when properly planned and coordinated, this master's thesis shifts the focus from a broad, high-level analysis of the power grid to an in-depth examination of the low-voltage network. Instead of exploring system-wide impacts, this research investigates the origin of these attacks, the low-voltage networks where smart home and IoT devices are interconnected. The study examines the necessary conditions for carrying out these attacks, including the types and number of devices involved, synchronization requirements, and the effectiveness of protective mechanisms within the low-voltage domain. By addressing vulnerabilities at the source, this thesis seeks to provide a more nuanced understanding of the feasibility of these attacks and their potential consequences for grid stability.

3.2 Threat Analysis and Risk Assessment Frameworks

TARA methods have proven to be valuable qualitative tools for proactively planning security measures and enhancing decision-making, particularly considering legal and financial factors. Various frameworks and tools have been developed to support and implement these processes effectively. The origins of these frameworks can be traced to the need for a systematic approach to identifying, evaluating, and mitigating threats, especially in the domain of IT security. As the significance of these analyses has grown, formalized standards have been introduced to establish uniform methodologies that can be applied across different domains. This section focuses on frameworks that enable multi-level abstraction, emphasizing a comprehensive system-level perspective, which is then leveraged to analyze specific attack scenarios on smart home systems.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [57] is one of the most widely recognized frameworks, with applications spanning across multiple domains. Developed by the NIST, the CSF is designed to assist organizations in systematically managing and reducing their cybersecurity risks. Initially published in 2014, this global standard is continuously refined and updated to accommodate emerging challenges and technological advancements. The framework is structured into three main components: the Framework Core, the Implementation Tiers, and the Profiles.

The Framework Core serves as the foundation and is organized around five essential functions: Identify, Protect, Detect, Respond, and Recover. These functions provide a comprehensive and structured approach to cybersecurity risk management:

1. **Identify:** This initial function involves identifying critical assets, including components, data, and communication interfaces, that could lead to significant issues if compromised. It also includes identifying potential threats and vulnerabilities, which is vital for gaining a clear understanding of the organization's or system's cybersecurity state.

2. **Protect:** This function focuses on implementing protective measures to mitigate identified threats and address vulnerabilities, thereby strengthening the organization's defenses.

3. **Detect:** This function emphasizes the development and implementation of capabilities to detect cybersecurity incidents in a timely manner.

4. **Respond:** This function addresses the actions required once security-related incidents are identified, aiming to minimize the impact and contain the threat.

5. **Recover:** The final function involves planning and implementing measures to restore disrupted services and functions following cybersecurity incidents, ensuring resilience and continuity.

6. **Govern (New in NIST CSF 2.0 - 2024):** This function emphasizes the governance aspect to underscore the importance of well-defined management processes in effectively addressing security risks. By clearly defining roles and responsibilities, it ensures that all stakeholders are aware of their specific duties and areas of accountability. This component serves as a foundational element of the framework, reinforcing the understanding that cybersecurity is a continuous process requiring ongoing oversight and regular adaptation to evolving threats.

The Implementation Tiers serve to assess and enhance the maturity of an organization's cybersecurity practices. The tiers range from Tier 1 (Partial) to Tier 4 (Adaptive), progressing through Tier 2 (Risk-Informed) and Tier 3 (Repeatable). This tiered approach enables organizations to evaluate the effectiveness and adaptability of their cybersecurity strategies.

Profiles offer the flexibility to tailor the framework to an organization's specific needs and strategic goals. A Profile describes the organization's current state of integrated security measures, which can be expanded to align cybersecurity outcomes with business requirements and priorities.

While the NIST CSF operates primarily at an organizational level, offering a broad strategic perspective for comprehensive cybersecurity planning and implementation, other well-known threat analysis frameworks focus more on technical aspects. One such framework is the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) threat model [58], developed by Microsoft, which is specifically designed to identify and categorize threats. Unlike broader frameworks, STRIDE can be effectively applied to lower-level applications, such as software programs and other technical systems. The acronym STRIDE represents six fundamental categories of computer security threats:

- **Spoofing:** Refers to identity forgery, where an attacker impersonates a legitimate user or system to gain unauthorized access to an asset.
- **Tampering:** Involves the unauthorized modification of data, communications, or system components.
- **Repudiation:** Describes scenarios where an individual or entity can deny having performed a particular action or event.
- **Information Disclosure:** Entails the unauthorized exposure or leaking of sensitive information.
- **DoS:** Focuses on attacks that aim to make services unavailable to legitimate users by overloading or disrupting the targeted system.
- **Elevation of Privilege:** Refers to unauthorized escalation of user privileges to higher levels, such as gaining administrative rights

The STRIDE model offers a systematic approach to identifying vulnerabilities and threats, serving as a proactive measure to integrate security considerations early in the development process. Its straightforward structure facilitates interdisciplinary collaboration and communication between developers and security professionals, making it a valuable tool for enhancing system security.

In addition to established frameworks, there are also guidelines and reports that provide valuable support in addressing this topic. The European Union Agency for Cybersecurity (ENISA) published the study' Threat Landscape for Smart Home, and Media Convergence' [59] to identify, analyze, and assess threats and risks in the context of smart homes and convergent media. Another key framework is the IoT Security Maturity Model (SMM) [60], which assists organizations in evaluating and enhancing the maturity of their IoT security practices to achieve long-term security objectives.

The 'Internet of Things Security Framework (IoTSF) Best Practices: Guidelines' [61] also serves as a foundational resource, offering comprehensive best practices for manufacturers, developers, and users of IoT systems. These guidelines provide detailed instructions on effectively securing IoT devices and their networks.

Furthermore, although not specific to smart homes, the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework [62] is an indispensable tool for threat analysis. This framework functions as a comprehensive knowledge base, offering a detailed overview of adversarial tactics, techniques, and behaviors based on real-world observations. It is one of the most established frameworks in the field and provides a substantial foundation for analyzing threats and devising appropriate responses across various technological domains.

Another well-established methodology developed by MITRE is the Threat Assessment and Remediation Analysis (TARA) [63]. This framework is specifically designed to identify vulnerabilities and implement effective countermeasures. As part of MITRE's Systems Security Engineering portfolio, TARA supports the cybersecurity assurance of technical systems. Its systematic approach is rooted in the integration of known attack patterns, attack vectors, and countermeasures cataloged within MITRE's resources. TARA enables the assessment and prioritization of risks, facilitating the proactive development of security solutions aligned with the specific goals of a system or organization. The TARA methodology is structured as follows:

1. **Asset Identification:** Determining the most valuable and critical system components that require protection.

2. **Threat Evaluation:** Analyzing potential threats and attack vectors that could target these assets.

3. **Vulnerability Assessment:** Examining existing vulnerabilities within the identified assets.

4. **Countermeasure Implementation:** Selecting and applying suitable measures to mitigate identified vulnerabilities.

5. **Effectiveness Evaluation:** Reviewing the effectiveness of implemented measures and making necessary adjustments.

However, the framework developed in this thesis, utilizes a distinct TARA methodology: Threat Analysis and Risk Assessment [64]. This approach has gained significant traction within the automotive sector and closely parallels MITRE's TARA framework. A distinct advantage of the automotive TARA is its foundation in regulatory standards, including ISO/SAE 21434, which ensures a rigorous, standardized approach to threat analysis and risk assessment. This structure is supported by EU regulations, making it a reliable and consistent methodology. A detailed description will be provided in the Methodology chapter 4.

The proposed framework leverages the fact that both vehicles and smart homes are highly complex, networked cyber-physical systems. The automotive TARA methodology effectively addresses both software and hardware vulnerabilities, making it well-suited to analyzing security risks in smart home networks. Furthermore, this approach can be expanded through the integration of the STRIDE framework and MITRE's threat catalogs and databases, enabling a highly detailed and comprehensive level of threat analysis.

CHAPTER 4

Methodology

This thesis investigates the feasibility of disrupting the low-voltage grid and, by extension, the entire power grid through coordinated and synchronized cyber-attacks targeting high-wattage loads within a smart home environment. To assess the potential impacts of such load-manipulation attacks, the discrete simulation environment BIFROST is utilized. BIFROST offers sophisticated dynamic simulation capabilities and extensive customization features, which enable detailed modeling and analysis of complex energy systems.

After the simulation-based section, a TARA framework is introduced and demonstrated through an exemplary analysis. The developed framework primarily adopts the structure of the automotive industry standard TARA, which is selected for its systematic and proven methodology. The analysis is facilitated by the ISO-compliant tool Itemis Secure, which enhances the assessment of complex systems by automating processes to improve traceability, scalability, and reproducibility. Furthermore, well-established frameworks such as MITRE ATT&CK and STRIDE are integrated into the proposed method to ensure a comprehensive representation of attack vectors and mitigation strategies

4.1 Power Grid Simulation

As outlined earlier, the simulation will concentrate exclusively on the low-voltage grid to evaluate the feasibility of coordinated load-manipulation attacks. This approach involves adjusting the individual load profiles of groups of houses connected to a single transformer. To enhance accuracy and realism, external data sources will be leveraged to model the number of houses and authentic load profiles reflective of typical residential consumption patterns.

The analysis will encompass various scenarios, examining factors such as the number of houses, seasonal settings, and different times of day. This multifaceted exploration

aims to identify the most advantageous periods for launching an attack. Furthermore, different types of high-wattage loads, such as air conditioners and water heaters, will be incorporated, each with its characteristic maximum power draw. The study will determine which configurations are most plausible and effective in generating significant grid disruptions by simulating various combinations.

4.1.1 BIFROST

BIFROST is a cutting-edge digital simulation tool developed by Siemens, leveraging advanced web technologies to simulate and visualize complex energy supply scenarios. This web-based platform allows for creating and simulating virtual cities and energy infrastructures. Users can incorporate a wide range of elements, including residential buildings, commercial facilities, roads, lakes, power lines, transformers, and more, into the virtual environment. The tool supports dynamic simulations, demonstrating how various factors, such as weather conditions or specific events within the virtual city, impact the power grid. Furthermore, BIFROST incorporates multiple layers to facilitate detailed simulations. For instance, there are layers dedicated to landscape modeling, low-voltage grids, medium-voltage grids, data grids for communication networks, and thermo-grids for thermal simulations. Users can adjust the simulation speed and explore diverse scenarios to effectively analyze system behavior under different conditions.

The tool employs WebGL, a JavaScript Application Programming Interface (API), to render interactive and immersive 3D graphics, enhancing the visualization of simulations. It provides a user-friendly interface that encourages exploration and facilitates analysis, enabling users to optimize power grid configurations and improve system performance efficiently. The BIFROST simulation environment is composed of three primary components: the BIFROST core, a database, and external modules, as illustrated in fig. 4.1[65].

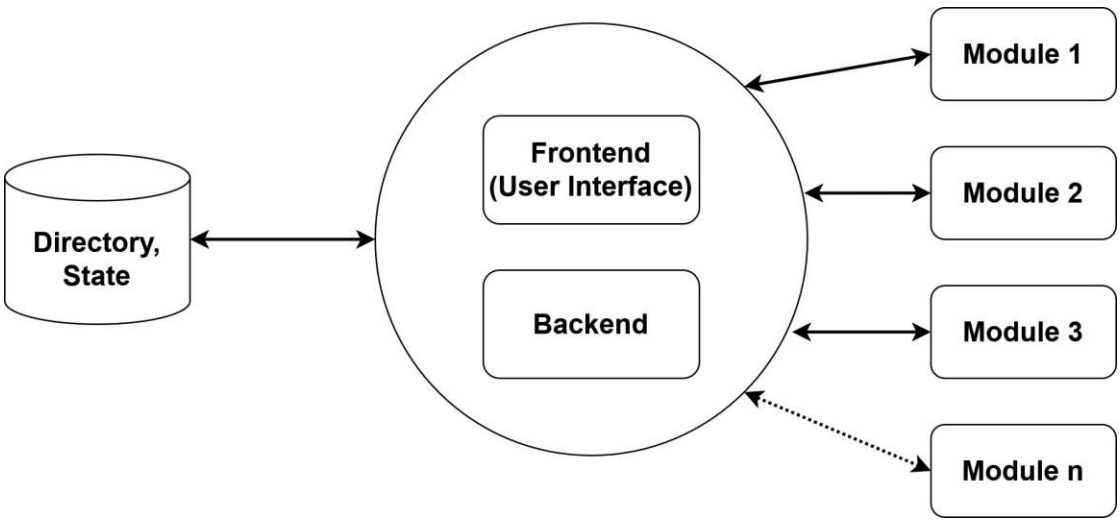


Figure 4.1: BIFROST Architecture based on [65]

BIFROST Database

The database is divided into two primary components: the directory and the state. The directory serves as a comprehensive repository, storing detailed information about the structures and parameters available within the simulation tool. This includes data on building types, electrical equipment, road networks, and other essential elements required for designing and customizing infrastructure layouts. By providing a structured inventory of these components, the directory enables users to construct and modify settlements with precision.

In contrast, the state represents the dynamic condition of a constructed settlement or city at a specific point in time. It captures not only the physical configuration of the infrastructure but also the latest simulation status, including operational parameters and system interactions. This dual-layered approach ensures that the simulation environment remains both flexible and reflective of real-time changes.

Both the directory and the state are stored in JavaScript Object Notation (JSON) format, which facilitates simple data accessibility, readability, and interoperability. This format supports efficient data parsing and integration with external tools or modules, enhancing the scalability and adaptability of the simulation environment.

BIFROST Core

At the center of BIFROST lies the Core, which is composed of two main components: the backend and the frontend. The backend serves as the central engine, managing interactions between the directory, state, and internal data model. It ensures efficient data coordination, storage, and retrieval, providing the foundational infrastructure for data management and system operations.

The frontend, on the other hand, acts as the user-facing interface, designed to streamline interaction with the tool (see fig. 4.2). An intuitive design allows users to easily construct settlements using drag-and-drop functionality and customizable parameter settings. This user-centric approach enhances accessibility and reduces the complexity of designing and modifying virtual environments.

A critical aspect of the Core is that it does not autonomously generate simulation data. Instead, it relies on external modules, which are integrated via Representational State Transfer (REST) APIs. These modules introduce specific behaviors and enable the simulation of diverse events by interacting with the Core. This modular architecture not only enhances the system's adaptability but also allows extending its functionality. New modules can be incorporated without disrupting the existing framework, ensuring the simulation environment remains flexible and scalable to meet evolving requirements.

BIFROST Modules

The modules are specialized software components that play a central role in defining and driving the simulation's behavior within the BIFROST environment. Among the key

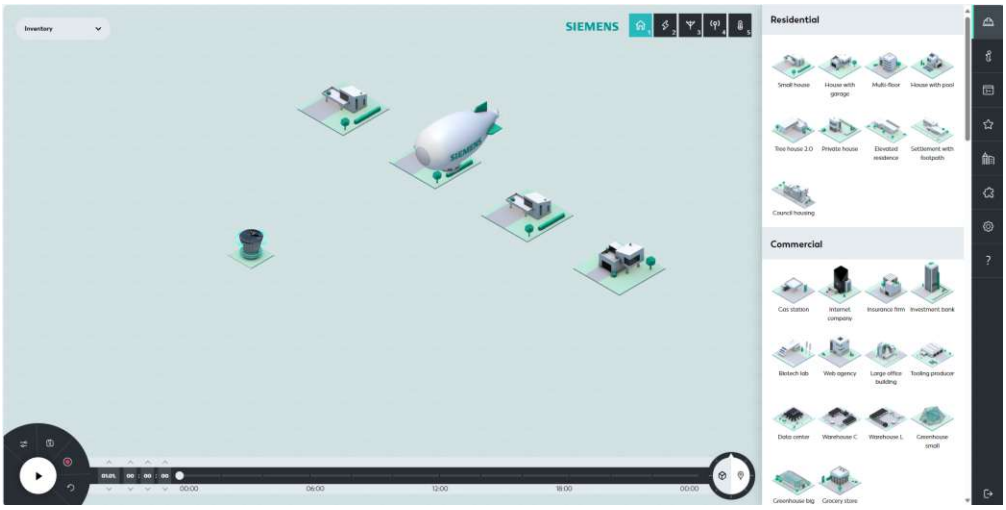


Figure 4.2: BIFROST User Interface

integrated modules are Fenrir, a sophisticated load flow solver; a comprehensive building model; and a weather generator, which provides dynamic environmental inputs for the simulation.

For the specific objectives of this thesis, a custom module is developed to simulate the shutdown and protection mechanisms of transformers and buildings. This module is designed to enable the detailed analysis of critical failure scenarios, facilitating an in-depth understanding of system vulnerabilities.

Simulation Process

The simulation operates in a time-discrete manner, commencing with an initialization phase during which all participating modules are configured and prepared. Once the initialization is complete, the simulation transitions into an iterative sequence of updates, where each module is processed in a predefined order. During each simulation step, a module retrieves relevant data from the current state, performs the required calculations based on its functionality, and updates the state with the computed values. This updated state is then made available to subsequent modules in the predefined sequence, ensuring a coherent flow of information and consistent integration across all components. This iterative process is repeated for each simulation step until the specified simulation period concludes. Such a structured approach ensures precise modeling of dynamic scenarios, enabling detailed and accurate analysis of the system's behavior over time.

The tool's inherent modularity, along with its ability to significantly expand and adapt the simulation environment through the integration of additional modules, presents a substantial advantage over conventional load flow calculators typically used for analyzing

power systems. This flexibility allows for a more comprehensive approach, particularly in scenarios requiring the adjustment of load profiles over specific time periods, a crucial feature for simulating synchronized and coordinated load attacks. Additionally, the tool's visualization capabilities further enhance its usability, enabling clearer presentation and interpretation of results. The load profiles used in the simulations are derived from historical data and offer a robust foundation for accurate and credible analysis.

4.2 Threat Analysis and Risk Assessment Framework

This section outlines the methodology for conducting a comprehensive threat and risk analysis. It explains the approach used to develop the framework and describes the key steps taken to achieve the intended results. Furthermore, it highlights the tool used during the analysis process, showcasing its contribution to effectively addressing the task.

A step-by-step explanation of the approach is included to ensure reproducibility and transparency. By detailing the structured process and adhering to established frameworks, this section underscores the methodological rigor applied, ultimately enhancing the reliability and validity of the results.

It is essential to emphasize that the analyzed system represents a generic model. A precise evaluation can, therefore, only be conducted when all specific technical details are fully available. Additionally, it is important to understand that the TARA is a dynamic and evolving document. This means it can be continuously extended and adapted as new information becomes available or as the system evolves. The level of detail within the TARA can be adjusted to varying degrees of granularity to align with the system's requirements and its current stage of development.

This flexibility ensures that the TARA remains relevant throughout the system's lifecycle, providing a robust framework for identifying and addressing emerging threats as they arise. Furthermore, the iterative nature of the TARA allows it to be revisited and refined based on ongoing analyses, technological advancements, or changes in the operational environment. This adaptability is particularly crucial for complex systems, such as smart home networks or other cyber-physical systems, where new vulnerabilities may emerge as the system scales or integrates additional components.

4.3 ISO/SAE 21434

The ISO/SAE 21434, commonly referred to as "Road Vehicles - Cybersecurity Engineering," is an international standard published in 2021 by the International Organization for Standardization (ISO) and the SAE. This comprehensive standard addresses cybersecurity across the entire lifecycle of vehicles, from conception, design, and production to operational use, maintenance, and eventual decommissioning. Its primary objective is to enable manufacturers and suppliers in the automotive sector to enhance the security of their products while ensuring compliance with mandatory regulatory frameworks such as United Nations Economic Commission for Europe (UNECE) Regulation R155. This regulation mandates specific certifications for products entering the EU market, facilitating effective countermeasures against cyber threats to protect both vehicles and their users.

The ISO/SAE 21434 provides a robust framework for identifying risks, analyzing threats, and implementing risk mitigation strategies by promoting a unified and structured approach to cybersecurity. Although the standard covers a broad spectrum of elements (see fig. 4.3), including organizational requirements and decision-making processes, this thesis focuses on a crucial subset: the TARA Methods (Clause 15) and the Item Definition from the Concept (Clause 9), which are highlighted in green in fig. 4.3. These components are utilized due to their direct relevance to evaluating system-level cybersecurity risks. Other sections of the ISO/SAE 21434 framework are excluded, as they concern product-centric processes and organizational structures, neither of which are applicable within the context of this research. Specifically, elements concerning the implementation of security culture, supplier management, and organizational responsibilities are omitted, as no formal organization or product development lifecycle is associated with the examined system. The product and post-product development phases are also not included, given the absence of a physical product and related operational processes. By focusing exclusively on the relevant subset of the framework, this thesis provides a targeted and in-depth assessment of the cybersecurity risks and mitigation strategies for a simulated smart home system. This selective application ensures methodological rigor while maintaining relevance to the thesis objectives. The chosen subset offers a systematic approach for identifying, evaluating, and mitigating cybersecurity threats, consisting of the following steps (see fig. 4.4), with the listed chapters directly derived from ISO/SAE 21434:

- **Item Definition (Chapter 9.3):** Define the system to be secured, detailing its components, interfaces, functions, and data. This step establishes system boundaries and structure, serving as the foundational starting point for the analysis.
- **Asset Identification (Chapter 15.3):** Identify critical assets, such as components, interfaces, and data, that are essential to system functionality and must be protected and secured.

- **Threat Scenario Identification (Chapter 15.4):** Identify potential threat scenarios that could compromise the previously defined assets. These scenarios consider system vulnerabilities and potential attack methods that could exploit them.

- **Impact Rating (Chapter 15.5):** Assess the potential impact of identified threats, focusing on aspects such as financial damage, safety, privacy, and operational availability. This evaluation is based on the severity of consequences and the likelihood of their occurrence.

- **Attack Path Analysis (Chapter 15.6):** Analyze potential attack paths, considering how an attacker might exploit vulnerabilities to execute threat scenarios. This step includes assessing preparatory activities and intermediate steps.

- **Attack Feasibility Rating (Chapter 15.7):** Evaluate the feasibility of attacks based on factors such as the required equipment, expertise, knowledge, window of opportunity, and elapsed time. This helps prioritize realistic and actionable threat scenarios.

- **Risk Value Determination (Chapter 15.8):** Determine the risk by combining impact ratings with attack feasibility ratings. This metric aids in the prioritization of risks and the allocation of resources for mitigation.

- **Risk Treatment Decision (Chapter 15.9):** Decide how to address identified risks through measures such as risk mitigation, transfer, or acceptance. These decisions inform the implementation of appropriate countermeasures.

- **Cybersecurity Goals (Chapter 9.4):** Define specific security objectives to address the risks identified, ensuring effective mitigation and alignment with organizational or system-wide safety requirements. This aspect falls outside the scope of this thesis.

- **Cybersecurity Concept (Chapter 9.5):** Develop a comprehensive cybersecurity concept based on the analysis. This step focuses on the implementation of security measures and the continuous monitoring and improvement of the system's security posture. This section is beyond the focus of this thesis.

The ISO/SAE 21434 standard not only provides a solid foundation for addressing modern cybersecurity challenges in the automotive sector but also serves as a valuable model for other cyber-physical systems. Its systematic emphasis on both hardware and software vulnerabilities, along with alignment with regulatory requirements, ensures robust protection against emerging cyber threats. The principles of this methodology can be effectively extended to other domains, such as smart homes, offering a structured approach to mitigate risks in highly interconnected environments.

