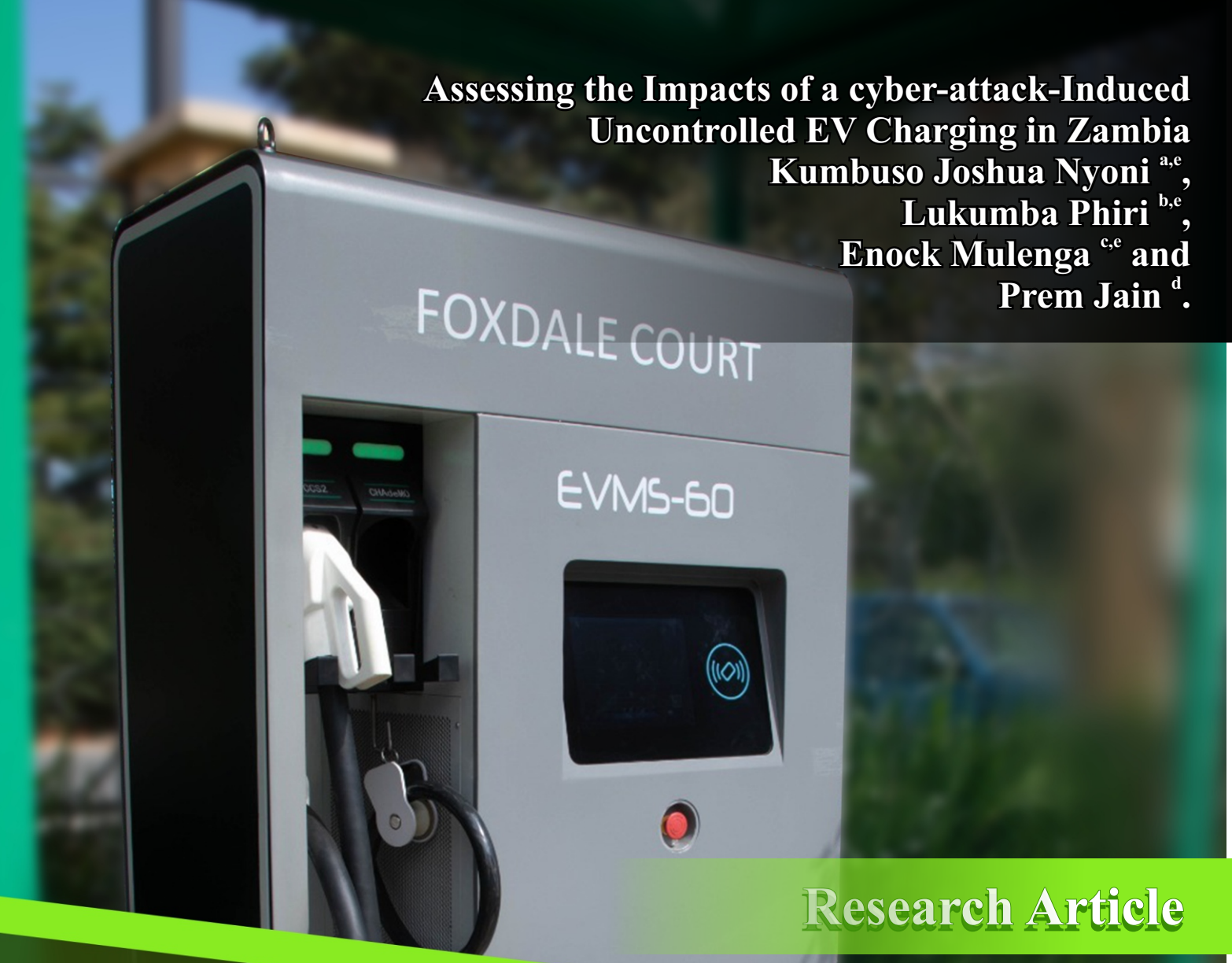
Assessing the Impacts of a cyber-attack-Induced Uncontrolled EV Charging in Zambia

Kumbuso Joshua Nyoni [a,e], Lukumba Phiri [b,e], Enock Mulenga [c,e] and Prem Jain [d].