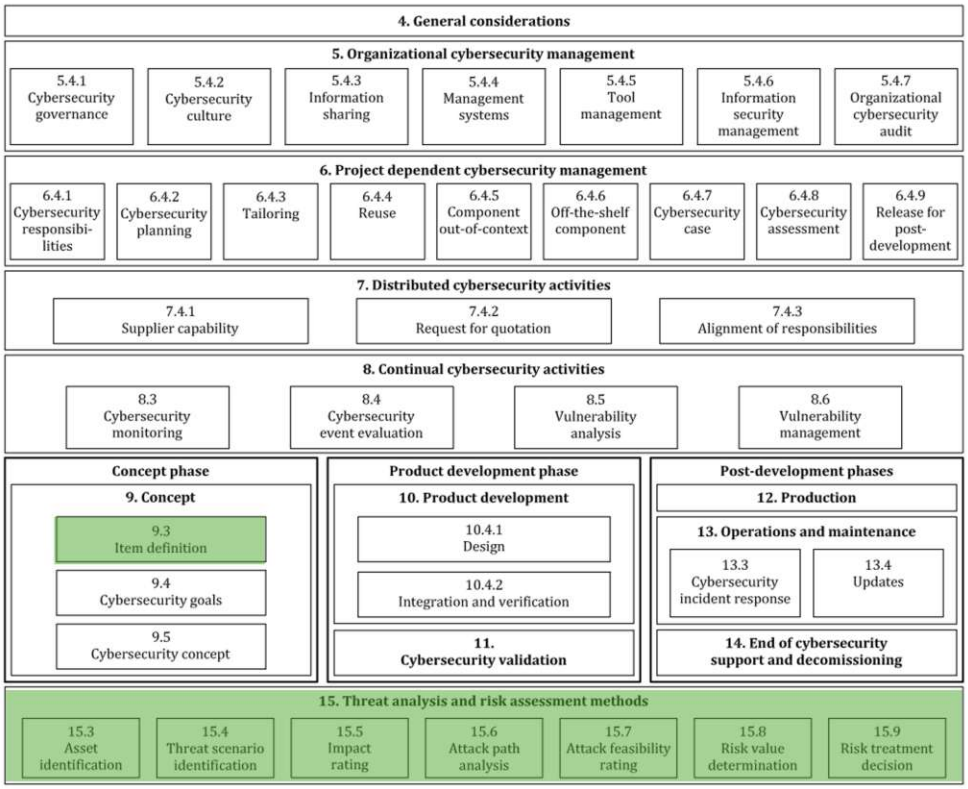


Figure 4.3: ISO/SAE 21434 Overview [64]

4.4 Itemis Secure

Itemis Secure is an advanced tool specifically designed to simplify the TARA process. Built-in compliance with the ISO/SAE 21434 standard, it offers a comprehensive and structured approach to cybersecurity engineering for complex systems. By leveraging a model-based methodology, Itemis Secure delivers several significant benefits such as:

- **Systematic and Holistic Analysis:** Model based approaches enable a systematic breakdown of complex systems into individual components, interfaces, and resources. This granular analysis simplifies the identification of potential vulnerabilities and failure points, allowing for targeted risk mitigation strategies. Additionally, the holistic nature of the model ensures that interactions between components are also considered, providing a complete view of system security.
- **Consistency and Reusability:** Models offer a unified representation of the system, thus ensuring consistency across various disciplines (e.g. Hardware and Software). Furthermore, the reusability of system models minimizes the need for repeated efforts, allowing for efficient updates with minimal adjustments.

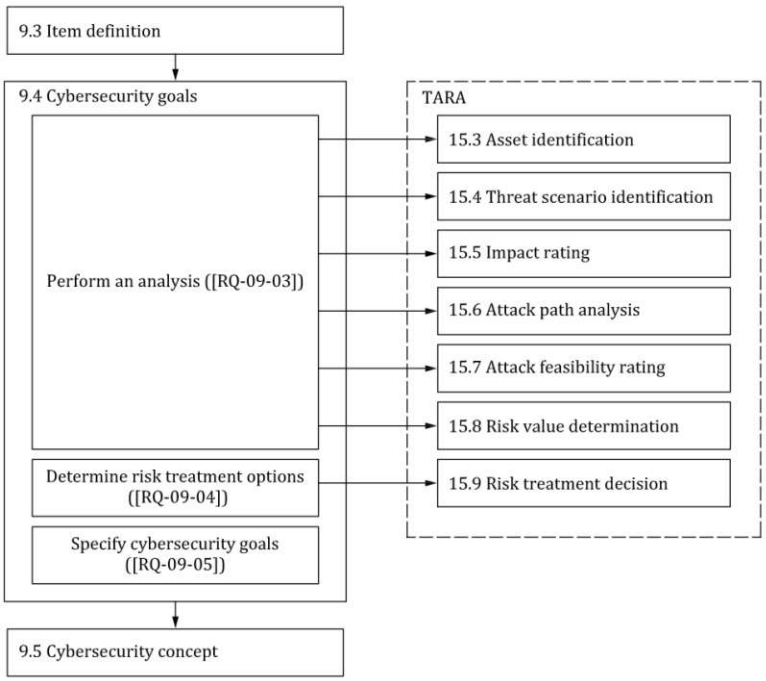


Figure 4.4: TARA Steps and Associated Processes according to [64]

This feature is particularly advantageous in iterative development environments, saving both time and resources.

- **Traceability and Compliance:** Traceability is a cornerstone of effective cybersecurity practices. It provides detailed documentation of all analysis steps, which is critical for compliance with regulations, standards, and industry best practices. Traceability also aids in quality assurance, error detection, and accountability, ensuring a transparent and auditable cybersecurity process.
- **Scalability for Evolving Systems:** Modern systems are dynamic, requiring frequent updates and expansions to accommodate new components, functionalities, or operational requirements. A model-based approach inherently supports scalability, making it easy to adapt models to reflect these changes without compromising analytical accuracy or efficiency.

An academic license, requested via **secure-info@itemis.com**, is utilized for this thesis. The provided license enables the use of this ISO/SAE 21434-compliant tool (version 24.2) to conduct the TARA process, ensuring that the analysis adheres to industry standards for cybersecurity. The step-by-step methodology is clearly outlined and demonstrated, making full use of the tool's advanced features to support a structured and comprehensive analysis of vulnerabilities and risks.

This approach ensures that all critical aspects of the system are thoroughly assessed, providing a solid foundation for reproducible and reliable results.

Figure 4.5 provides a high-level overview of the TARA process, tracing its progression from Item Definition through Threat Analysis, Asset Identification, and Impact Rating, ultimately leading to the Risk Assessment, as detailed in Section section 4.3.

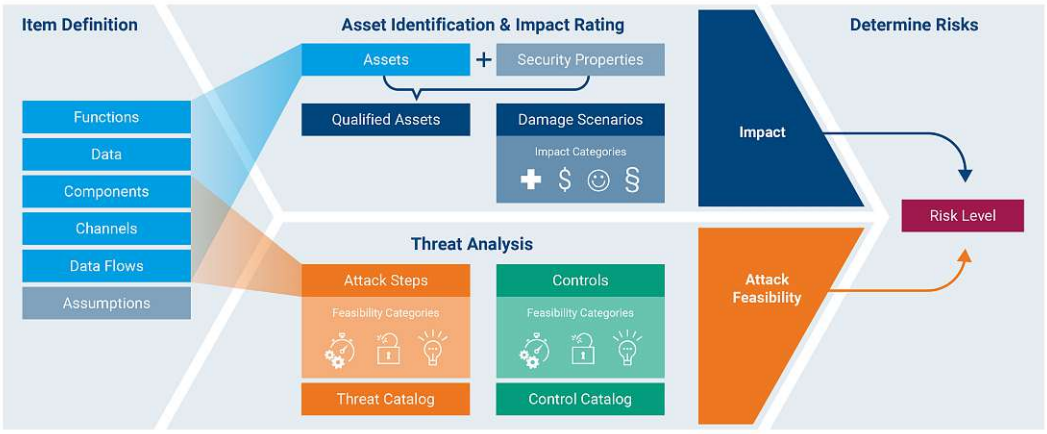


Figure 4.5: TARA process high-level Overview [66]

4.5 STRIDE and MITRE Frameworks

The STRIDE methodology and the MITRE framework are integral to the approach proposed in this thesis, as they offer a structured foundation for identifying, categorizing, and mitigating potential attack scenarios. Although not part of the ISO/SAE 21434 standard, these frameworks have been purposefully integrated to enhance the quality of the analysis framework. Leveraging comprehensive catalogs of attack techniques and controls enables a systematic and validated approach to assessing vulnerabilities, ensuring a more thorough, robust, and reliable evaluation of security risks.

4.5.1 STRIDE

The STRIDE methodology organizes potential threats into six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. This classification provides a clear approach for mapping threats to specific security objectives, making identifying and aligning vulnerabilities with appropriate mitigation strategies easier. By grouping risks into these categories, STRIDE facilitates a structured and methodical approach to securing systems, ensuring all critical aspects are considered.

4.5.2 MITRE ATT&CK

The MITRE ATT&CK framework complements this by integrating real-world, well-documented attack techniques into the analysis. Its focus on real-world adversarial behavior ensures that the scenarios considered are realistic. The framework categorizes techniques into 14 distinct tactics, each representing a specific stage or goal within an attacker's lifecycle. These tactics provide a comprehensive view of attacker behavior, enabling a deeper understanding of potential risks and more effective defense planning. These are the 14 tactics detailed in [62]:

- **Reconnaissance:** The collection of information about a target system to identify vulnerabilities and plan attacks.
- **Resource Development:** Building tools, acquiring credentials, or establishing infrastructure to prepare for attacks.
- **Initial Access:** The attacker's first breach into a system, often through phishing, exploiting vulnerabilities, or using stolen credentials.
- **Execution:** Running malicious code on a target system to establish control or execute payloads.
- **Persistence:** Maintaining access to a compromised system, often by creating backdoors or modifying system configurations.
- **Privilege Escalation:** Gaining elevated permissions, such as administrative rights, to increase access within the system.
- **Defense Evasion:** Avoiding detection by security systems, often through encryption, obfuscation, or disabling security features.
- **Credential Access:** Stealing credentials like passwords to gain further access and control of a system.
- **Discovery:** Identifying system details and resources to plan the next stages of the attack.
- **Lateral Movement:** Moving across the network to access additional systems and resources.
- **Collection:** Gathering sensitive data from compromised systems for further use or exfiltration.
- **Command and Control:** Establishing communication between compromised systems and attacker-controlled infrastructure to execute commands.
- **Exfiltration:** Stealing and transferring data from the target system to the attacker.
- **Impact:** Actions aimed at disrupting, damaging, or destroying the target system, such as wiping data for example.

MITRE Techniques

MITRE Techniques describe specific methods attackers use to achieve their goals. Each technique is tied to one or more tactics, providing detailed descriptions of the attacker's actions, the associated risks, and potential detection methods. For instance, techniques are assigned unique identifiers (Txxxx) for precise referencing, making them an essential tool for defenders to predict and counteract specific threats.

MITRE Mitigations

MITRE Mitigations are established strategies designed to counter the techniques outlined in the framework. These measures range from technical controls to organizational policies, offering actionable guidance to prevent or mitigate attacks. For example, M1030: Account Use Policies provides guidelines for enforcing account restrictions, reducing the likelihood of unauthorized access. Mitigations also have unique IDs starting with the letter M followed by a specified number, i.e., Mxxxx.

By integrating STRIDE categories with the MITRE data, this thesis adopts a comprehensive approach to analyzing and mitigating threats. STRIDE offers a high-level categorization of potential threats, while MITRE provides detailed insights into attack methods and corresponding mitigation strategies. This combined approach enables the proposed framework to facilitate a systematic assessment of vulnerabilities, ensuring the identification of realistic attack scenarios and the implementation of robust defenses tailored to cyber-physical systems.

CHAPTER 5

Experiments and Results of the LV-Grid Simulation

This chapter introduces the simulation setup and results, analyzing the impact of synchronized cyberattacks at the LV level. Additionally, it outlines and discusses the assumptions and parameters used in different configurations. These findings offer valuable insights into the effectiveness of such attacks.

5.1 Simulation Setup and Goals

The simulation is conducted using BIFROST version 6.0, with its load flow solver "Fenrir" playing a central role in determining load flows and associated electrical parameters at each simulation step. Figure 5.1 depicts the simulated network, where the number of connected houses increases based on the loading scenario while the overall structure remains unchanged.

A 400 kVA distribution transformer is modeled in the simulation. As outlined in section 2.2.5, distribution transformers typically operate within a loading range of 20-80%. Two scenarios are considered to effectively capture and analyze the impact of varying load conditions: 110 and 230 households. This range represents typical operating conditions for a 400 kVA transformer [53]. Furthermore, a standardized load profile is used to represent the average energy consumption of a single-family home with two occupants, including hot water usage. This profile, totaling approximately 3300 kWh, was developed by the Energy & IT Group of the Institute of Computer Technology (ICT) at TU Wien. Figure 5.2 depicts the annual power consumption for the specified load profile.

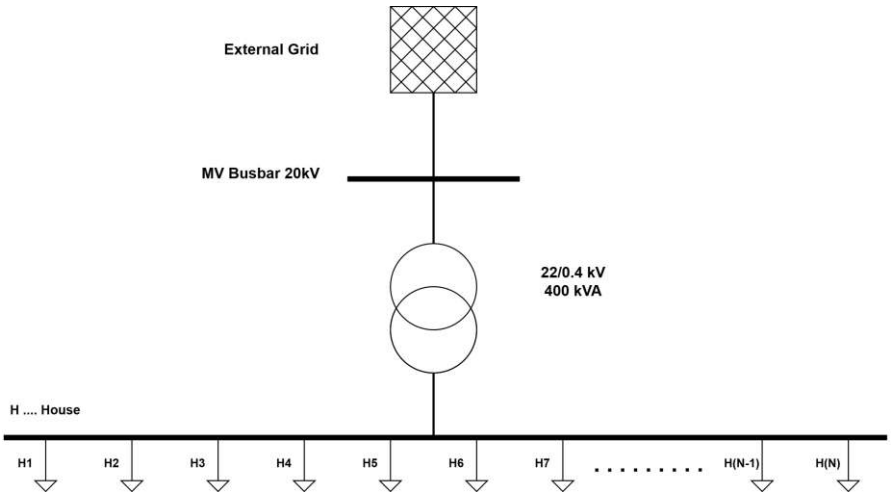


Figure 5.1: Simulated Grid

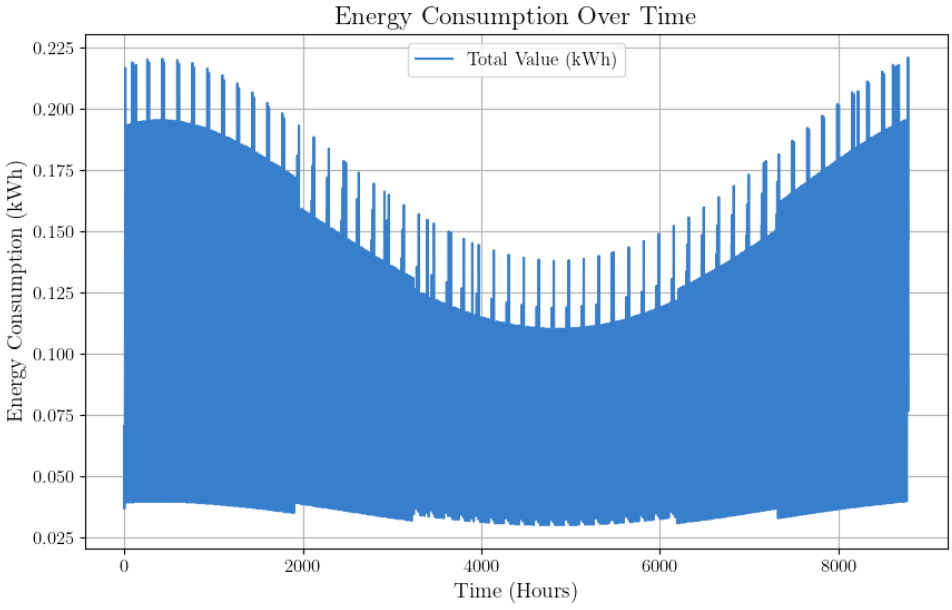


Figure 5.2: Annual energy consumption of the utilized load profile. The visible peaks represent weekend load surges, which are illustrated in greater detail in fig. 5.3 and fig. 5.4

The simulation incorporates four high-wattage devices: EVs, electric water heaters, air conditioners, and electric ovens, with the latter three representing common home appliances. Table 5.1 outlines the maximum power draw for each of these high-wattage devices.

High Wattage Device	Maximum Power Draw
EV (charging at home)	**11 kW**
Electric Oven + Cooktop	**3.6 kW [67] + 6 kW [68]**
Electric Water Heater	**5.5 kW [69]**
Air Conditioner	**3.5 kW [70]**

Table 5.1: Maximum Power Draw

The simulations are conducted separately for each device to assess its specific impact. The proportion of compromised devices will be gradually increased in 5% increments until reaching 60% to simulate realistic scenarios. A higher percentage is considered highly unlikely. This is addressed in chapter 7. Each house is assumed to have exactly one device per category (i.e., one EV, one Electric Oven, one Water Heater, and one AC). When analyzing compromised devices, the focus is on a single device type at a time rather than a mix of different categories. This reflects how vulnerabilities typically affect specific device types, as attackers usually target one type rather than multiple categories simultaneously. For instance, in a scenario with 100 homes and a 5% compromise rate, five water heaters would be affected across the simulated residential area. Additionally, when calculating percentages, the number of compromised devices is rounded to the nearest whole number. This means that, for example, in a system with 110 houses, 5% equals 5.5, which is rounded up to 6 devices.

As shown in fig. 5.2, energy demand is noticeably higher in the winter, mainly due to shorter daylight hours requiring more lighting, increased demand for hot water, and higher indoor activity as people tend to spend more time at home. As a result, attacks on EVs, electric ovens, and water heaters are simulated during the winter months, while the air conditioner, primarily used for cooling, is analyzed in the summer. Figure 5.3 illustrates the typical weekly energy consumption pattern in the winter, while fig. 5.4 shows the corresponding pattern for the summer.

These patterns suggest that in the winter, an attack would be most effective on the weekend, as baseline consumption is already higher than on weekdays. A similar trend appears in the summer, with Sunday having the highest energy demand. Figure 5.5 and fig. 5.6 highlight the typical daily energy consumption profiles for a winter Saturday and a summer Sunday, respectively, showing peak load periods. In winter, peak demand occurs between 16:30 and 19:30 on Saturdays, while in summer, it falls between 8:00 and 11:30 on Sundays. This analysis serves as the foundation for defining the simulation configurations shown in table 5.2.

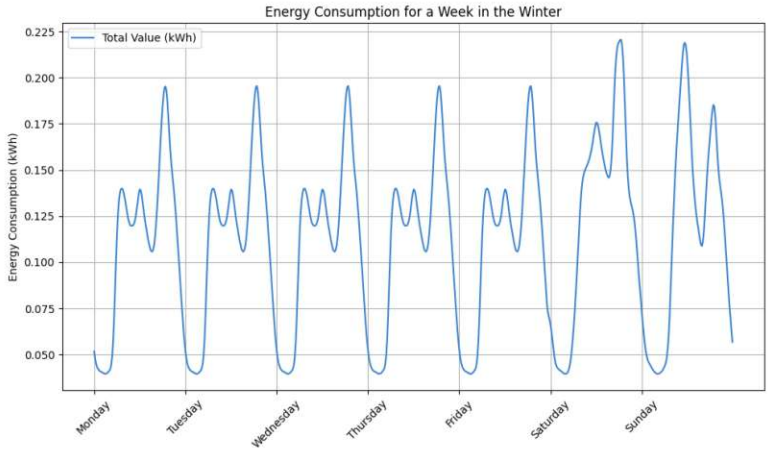


Figure 5.3: Weekly energy consumption pattern in the winter.

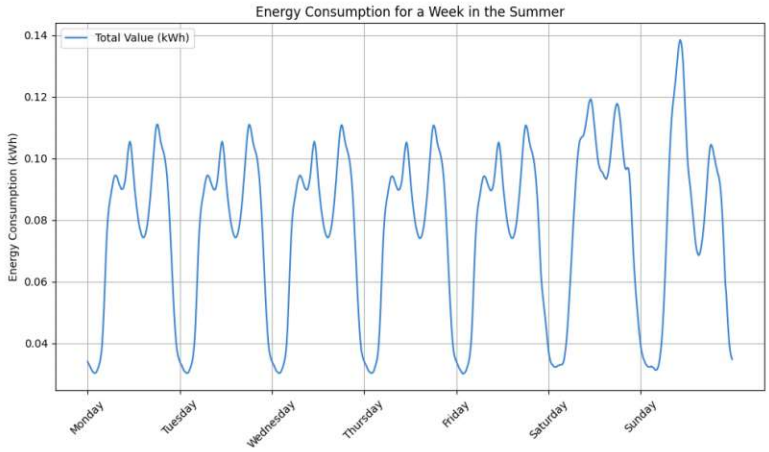


Figure 5.4: Weekly energy consumption pattern in the summer.

Number of Households	High Wattage Device	Compromised Devices/Households	Season	Time of Attack
110, 230	EVs, Electric Water Heater, Electric Oven	5%, 10%, 15%, ... 60%	Winter	Saturday 18:00
	Air Conditioner		Summer	Sunday 10:00

Table 5.2: Configurations for the Simulation

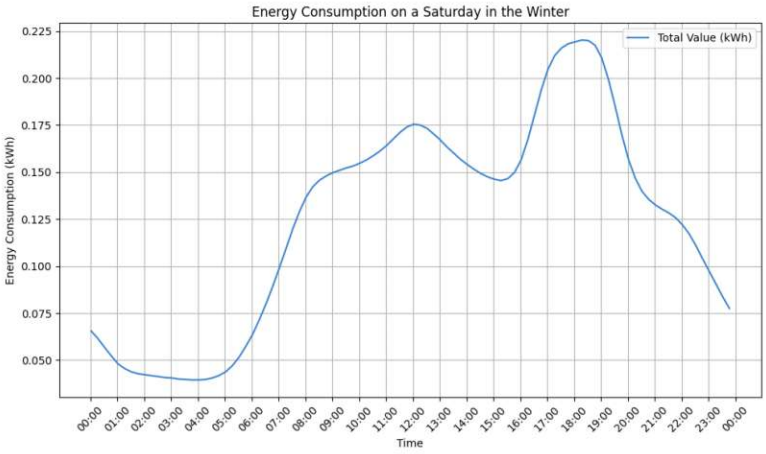


Figure 5.5: Energy consumption pattern on a Saturday in the winter

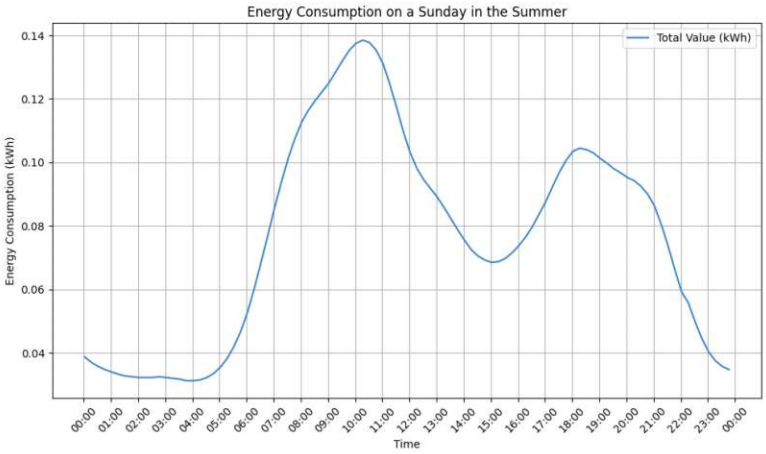


Figure 5.6: Energy consumption pattern on a Sunday in the summer

The main protective mechanism implemented for the transformer is over-current protection, which is designed to keep the transformer from overheating due to overloads or short circuits. This occurs when increased power demand at a constant voltage is needed or when faults appear in the system, resulting in a higher current. To implement this mechanism, the time-current curves of several products (see [71]) are analyzed. These functions describe the relationship between the current flowing through a fuse and the time required for it to blow, all relative to current intensity: the higher the current, the faster the fuse reacts. A curve-fitting algorithm is developed to model this relationship, resulting in this 9th-degree polynomial (see eq. (5.1)). Since the product specifications start at an over-current level of 1.5 times the rated current, with no data available for lower currents, the algorithm is designed to estimate values for tripping time below this threshold. This enables the simulation to account for all current values related to overload conditions.

$$t(I) = 10^{\begin{array}{l}(a_9(\log_{10}(I))^9 + a_8(\log_{10}(I))^8 + a_7(\log_{10}(I))^7 + \\ a_6(\log_{10}(I))^6 + a_5(\log_{10}(I))^5 + a_4(\log_{10}(I))^4 + \\ a_3(\log_{10}(I))^3 + a_2(\log_{10}(I))^2 + a_1\log_{10}(I) + a_0)\end{array}} \tag{5.1}$$

where t represents the disconnection time and I the current.

$$\begin{aligned}
a_9 &= 2.321977960757671 \times 10^2 \\
a_8 &= -5.337493604105784 \times 10^3 \\
a_7 &= 4.958370604233551 \times 10^4 \\
a_6 &= -2.193450883364582 \times 10^5 \\
a_5 &= 2.757241340863393 \times 10^5 \\
a_4 &= 1.773601391469637 \times 10^6 \\
a_3 &= -9.808109778518537 \times 10^6 \\
a_2 &= 2.219915566210992 \times 10^7 \\
a_1 &= -2.513997605611656 \times 10^7 \\
a_0 &= 1.169576770765605 \times 10^7
\end{aligned}$$

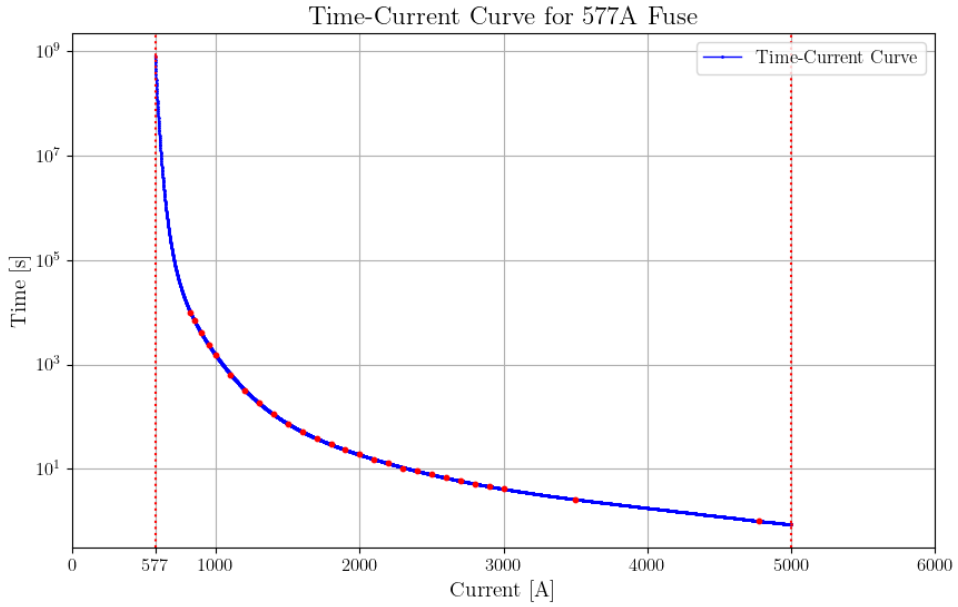


Figure 5.7: Time-current curve for a 577A fuse, with red data points indicating the values used in the curve-fitting algorithm to generate the displayed curve.

The rating for the fuse (per phase) is determined by the following equation, assuming a balanced three-phase system where the phases are separated by exactly 120 degrees. In this equation, S represents the apparent power/rated power of the transformer, measured in volt-amperes (VA):

$$I_{\text{rated}} = \frac{S}{\sqrt{3} \times V_{\textit{line-to-line}}} = \frac{400000}{\sqrt{3} \times 400} = 577\,\text{A} \tag{5.2}$$

Each simulation assumes a 15-minute attack duration, designed to reflect a stealthy and targeted approach. Since we already assume that the devices are compromised, the attack consists of adjusting these devices to draw the maximum possible power, as specified in table 5.1. This manipulation occurs during peak hours, when indoor activity is typically at its highest, meaning that residents are more likely to be at home. The brief duration of the attack reduces the likelihood of detection, as sudden power spikes may be mistaken for normal fluctuations in household energy consumption. Additionally, by limiting the attack window, adversaries can minimize anomalies that might trigger protective mechanisms or raise suspicion among occupants and grid operators. Throughout all simulations, a power factor of 0.9 is assumed, and the attack duration shall remain 15 minutes. In the result tables of the following sections, the "Overload Factor" refers to the ratio between the power drawn during the attack and the transformer's maximum capacity, which is 360 kW (the rated capacity multiplied by the power factor) in this

case. This means that if the attack leads to a 540 kW load, the corresponding overload factor would be 1.5. A successful attack is defined by the activation of the protection mechanism within a 15-minute attack window. Attacks that cause an overload but fail to trigger the protection mechanism within this period are deemed unsuccessful. The goal is to determine the percentage of devices needed to enable a successful attack within this 15-minute time frame.

5.2 Results of the 110-Household Simulation

In the result tables below, the 'Overload Factor' represents the ratio of the power drawn during the attack to the transformer's maximum capacity, which is 360 kW. Disconnection times are indicated as follows: '-' indicates no effect, '***' indicates over a month, '**' over a week and '*' over a day.

These disconnection times indicate how long it would take for the transformer to overheat and disconnect if grid operators were not to intervene. In practice, prolonged overloads that would take weeks or months to cause failure would not go unnoticed, as operators would detect abnormal loads and take appropriate measures to prevent damage. This is why the attack aims to induce higher overloads that force the transformer to disconnect within just a few minutes, reducing the opportunity for intervention and increasing the likelihood of a successful disruption.

5.2.1 EVs

Percentage of Compromised Devices [%] (Number of Devices)	Overload Factor	Time until Disconnection [hh:mm:ss]
5% (6)	0.45	-
10% (11)	0.61	-
15% (17)	0.79	-
20% (22)	0.94	-
25% (28)	1.13	***
30% (33)	1.28	**
35% (39)	1.47	07:06:17
40% (44)	1.63	02:00:52
45% (50)	1.81	00:41:05
50% (55)	1.97	00:19:25
55% (61)	2.16	00:08:50
60% (66)	2.32	00:04:59

Table 5.3: Time until transformer disconnection and overload due to compromised EVs (110 household scenario).

The results in table 5.3 highlight the relationship between the percentage of compromised EVs and the corresponding transformer response, as reflected in the time until disconnection and the overload factor columns. At low levels of compromise (5–20%), the transformer remains stable, with the overload factor staying below 1. Since the system operates within its normal capacity, no critical limits are exceeded, and there is no risk of disconnection.

At moderate levels of compromise (25–35%), the transformer begins to experience strain. At 25%, the system would still have the capacity to operate for over a month in a hypothetical scenario where no intervention from grid operators or other external entities occurs. In reality, however, such a localized overload would likely prompt a response from grid operators to mitigate the issue. At 35%, the overload becomes more severe, leading to transformer failure within seven hours.

At high levels of compromise (40–60%), the time until disconnection decreases sharply. With 40% of EVs compromised, failure occurs within a few hours, and at 50%, the transformer disconnects in just 19 minutes. Once the overload reaches nearly twice the allowed capacity, the attack is considered successful, as the transformer disconnects within the critical 15-minute threshold, cutting off the energy supply to the affected low-voltage grid.

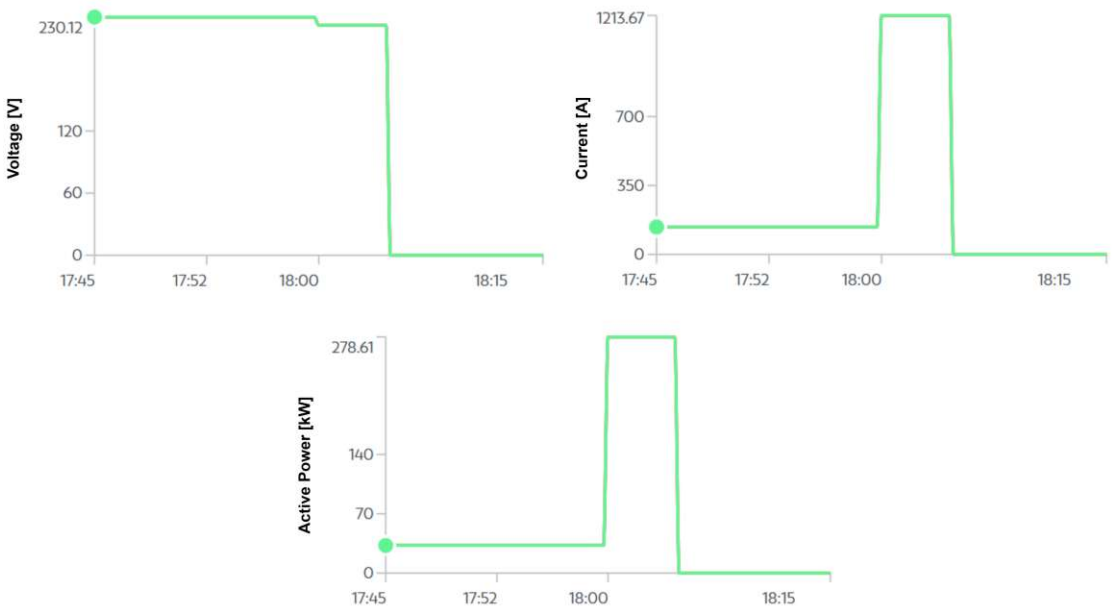


Figure 5.8: Current, Voltage, and Active Power of a Transformer Phase Under an Attack Controlling 66 EVs in a 110-Household Settlement (Attack on a Saturday at 18:00)

The three graphs shown in fig. 5.8 illustrate the different electrical parameters (Voltage, Current, and Power) being analyzed. As the attack takes effect, the voltage experiences a slight dip while the current rises sharply to meet the sudden increase in power demand.

The eventual drop of all three curves to zero signifies the activation of the protection mechanism, which disconnects the transformer. This cutoff prevents further energy from reaching the households, indicating a successful attack.

5.2.2 Electric Oven and Cooktops

Percentage of Compromised Devices [%] (Number of Devices)	Overload Factor	Time until Disconnection [hh:mm:ss]
5% (6)	0.43	-
10% (11)	0.57	-
15% (17)	0.73	-
20% (22)	0.87	-
25% (28)	1.03	-
30% (33)	1.17	***
35% (39)	1.33	*
40% (44)	1.47	06:50:12
45% (50)	1.64	01:50:48
50% (55)	1.78	00:49:4
55% (61)	1.95	00:21:41
60% (66)	2.09	00:11:47

Table 5.4: Time until transformer disconnection and overload due to compromised Electric Ovens and Cooktops (110 household scenario).

Table 5.4 shows the results for the Oven + cooktops simulation. The system remains stable at lower compromise levels (5–25%), with the overload factor staying below 1.03. This indicates that the transformer is able to withstand the additional loads introduced.

At moderate levels of compromise (30–35%), the risk of failure begins to increase. At 30%, the system can theoretically sustain operation for over a month, suggesting that intervention from grid operators would likely prevent failure. However, at 35%, the overload factor increases to 1.33 and failure is expected within a few days.

At higher compromise levels (40–60%), disconnection becomes significantly more imminent. With 40% of devices compromised, transformer disconnection occurs in approximately 6 hours and 50 minutes, while at 45%, this drops to just under 2 hours. At 50%, the system collapses within 49 minutes, and by 55%, failure occurs in only 21 minutes. Once 60% of the ovens and the cooktops are compromised (overload factor 2.09), the transformer disconnects in 11 minutes and 47 seconds, meaning the attack meets the 15-minute success threshold, effectively taking down the power supply for the affected area.

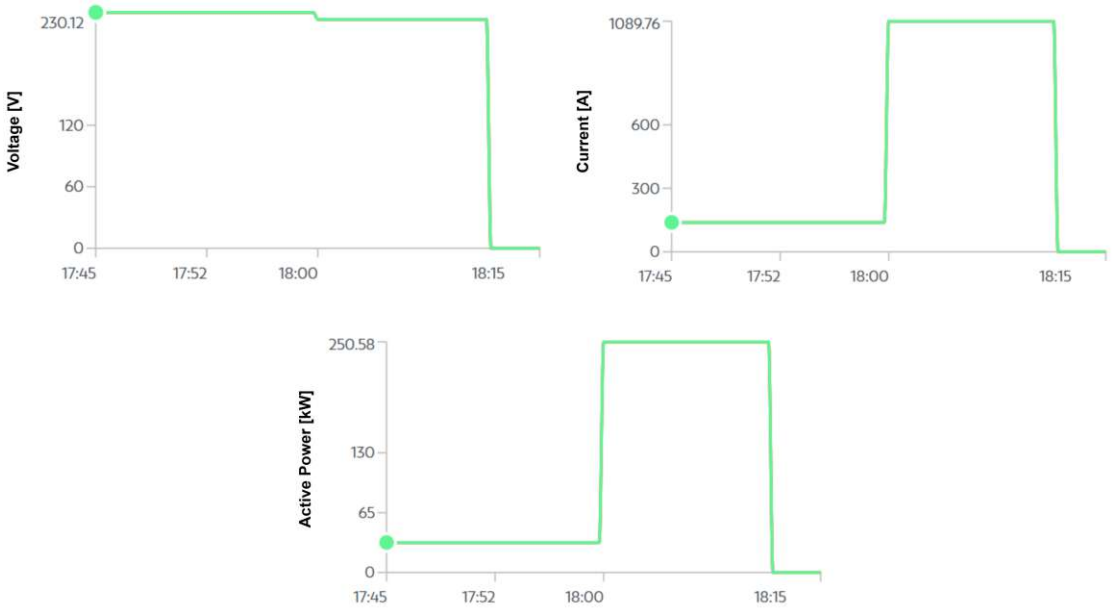


Figure 5.9: Current, Voltage, and Active Power of a Transformer Phase Under an Attack Controlling 66 Electric Oven + Cooktops in a 110-Household Settlement (Attack on a Saturday at 18:00)

The graphs in fig. 5.9 show that, for the equivalent scenario in the EV simulation (see fig. 5.8), the oven simulation also leads to a successful attack. However, the disconnection takes a few minutes longer, making the attack less efficient, though still effective, just requiring more time to achieve its goal.

5.2.3 Water Heater

The results listed in table 5.5 indicate that while cyber-attacks targeting water heaters can lead to increased transformer load, they do not pose an immediate threat of failure. Even at 60% compromise, the overload factor remains at 1.30, meaning the system experiences strain but does not reach critical instability within a short time frame.

Unlike attacks on EVs or electric oven + cooktops, where transformer disconnection can occur within minutes, compromised water heaters result in only a gradual overload. Even at high compromise levels, the system remains operational, with theoretical disconnection times exceeding a week. This indicates that, although targeting water heaters may contribute to long-term stress on the power grid, it is not an effective strategy for initiating a rapid and successful attack intended to trigger transformer disconnection, at least within the scope of the 110-household scenarios analyzed.

Percentage of Compromised Devices [%] (Number of Devices)	Overload Factor	Time until Disconnection [hh:mm:ss]
5% (6)	0.36	-
10% (11)	0.44	-
15% (17)	0.53	-
20% (22)	0.61	-
25% (28)	0.71	-
30% (33)	0.78	-
35% (39)	0.88	-
40% (44)	0.95	-
45% (50)	1.05	-
50% (55)	1.13	***
55% (61)	1.22	***
60% (66)	1.30	**

Table 5.5: Time until transformer disconnection and overload due to compromised Water Heaters (110 household scenario).

5.2.4 Air Conditioner

Table 5.6 lists the simulation results for the AC scenario. They show that even with a high percentage of compromised air conditioners, the transformer does not experience overloading. At 60% compromise, the overload factor remains at 0.82, meaning the system operates well within its capacity. However, it is essential to consider that many households may have multiple air conditioning units. In the event of an attack compromising several units per household, the resulting load could exceed the expected values, placing greater strain on the grid. Moreover, it is important to recognize that the base load of a household tends to be significantly lower in the summer than in the winter, as depicted in fig. 5.2. This is particularly true in countries with typically colder climates. This seasonal variation plays a crucial role in the overall effectiveness of an attack, as the lower baseline energy consumption during the summer months results in a reduced impact on the grid compared to winter.

Percentage of Compromised Devices [%] (Number of Devices)	Overload Factor	Time until Disconnection [hh:mm:ss]
5% (6)	0.23	-
10% (11)	0.28	-
15% (17)	0.34	-
20% (22)	0.39	-
25% (28)	0.45	-
30% (33)	0.49	-
35% (39)	0.55	-
40% (44)	0.60	-
45% (50)	0.66	-
50% (55)	0.71	-
55% (61)	0.77	-
60% (66)	0.82	-

Table 5.6: Time until transformer disconnection and overload due to compromised Air Conditioners (110 household scenario).

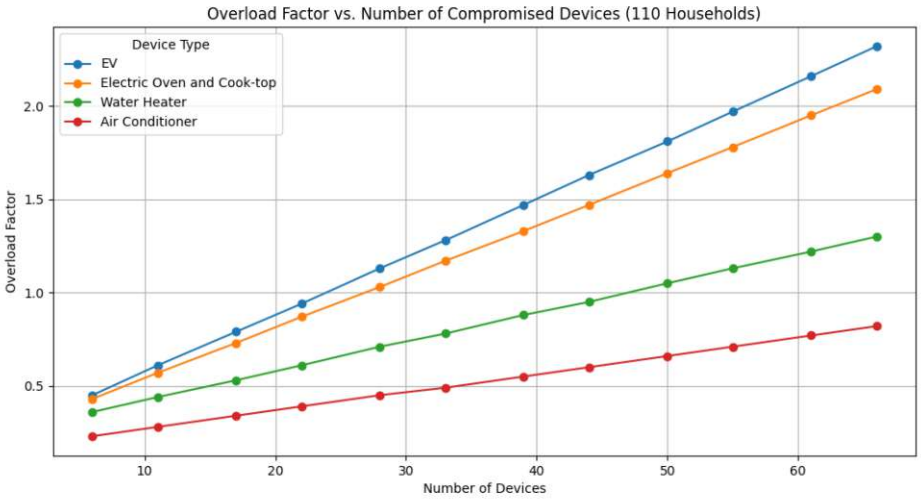


Figure 5.10: Figure: Overload Factor vs. Number of Compromised Devices for Different Device Types in a 110 Household Scenario.

Figure 5.10 illustrates that the overload factor rises accordingly as the percentage of compromised devices increases. A significant increase is observed beyond 25% compromise for EV and electric ovens, indicating their strong impact on grid stability. In contrast, air conditioners and water heaters contribute less to the overload, resulting in longer transformer disconnection times compared to EVs and electric ovens.

5.3 Results of the 230-Household Simulation

5.3.1 EVs

Percentage of Compromised Devices [%] (Number of Devices)	Overload Factor	Time until Disconnection [hh:mm:ss]
5% (12)	0.94	-
10% (23)	1.27	*
15% (35)	1.65	01:44:17
20% (46)	2.00	00:17:25
25% (58)	2.38	00:04:10
30% (69)	2.73	00:01:36
35% (81)	3.12	00:00:45
40% (92)	3.49	00:00:27
45% (104)	3.89	00:00:16
50% (115)	4.26	00:00:11
55% (127)	4.67	00:00:08
60% (138)	5.06	00:00:06

Table 5.7: Time until transformer disconnection and overload due to compromised EVs (230 household scenario).

In the 230-household simulation, EVs continue to be the most critical attack vector (see table 5.7). Even at just 10% compromise (23 EVs), the transformer reaches overload. However, no immediate disconnection occurs at this stage. When the attack level rises to 15% (35 EVs), the transformer sustains the load for approximately one hour and 44 minutes before shutting down.

As the percentage of compromised EVs increases, the disconnection time decreases drastically. At 20% (46 EVs), the transformer fails in just 17 minutes, and by 30% (69 EVs), the system collapses in under two minutes. This indicates that an attack becomes successful at just over the 20% (46 EVs) mark, as the transformer shuts down in less than 15 minutes. Beyond 35% (81 EVs), failure occurs within seconds, demonstrating how a large-scale EV-based attack could rapidly destabilize the grid. This quick failure highlights how sensitive the transformer is to EV-related attacks and the significant risk they pose for widespread power disruptions.

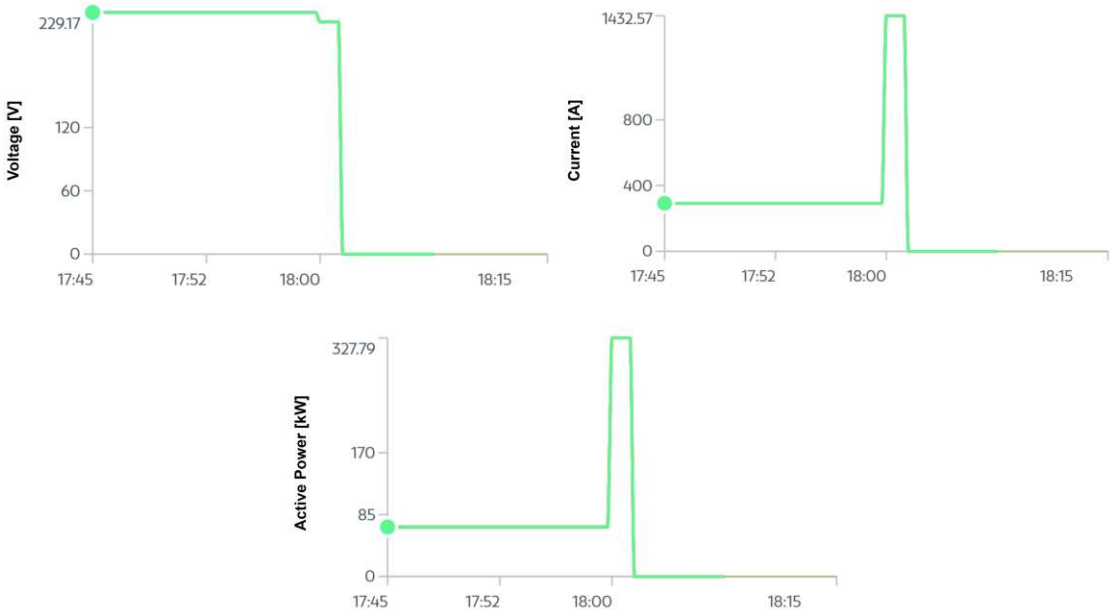


Figure 5.11: Current, Voltage, and Active Power of a Transformer Phase Under an Attack Controlling 69 EVs in a 230-Household Settlement (Attack on a Saturday at 18:00)

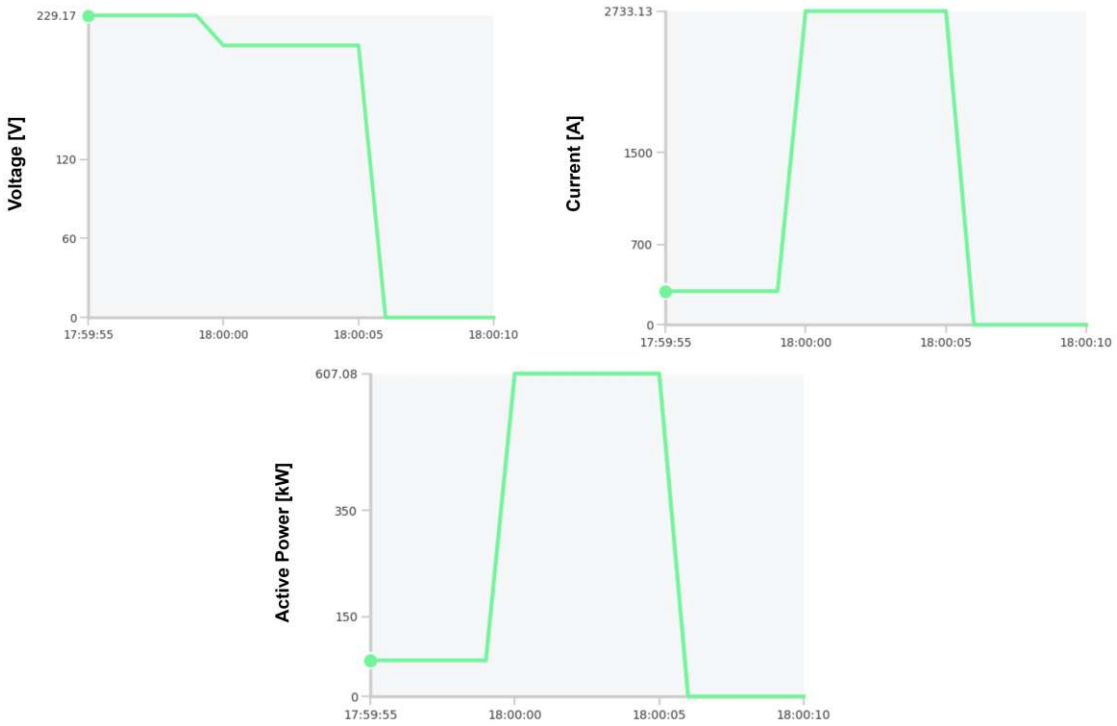


Figure 5.12: Current, Voltage, and Active Power of a Transformer Phase Under an Attack Controlling 138 EVs in a 230-Household Settlement (Attack on a Saturday at 18:00)

Figure 5.11 and fig. 5.12 present the results for scenarios in which 30% and 60% of EVs are compromised, respectively. In the 30% scenario, which corresponds to 69 vehicles and closely matches the 66 EVs affected in fig. 5.8 under the 110-household configuration, the transformer disconnects after just 1 minute and 36 seconds. Despite the comparable number of compromised EVs, the difference in household count plays a critical role in amplifying the impact. The significantly higher baseline load in the 230-household scenario intensifies the effects of the attack, highlighting the importance of system size in determining vulnerability. As a result, the failure occurs more than three times faster than in the 110-household case, where the same outcome takes nearly five minutes, representing a reduction by a factor of 3.125.