Research Article

Zambian Electric Mobility Innovation Alliance

https://www.zemia.org/ https://web.facebook.com/profile.php?id=100094171776026 twitter.com/ZEMIA_Zambia
www.linkedin.com/company/zambia-electric-mobility-innovation-alliance www.instagram.com/zemia_zambia
PLOT NO. 27, NCHENJA ROAD, OFF PASELI ROAD, NORTHMEAD, LUSAKA, ZAMBIA

Article

Assessing the Impacts of a cyber-attack-Induced Uncontrolled EV Charging in Zambia

Kumbuso Joshua Nyoni [a,e], Lukumba Phiri [b,e], Enock Mulenga [c,e] and Prem Jain [d].

[a] College of Science and Engineering, School of Geosciences, University of Edinburgh, UK
[b] Department of Electrical and Electronic Engineering, School of Engineering, University of Zambia, Lusaka, Zambia
[c] Department of Engineering Sciences and Mathematics, Energy Science-Electric Power Engineering, Luleå University of Technology, Skellefteå-Sweden
[d] Department of Physics, School of Natural Sciences, University of Zambia, Lusaka, Zambia
[e] Zambian Electric Mobility Innovation Alliance (ZEMIA)

For more information, please contact the Lead Researcher, Kumbuso Joshus Nyoni on;

kumbuso@zemia.org

https://orcid.org/0000-0003-3831-8981

https://www.zemia.org

ZAMBIAN ELECTRIC MOBILITY INNOVATION ALLIANCE (ZEMIA) INCEPTION REPORT (2022-2023)

Introduction The Zambian Electric Mobility Innovation Alliance (ZEMIA) is a non-profit organization established in June 2022 with a mission to promote and develop the electric vehicle (EV) ecosystem in Zambia. ZEMIA comprises diverse stakeholders from various fields, including automotive, renewable energy, academia, government, and NGOs, working collaboratively to drive sustainable and low-carbon transportation in the country. With over 30 active members, ZEMIA leverages its expertise and network to advocate for EV-friendly policies and environmentally responsible practices within the battery metal value chain.

Mission and Objectives *Mission*: To accelerate the adoption, development, and growth of the electric mobility ecosystem in Zambia, fostering a sustainable and low-carbon transportation future.

ZEMIA lead by ;

1. **President - Kabayo Muhau**
2. **Vice President - Kumbuso Joshua Nyoni**
3. **Head – Research & Development - Clement Sichimwa**
4. **Head - Leads Market & Partner Cooperation - Michael Sakala**
5. **Adoption Enablers - Alexandros Germanis**
6. **Adoption Enablers - Musiyani Gavin Chewe**
7. **Adoption Enablers - Chilombo Chila**

***OBJECTIVES*:**

1. **Foster Adoption: Promote EV adoption by raising awareness and facilitating collaboration among stakeholders.**
2. **Drive Development: Support charging infrastructure, local EV manufacturing, and research and development.**
3. **Advocate for Policies: Influence policies to support EV adoption, including incentives and renewable energy integration.**
4. **Promote Sustainability: Prioritize environmental responsibility in the battery metal value chain.**
5. **Pioneering Excellence: Encourage innovation and knowledge sharing in the EV sector.**

WORKING GROUPS

ZEMIA has seven working groups focusing on:

1. **Adoption Enablers (Incentives, Policy, Regulation & Standards)**
2. **Charging Infrastructure**
3. **Research & Development (Academic & Workforce Programs)**
4. **Electric Motor Vehicles & Cycles**
5. **Technology**
6. **Battery Storage**
7. **Supply Chain Attraction and Innovation**

These groups collaborate to advance electric mobility in Zambia, addressing various aspects of the ecosystem.