In the 60% compromise scenario, the transformer disconnects in as little as six seconds. While this outcome may appear more effective from an attacker's standpoint, achieving such a high compromise rate may be less practical to achieve over multiple LV grids simultaneously.

5.3.2 Electric Oven and Cooktop

Percentage of Compromised Devices [%] (Number of Devices)	Overload Factor	Time until Disconnection [hh:mm:ss]
5% (12)	0.89	-
10% (23)	1.20	***
15% (35)	1.53	04:11:38
20% (46)	1.83	00:36:58
25% (58)	2.17	00:08:31
30% (69)	2.48	00:03:01
35% (81)	2.83	00:01:18
40% (92)	3.15	00:00:43
45% (104)	3.50	00:00:26
50% (115)	3.83	00:00:18
55% (127)	4.19	00:00:12
60% (138)	4.52	00:00:09

Table 5.8: Time until transformer disconnection and overload due to compromised Electric Ovens and Cooktops (230 household scenario).

For electric ovens and cooktops, the results listed in table 5.8 indicate that while they are not as disruptive as EVs, they still pose a significant risk to grid stability. At just 10% compromise (23 appliances), the transformer is already overloaded, though no immediate disconnection occurs. When the attack reaches 15% (35 devices), the system endures the load for over four hours, demonstrating a slower buildup of stress compared to EVs, yet proving to be highly effective.

As more devices are compromised, the failure time decreases significantly. At 20% (46 devices), the transformer disconnects in approximately 37 minutes. When the compromise reaches 25% (58 ovens + cooktops), failure occurs in just eight minutes and 31 seconds, suggesting a successful attack. Beyond this point, any further increase in compromised devices ensures a successful attack, with the transformer failing in under 15 minutes. Once slightly more than 35% of electric ovens and cooktops are compromised, the system collapses in a matter of seconds.

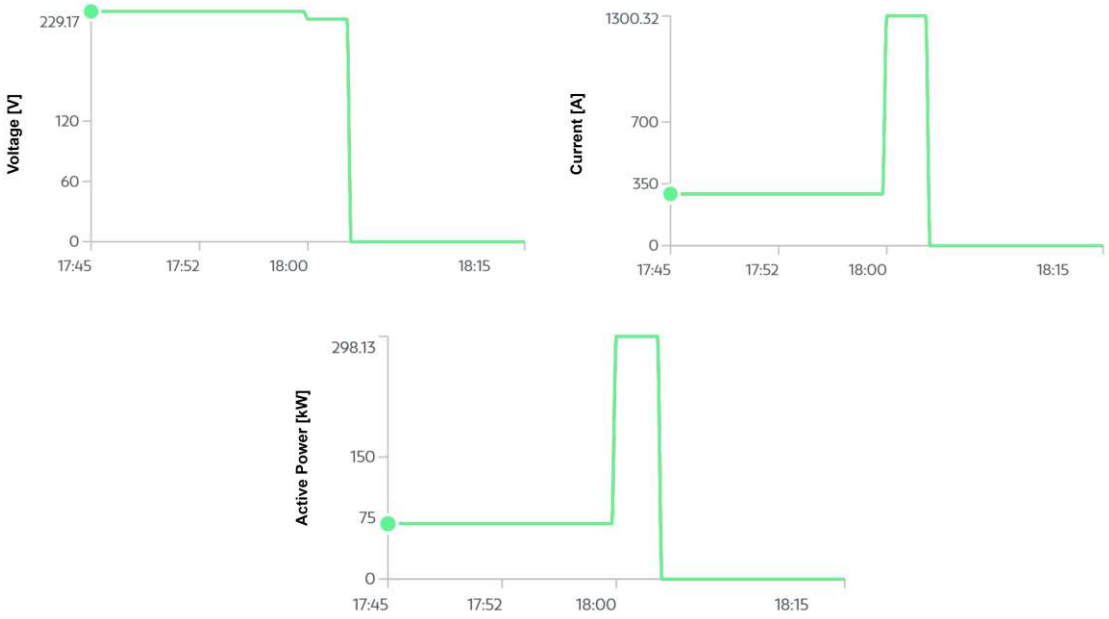


Figure 5.13: Current, Voltage, and Active Power of a Transformer Phase Under an Attack Controlling 69 Electric Oven + Cooktops in a 230-Household Settlement (Attack on 11.01 18:00)

The impact of compromising electric ovens and cooktops is illustrated in fig. 5.13 and fig. 5.14, representing scenarios where 30% and 60% of these devices are affected. When 30% are compromised, corresponding to 69 devices, the transformer disconnects after 3 minutes and 1 second. The effect unfolds much faster in this case, compared to the 110-household scenario, due to the higher baseline demand of the 230-household system. For comparison, the same number of compromised devices in a 110-household setting results in a disconnection time of 11 minutes and 47 seconds, highlighting the amplifying influence of system size and overall load conditions.

At 60% compromise or 138 devices, the response is nearly immediate, with the transformer disconnecting in just 9 seconds. This underscores the potential severity of such an attack, especially in larger networks.

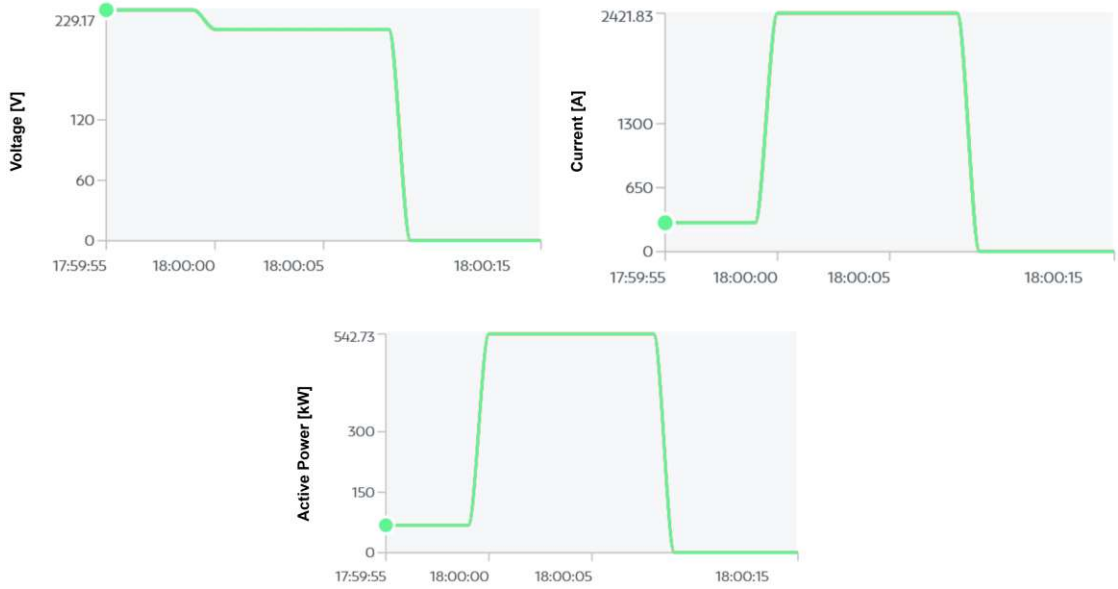


Figure 5.14: Current, Voltage, and Active Power of a Transformer Phase Under an Attack Controlling 138 Electric Oven + Cooktops in a 230-Household Settlement (Attack on 11.01 18:00)

5.3.3 Water Heater

For water heaters, the impact on the transformer builds up more slowly compared to EVs and electric ovens, as shown in table 5.9. At lower compromise levels, the system remains stable without immediate overload. However, once more than 25% (58 devices) of the water heaters are compromised, the transformer begins to struggle. The 40-41% mark is the threshold at which the attack becomes successful, causing the system to fail in under 15 minutes. While water heaters do not cause an instant breakdown, if enough units are affected, they can still lead to a successful and disruptive attack; however, a larger residential area is necessary to achieve this.

5.3.4 Air Conditioner

In the case of the air conditioners, even with up to 60% of devices compromised (which corresponds to 138 ACs in this simulation), the transformer is able to withstand the load for over an hour (see table 5.10). This means that no attack reaches the critical threshold of causing disconnection within 15 minutes. However, as previously noted, it is common for households to have multiple air conditioners, often from the same manufacturer. This increases the likelihood of a more realistic attack scenario, where the simultaneous compromise of multiple devices could lead to a much faster system failure than what the simulation results suggest. Furthermore, the seasonal fluctuations in energy demand, particularly the lower baseload in the summer compared to winter, also significantly reduce the overall effectiveness of such an attack.

Percentage of Compromised Devices [%] (Number of Devices)	Overload Factor	Time until Disconnection [hh:mm:ss]
5% (12)	0.75	-
10% (23)	0.93	-
15% (35)	1.11	-
20% (46)	1.29	*
25% (58)	1.48	06:34:57
30% (69)	1.65	01:43:02
35% (81)	1.84	00:35:35
40% (92)	2.02	00:15:39
45% (104)	2.21	00:07:17
50% (115)	2.39	00:03:58
55% (127)	2.59	00:02:16
60% (138)	2.77	00:01:28

Table 5.9: Time until transformer disconnection and overload due to compromised Water Heaters (230 household scenario).

Percentage of Compromised Devices [%] (Number of Devices)	Overload Factor	Time until Disconnection [hh:mm:ss]
5% (12)	0.47	-
10% (23)	0.61	-
15% (35)	0.70	-
20% (46)	0.81	-
25% (58)	0.93	-
30% (69)	1.04	-
35% (81)	1.16	***
40% (92)	1.27	*
45% (104)	1.39	19:33:44
50% (115)	1.50	05:29:11
55% (127)	1.62	02:08:47
60% (138)	1.73	01:05:33

Table 5.10: Time until transformer disconnection and overload due to compromised Air Conditioners (230 household scenario).

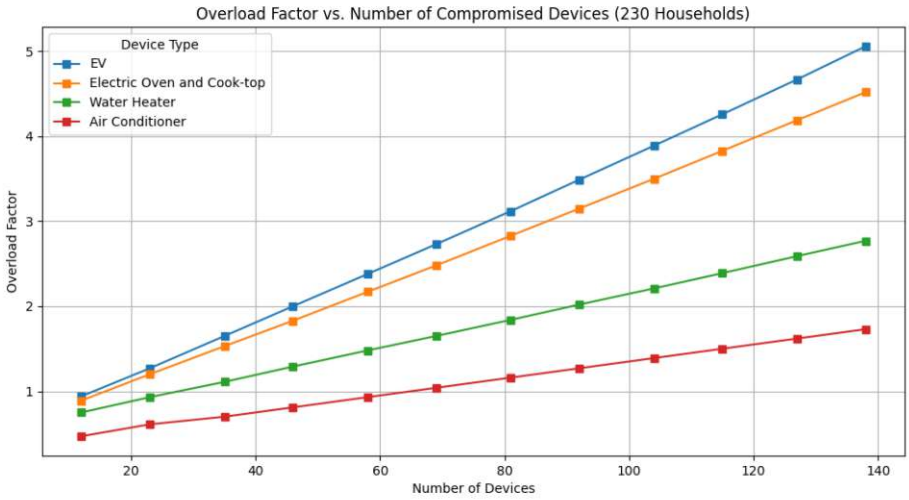


Figure 5.15: Figure: Overload Factor vs. Number of Compromised Devices for Different Device Types in a 230 Household Scenario.

The results for the 230-household scenario show a more significant rise in the overload factor as the percentage of compromised devices increases (see fig. 5.15). EVs and electric ovens, in particular, experience a sharp increase starting at around 15% compromise, which becomes even more pronounced beyond 25%. This suggests that larger household scenarios are more sensitive to device failures, especially for EVs and electric ovens. At the same time, water heaters and air conditioners have a comparatively lower impact on overload levels.

CHAPTER 6

Experiments and Results of the Threat Analysis and Risk Assessment

This chapter provides a practical demonstration of the developed TARA framework using the Itemis SECURE tool to illustrate the key steps. It presents a comprehensive walk-through of a specifically selected scenario, showcasing the analysis process and results. The structure is organized into sections that pair consecutive steps of the TARA process, as outlined in section 4.3 of the Methodology chapter. Each section combines two related components, beginning with Item Definition and Asset Identification, followed by Threat Scenario Identification and Impact Rating, and continuing with Attack Path Analysis and Attack Feasibility Rating. The final section covers Risk Value Determination and Risk Treatment Decisions. This paired-chapter approach ensures a logical flow through the entire analysis, detailing relevant tool interactions and summarizing the outcomes for the chosen scenario at each step. It provides a comprehensive, structured presentation of the process, promoting clarity, traceability, and a deeper understanding of the findings.

Figure 6.1 illustrates a simplified network diagram of the analyzed system, providing an overview of its key components and structure. A more detailed and comprehensive representation is the system diagram in the tool (see fig. 6.7), offering an in-depth technical depiction of the system's configuration and interactions. It consists of key components, including high-wattage household appliances, a home router that mediates connectivity, the internet as the broader network, an attacker targeting the system, Cloud Services (not considered in the analysis), and the Homeowner (HO) accessing the devices via a smartphone. The specific scenario under investigation involves compromising the Heating, Ventilation and Air Conditioning (HVAC) system to simulate an unauthorized temperature reduction, exploring the resulting risks and potential damages. This scenario was intentionally chosen as it exemplifies the compromise of a high-wattage device, a

critical component relevant to the simulated analyses and findings detailed in chapter 5 of this thesis. Specifically, it represents the simulation of coordinated attacks targeting high-wattage devices in smart homes to manipulate and increase energy consumption. Its selection ensures a strong alignment with the core research objectives, highlighting and reinforcing the key aspects and outcomes of the study related to load manipulation and its potential impact on grid stability.

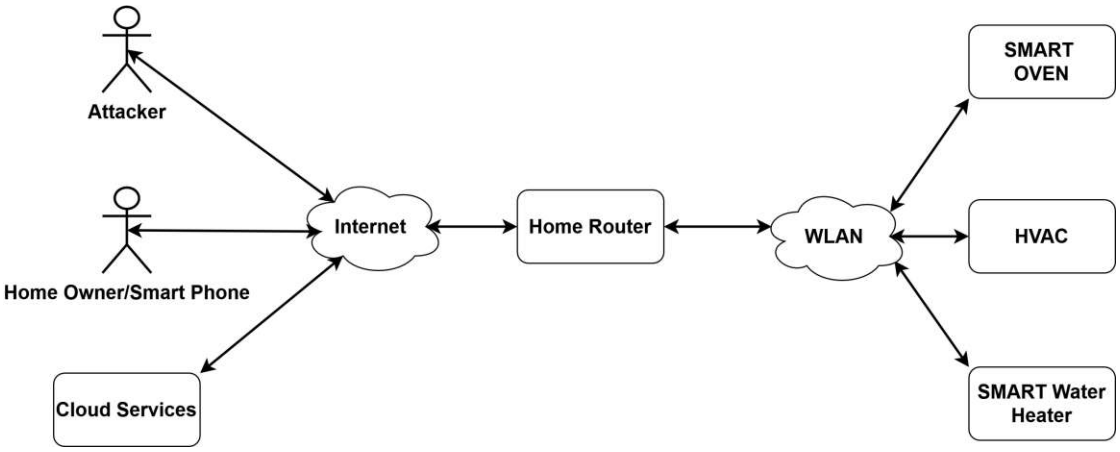


Figure 6.1: Network Diagram of the considered system

The results of this analysis are accessible through the tool as a packaged project file, thesis_tara.zip, enabling interactive exploration within Itemis SECURE. Additionally, a detailed report, tara_report.docx, compiles the complete analysis and findings, serving as a comprehensive and structured narrative of the threat modeling process, impact assessment, and recommended mitigations. This report provides a valuable alternative for scenarios where the tool is unavailable, or the project file cannot be accessed, ensuring that the complete analysis remains reviewable and reproducible. Both formats support in-depth technical evaluation and accessible documentation of the results.

6.1 Item Definition & Asset Identification

6.1.1 Item Definition & Asset Identification Tool Details

In the Item Definition phase, the system diagram within the tool is utilized to model the analyzed system. Various elements represent different aspects of the system, as shown in fig. 6.2. These include *Component*, *Data*, and *Channel* elements. Physical hardware components (e.g., HVAC systems, routers) are modeled as *Component* elements. Software, communication signals, and messages are represented as *Data* elements, while the communication pathways between hardware components are modeled as *Channel* elements. The selection for the *Data* elements is a deliberate methodological choice rather than a requirement of the tool, as representing these digital components as data elements provide a more precise and contextually appropriate abstraction for the analysis.

All the listed elements can be directly created within the system diagram or through system chunks, which offer additional detail while still creating the blocks in the system diagram.

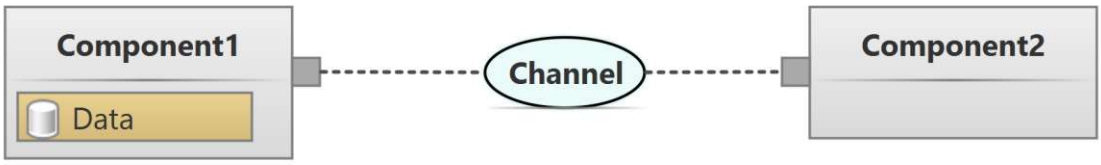


Figure 6.2: Element blocks in the tool

Component chunks (see fig. 6.3) define physical or logical components and are structured as follows:

- **Name:** A unique identifier for the component.
- **Title:** A descriptive title.
- **Description:** An explanation of the component's role or purpose.
- **Stored Data:** Any data or software stored in or running on the component.
- **Technologies:** Supported communication technologies e.g. Ethernet, Transport Control Protocol (TCP)/Internet Protocol (IP).
- **Child Components:** Subcomponents of the described component e.g. the microcontroller of the HVAC system.

```
Component Component_Name: Component_Title
Component_Description Edit
Stored Data  <no stored data>
Technologies <no technologies>
{ <0 child components> }
```

Figure 6.3: A *Component* chunk depicted in the tool

Data chunks (illustrated in fig. 6.4) define data elements (e.g. software, signals and messages) and follow this structure:

- **Name:** The data element name (e.g., HVAC_FW). For this analysis message names start with "MSG_"
- **Title:** A descriptive title (e.g., HVAC Firmware).
- **Description:** A detailed description of the data.

- **Contained Data:** Any nested data elements e.g. a specific routine defined in the Software.

```
Data Data_Name: Data_Title
Data_Description Edit
{
  Contained Data <no contained data>
}
```

Figure 6.4: *Data* chunk structure

Channel chunks (see fig. 6.5) define communication pathways between n components and are organized as:

- **Name:** A unique channel name starting with "CH_" in the case of the implemented system.
- **Title:** A descriptive title (e.g., TCP Channel).
- **Description:** An explanation of the channel's purpose.
- **Endpoints:** Components connected by the channel.
- **Technologies:** Communication technologies supported by the channel.
- **Data Flow:** A different element explained in the next paragraph.

```
Channel Channel_Name: [No Endpoints] [-]
Channel_Description Edit
Endpoints    <no endpoints>
Technologies <no technologies>
{
    Data Flow Dataflow_Name: [No Data]: [No Source] -> [No Target] [-]
    Dataflow_Description Edit
    {
      Direction        <no source> -> <no target>
      Transferred Data <no transferred data>
      Technologies     <no technologies>
    }
}
```

Figure 6.5: *Channel* chunk structure

Furthermore, *Functions* and *Data Flows* play a crucial role in modeling system behavior, even though they are not explicitly depicted in the system diagram. *Functions* describe

system operations, while *Data Flows* represent information transfer between exactly two endpoints on a channel, specifying the direction and type of data being exchanged.

Data Flows chunks are always part of a channel (see fig. 6.5) and have the following properties:

- **Name:** A short identifier for the data flow.
- **Title:** A descriptive title.
- **Description:** A detailed description of the data flow.
- **Direction:** Specifies the source and target components.
- **Transferred Data:** References to the data elements transmitted.
- **Technologies:** Technology tags derived from the channel or customized for the specific data flow (e.g., Bluetooth or TCP/IP).

Finally *Function* chunks are defined as follows:

- **Name:** A unique function name (e.g., Func_HVAC_ON). For the implemented analysis all function names start with "Func_".
- **Title:** A descriptive title (e.g., Turn HVAC ON).
- **Description:** A detailed description of the function.
- **Child Functions:** Nested subfunctions e.g. the function turning on the HVAC system could have a child function specifying the message necessary to turn on the device.

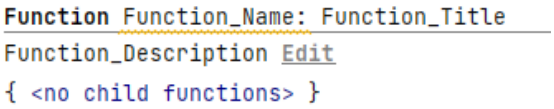
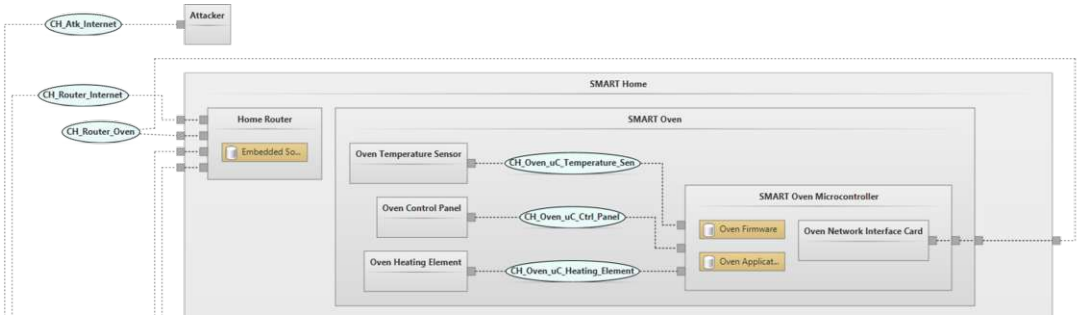


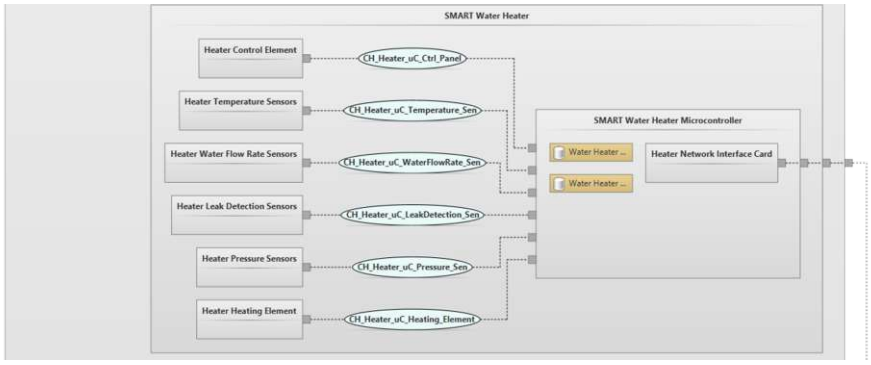
Figure 6.6: *Function* chunk in the tool

6.1.2 Item Definition & Asset Identification Outcomes

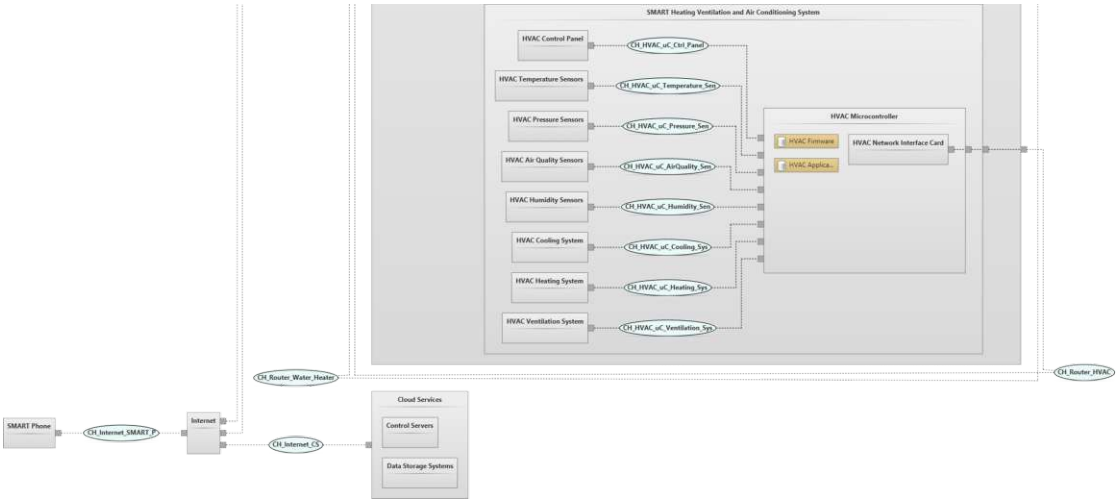
The system under investigation (see fig. 6.7) represents a smart home equipped with high-wattage devices, which are central to the thesis topic. To facilitate a structured analysis, a simplified system model is considered, comprising a smart water heater, smart oven, HVAC system, and a home router. External entities, such as the internet, potential attackers, and the smartphone of the HO, are also included in the analysis, as they play a significant role in influencing the system's security, even though they are not direct components of the system.



(a) System Diagram (a)



(b) System Diagram (b)



(c) System Diagram (c)

Figure 6.7: System Diagram of System Under Investigation

Each smart home device within the system integrates essential sensors and actuators to execute their designated functions. For example, the HVAC system includes the following key components:

- **Control Panel**
- **Temperature Sensors**
- **Pressure Sensors**
- **Air Quality Sensors**
- **Humidity Sensors**
- **Cooling System**
- **Heating System**
- **Ventilation System**
- **Microcontroller**

Beyond physical components, the microcontroller that handles the control logic incorporates both firmware and application software. Additionally, specific messages are defined to initiate and control various functions of the HVAC system. Both the software components and corresponding messages are modeled as data elements, represented by *Data* chunks, as shown in fig. 6.8.

```
Data HVAC_Firmware: HVAC Firmware
<no description> Edit
{
  Contained Data <no contained data>
}
Data HVAC_APP_SW: HVAC Application Software
<no description> Edit
{
  Contained Data <no contained data>
}
```

```
Data MSG_Increase_HVAC_Temp: Increasing HVAC temperature
<no description> Edit
{
  Contained Data <no contained data>
}
Data MSG_Decrease_HVAC_Temp: Decrease HVAC temperature
<no description> Edit
{
  Contained Data <no contained data>
}
```

Figure 6.8: Data elements of the analyzed scenario

Another key aspect of the analysis focuses on the communication channels between components responsible for transmitting signals and messages. Identifying the technologies or protocols used for these communications allows for more granular analysis and the selection of appropriate security measures. The HVAC system, along with other household appliances, is connected to the internet via the home router, providing access to external entities such as the homeowner's smartphone or potential attackers. Figure 6.9 illustrates the channel defined between the Network Interface Card (NIC) of the HVAC system and the home router. Additionally, two data flows are specified to represent the activation

and deactivation of the home appliance. Both data flows originate from the router and are directed toward the HVAC system, reflecting control messages sent from external devices like the homeowner's smartphone. In the tool, data flows capture the direction of communication, the communication partners, and the messages or signals transmitted between components.

```
Channel CH_Router_HVAC: Home_R, HVAC_NIC [Wi-Fi]
<no description> Edit
Endpoints     [E_1] Home_R: Home Router
              [E_2] HVAC_NIC: HVAC Network Interface Card
Technologies Wi-Fi: Wirless Network Protocol
{
    Data Flow DF.5: MSG_Turn_ON_HVAC: Home_R -> HVAC_NIC [Wi-Fi]
    <no description> Edit
    {
      Direction        E_1 (Home_R: Home Router) -> E_2 (HVAC_NIC: HVAC Network Interface Card)
      Transferred Data MSG_Turn_ON_HVAC: Command to turn ON HVAC
      Technologies     Wi-Fi: Wirless Network Protocol
    }
    Data Flow DF.6: MSG_Turn_OFF_HVAC: Home_R -> HVAC_NIC [Wi-Fi]
    <no description> Edit
    {
      Direction        E_1 (Home_R: Home Router) -> E_2 (HVAC_NIC: HVAC Network Interface Card)
      Transferred Data MSG_Turn_OFF_HVAC: Command to turn OFF HVAC
      Technologies     Wi-Fi: Wirless Network Protocol
    }
}
```

Figure 6.9: Channel between the HVAC system and the Home Router

After specifying the physical and digital elements of the system, the next step involves defining its functions, which represent the operations or tasks performed by the system or its individual parts. These functions encompass a wide range of activities, from technical processes such as software updates to routine actions like heating, cooling, or ventilation within a smart home environment. For example, fig. 6.10 provides an overview of key functions executed by the HVAC system, highlighting its essential role in regulating and maintaining the home's climate control.

```
Function Func_ON_HVAC: Turn ON HVAC
<no description> Edit
{ <no child functions> }
Function Func_OFF_HVAC: Turn OFF HVAC
<no description> Edit
{ <no child functions> }
Function Func_Increase_Home_Temp: Increase home temperature
<no description> Edit
{ <no child functions> }
Function Func_Decrease_Home_Temp: Decrease home temperature
<no description> Edit
{ <no child functions> }
```

Figure 6.10: Functions in the TARA tool

By clearly defining components, data, data flows, communication channels, and functions, the analysis establishes a comprehensive understanding of the system, forming the foundation for identifying vulnerabilities, assessing risks, and implementing targeted security measures. All defined elements have to be individually assessed to determine whether they qualify as assets. An element is considered an asset if its compromise could lead to adverse consequences, such as physical harm, disruption of services, or breaches of digital privacy, thereby impacting individuals, most notably homeowners.

In the analyzed smart home context, all defined system elements, including physical devices, software, communication channels, and associated data, have been classified as assets due to their critical role in maintaining system functionality and security. Any compromise of these assets could result in significant damage, such as unauthorized control over high-wattage devices, privacy violations, or disruptions to household operations. This classification ensures that the subsequent threat analysis and risk assessment comprehensively address potential vulnerabilities and their impacts on the system and its users.

As outlined previously, the system components identified as assets must be adequately protected, as their compromise could result in significant damage. Within the context of the TARA methodology, such damages are documented as Damage Scenarios. According to ISO/SAE 21434, a Damage Scenario defines a specific situation in which potential Threat Scenarios expose the system or its components to negative impacts, leading to disruptions in functionality and possibly causing harm to individuals, property, or the environment.

Damage Scenarios play a critical role in identifying and understanding the consequences of Threat Scenarios, enabling the implementation of targeted mitigation measures and effective risk management strategies. For the TARA conducted in this thesis, the Damage Scenario "Unauthorized decrease of home temperature" is considered. The selection of this Damage Scenario is driven by its direct impact on increased energy consumption, making it a highly relevant example for the focus of this thesis. The steps described throughout this chapter are illustrated using this Damage Scenario to provide a clear and cohesive explanation of the methodology. Additional Damage Scenarios of interest for this analysis, though beyond the scope of this thesis, could include:

- **Oven overheating (continuous operation):** Potential fire hazards or energy wastage.
- **Constant water heating (continuous operation):** Increased energy consumption and potential system degradation or failure.
- **Disabling safety features of the water heater:** Increased risk of overheating or scalding.
- **Disabling HVAC energy-saving modes:** Inefficient energy usage and increased operational costs.

6.2 Threat Scenario Identification & Impact Rating

6.2.1 Threat Scenario Identification & Impact Rating Tool Details

Impact Rating

A critical component of the TARA process is the Impact Rating, which evaluates the potential consequences of a Damage Scenario. This assessment considers the worst-case direct effects on the system and its stakeholders. In accordance with ISO/SAE 21434 [64] and the Itemis Secure tool [66] employed in this thesis, four key categories are analyzed, each graded on a four-level scale of severity:

- **Safety:** This category evaluates the risks to individuals' physical well-being that could arise from a compromised system or component. It accounts for potential physical injuries or health hazards.
  - **0 - Negligible:** No injuries.
  - **1 - Moderate:** Light to moderate injuries.
  - **2 - Major:** Severe or life-threatening injuries, but survival is probable.
  - **3 - Severe:** Life-threatening injuries where survival is uncertain or fatal outcomes are possible.
- **Operational:** This measures the effects on system functionality and performance. It considers disruptions that might lead to inefficiencies or failures in providing intended services.
  - **0 - Negligible:** No impairment or non-perceivable impact on system functions.
  - **1 - Moderate:** Partial degradation of system functions (e.g., reduced user satisfaction).
  - **2 - Major:** Significant loss or impairment of an important system function (e.g., major annoyance to the user).
  - **3 - Severe:** Complete loss or impairment of core system functionality (e.g., system becomes non-operational or exhibits unexpected behavior in critical functions).
- **Financial:** This category assesses the economic consequences of a Damage Scenario, including repair costs, legal liabilities, or other financial burdens faced by individuals or organizations.
  - **0 - Negligible:** Negligible financial effects or irrelevant consequences.
  - **1 - Moderate:** Minor consequences that can be addressed with limited resources.
  - **2 - Major:** Substantial financial consequences that are challenging but manageable.

  - **3 - Severe:** Catastrophic financial losses that the affected party might not overcome (bankruptcy).

- **Privacy:** This category evaluates the potential consequences of unauthorized access or disclosure of sensitive information, leading to breaches of data confidentiality.
  - **0 - Negligible:** No privacy-related effects or irrelevant consequences. Information is not sensitive and difficult to link to a specific individual (Personal Identifiable Information (PII) principal).
  - **1 - Moderate:** Minor inconvenience to the individual. Information is either sensitive but difficult to link, or non-sensitive but easy to link to a PII principal.
  - **2 - Major:** Serious privacy impact. Information is either highly sensitive and difficult to link, or sensitive and easy to link to a PII principal.
  - **3 - Severe:** Significant or irreversible privacy impact. Information is highly sensitive and easily attributable to a specific individual.

The Impact Rating not only helps to understand the severity of potential Damage Scenarios but also provides a foundation for prioritizing risks and implementing targeted mitigation measures. By systematically categorizing and evaluating these impacts, TARA ensures a comprehensive and structured approach to securing systems against both foreseeable and unforeseen threats.

This methodology underscores the importance of addressing safety, operational reliability, financial resilience, and data protection in the design and management of smart systems.

Damage Scenarios

In the tool, a Damage Scenario is represented using a dedicated Damage Scenario chunk, as illustrated in fig. 6.11 . This chunk contains the following key properties:

- **Name:** A unique name or identifier for the Damage Scenario e.g., DS.1.
- **Title:** A descriptive label providing an intuitive understanding of the Damage Scenario.
- **Description:** A comprehensive explanation detailing the nature and context of the Damage Scenario.
- **Concerns:** A structured list of qualified assets, each pairing a cybersecurity property with a specific system element or function. These qualified assets represent the specific components and their relevant security attributes that are affected by the Damage Scenario.
- **Impact:** An evaluation of the scenario's impact, evaluated according to the predefined Impact Categories described in section 6.2.1.

- **Threat Scenarios:** A read-only attribute automatically listing the Threat Scenarios linked to the Damage Scenario, providing traceability within the analysis.

The Impact Level (IL) (top right corner) for the Damage Scenario depicted in fig. 6.11 is determined by identifying the highest impact across all evaluated categories (Safety, Financial, Operational, Privacy) i.e. if the "Operational" category has an impact level of 2 (Major) and all other categories have lower values, the overall impact level of the Damage Scenario will be 2 (Major). This is illustrated more clearly in fig. 6.13.

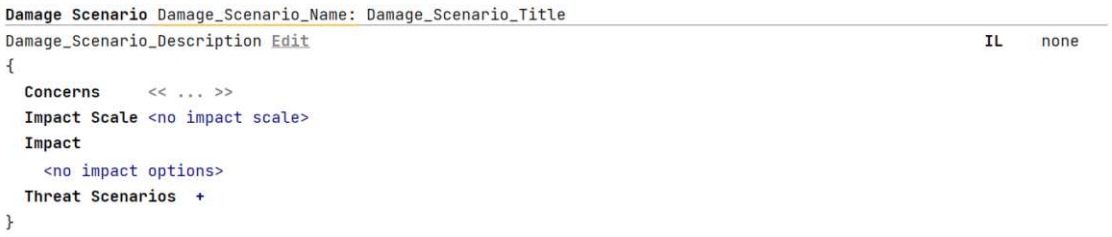


Figure 6.11: Damage Scenario in the TARA tool

Threat Scenarios

A Threat Scenario represents a potential high-level attack that can lead to one or multiple Damage Scenarios. It is implemented through a series of attack steps, often modeled as attack trees. The following properties describe a Threat Scenario chunk (see fig. 6.12):

- **Name:** A unique name or identifier for the Threat Scenario e.g., TS.1.
- **Title:** A descriptive title that clearly conveys the nature of the Threat Scenario.
- **Description:** A detailed explanation outlining the context and characteristics of the Threat Scenario.
- **Cause of Compromise:** The STRIDE category responsible for the compromise, selected from the active Threat Catalog, which can be customized to meet specific analytical needs. For the purposes of this thesis, the threat catalog has been specifically adapted using the STRIDE and MITRE ATT&CK frameworks. A comprehensive discussion of the threat catalog is presented in section 6.3.3.
- **Acts on:** The system element directly affected by the Threat Scenario.
- **Compromises:** A read-only attribute listing the cybersecurity properties that are compromised. It is derived from the "Cause of Compromise" property.
- **Threatens:** An optional attribute listing other Threat Scenarios that are influenced or exacerbated by the current scenario. This attribute is not utilized in this thesis.

- **Attack Tree:** Maps the sequence of attacks that could result in the realization of the Threat Scenario. The Attack tree can consist of a single attack step or a sequence/combination of multiple attack steps.
- **Realizes:** Lists the Damage Scenarios that may arise as a result of the described Threat Scenario.
- **Lessened by:** A list of assumptions that reduce the risk associated with the Threat Scenario. This property is not incorporated in the analysis as no assumptions are defined.
- **Local Risk Level:** The calculated Risk Level (RL). When expanded, it displays the RL categorized by stakeholder and impact category. In the context of this analysis, the sole stakeholder is the HO. The calculation of the RL is derived from the Risk Matrix, which is discussed in section 6.4.1.

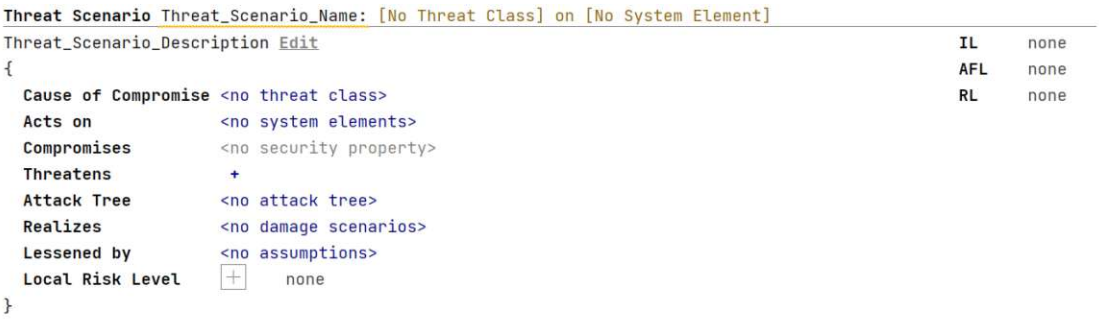


Figure 6.12: Threat Scenario in the TARA tool

Like Damage Scenarios, Threat Scenarios are also assigned an IL, which they inherit from the Damage Scenarios they realize. For instance, if a Threat Scenario encompasses Damage Scenarios DS.1, DS.2, and DS.3 with ILs of "Negligible," "Moderate," and "Severe," respectively, the Threat Scenario adopts the highest IL - in this case "Severe."

In addition to an IL, the Threat Scenario is characterized by an Attack Feasibility Level (AFL) and a RL. The AFL is derived from the attack steps listed in the "Attack Tree" property by selecting the highest AFL among them. Possible AFL ratings include "Very Low", "Low", "Medium", and "High" with detailed evaluation criteria explained in section 6.3.1. Attack steps may involve logical relationships, including AND connections (e.g., must(AS.1, AS.2, ...)) and OR connections (e.g., may(AS.3, AS.4, ...)), or combinations of both (e.g., must(AS.1, AS.2, may(AS.3, AS.4))). These logical operators determine whether all listed steps are mandatory or if multiple optional paths can achieve the Threat Scenario.

If a Threat Scenario contains only one attack step, its AFL is identical to that of the listed step. In OR (may()) operations, the AFL is the highest among the available steps, as an attacker will typically choose the most effective path. For example, may(AS.1, AS.2,

AS.3) with AFLs of "Low", "Very Low", and "Medium", respectively, assigns "Medium" as the AFL for the Threat Scenario. Conversely, in AND (must()) operations, the AFL reflects the lowest feasibility level since the attacker must overcome all steps. Therefore, must(AS.1, AS.2, AS.3) with corresponding AFLs of "Low", "Very Low", and "Medium" yields an overall AFL of "Very Low", as the hardest step limits the attack's success. For nested combinations, such as may(AS.1, AS.2, must(AS.3, AS.4)), the rules are applied hierarchically, evaluating from the innermost logic outward.

Finally, the RL is determined by combining the IL and AFL using the Risk Matrix described in section 6.4 and depicted in fig. 6.23. This structured methodology ensures a holistic and rigorous risk assessment by integrating both the severity of potential impacts and the feasibility of attacks.

6.2.2 Threat Scenario Identification & Impact Rating Outcomes

Impact Rating

Based on the Damage Scenario "Unauthorized Decrease of Home Temperature", as illustrated in fig. 6.13, the following impact ratings have been determined, with the following rationale for each rating:

- **Safety - Impact Level 1 (Moderate):** The safety impact is classified as "Moderate" because a significant drop in home temperature could pose health risks, particularly to vulnerable individuals such as children, the elderly, or those with medical conditions. Prolonged exposure to excessively low temperatures may lead to discomfort or mild health issues, but it is unlikely to cause life-threatening harm under typical circumstances.
- **Financial - Impact Level 1 (Moderate):** The financial impact is rated as "Moderate" because recovering from unauthorized temperature control can increase energy consumption and utility costs. Additionally, persistent misuse of the HVAC system may accelerate component degradation, potentially leading to the need for repairs or replacement of critical components. The combined cost of heightened energy usage and potential equipment maintenance contributes to the moderate financial burden associated with this scenario.
- **Operational - Impact Level 3 (Severe):** The operational impact is considered "Severe" because the unauthorized control of the HVAC system represents a fundamental compromise of system functionality. The inability to maintain desired indoor conditions directly affects the core purpose of the HVAC system, potentially rendering it non-operational for its intended use.
- **Privacy - Impact Level 0 (Negligible):** Privacy impact is deemed "Negligible" as this scenario does not involve unauthorized access to personal data or sensitive information. The attack targets operational control rather than data theft or exposure, minimizing concerns related to confidentiality.

Damage Scenarios

Figure 6.13 illustrates the implemented Damage Scenario, "Unauthorized decrease of home temperature". This scenario represents the consequences of an attacker gaining control of the system, leading to compromised operational integrity, availability, and other critical cybersecurity properties. These critical aspects are captured under the "Concerns" property, which lists the integrity of the HVAC system firmware, the integrity of the temperature-decreasing function, the availability of the temperature-increasing function, and other associated qualified assets.The impact rating, previously discussed, outlines the severity of consequences associated with this compromise. Additionally, relevant Threat Scenarios capable of realizing this Damage Scenario are also identified and modeled, providing a foundation for understanding potential attack vectors and mitigation strategies. These are discussed in the following paragraph.

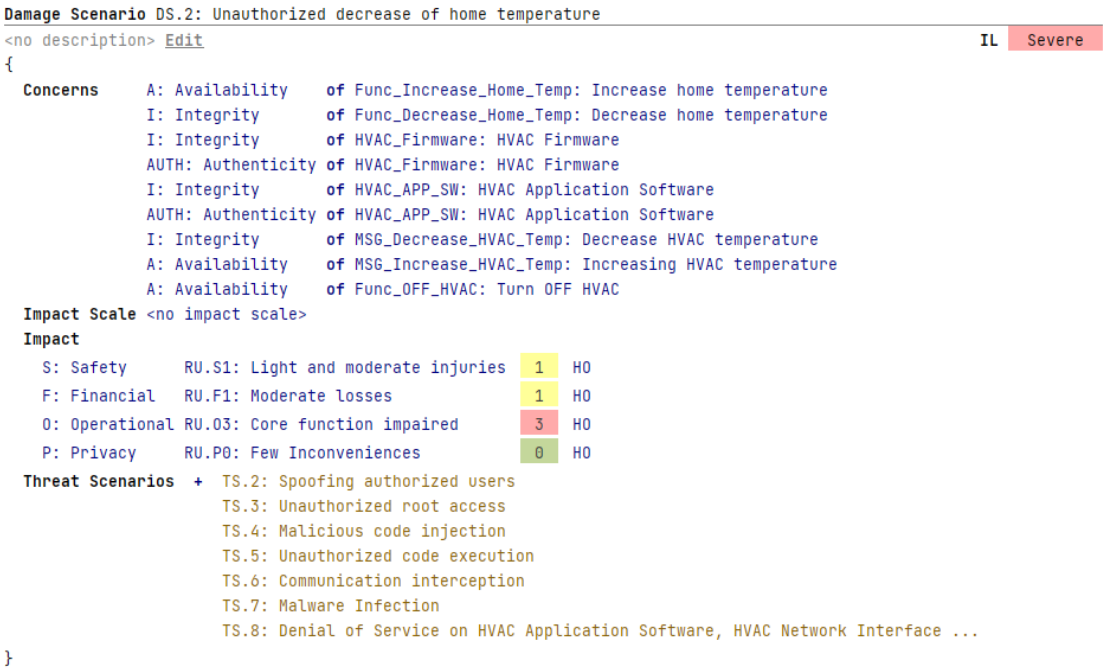


Figure 6.13: Damage Scenario "Unauthorized decrease of home temperature"

Threat Scenarios

The view selected Threat Scenarios represent a comprehensive and realistic set of security challenges relevant to a smart home environment. Each scenario was chosen based on its potential to compromise the integrity, availability, and confidentiality of critical systems, directly aligning with the focus of this thesis on evaluating cybersecurity risks within a smart home context. This list is not exhaustive and can be extended as required:

- **TS.1 - Spoofing Authorized Users:** Impersonating a legitimate homeowner to gain unauthorized access to the HVAC system. By bypassing authentication, attackers could send false commands to decrease the home temperature without user consent, compromising the integrity and security of the control mechanism.
- **TS.2 - Unauthorized Root Access:** Exploiting vulnerabilities to obtain administrative privileges allows unrestricted control over the HVAC system. An attacker with root access could directly manipulate firmware or application software, enabling malicious actions like unauthorized temperature reductions and overriding user settings.
- **TS.3 - Malicious Code Injection:** Introducing harmful code into the HVAC system can alter its functionality, making it respond to unauthorized temperature change commands. This threat compromises the integrity of control logic and could result in sustained, unauthorized operation that mimics normal behavior.
- **TS.4 - Unauthorized Code Execution:** Executing unauthorized or harmful code on the HVAC system enables attackers to alter its behavior, including forcing a temperature drop. This compromises operational integrity, allowing attackers to bypass intended protection mechanisms.
- **TS.5 - Communication Interception:** Eavesdropping on or tampering with data exchanged between the home router and the HVAC system could allow attackers to inject false commands or block legitimate ones. This threat impacts the confidentiality and integrity of communication, facilitating unauthorized temperature changes.
- **TS.6 - Malware Infection:** Deploying malicious software on the HVAC system compromises its operations, potentially altering control logic to continuously decrease the temperature. Malware could also disable safety mechanisms, exacerbating the damage.
- **TS.7 - Denial of Service Targeting the HVAC Application Software or Network Interface Card (NIC):** Overloading resources linked to the HVAC system renders it non-functional, disrupting the ability to increase temperature or respond to user commands. This attack compromises system availability, making it difficult to restore normal operations or mitigate unauthorized temperature decreases.