RECENT ACTIVITIES & INITIATIVES

- **Public Sector Engagement and Lobbying: Successfully influenced a reduction in Customs Duties for EVs in the 2023 National Budget.**
- **National Charging Infrastructure Rollout Strategy & Action Plan: Collaborated on a comprehensive plan for convenient EV charging access.**
- **Research and Knowledge Dissemination: Contributed to research papers on EV adoption and cybersecurity.**
- **International Engagements: Joined the Global Electric Vehicle Alliance (GEVA) and collaborated with Africa Electric Mobility Alliance (AEMA) and United Nations Environment Programme (UNEP).**
- **Information and Awareness Raising Initiatives: Utilized social media, surveys, and TV interviews to educate the public about EVs.**

FUTURE PLANS

- **LEAP Fund Award: Implementing the "Accelerating Zero-Emission Public Transportation in Zambia (ZAMBIAeMobilize)" project to revolutionize public transportation.**
- **Global Environment Facility (GEF 8) Project: Collaborating on "Supporting the Shift to Electric Mobility in the Republic of Zambia" to encourage EV adoption through policy advocacy, research, and innovation.**

CONCLUSION

ZEMIA has made significant strides in advancing electric mobility in Zambia through policy advocacy, knowledge dissemination, and international collaborations. Its commitment to sustainability and innovation positions it as a key player in shaping Zambia's transportation future towards zero-emission solutions.

BIBLIOGRAPHY

- **Global Electric Vehicle Alliance. (2023). Zambian Electric Mobility Innovation Alliance. Link**
- **Musokotwane, S. (2023). Budget Address. Link**
- **Nyoni, K.J. (2023). Electric Mobility Rollout Potential in Zambia: Initiating the discourse on the missing links. Link**
- **Zambian Electric Vehicle Innovation Alliance. (2023). ZEMIA. Link**
- **ZEMIA. (2023). ZEMIA on ZNBC TV2's Morning Live Interview. Link**

Abstract:

The electrification of public road transportation in Zambia is considered a critical step in reducing greenhouse gas emissions to safe levels, although it is still in its early stages. This process involves intricate technological developments, infrastructure, behaviors, stakeholders, business models, and interactions. To ensure the safe operation of the charging infrastructure, protective measures such as cyber-security, and coordinated and controlled charging must be in place. However, cyber attacks pose a potential risk to the charging infrastructure in Zambia, which could lead to uncontrolled charging. A study was conducted on a shopping mall in Lusaka, Zambia, identified as a crucial facility for the roll-out of public charging stations. To enhance uptake, innovative funding agencies should implement the recommendations made in this paper, which assess the existing conditions of the landscape. The Power Factory's DIgSILENT Quasi Dynamic Simulation was used to replicate charging behavior and evaluate the impact of electric vehicles (EVs). The findings revealed that cyber attacks on these systems could have severe consequences, ranging from regional disruptions in the short term to national disturbances in voltage levels and thermal loading in the long term. It was also found that the last-mile transformers could become overloaded and bottleneck EV charging due to cyber-induced uncontrolled charging.

Keywords: Cyber-Attack; Distribution network;
uncontrolled charging; Electric Vehicles; Undervoltage; Greenhouse Gas Emissions (GHG)

1. Introduction

One of the most vibrant markets in the clean energy industry is the one for electric vehicles [1]. Sales of electric vehicles (EVs) increased by 50% in 2021 over the previous year to a new high of 6.6 million. In 2012, only 120 000 electric vehicles were sold worldwide. In 2021, more than that number were sold each week. The electric vehicle market share increased fourfold between 2019 and 2021[1, 2]. With this, there are currently three times as many electric vehicles on the road globally—over 16.5 million—as there were in 2018. The market for electric vehicles has continued to expand quickly, with 2 million electric vehicle sales in the first quarter of 2022, a 75 percent rise over the same period in 2021 [1, 3].