These Threat Scenarios demonstrate the various pathways through which attackers can compromise HVAC system functionality, directly realizing the Damage Scenario of an unauthorized temperature decrease. Figure 6.14 presents the Threat Scenario "Unauthorized root access" describing a situation in which an attacker gains root access and associated administrative privileges. The STRIDE category for the "Cause of Compromise" is "Elevation of Privilege", as this scenario involves unauthorized escalation of access rights. The "Acts on" attribute specifies the affected elements within the system: the firmware, application software, and NIC of the HVAC system. This Threat Scenario is realized through multiple potential attack paths, represented in the "Attack Tree" attribute and directly enables the Damage Scenario "Unauthorized decrease of home temperature." By obtaining elevated privileges, the attacker can replace legitimate firmware or application software with malicious code, execute unauthorized commands, or override and discard valid operations.

The IL for this Threat Scenario is classified as *"Severe"* directly derived from the realized Damage Scenario "Unauthorized decrease of home temperature". The AFL is evaluated as *"Very Low"* based on attack steps AS.14, AS.23, and AS.27 all of which have the highest feasibility rating of *"Very Low"*, thus the derived AFL follows the concept explained in section 6.2.1. Finally, the RL (2) is determined by combining the IL with the AFL, as outlined in section section 6.4 and visualized in the Risk Matrix (see fig. 6.23). This approach ensures a comprehensive and systematic assessment, accounting for both the potential severity of the impact and the likelihood of an attack. This structured approach ensures that each Threat Scenario is systematically linked to both the damage it may cause and the attack paths that could lead to its realization. By doing so, it establishes a comprehensive framework for analyzing vulnerabilities and identifying effective mitigation strategies.

Threat Scenario TS.3: Unauthorized root access

<no description> Edit

{

Cause of Compromise	TC.6: Elevation of privilege	**IL**	Severe
Acts on	HVAC_Firmware: HVAC Firmware	**AFL**	Medium
	HVAC_APP_SW: HVAC Application Software	**RL**	4
	HVAC_NIC: HVAC Network Interface Card		
Compromises	C: Confidentiality, I: Integrity, A: Availability (Derived)		
Threatens	+		
Attack Tree	may(AS.14, AS.27, AS.23)		
Realizes	DS.2: Unauthorized decrease of home temperature		
Lessened by	<no assumptions>		
Local Risk Level	4		

}

Figure 6.14: Threat Scenario "Unauthorized root access"

6.3 Attack Path Analysis and Attack Feasibility Rating

6.3.1 Attack Path Analysis and Attack Feasibility Rating Tool Details

Attack Feasibility Rating

Attack Path Analysis aims to identify and define the specific steps an attacker would need to execute to realize a Threat Scenario and achieve the intended damage. This process involves mapping potential attack paths and assessing the feasibility of each step. To evaluate feasibility, an *"Attack Potential-based"* approach is utilized, in which each attack is systematically rated according to five key criteria as defined in ISO/SAE 21434 [64]:

- **Elapsed Time (ET):** This parameter evaluates the time required to identify a vulnerability, develop an exploit, and successfully apply it. The rating depends on the state of expert knowledge and available resources at the time of assessment.
  - **ET0:** Less than or equal to a day.
  - **ET1:** Less than or equal to a week.
  - **ET2:** Less than or equal to a month.
  - **ET3:** Less than or equal to 6 months.
  - **ET3:** More than 6 months.
- **Expertise (SE):** This criterion assesses the attacker's capabilities based on their skills and experience.
  - **SE0 - Layman:** Unknowledgeable compared to experts or proficient persons, with no particular expertise - i.e., ordinary person using step-by-step descriptions of an attack that is publicly available.
  - **SE1 - Proficient:** Knowledgeable in that they are familiar with the security behavior of the product or system type - i.e., experienced owner, ordinary technician knowing simple and popular attacks.
  - **SE2 - Expert:** Familiar with the underlying algorithms, protocols, hardware, structures, security behavior, principles and concepts of security employed, techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc. implemented in the product or system type - i.e., experienced technician or engineer.
  - **SE3 - Multiple Experts:** Different fields of expertise are required at an expert level for distinct steps of an attack - i.e., multiple highly experienced engineers who have expertise in different fields, and which are required at an expert level for distinct steps of an attack.

- **Knowledge of Item or Component (KoIC):** This parameter evaluates the attacker's access to information about the target.
  - **KoIC0 - Public Information:** Public information concerning the item or component - i.e., information and documents published on the product homepage or on an internet forum.
  - **KoIC1 - Restricted Information:** Restricted information concerning the item or component - i.e. knowledge that is controlled within the developer organization and shared with other organizations under a non-disclosure agreement e.g., design specifications.
  - **KoIC2 - Confidential Information:** Confidential information about the item or component - i.e., knowledge that is shared between discrete teams within the developer organization, access to which is constrained only to members of the specified teams e.g., software source code.
  - **KoIC3 - Strictly Confidential Information:** Strictly confidential information about the item or component - i.e., knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking e.g. memory maps.
- **Window of Opportunity (WoO):** This factor considers access conditions and duration needed to execute the attack
  - **WoO0 - Unlimited:** High availability via public/untrusted network without any time limitation - i.e., asset is always accessible.
  - **WoO1 - Easy:** High availability and limited access time. Remote access without physical presence to the item or component - e.g., pairing time of Bluetooth or remote software update.
  - **WoO2 - Moderate:** Low availability of the item or component. Limited physical and/or logical access. Physical access to the system interior or exterior without using any special tools.
  - **WoO3 - Difficult:** Very low availability of the item or component. Impractical level of access to the item or component to perform the attack - e.g., decapping an integrated circuit to extract information, cracking a cryptographic key by brute force faster than the key is rotated.
- **Equipment (Eq):** This measures the tools and resources required for the attack.
  - **Eq0 - Standard:** Equipment is readily available to the attacker. This equipment can be a part of the product itself (e.g., a debugger in an operating system), or can be readily obtained (e.g. internet sources, protocol analyser or simple attack scripts) - e.g., laptop.

- **Eq1 - Specialized:** Equipment is not readily available to the attacker but can be acquired without undue effort. This can include purchase of moderate amounts of equipment (e.g., power analysis tools, use of hundreds of PCs linked across the internet would fall into this category), or development of more extensive attack scripts or programs. If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack this would be rated as bespoke - e.g., specialized hardware debugging device, high-grade oscilloscope, signal generator, special chemicals.
- **Eq2 - Bespoke:** Equipment is specially produced (e.g., very sophisticated software) and not readily available to the public (e.g., black market), or the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment is very expensive - e.g., manufacturer-restricted tools, electron microscope.
- **Eq3 - Multiple Bespoke:** Is introduced to allow for a situation, where different types of bespoke equipment are required for distinct steps of an attack.

The Attack Feasibility Level is calculated using the Attack Feasibility Model depicted in fig. 6.15. In this model, each evaluation category is assigned a specific point value corresponding to its difficulty level. The overall AFL is determined by summing the point values from all evaluated categories. A lower total score indicates a more feasible and dangerous attack, reflecting minimal barriers for an adversary to exploit the system. Conversely, a higher score signifies increased complexity and reduced feasibility, implying more robust security.

Attack Feasibility Levels

```
AF Comparator: default comparator (lower numbers are more critical)
Very Low = 25  (when AF >= 25)
Low      = 20  (when 25 > AF >= 20)
Medium   = 14  (when 20 > AF >= 14)
High     = 0   (when 14 > AF >= 0)
```

Figure 6.15: Attack Feasibility Model according to ISO/SAE 21434

Table 6.1 provides a detailed breakdown of the point distribution and weighting for each feasibility category.

For instance, an attack characterized by E03, SE1, KoIC1, WoO2, and Eq0 would yield a point calculation of 10 + 3 + 3 + 4 + 0, resulting in a cumulative score of 20. According to the feasibility model, this score corresponds to an Attack Feasibility Level of "Very Low".

Feasibility Category	Feasibility Rating	Value
ET: Elapsed Time	ET0: $\leq$ 1 day	0
	ET1: $\leq$ 1 week	1
	ET2: $\leq$ 1 month	4
	ET3: $\leq$ 6 months	10
	ET4: $>$ 6 months	19
SE: Specialist Expertise	SE0: Layman	0
	SE1: Proficient	3
	SE2: Expert	6
	SE3: Multiple Experts	8
KoIC: Knowledge of the Item or Component	KoIC0: Public Information	0
	KoIC1: Restricted Information	3
	KoIC2: Confidential Information	7
	KoIC3: Strictly Confidential Information	11
WoO: Window of Opportunity	WoO0: Unlimited	0
	WoO1: Easy	1
	WoO2: Moderate	4
	WoO3: Difficult	10
Eq: Equipment	Eq0: Standard	0
	Eq1: Specialized	4
	Eq2: Bespoke	7
	Eq3: Multiple Bespoke	9

Table 6.1: Feasibility Rating Values

Attack Steps

An Attack Step Chunk (see fig. 6.16) is a structured component used to model individual steps within an attack path by linking an attack from the catalog of Threat Classes (see section 6.3.3) to the corresponding affected system component, data, function, or other elements. Its structure and attributes are defined as follows:

- **Name:** Typically a concise identifier, such as "AS.2" providing a unique reference for the attack step within the analysis framework.
- **Title:** A brief, descriptive label outlining the purpose or action of the Attack Step, offering clarity for documentation and traceability.
- **Instantiates:** This field connects the Attack Step to a predefined Threat Class (see section 6.3.3) from the Threat Catalog, which includes feasibility ratings for known attacks. Instantiating a Threat Class provides a standardized foundation for evaluating attack feasibility.

- **Acts on:** Specifies the architectural component, data, or channel targeted by the Attack Step. Defining this relationship aids in understanding the system's vulnerabilities and their potential exploitation.
- **Threatens:** Lists the Threat Scenarios influenced or realized by the Attack Step. While this association is defined within the Threat Scenario itself, displaying it here enhances visibility and traceability of dependencies.
- **Mitigated by:** Links documented Security Controls that mitigate the Attack Step. This attribute facilitates integrating countermeasures into the analysis, providing a comprehensive risk management strategy.
- **Prepared by:** Indicates Attack Steps necessary before executing the current described step. This attribute can reference individual steps or complex trees utilizing logical operators such as must() and may(), defining dependencies and alternative paths within an attack.
- **Attack Feasibility:** Determines the AFL for executing the Attack Step, derived from feasibility models using defined categories. For compound steps, the accumulated feasibility rating is calculated by integrating other Attack Steps in the tree and associated Controls. The detailed concepts of Threat Classes and Control Classes will be explored in section 6.3.3.
- **Local Risk Level:** Represents the Risk Level at the Attack Step, calculated by combining the Attack Feasibility Level with the Impact Level. This risk can be further segmented by cybersecurity properties (e.g., confidentiality, integrity) and stakeholders (e.g., the homeowner).

In this context, Attack Steps derive their IL indirectly through Damage Scenarios, as they are linked only through the intermediate Threat Scenarios. This means that if, for example, AS.1 potentially realizes multiple Threat Scenarios e.g., TS.1, TS.2, and TS.3 with respective ILs of "Negligible", "Moderate", and "Major" the Attack Step inherits the highest IL, which in this case is "Major". The AFL is initially derived from the associated Threat Class instantiated for the Attack Step. However, if mitigation Controls are specified under the "Mitigated by" property, these Controls influence and ultimately determine the AFL. When a may() relationship is utilized, the AFL of the Attack Step is set by the Control with the highest AFL. This reflects the attacker's likely strategy of exploiting the weakest defense to carry out the attack. For example, given may(C.1, C.2, C.3) with AFLs "Very Low", "Low", and "High" the resulting AFL for the Attack Step is "High", as it represents the most favorable condition for the attacker. Conversely, in a must() relationship, all listed Controls must be bypassed, making the strongest control i.e., the one with the lowest AFL the limiting factor. Therefore, the AFL of the Attack Step in this case is set to the lowest value among the Controls. For nested combinations, again, the rules are applied hierarchically evaluating from the innermost logic outward. Finally, the RL for the Attack Step is calculated by applying the Risk Matrix, which combines the IL and the determined AFL.

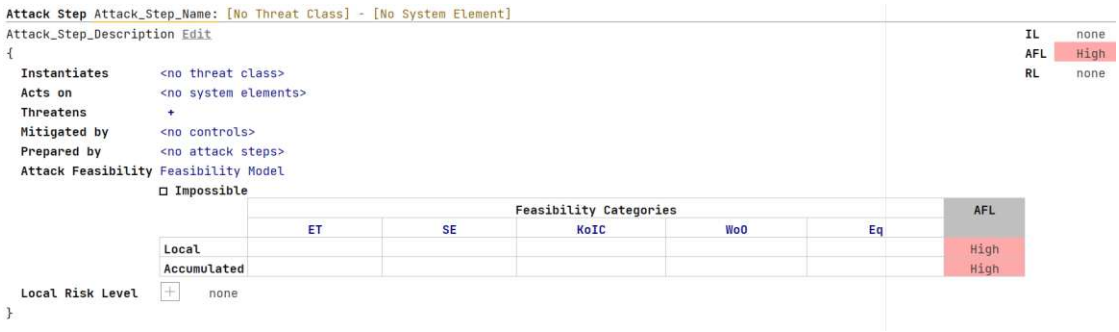


Figure 6.16: Attack Step Chunk in the TARA tool

Controls

Similar to Attack Steps, Controls in this context integrate Control Classes with their corresponding system elements (e.g., components, data, functions etc.). As illustrated in fig. 6.17, a control element is characterized by several key attributes.

- **Name:** A unique name for the Control such as "C.1".
- **Title:** A descriptive title outlining the purpose of the Control.
- **Instantiates:** A link to Control Classes (see section 6.3.3) from a predefined catalog, which includes pre-assessed feasibility ratings.
- **Threatened by:** Specifies the Threat Scenarios that may compromise the Control. For simplification purposes this is not included in the analysis.
- **Mitigates:** Lists the Attack Steps mitigated by the Control (assignment defined in the relevant Attack Step). This relationship illustrates how the Control limits or prevents specific attack vectors.
- **Effect:** Describes the expected impact reduction if the Control is effective, removing associated attack paths from consideration. While this attribute can enhance detailed modeling, it is not explicitly utilized in this thesis.
- **Attack Feasibility:** Evaluated similarly to Attack Steps, this attribute reflects the feasibility of breaching the Control.
- **Local Risk Level:** Combination of IL and the AFL.

In this instance, the IL is indirectly inherited from the Damage Scenario. This inheritance process starts with the Threat Scenario and is subsequently passed through the Attack Steps associated with the Control i.e. the Control gets the highest IL of the Attack Steps it is supposed to mitigate or neutralize. The AFL is derived from the inherited Control Class. Once these levels are determined, the overall risk is again assessed using the Risk Matrix.

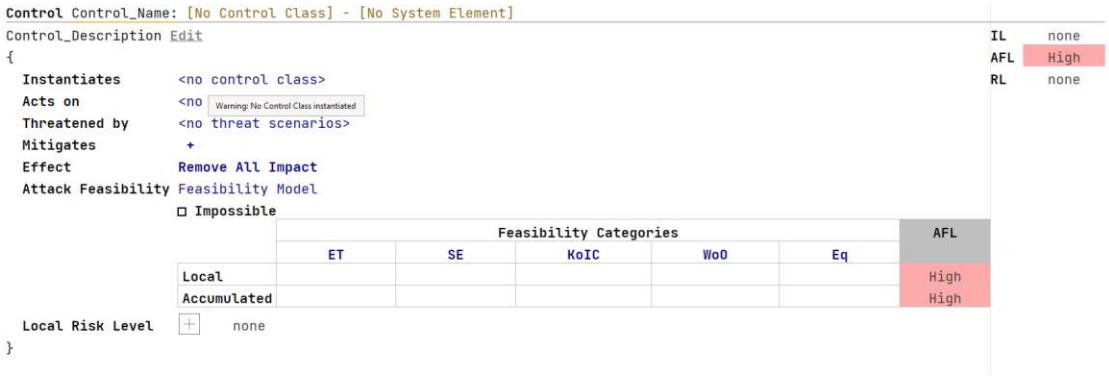


Figure 6.17: Control Chunk in the TARA tool

6.3.2 Attack Path Analysis and Attack Feasibility Rating Outcomes

Attack Steps

Figure 6.18 illustrates one of the implemented Attack Steps AS.3, which models a Brute-force Password-Guessing attack (MITRE T1110.001) targeting the Firmware and Application software of the HVAC system. The attack instantiates the "Brute-force attack" Threat Class from the MITRE framework, highlighting its direct impact on both system components. To mitigate this attack, two Controls are applied: C.25 and C.2. Control C.25 represents "Account Use Policies (MITRE M1036)", implementing rate limiting to restrict repeated login attempts, while control C.2 enforces "Password Policies (MITRE M1027)", ensuring robust password management. The "Prepared by" property identifies AS.22, "Valid Accounts: Default Accounts (MITRE T1078.001)", as a prerequisite, modeling the use of weak or default credentials that enable the brute-force attack. The Attack Feasibility Level for AS.3 is evaluated as "Very Low" determined by the must() combination of the Controls where the strongest Control (C.2 with an AFL of "Very Low") limits the feasibility of the attack. The Impact Level for AS.3 is rated as "Severe" because it contributes to the realization of Threat Scenarios "TS.2: Spoofing authorized users", "TS.3: Unauthorized root access", and "TS.5: Unauthorized code execution" each carrying an IL of "Severe". Consequently, the overall Risk Level for this Attack Step is determined to be 2, following the Risk Matrix model. This structured analysis demonstrates how layered defenses reduce attack feasibility while aligning with the broader risk management framework.

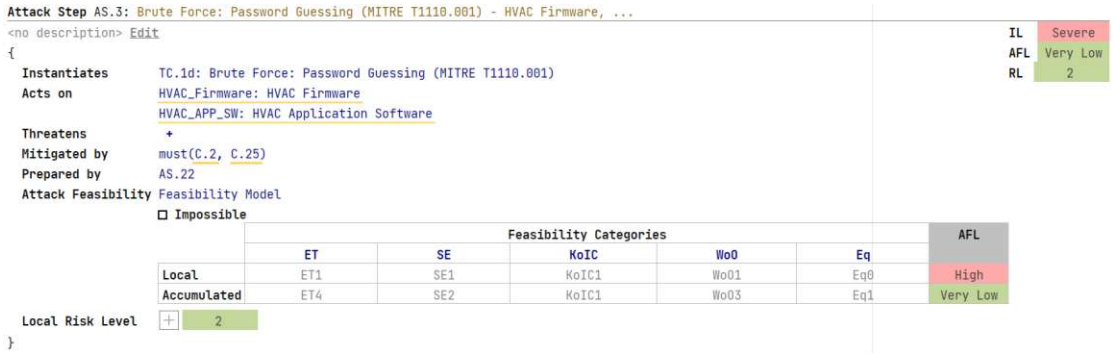


Figure 6.18: Attack Step "Brute Force: Password Guessing (MITRE T1110.001) - HVAC Firmware, HVAC Application Software"

Controls

The Control "Password Policies (MITRE M1027) – HVAC Firmware, HVAC Application Software", shown in fig. 6.19, exemplifies one of the key security measures implemented to mitigate cybersecurity risks in the analyzed system. This Control instantiates the "Password Policies (MITRE M1027)" Control Class from the MITRE framework, specifically targeting the Firmware and Application software of the HVAC system. Its purpose is to enforce robust password management practices, thereby preventing unauthorized access through password-related vulnerabilities. The Control effectively mitigates multiple Attack Steps, demonstrating its broad applicability in enhancing system security. The Feasibility Rating of the Control is evaluated as "Very Low", consistent with the predetermined rating of the instantiated Control Class, indicating a strong defensive posture against password-based attacks. The Impact Level is classified as "Severe" because it reflects the highest impact Level Associated with the Attack Steps mitigated by this Control, i.e., if the Control is breached, the resulting impact will be that of the Threat Scenarios realized by the Attack Steps that should have been neutralized. Following the risk assessment methodology and using the Risk Matrix, the combination of a "Severe" Impact Level and a "Very Low" Attack Feasibility Level yields a Risk Level of 2.

6.3.3 Threat and Control Classes

The Threat and Control Classes encompass the categories of attacks and their corresponding mitigations. Within the developed framework, these classes are derived from the STRIDE and MITRE ATT&CK methodologies but can be customized using other datasets, depending on the analysis's specific requirements and scope. Table 6.2 provides an overview of the identified attacks along with their feasibility ratings, while table 6.3 details the associated mitigations and their ratings. These ratings can be adjusted within the tool at any given time to accommodate varying scenarios, assessment requirements, or changes arising from gained knowledge/information.

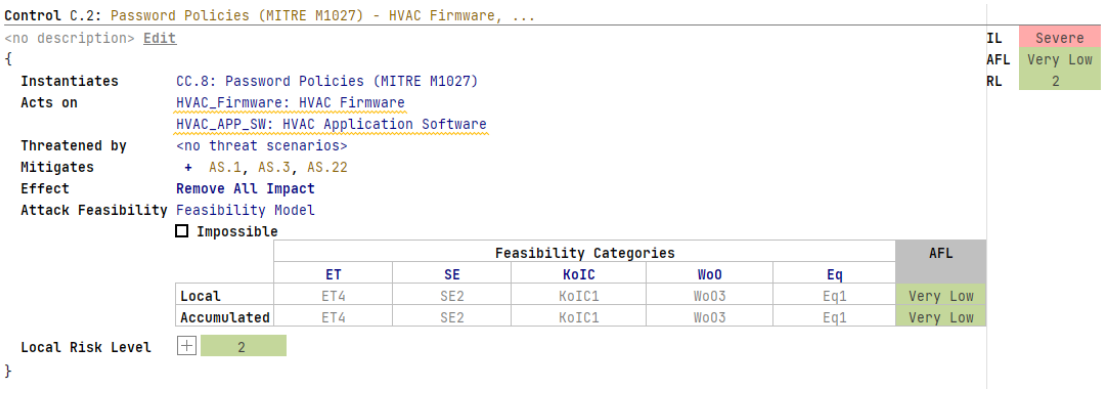


Figure 6.19: Implemented Control Chunk "Password Policies (MITRE M1027) – HVAC Firmware, HVAC Application Software"

Table 6.2: Attack Strategies

Threat	ET	SE	KoIC	WoO	Eq
Remote Services (MITRE T1021) - Telnet Connection	ET0	SE1	KoIC0	WoO1	Eq0
Remote Services (MITRE T1021) - SSH Connection	ET0	SE1	KoIC0	WoO1	Eq0
Network Sniffing (MITRE T1040)	ET1	SE1	KoIC1	WoO2	Eq1
Exfiltration Over C2 Channel (MITRE T1041) - Credentials in Transit	ET1	SE2	KoIC2	WoO2	Eq1
Network Service Discovery (MITRE T1046) - Network Scanning	ET0	SE0	KoIC0	WoO0	Eq0
Input Capture (MITRE T1056) - Login Credential Access Application (assuming victim provides credentials through Phishing Technique)	ET0	SE0	KoIC1	WoO0	Eq0
Command and Scripting Interpreter (MITRE T1059) - Abusing Command Line Interfaces	ET1	SE1	KoIC0	WoO1	Eq0
Command and Scripting Interpreter (MITRE T1059) - Execute Malware	ET1	SE1	KoIC1	WoO2	Eq0
Command and Scripting Interpreter (MITRE T1059) - Code Injection	ET2	SE1	KoIC1	WoO2	Eq0
Command and Scripting Interpreter (MITRE T1059) - Command Injection	ET1	SE1	KoIC1	WoO2	Eq0
Exploitation for Privilege Escalation (MITRE T1068) - Root Access (assuming weak/default credentials)	ET1	SE1	KoIC0	WoO1	Eq0

Threat	ET	SE	KoIC	WoO	Eq
Exploitation for Privilege Escalation (MITRE T1068) - Privilege Escalation (assuming weak/default credentials)	ET0	SE1	KoIC0	WoO1	Eq0
Application Layer Protocol: Mail Protocols (MITRE T1071.003) - Malicious E-Mail Delivery	ET0	SE0	KoIC0	WoO0	Eq0
Valid Accounts (MITRE T1078) - MAC Spoofing	ET1	SE1	KoIC1	WoO1	Eq0
Valid Accounts: Default Accounts (MITRE T1078.001) - Weak/Default Credentials	ET1	SE1	KoIC1	WoO1	Eq0
Ingress Tool Transfer (MITRE T1105) - Remote File Download	ET1	SE0	KoIC0	WoO0	Eq0
Brute Force: Password Guessing (MITRE T1110.001)	ET1	SE1	KoIC1	WoO1	Eq0
Drive-by Compromise (MITRE T1189)	ET2	SE2	KoIC0	WoO1	Eq0
Exploit Public-Facing Application (MITRE T1190)	ET3	SE2	KoIC2	WoO3	Eq1
Exploitation for Client Execution (MITRE T1203) - Local Code Execution	ET2	SE2	KoIC2	WoO3	Eq1
Exploitation of Remote Services (MITRE T1210) - Lateral Movements	ET3	SE3	KoIC2	WoO3	Eq2
File and Directory Permissions Modification (MITRE T1222)	ET2	SE1	KoIC1	WoO2	Eq0
Adversary-in-the-Middle (MITRE T1557)	ET2	SE2	KoIC2	WoO3	Eq1
Phishing (MITRE T1566) - Fake Login Page	ET2	SE1	KoIC1	WoO2	Eq1
Phishing: Spearphishing Attachment (MITRE T1566.001)	ET2	SE1	KoIC0	WoO1	Eq0
Phishing: Spearphishing Link (MITRE T1566.002)	ET1	SE1	KoIC0	WoO1	Eq0
Develop Capabilities: Exploits (MITRE T1587.004)	ET4	SE2	KoIC2	WoO3	Eq3
Gather Victim Host Information (MITRE T1592)	ET0	SE1	KoIC0	WoO0	Eq0
Active Scanning (MITRE T1595)	ET0	SE0	KoIC0	WoO0	Eq0
Active Scanning: Vulnerability Scanning (MITRE T1595.002)	ET2	SE2	KoIC1	WoO2	Eq1

Table 6.3: Mitigation Strategies

Control/Mitigation	ET	SE	KoIC	WoO	Eq
Application Developer Guidance (MITRE M1013) - Secure Coding Practices	ET4	SE2	KoIC2	WoO3	Eq1
User Training (MITRE M1017) - Security Awareness	ET0	SE2	KoIC0	WoO0	Eq0
Privileged Account Management (MITRE M1026) - Limit Remote Access	ET2	SE2	KoIC2	WoO3	Eq0
Privileged Account Management (MITRE M1026) - Least Privilege	ET2	SE1	KoIC1	WoO2	Eq0
Password Policies (MITRE M1027)	ET4	SE2	KoIC1	WoO3	Eq1
Network Segmentation (MITRE M1030)	ET3	SE2	KoIC2	WoO3	Eq1
Network Intrusion Prevention (MITRE M1031)	ET3	SE2	KoIC1	WoO3	Eq1
Network Intrusion Prevention (MITRE M1031) - Zero-Day Exploit Monitoring	ET3	SE2	KoIC1	WoO2	Eq1
Multi-Factor Authentication (MITRE M1032)	ET2	SE2	KoIC2	WoO3	Eq1
Limit Access to Resource Over Network (MITRE M1035) - Account Lockout	ET1	SE1	KoIC1	WoO2	Eq0
Account Use Policies (MITRE M1036) - Rate Limiting	ET1	SE1	KoIC0	WoO1	Eq0
Filter Network Traffic (MITRE M1037) - Email Filtering	ET1	SE1	KoIC0	WoO1	Eq0
Filter Network Traffic (MITRE M1037) - Spam Filters	ET1	SE1	KoIC0	WoO1	Eq0
Filter Network Traffic (MITRE M1037) - Firewall Protections	ET3	SE2	KoIC2	WoO2	Eq1
Filter Network Traffic (MITRE M1037) - Content Filtering	ET1	SE1	KoIC0	WoO1	Eq0
Behavior Prevention on Endpoint (MITRE M1040) - Logging and Monitoring	ET4	SE3	KoIC2	WoO3	Eq2
Encrypt Sensitive Information (MITRE M1041) - Encrypted Communications	ET4	SE3	KoIC2	WoO3	Eq2
Code Signing (MITRE M1043)	ET3	SE2	KoIC1	WoO3	Eq2
Disable or Remove Feature or Program (MITRE M1043) - Application Whitelisting	ET2	SE1	KoIC0	WoO2	Eq0
Audit (MITRE M1047) - Code Auditing	ET4	SE2	KoIC2	WoO3	Eq1
Audit (MITRE M1047) - Regular Testing	ET4	SE3	KoIC1	WoO3	Eq2

Control/Mitigation	ET	SE	KoIC	WoO	Eq
Application Isolation and Sandboxing (MITRE M1048)	ET2	SE2	KoIC1	WoO2	Eq1
Antivirus/Antimalware (MITRE M1049) - Endpoint Protection	ET3	SE2	KoIC2	WoO2	Eq1
Antivirus/Antimalware (MITRE M1049) - Mutual Authentication	ET4	SE2	KoIC2	WoO3	Eq1
Exploit Protection (MITRE M1050) - Regular Vulnerability Management	ET1	SE1	KoIC0	WoO1	Eq0
Exploit Protection (MITRE M1050) - Input Validation	ET2	SE1	KoIC1	WoO2	Eq0
Update Software (MITRE M1051) - Patching	ET2	SE1	KoIC1	WoO2	Eq0

Figure 6.20 illustrates one of the implemented Threat Classes, triggered by associated Attack Steps within the system. Conversely, fig. 6.21 presents an example of a Control

Threat Class TC.1d: Brute Force: Password Guessing (MITRE T1110.001) **Refines** TC.1: Spoofing

Attempting multiple passwords to gain access to an account. Edit

{

Threatens	C: Confidentiality	(equals refined class)
	I: Integrity	
Architecture	Data Flow	(equals refined class)
	Channel	
Technologies	<no technologies>	
Attack Feasibility	Feasibility Model	

☐ Impossible

	Feasibility Categories					AFL
	ET	SE	KoIC	WoO	Eq	
Local	ET1	SE1	KoIC1	WoO1	Eq0	High

}

Figure 6.20: Threat Class "Brute Force: Password Guessing (MITRE T1110.001)"

Class that has also been integrated into the model. However, certain properties have been excluded from this analysis as they fall outside the specific scope and do not contribute to any results of practical relevance to this thesis.

These evaluations were conducted through thorough research, including references to the MITRE ATT&CK framework and in consultation with a cybersecurity expert. It is important to note that precise evaluations are not feasible without detailed technical information. Therefore, these assessments were conducted to the best of available knowledge and judgment in accordance with established practices in the field. Certain assumptions have also been incorporated, such as considering Weak/Default Credentials as the starting point for the "Privilege Escalation (MITRE T1068)" attack, which has been explicitly noted in the analysis. The rationale for the assigned ratings for the attack "Privilege Escalation (MITRE T1068) with Weak/Default Credentials" is detailed below:

Control Class CC.8: Password Policies (MITRE M1027) **Refines** <nothing>

Enforce strong password complexity and regular password rotation. Edit

{

Protects <no security properties>

Protects Against <no threat classes>

Architecture <no architecture>

Technologies <no technologies>

Assumption Classes <no assumption classes>

Attack Feasibility Feasibility Model

☐ **Impossible**

	Feasibility Categories					AFL
	ET	SE	KoIC	WoO	Eq	
Local	ET4	SE2	KoIC1	WoO3	Eq1	Very Low

}

Figure 6.21: Control Class "Password Policies (MITRE M1027)"

Privilege escalation through weak or default credentials exploits poorly secured authentication mechanisms to gain unauthorized access to elevated permissions. This vulnerability often stems from default settings in hardware, software, or applications that have not been properly configured or updated. According to MITRE ATT&CK, such attacks are prevalent in systems where security policies are insufficiently enforced. The feasibility rating is justified as follows:

- **ET0:** Given the assumption of weak or default credentials, the time required to exploit this vulnerability is minimal.
- **SE1:** While the attack requires only basic expertise, the attacker must still possess some familiarity with tools and techniques for locating and exploiting weak credentials.
- **KoIC0:** Default credentials are often readily accessible through public sources or vendor documentation, making the knowledge requirement for this attack very low.
- **WoO1:** When weak or default credentials are used, there is a high likelihood that additional authentication mechanisms, such as account lockout policies, are absent. This allows the attacker to attempt the exploit over an extended period without restrictions.
- **Eq0:** Executing this attack requires only a computer with an internet connection and readily available open-source tools (e.g., Hydra or John the Ripper).

6.4 Risk Value Determination and Risk Treatment Decision

6.4.1 Risk Value Determination

Risks provide a structured evaluation of the potential RLs inherited from a Threat Scenario, Attack Step, or Security Control. Through a risk element, it is possible to identify affected stakeholders, assess associated impact categories, and compare various control scenarios (e.g., all Controls/mitigations activated, no Controls/mitigations deactivated, or selective activation of specific Controls/mitigations). However, this analysis specifically focuses on risks directly associated with Threat Scenarios, analyzing two distinct control scenarios: one in which all controls are activated and another where no controls are implemented. The identified risks and RLs are as follows:

- **Risk 1 - Unauthorized Access and Control of Home Appliances:** Refers to scenarios where attackers gain unauthorized control of household devices, potentially leading to misuse, service disruption, or safety concerns.
  - **All Controls**: Risk Level 2
  - **No Controls**: Risk Level 5
- **Risk 2 - Unauthorized Access to Sensitive Data:** Encompasses scenarios related to the exposure of confidential information to unauthorized parties, posing significant privacy and security threats.
  - **All Controls**: Risk Level 2
  - **No Controls**: Risk Level 5
- **Risk 3 - System Integrity Compromise:** Involves the alteration or corruption of system data or functionality, undermining system reliability and trustworthiness.
  - **All Controls**: Risk Level 2
  - **No Controls**: Risk Level 5
- **Risk 4 - System Instability or Downtime:** Describes situations where system performance is degraded, or services are disrupted, negatively impacting availability and user experience.
  - **All Controls**: Risk Level 2
  - **No Controls**: Risk Level 5
- **Risk 5 - Increased Operational Costs:** Includes the financial implications for the homeowner, such as increased energy costs, repair or replacement expenses for damaged devices, and other operational costs resulting from compromised system functionality or security breaches.

– **All Controls**: Risk Level 2
– **No Controls**: Risk Level 5

Figure 6.22 illustrates a risk element within the tool. The *"Impact Category"* attribute provides a breakdown of the RLs for each category, offering insights into the aspects (e.g., Safety, Operational, Financial, Privacy) that contribute to the overall risk. By analyzing risks from a stakeholder perspective, the evaluation highlights the RLs experienced by each stakeholder group under different control scenarios. This approach is particularly beneficial for comparing risks across various perspectives, such as the impact on end-users versus organizational operations. However, this thesis exclusively focuses on the HO, as outlined at the beginning, identifying them as the primary stakeholder under consideration.

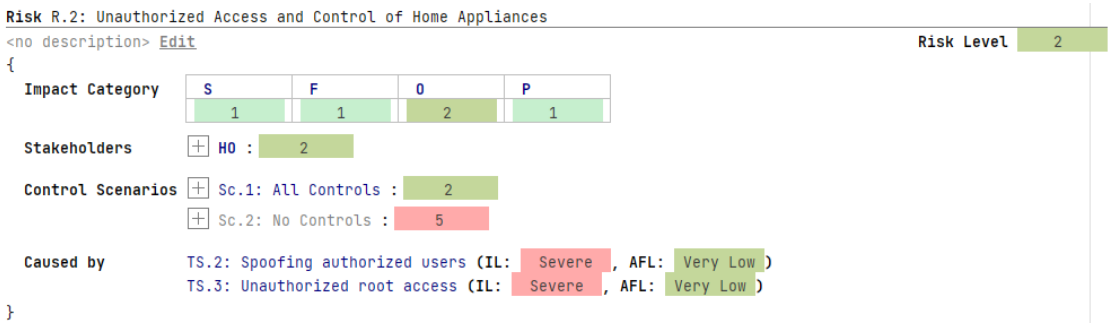


Figure 6.22: Risks in the TARA tool

Control scenarios focus on evaluating the RL for specific stakeholders under varying configurations of security controls. Additionally, the *"Caused by"* part lists the specific Threat Scenarios or Attack Steps responsible for triggering the identified risks.

The RL is determined using the Risk Matrix (see fig. 6.23). This matrix combines the highest IL and the highest AFL from the responsible Threat Scenarios. The resulting combination is used to calculate the overall risk level, ensuring a structured and standardized evaluation process.

In conclusion, fig. 6.25 provides a detailed depiction of the comprehensive attack tree (automatically generated in the tool through the dependencies created during the analysis) leading to the risk of "Unauthorized Access and Control of Home Appliances". This visualization underscores the intricate dependencies between risk, Threat Scenarios, and their associated Attack Steps. Even with a moderate level of analytical detail, the attack tree reveals the complexity of potential attack paths, demonstrating the multifaceted nature of cybersecurity risks in smart home systems. All resulting attack trees are accessible within the tool for clearer and more comprehensive analysis.

Despite their complexity, such attack trees offer significant advantages, particularly in ensuring traceability throughout the analysis process.

Risk Matrix

Feasibility Model AFLs

Risk Matrix	Refresh	Attack Feasibility			
		Very Low	Low	Medium	High
Impact	Negligible	1	1	1	1
	Moderate	1	2	2	3
	Major	1	2	3	4
	Severe	2	3	4	5

Figure 6.23: Risk Matrix according to ISO/SAE 21434

Figure 6.25 not only illustrates how specific Threat Scenarios materialize through a series of Attack Steps but also identifies the Controls implemented to mitigate these risks. By doing so, it highlights the interconnectedness of risks, threats, and mitigations, providing a robust framework for evaluating and addressing vulnerabilities within the system. Figure 6.24 provides a simplified representation of the attack tree, illustrating the hierarchical relationships and dependencies between Risks, Damage Scenarios, Threat Scenarios, Attack Steps, and their corresponding Controls.

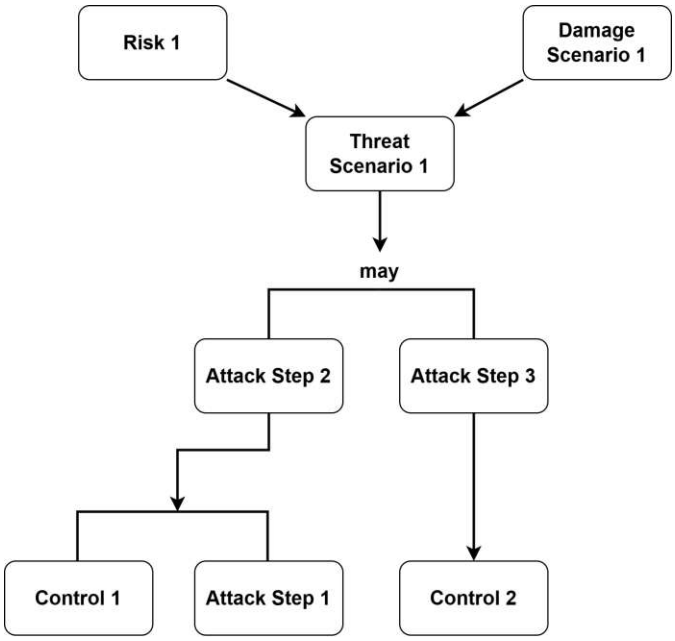


Figure 6.24: Simplified Attack Tree

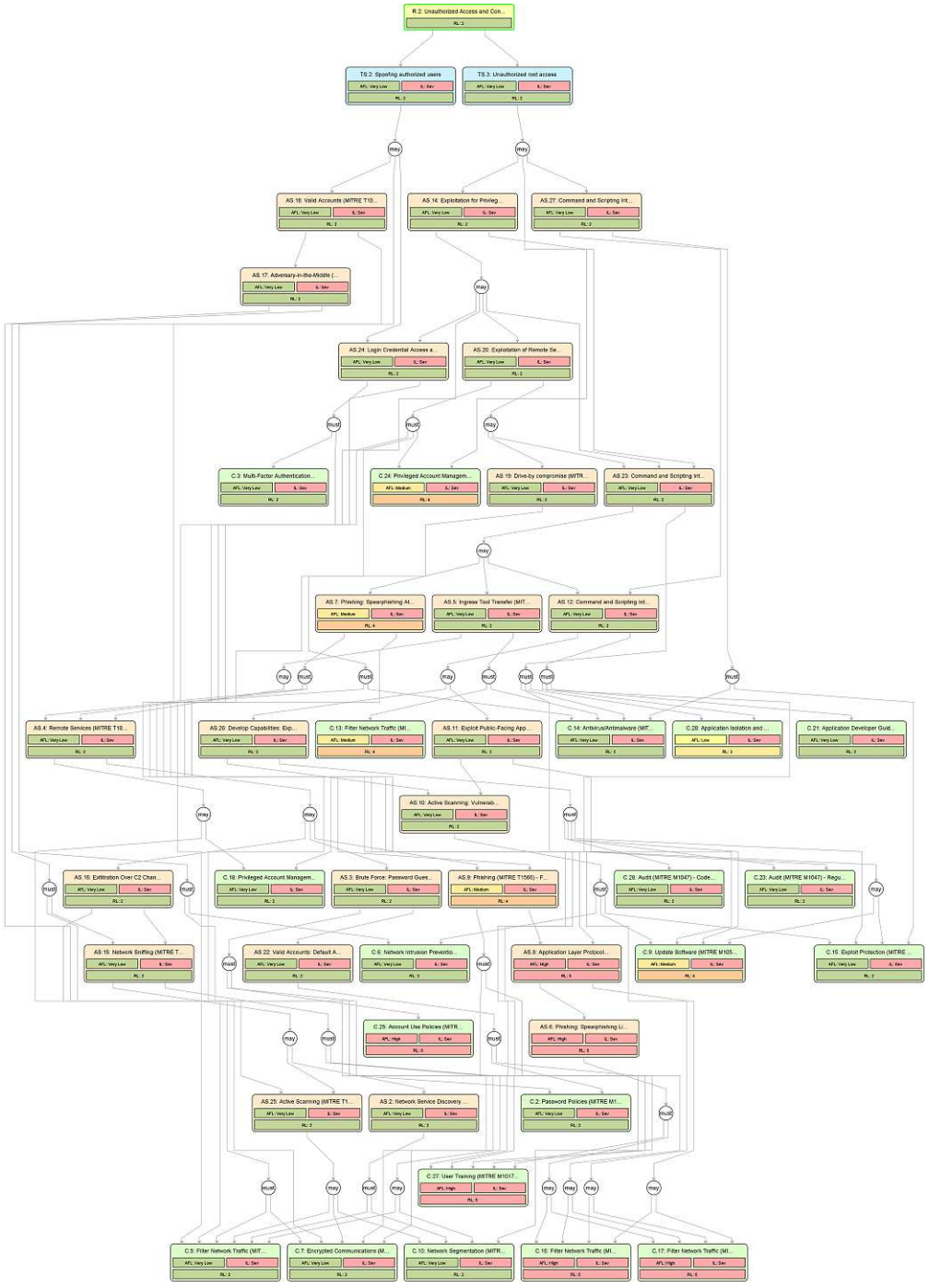


Figure 6.25: Attack Tree for the Risk "Unauthorized Access and Control of Home Appliances"

6.5 Risk Treatment Decision

Once risks have been identified, the next step is to determine an appropriate course of action to address them. There are four primary strategies for managing risks, each tailored to specific circumstances and organizational priorities:

- **Avoidance (Av):** This approach involves eliminating the risk entirely by removing the threatened asset or altering the system design to ensure the risk cannot materialize. Avoidance is often preferred when the potential impact of the risk is too severe to mitigate effectively or when alternative solutions are feasible without compromising system functionality.
- **Reduction (R):** Reduction focuses on minimizing the likelihood or impact of the risk by implementing mitigating controls. This strategy often includes technical, procedural, or organizational measures, such as deploying security mechanisms, strengthening access controls, or applying encryption to sensitive data. Reduction is commonly used when the risk cannot be entirely avoided but can be effectively managed. This is the main strategy applied in this thesis.
- **Sharing or Transferring (SoT):** This strategy involves sharing the risk with another party, such as a supplier, partner, or insurance provider. For instance, contractual agreements may transfer specific cybersecurity responsibilities to a vendor, while insurance policies can cover potential financial losses. Sharing or transferring risk is particularly useful when an organization lacks the resources or expertise to address it independently.
- **Acceptance (Ac):** Acceptance entails acknowledging the risk and deciding not to take any additional actions to mitigate it. This option is typically chosen when the RL is deemed tolerable, either because the likelihood of occurrence is low or the impact is minimal compared to the cost and effort required to address it.

Deciding on the most appropriate solution to address identified risks requires a careful and balanced evaluation of several key factors. One of the primary considerations is development time, which involves assessing how long it will take to implement the chosen solution, particularly in relation to ongoing system development or maintenance timelines. Another crucial aspect is cost, encompassing not only the initial investment required but also operational expenses and potential long-term savings. The complexity of the solution is equally significant, as it reflects the technical and organizational challenges that may arise during implementation, especially for intricate systems with highly interconnected components. Finally, the system impact must be considered, as risk mitigation measures often involve trade-offs that can affect system functionality, usability, or performance. For the purposes of the analysis conducted in this thesis, risk management strategies involving Avoidance, Risk Sharing, or Transfer and Acceptance are beyond the scope of consideration. This limitation arises from the focus on evaluating an existing system, where the primary objective is to explore and implement measures for risk reduction.

CHAPTER 7

Discussion

7.1 Synchronized Attacks Simulations

The simulation results for 110 and 230 households clearly demonstrate that coordinated cyberattacks on high-wattage devices can lead to both localized and widespread blackouts. Analysis of various attack vectors, including EVs, electric ovens, water heaters, and air conditioners, indicates that these high-energy consumers have the capacity to put significant strain on the power grid.

For 110 households, compromising 50% (55) of the EVs leads to transformer disconnection within 19 minutes and 25 seconds. In contrast, for 230 households, compromising just over 20% (46) of the EVs causes a transformer shutdown within a similar timeframe despite involving fewer compromised vehicles. These findings highlight the substantial risk posed by EVs, given their high power consumption when manipulated simultaneously.

Electric ovens and cooktops present a comparable threat. For 110 households, compromising 55% (61) of these appliances results in transformer failure within 21 minutes and 41 seconds. However, for 230 households, the impact is far more severe as compromising just 25% of the devices leads to shutdown within just 8 minutes and 31 seconds, effectively halving the disconnection time. This indicates that the absolute number of available households is the most critical factor. A higher number of households corresponds to an increased number of household appliances, which in turn raises the likelihood of device vulnerabilities. Consequently, this facilitates the efficiency of the attack process. These results underscore the considerable stress electric ovens place on the grid when activated in large numbers simultaneously.

While water heaters and air conditioners pose a lesser immediate risk, they still contribute to long-term grid strain. Even when 60% of these devices are compromised in both the 110- and 230-household scenarios, they do not cause an immediate transformer overload. However, when combined with other attack vectors, they could further destabilize the

grid. Furthermore, it is important to note that households typically own multiple air conditioners, often from the same manufacturer, as they are frequently purchased together. This increases the likelihood of a successful attack, as multiple devices could be compromised simultaneously. While the simulations indicate a lower immediate risk, this factor makes such an attack more feasible in real-world scenarios.

When combining these simulation results with the literature research from the state-of-the-art chapter, it becomes evident that these attacks are not only theoretically possible but also practically feasible. In reality, coordinated cyberattacks could lead to localized blackouts that escalate rapidly, affecting larger regions. This underscores the significant threat to supply security and highlights the urgent need for preventive measures.

However, certain limitations must be considered when interpreting these results. The simulations assume a widespread use of these devices, which may not accurately reflect current real-world conditions, as the adoption of EVs and smart appliances is presently more concentrated in higher-income areas [72][73]. Additionally, different households typically use appliances from various manufacturers, meaning not all devices share the same vulnerabilities, which could reduce the total number of compromisable devices. Nevertheless, projections and government regulations (specifically in the EV case) indicate rapid growth in the near future, increasing the likelihood of such attacks.