A variety of variables influence the popularity of EVs. The main pillar is consistent policy support. Incentives and subsidies from the government for EVs increased by about 30 billion USD in 2021[4]. A rising number of nations have made commitments to phase out internal combustion engines or have aggressive goals for the future electrification of vehicles. Many automakers, meanwhile, have longer-term plans to electrify their fleets than the policy targets call for [5]. Finally, there were five times as many new EV models available in 2021 as there were in 2015, making them more appealing to buyers. Around 450 EV models are now on the market [4-6].

1.1. Overview of EV Progress in Zambia

The desire to have the first electric vehicle (EV) in Zambia was made public in 2018. It was mentioned that introducing electric vehicles would help reduce carbon emissions and contribute to the fight against climate change. It is envisioned that Zambia would be the hub of EV manufacturing in the SADC region [7]. A business forum in November 2021 on "Fostering the development of a battery, electric vehicle and renewable energy industry value chain and market in Africa" ended with the signing of a Memorandum of Understanding for Zambia and DRC in April 2022. The two countries agreed to increase their contribution to the electric vehicle (EV) value chain and thus benefit from this emerging global market. It will eliminate undue competition by preventing a race to the bottom. It is meant to instead maximize mutual benefits between the two countries [7-9].

1. Introduction -Cont.

Against the backdrop of developments in the field, several government agencies in Zambia, including ZESCO, the Energy Regulation Board (ERB), and car dealers such as Toyota Zambia and Jaguar, have announced their plans for the preparation and deployment of electric vehicles in the country.

There will be added requirements, such as the infrastructure. The infrastructure for EV charging has to be built. The progress will culminate in rapid EV adoption in Zambia [10-13].

1.2. Problem statement and rationale

There are about 876,520 registered vehicles in Zambia [13]. There will be added complexity to the current smart grid If half of the registered vehicles are the projected number of EVs to be implemented. The distribution network and EV infrastructure had many parties active with Information Communications Technology (ICT) systems working together. There is a risk that multiple cyberattack surfaces are possible for attack or disruption. Although smart Electric Vehicle Control Centres (EVCSs) have not yet experienced large-scale and high-profile cyberattacks, threats and plausible attack vectors, have been reported. It is reported in [14] that there were security flaws in the Charge Point Home smartphone application for EV charging. The flaw would enable a remote attacker to intrude into the charger and tamper with EV charging via the WiFi connection to the charging device. Similar security flaws were also identified in EVlink chargers. The flaw would allow a remote attacker to bypass hard-coded authentication credentials, inject malware and disable the charger. This vulnerability would exploit the weak login credentials stored as plain text for EV charging. There are two types of charging, namely, controlled and uncontrolled charging. The impact of a (targeted) infrastructure disruption can be very great, especially for the controlled charging aspect.

Both upstream (to the Distribution System Operators (DSO) and Transmission System Operators (TSO)) and downstream (via electric cars to mobility and the shutdown of substantial parts of national transport to the disruption of other vital sectors). The safe integration of e-mobility is a big problem. Additionally, any disruptions or changes in either behavior might have serious impacts on the other due to the close connection between the power grid and the e-mobility infrastructure. For instance, uncontrolled EV charging is frequently projected to have detrimental consequences on the electrical grid.

1.Introduction -Cont.

The impacts of uncontrolled EV charging range from lower power quality to a drop in transformer life span to greater line loss[15]. It is owing to the constant rise of the electric vehicle (EV) sector. Controlled charging (e.g., shifting the majority of the EV load to night) can help with this problem [16], and using Vehicle to Grid (V2G), power transfer may even help to improve grid stability [17]. However, to effectively use either of these technologies, a reliable e-mobility infrastructure that properly implements grid-friendly charging schedules (defining consumption over time) and V2G strategies is usually necessary.

Traditional methodologies for grid stability thus fail when taking into account an active attacker with (partial) influence over the e-mobility infrastructure, and the potential of targeted demand-side attacks emerges. For instance, a hacker in charge of a botnet of infected EVs or Charge Points (CPs) can alter the charging schedules to carry out demand-side assaults that result in power outages and line failures. It is vital to understand the behavior of the power grid under assault and the potential effects of the attacker to build resilient solutions.