Another key assumption in this simulation is that all households follow a uniform load profile. However, in reality, energy consumption varies significantly between households due to factors such as household size, lifestyle habits, the type and number of devices used, and regional differences.

While it would be possible to run simulations with diverse load profiles, obtaining real-world data for such an analysis is challenging. Household load profiles are often difficult to access due to privacy restrictions or are only available in aggregated form, limiting their applicability.

Nonetheless, it is important to consider how variations in energy consumption could influence the results. Households with exceptionally high electricity usage could exacerbate the impact of a coordinated attack, creating more severe load spikes and increasing strain on the grid. Conversely, lower consumption in some households might help dampen the effects, providing a degree of resilience.

Despite these limitations, the load profile used in this study represents the average across households and, therefore, serves as a strong reference point for analysis. It provides a realistic assessment of the potential impact of coordinated attacks on the power grid and forms a solid foundation for further research.

A significant finding by Spanish researchers, identified during the course of this thesis, further reinforces its argument [74]. Their research uncovered backdoors in the ESP32 Wi-Fi/Bluetooth microchip, produced by a Chinese manufacturer and integrated into over a billion IoT devices.

This discovery highlights that cyberattacks are not confined to specific device types but can extend across a wide range of products utilizing the same vulnerable hardware. Such a systemic weakness could facilitate more sophisticated and coordinated attacks, posing a substantial risk to the stability of the power grid on a much larger scale.

In conclusion, these simulations provide valuable insights into the potential consequences of coordinated cyberattacks on the power grid. They confirm that such attacks are not only possible but could also have severe impacts. Therefore, it is essential for grid operators, device manufacturers, and policymakers to collaborate in strengthening the security of the power grid and implementing proactive measures to mitigate these threats.

7.2 Threat Analysis and Risk Assessment Framework

Identifying and evaluating existing frameworks and tools for conducting comprehensive threat analysis and risk assessment in the context of IoT and smart homes have proven to be challenging. Key issues are the limited availability of specialized frameworks tailored to this domain and the fact that existing security frameworks from other areas are largely focused on data and software. While these aspects are crucial within the IoT ecosystem, they represent only a partial view of the overall security landscape, overlooking critical components of overall system security. This is why a more comprehensive approach is required, one that encompasses both the physical and digital components of the system, along with their complex interdependencies. Adapting the ISO/SAE 21434 standard, the MITRE ATT&CK framework, and the STRIDE framework into a unified security strategy has demonstrated significant advantages, even when applied to a generic smart home system. By leveraging the strengths of these established frameworks, a more robust and adaptable security methodology was developed, enhancing the ability to identify and mitigate security threats effectively. This effectiveness is reflected in the notable reduction of risk levels from Level 5 to Level 2 across the selected scenarios, highlighting the framework's capability to enhance the security of smart home/IoT environments. In addition to the Damage and Threat scenarios developed as part of this framework, which can be applied in a generalized manner for further analyses, numerous attack and defense mechanisms were systematically evaluated and integrated as predefined classes or catalogs. These elements provide a valuable foundation for subsequent analyses. The adaptation of other frameworks to the required analytical outcomes was also successfully achieved, with substantial support from the Itemis SECURE tool, which facilitated maintaining a structured and comprehensive overview despite the system's inherent complexity. However, it is important to note that using this tool is not a prerequisite for employing the developed framework; rather, it enhances usability and optimizes its implementation. Furthermore, the framework's ability to identify critical attack paths not only enhances the overall threat analysis but also offers valuable insights that inform the development of targeted and effective risk mitigation strategies.

A key factor contributing to the framework's success was the structured approach provided by the ISO standard, which ensured a precise and standardized method for system description and interaction modeling. This allowed for a more comprehensive evaluation of dependencies, traceability, and scalability, all of which are essential for a holistic security assessment. The MITRE ATT&CK and STRIDE frameworks further enriched the analysis by offering detailed attack and defense mechanisms tailored to smart home environments. These elements collectively contributed to a more thorough and structured risk assessment, allowing for more effective security interventions.

Despite these promising results, there remain opportunities for further refinement. Future research could extend the framework by incorporating additional attack scenarios and defense strategies to improve its applicability to real-world smart home ecosystems. Additionally, a more detailed technical description of the system would enhance accuracy in modeling security threats and vulnerabilities. As this analysis represents a proof of concept, its findings provide a solid foundation for further exploration of integrated security approaches. It demonstrated the value of combining multiple methodologies to develop a comprehensive TARA framework for smart home/IoT systems.

CHAPTER 8

Conclusion

This thesis explores the impact of coordinated cyber-attacks on smart home and IoT devices, focusing on their effect on power grid stability. Through simulations and analysis, it is clear that distributed load manipulation poses a serious risk to grid stability. Key factors such as the number and type of compromised devices, their distribution, and the level of coordination play a crucial role in determining the severity of disruptions.

Simulations involving 110 and 230 households demonstrated that high-power devices like EVs, electric ovens, water heaters, and air conditioners can trigger both localized and widespread blackouts. Even a small percentage of compromised devices can cause transformer failures within minutes, highlighting the rapid escalation potential of such attacks.

The results also suggest that achieving a fast disconnection requires a load slightly more than double the transformer's maximum capacity of 360 kW. This indicates that attackers would need to coordinate the power draw of multiple devices to reach this threshold. Additionally, these simulations, based on energy consumption patterns in Germany and Austria, suggest that these attacks are more successful during the winter months when higher baseline energy consumption makes disruptions easier with fewer compromised devices.

To enhance the security of smart home systems, this thesis proposes a TARA framework developed using methodologies from the automotive, software, and networking sectors. The framework incorporates elements from the ISO/SAE 21434 standard, as well as the MITRE ATT&CK and STRIDE models. These approaches provide structured ways to assess and mitigate risks, improving cybersecurity measures.

Recent findings regarding the ESP32 Wi-Fi/Bluetooth chip, used in over a billion IoT devices, further highlight the potential for large-scale, coordinated attacks due to systemic vulnerabilities. This underscores the need for proactive security measures to address such weaknesses.

In conclusion, this research highlights the potential impact of coordinated cyber-attacks on smart home and IoT devices on power grid stability. It demonstrates how factors such as household numbers, device types, seasonal variations, and attack coordination influence the severity of these impacts. Moreover, the exploration of strategies from other sectors, such as the automotive industry, shows the potential for using cross-disciplinary approaches to identify and address vulnerabilities in smart home systems. By incorporating established frameworks like ISO/SAE 21434, MITRE ATT&CK, and STRIDE, a more comprehensive and effective security strategy was developed, helping to better protect smart homes from evolving cyber threats. This research provides a solid foundation for future work, emphasizing the importance of collaboration between grid operators, device manufacturers, and policymakers to tackle these challenges proactively.

Appendix

Table of Abbreviations

DDoS Distributed Denial of Service

ICT Information- and Communication Technology

SCADA System Control and Data Acquisition

TU Wien Vienna University of Technology

EHV Extra-High Voltage

HV High Voltage

MV Medium Voltage

LV Low Voltage

PMU Phasor Measurement Unit

SCADA Supervisory Control and Data Acquisition

IoT Internet of Things

EV Electric Vehicle

TARA Threat Analysis and Risk Assessment

BSD Berkeley Software Distribution

UNIX Uniplexed Information Computing System

ENTSO-E European Network of Transmission System Operators for Electricity

RTO Regional Transmission Organization

ISO Independent System Operator

ICS Industrial Control Systems

DoS Denial of Service

MiM Man-in-the-Middle

DER Decentralized Energy Resources

IEEE Institute of Electrical and Electronics Engineers

NIST National Institute of Standards and Technology

CSF Cybersecurity Framework

ENISA European Union Agency for Cybersecurity

SMM Security Maturity Model

IoTSF Internet of Things Security Framework

SAE Society of Automotive Engineers

UNECE United Nations Economic Commission for Europe

EU European Union

STRIDE Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege

HVAC Heating, Ventilation and Air Conditioning

PII Personal Identifiable Information

API Application Programming Interface

JSON JavaScript Object Notation

REST Representational State Transfer

IL Impact Level

AFL Attack Feasibility Level

RL Risk Level

HO Homeowner

TCP Transport Control Protocol

IP Internet Protocol

NIC Network Interface Card

ICT Institute of Computer Technology

List of Figures

List of Tables

Übersicht verwendeter Hilfsmittel

AI-tool	Usage
ChatGPT-3.5 Turbo	Grammar, spelling, punctuation corrections, and minor phrasing adjustments

Bibliography

[1] Statista. Number of users of smart homes worldwide from 2019 to 2028 (in millions) [graph], September 2023. Last Accessed: September 24, 2024 - 14:35.

[2] Nivedita Singh, Rajkumar Buyya, and Hyoungshich Kim. Iot in the cloud: Exploring security challenges and mitigations for a connected world, 2024.

[3] Oludare Abiodun, Oludare Omolara, Moatsum Alawida, Rami Alkhawaldeh, and Humaira Arshad. A review on the security of the internet of things: Challenges and solutions. *Wireless Personal Communications*, 119:1–35, 08 2021.

[4] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. Understanding the mirai botnet. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 1093–1110, Vancouver, BC, August 2017. USENIX Association.

[5] Statistisches Bundesamt. Durchschnittliche anzahl der haushaltsmitglieder in deutschland von 1991 bis 2023 [graph]. https://de.statista.com/statistik/daten/studie/156957/umfrage/durchschnittliche-anzahl-der-haushaltsmitglieder-in-deutschland-seit-1991/, April 2 2024. Last Accessed: February 23, 2025 - 15:33.

[6] co2online. Stromverbrauch verstehen: Stromspiegel - stromverbrauch vergleichen. https://www.stromspiegel.de/stromverbrauch-verstehen/stromspiegel-stromverbrauch-vergleichen/, 2025. Last Accessed: February 23, 2025 - 15:53.

[7] Eurostat. Energy consumption in households - statistics explained. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Energy_consumption_in_households, 2025. Last Accessed: February 23, 2025 - 19:58.

[8] BDEW Bundesverband der Energie-und Wasserwirtschaft e.V. Wie heizt deutschland 2023? https://www.bdew.de/media/documents/231221-BDEW-WHD2023.pdf, 2023. Last Accessed: February 23, 2025 - 20:13.

[9] Statista. Electric vehicles - europe | statista market forecast. https://www.statista.com/outlook/mmo/electric-vehicles/europe, 2025. Last Accessed: February 23, 2025 - 22:24.

[10] European Heat Pump Association (EHPA). Heat pump sales drop 23% in 2024, leading to thousands of european job losses. https://www.ehpa.org/news-and-resources/press-releases/heat-pump-sales-drop-23-in-2024-leading-to-thousands-of-european-job-l 2025. Last Accessed: February 23, 2025 - 22:45.

[11] United Nations. Un news: Climate action summit 2024. https://news.un.org/en/story/2024/08/1152766, 2024. Last Accessed: February 23, 2025 - 23:00.

[12] Statista. Air conditioners - europe | statista market forecast. https://www.statista.com/outlook/cmo/household-appliances/major-appliances/air-conditioners/europe, 2025. Last Accessed: February 23, 2025 - 22:55.

[13] MBizon. Electricity grid schematic (english). https://commons.wikimedia.org/wiki/File:Electricity_Grid_Schematic_English.svg, 2010. Last Accessed: March 8, 2025 - 12:53.

[14] Austrian Power Grid. Austrian electricity market model. Last Accessed: September 24, 2024 - 19:04.

[15] Austrian Power Grid. Balancing - stability of system frequency. Last Accessed: September 20, 2024 - 15:27.

[16] Unknown. Schema einsatz von regelleistung. https://de.wikipedia.org/wiki/Regelleistung_(Stromnetz)#/media/Datei:Schema_Einsatz_von_Regelleistung.png, n.d. Last Accessed: March 8, 2025 - 12:53.

[17] Xinyu Liang, Hua Chai, and Jayashri Ravishankar. Analytical methods of voltage stability in renewable dominated power systems: A review. *Electricity*, 3:75–107, 02 2022.

[18] Joshua W. Busby, Kyri Baker, Morgan D. Bazilian, Alex Q. Gilbert, Emily Grubert, Varun Rai, Joshua D. Rhodes, Sarang Shidore, Caitlin A. Smith, and Michael E. Webber. Cascading risks: Understanding the 2021 winter blackout in texas. *Energy Research & Social Science*, 77:102106, 2021.

[19] CNN. Bangladesh suffers widespread blackouts after power grid failure. https://edition.cnn.com/2022/10/04/asia/bangladesh-blackouts-power-grid-failure-intl/index.html, 2022. Last Accessed: March 8, 2025 - 12:53.

[20] New York Times. Pakistan suffers nationwide blackout after power grid failure. https://www.nytimes.com/2021/01/09/world/asia/pakistan-blackout-power-failure.html, 2021. Last Accessed: March 8, 2025 - 12:53.

[21] Associated Press. Massive blackout hits tens of millions in south america. https://apnews.com/article/a29b1da1a91542faa91d68cf8e97a34d, 2019. Last Accessed: March 8, 2025 - 12:53.

[22] CNN. Monkey causes nationwide power outage in kenya. https://edition.cnn.com/2016/06/08/africa/kenya-monkey-power-outage-trnd/index.html, 2016. Last Accessed: March 8, 2025 - 12:53.

[23] CNN. Power outage hits much of turkey. https://edition.cnn.com/2015/03/31/middleeast/turkey-power-outage/index.html, 2015. Last Accessed: March 8, 2025 - 12:53.

[24] BBC News. India power cut leaves 300 million without electricity. https://www.bbc.com/news/world-asia-india-19060279, 2012. Last Accessed: March 8, 2025 - 12:53.

[25] The Guardian. Itaipu blackout hits brazil. https://www.theguardian.com/world/2009/nov/11/itaipu-blackout-hits-brazil, 2009. Last Accessed: March 8, 2025 - 12:53.

[26] AsiaNews. Indonesia: blackout leaves 120 million people without light. https://www.asianews.it/news-en/Indonesia:-blackout-leaves-120-million-people-without-light-3935.html, 2005. Last Accessed: March 8, 2025 - 12:53.

[27] NASA Safety Center. Northeast blackout of 2003. https://sma.nasa.gov/docs/default-source/safety-messages/safetymessage-2008-03-01-northeastblackoutof2003.pdf, 2008. Last Accessed: March 8, 2025 - 12:53.

[28] NBC News. Massive blackout hits brazil and paraguay. https://www.nbcnews.com/id/wbna33844757, 2009. Last Accessed: March 8, 2025 - 12:53.

[29] Bhaba Das. Transformers magazine, issue 1, vol 9, 2022: Ester-filled distribution transformers: The sustainable model to strengthen the low voltage grid. 01 2022.

[30] National Renewable Energy Laboratory. Thermal loading and protection of transformers. https://www.nrel.gov/docs/fy25osti/92076.pdf, 2025. Last Accessed: March 5, 2025 - 23:52.

[31] Ieee recommended practice and requirements for harmonic control in electric power systems. *IEEE Std 519-2014 (Revision of IEEE Std 519-1992)*, pages 1–29, 2014.

[32] Fatima Zahra Fagroud, Nouhaila Idrissi, El Habib Ben Lahmar, Ahmed Zellou, Hicham Toumi, Khadija Achtaich, and Sanaa El Filali. Iot architectures: A brief survey on layers' services. In *Proceedings of the 8th International Conference on Advanced Intelligent Systems and Informatics 2022*, pages 641–652. Springer International Publishing, 2023.

[33] Alae-Eddine Bouaouad, Adil Cherradi, Saliha Assoul, and Nissrine Souissi. The key layers of iot architecture. In *2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)*, pages 1–4, 2020.

[34] Mohammad Ali Jabraeil Jamali, Bahareh Bahrami, Arash Heidari, Parisa Allahverdizadeh, and Farhad Norouzi. *IoT Architecture*, pages 9–31. Springer International Publishing, Cham, 2020.

[35] Farhana Javed, Muhamamd Khalil Afzal, Muhammad Sharif, and Byung-Seo Kim. Internet of things (iot) operating systems support, networking technologies, applications, and challenges: A comparative review. *IEEE Communications Surveys & Tutorials*, 20(3):2062–2100, 2018.

[36] Mahdi Daghmehchi Firoozjaei, Nastaran Mahmoudyar, Yaser Baseri, and Ali A. Ghorbani. An evaluation framework for industrial control system cyber incidents. *International Journal of Critical Infrastructure Protection*, 36:100487, 2022.

[37] Dragos. Chernovite: Pipedream malware targeting industrial control systems. Technical report, Dragos, April 2022.

[38] Recorded Future. Cyber threat analysis: Targeting of indian critical infrastructure. Technical report, Recorded Future, February 2021.

[39] Recorded Future. Tag-38: Targeting of indian critical infrastructure. Technical report, Recorded Future, April 2022.

[40] Marcus Geiger, Jochen Bauer, Michael Masuch, and Jörg Franke. An analysis of black energy 3, crashoverride, and trisis, three malware approaches targeting operational technology systems. In *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, volume 1, pages 1537–1543, 2020.

[41] Pavel Kozak, Ivo Klaban, and Tomáš Šlajs. Industroyer cyber-attacks on ukraine's critical infrastructure. In *2023 International Conference on Military Technologies (ICMT)*, pages 1–6, 2023.

[42] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc., USA, 1st edition, 2001.

[43] Haseeb Touqeer, Shakir Zaman, Rashid Amin, Mudassar Hussain, Fadi Al-Turjman, and Muhammad Bilal. Smart home security: challenges, issues and solutions at different iot layers. *The Journal of Supercomputing*, 77(12):14053–14089, 2021.

[44] Asma Jahangeer, Sibghat Ullah Bazai, Saad Aslam, Shah Marjan, Muhammad Anas, and Sayed Habibullah Hashemi. A review on the security of iot networks: From network layer's perspective. *IEEE Access*, 11:71073–71087, 2023.

[45] Brian Krebs. Krebsonsecurity hit with record ddos, 2016. Last Accessed: October 12, 2024 - 14:35.

[46] OVHcloud. The ddos that didn't break the camel's back, 2024. Last Accessed: October 12, 2024 - 14:35.

[47] The Guardian. Ddos attack on dyn: Mirai botnet, 2016. Last Accessed: October 12, 2024 - 14:35.

[48] Antonia Affinito, Stefania Zinno, Giovanni Stanco, Alessio Botta, and Giorgio Ventre. The evolution of mirai botnet scans over a six-year period. *Journal of Information Security and Applications*, 79:103629, 2023.

[49] Adrian Dabrowski, Johanna Ullrich, and Edgar R. Weippl. Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well. In *Proceedings of the 33rd Annual Computer Security Applications Conference*, ACSAC '17, page 303–314, New York, NY, USA, 2017. Association for Computing Machinery.

[50] Saleh Soltan, Prateek Mittal, and H. Vincent Poor. Blackiot: Iot botnet of high wattage devices can disrupt the power grid. In *Proceedings of the 27th USENIX Conference on Security Symposium*, SEC'18, page 15–32, USA, 2018. USENIX Association.

[51] Bing Huang, Alvaro A. Cardenas, and Ross Baldick. Not everything is dark and gloomy: power grid protections against iot demand attacks. In *Proceedings of the 28th USENIX Conference on Security Symposium*, SEC'19, page 1115–1132, USA, 2019. USENIX Association.

[52] Tohid Shekari, Alvaro A Cardenas, and Raheem Beyah. Madiot 2.0: Modern high-wattage iot botnet attacks and defenses. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 3539–3556, USA, 2022. USENIX Association.

[53] Niklas Goerke, Alexandra Märtz, and Ingmar Baumgart. Who controls your power grid? on the impact of misdirected distributed energy resources on grid stability. In *Proceedings of the 15th ACM International Conference on Future and Sustainable Energy Systems*, e-Energy '24, page 46–54, New York, NY, USA, 2024. Association for Computing Machinery.

[54] Subhash Lakshminarayana, Sondipon Adhikari, and Carsten Maple. Analysis of iot-based load altering attacks against power grids using the theory of second-order dynamical systems, 2021.

[55] Subhash Lakshminarayana, Juan Ospina, and Charalambos Konstantinou. Load-altering attacks against power grids under covid-19 low-inertia conditions, 2022.

[56] Juan Ospina, Xiaorui Liu, Charalambos Konstantinou, and Yury Dvorkin. On the feasibility of load-changing attacks in power systems during the covid-19 pandemic. *IEEE Access*, 9:2545–2563, 2021.

[57] National Institute of Standards and Technology (NIST). Framework for improving critical infrastructure cybersecurity. https://www.nist.gov/cyberframework. Last Accessed: October 31, 2024 - 19:12.

[58] Microsoft. The stride threat model. https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN. Last Accessed: October 31, 2024 - 16:28.

[59] ENISA. European union agency for cybersecurity (enisa). https://www.enisa.europa.eu/. Last Accessed: November 1, 2024 - 10:30.

[60] Industrial Internet Consortium. Security maturity model (smm). https://www.iiconsortium.org/smm/. Last Accessed: November 1, 2024 - 14:45.

[61] IoT Security Foundation. Iot security foundation. https://iotsecurityfoundation.org/. Last Accessed: November 1, 2024 - 16:20.

[62] MITRE. Mitre att&ck. https://attack.mitre.org/. Last Accessed: November 2, 2024 - 18:00.

[63] MITRE. Threat assessment and remediation analysis (tara). https://www.mitre.org/news-insights/publication/threat-assessment-and-remediation-analysis-tara. Last Accessed: November 2, 2024 - 10:45.

[64] International Organization for Standardization (ISO). Iso/sae 21434:2021. https://www.iso.org/standard/70918.html. Last Accessed: November 2, 2024 - 17:15.

[65] Daniel Hauer, TU Österreich, Franz Zeilinger, Ralf Mosshammer, Thomas Leopold, and Stefan Wilker. Bifrost-a narrative simulation tool for smart energy scenarios-tutorial and hands-on. In *ComForEn 2021: 11. Symposium Communications for Energy Systems*, pages 123–129. Österreichischen Verbandes für Elektrotechnik, 2021.

[66] itemis. Tara process high-level overview. https://www.itemis.com/en/products/itemis-secure/documentation/user-guide/taraprocesshighleveloverview#taraprocesshighleveloverview. Last Accessed: December 14, 2024 - 15:21.

[67] Bosch. Hrg7784b1 einbau-backofen mit dampfunterstützung. https://www.bosch-home.at/shop/kochen-backen/herde-backoefen/einbau-backoefen/HRG7784B1, 2025. Last Accessed: March 3, 2025 - 15:20.

[68] Bosch. Pkn645ba2e elektro-kochfeld. https://www.bosch-home.at/shop/kochen-backen/kochfelder/elektro/PKN645BA2E#/Tabs=section-technical-overview/Togglebox=accessories/Togglebox=combinables/Togglebox=manuals/Togglebox=accessoriesOthers/, 2025. Last Accessed: March 3, 2025 - 15:20.

[69] Home Depot. 50-gallon electric tank water heaters. https://www.homedepot.com/b/Plumbing-Water-Heaters-Tank-Water-Heaters-Electric-Tank-Water-Heaters/50-gal/N-5yc1vZ2fkoqeqZ1z1t3pn, 2025. Last Accessed: March 3, 2025 - 14:51.

[70] LG Electronics. Lg klimaanlage libero smart 3.5 kw 12000btu wi-fi r32. https://www.elettronew.com/de/klimaanlagen/lg-klimaanlage-libero-smart-35-kw-12000btu-wi-fi-r32-aa-26643.html, 2025. Last Accessed: March 3, 2025 - 14:46.

[71] ETI Group. Fuse links nh gtr characteristic. https://www.etigroup.eu/products-services/fuse-links-nh/gtr-characteristic, n.d. Last Accessed: March 8, 2025 - 12:53.

[72] Rohan Best and Fatemeh Nazifi. Analyzing electric vehicle uptake based on actual household distributions: A contribution to empirical policy formulation. *Transport Policy*, 137:100–108, 2023.

[73] Hamed Naseri, E.O.D. Waygood, Zachary Patterson, and Bobin Wang. Who is more likely to buy electric vehicles? *Transport Policy*, 155:15–28, 2024.

[74] Bleeping Computer. Undocumented commands found in bluetooth chip used by a billion devices. https://www.bleepingcomputer.com/news/security/undocumented-commands-found-in-bluetooth-chip-used-by-a-billion-devices/amp/, 2024. Last Accessed: March 18, 2025 - 12:53.