1.3. Objectives and research contributions

In this paper, we propose a framework for simulating and analyzing the impact of electric vehicles (EV) based on the likelihood of attacks on the distribution network. The aspect of controlled EV charging is also investigated for the distribution network for Lusaka-Zambia and targeting Shopping malls. Shopping malls are the perceived first level of EV charging for potential future adopters. The study will show at what times of the day attacks are most easily carried out and how many are compromised. Various scenarios with different rated charging powers and increasing penetration levels - 25%, 50%, 75, and 100% - will be analyzed to evaluate the consequences on the power system and determine when and how the DSOs need to take action. Furthermore, the various penetration levels increase the total load of the system, causing growth in distribution losses, congestion, and under-voltage issues. This fact is strictly linked to the DSO role, passing on technical issues and economic expenses.

1. Introduction -Cont.

Implementing the framework will help analyze several case studies showing the impact of the different scenarios when there is an attack. The followings are the objectives and contributions of the underpinning study in this paper:

1. Analysis of the impact of the cyber-attack induced uncontrolled EV charging station loads at a shopping mall on transformers and cable.
2. Comprehensive analysis of the cyber-attack induced uncontrolled EV charging on the voltage level, supply cable, and transformer loading at the shopping mall.
3. Recommendations on the approach to the key challenges for efficient, effective, and sustainable integration of uncoordinated EV charging infrastructure in ZambiaThe rest of the paper is structured into six additional chapters; in Chapter 2, Literature related to the study is discussed. In Chapter 3, we discuss the research methodology applied to this research. In Chapter 4, we apply the proposed to some scenarios. Chapter 5 concludes our study. Chapter 6 provides recommendations to reduce the ramifications of EVs on the power grid infrastructure. A conclusion is made in Chapter 7.

2. State of the Art (Literature Review)

EV charging is achieved with controlled and uncontrolled [18]. The charging can be controlled towards an objective or controlled to limit the parameter impact of a distribution network. One objective is to limit the effects of solar PV during the time of highest production.

The other objective would be to limit the peaking of the load for a traditional distribution network. The first and most severe impact of EV charging is increasing the loading of the cable or transformer. EV charging is a new type of consumption. The implementation of controlled EV charging will help alleviate the likelihood of overloading [16]. The introduction of EV charging may require additional investment to counter the impact of overloading. The other important parameter that is impacted by EV charging is the voltage level in the distribution network.

2.1. Uncontrolled EV charging

As the plug-in electric vehicle (PEV) market continues to grow, an increase in the number of vehicles charging on the electric grid is expected [19]. However, this increase will significantly impact the stability and demand of the electric grid, particularly in scenarios where charging is uncontrolled [20]. Uncontrolled charging can lead to higher residential peak demand, and time-of-use utility rate schemes are likely to cause a significant increase in demand ramping. As a result, controlling at-home charging is essential to mitigating the impact of PEVs on the grid [20]. Moreover, uncontrolled charging may cause thermal line overloading and low voltage violations, resulting in grid instability and potential cybersecurity concerns. Simulation studies have demonstrated that while the impact of uncontrolled charging on voltage is modest, line loading impacts are more noticeable, with a maximum increase of about 15%. Furthermore, the peak load times for feeders may shift slightly due to uncontrolled charging.

2. State of the Art (Literature Review) Cont.

2.2. Protecting the Web of Energy: The Significance of Cybersecurity and Privacy for charging points

By using a charging device with a data link, smart charging and vehicle-to-grid (V2G) charging technologies connect an electric car to the power infrastructure. The latter enables information and command sharing between various EV ecosystem players, such as charge points, charge point operators, and grid network operators, among others.

Cybersecurity attacks with information theft, cyberwarfare, or organized crime as motivations could target any linked infrastructure [21]. To prevent threats from having an effect on both consumers and the electricity system as a whole, we must ensure the cyber security of these connected devices and the organizations responsible for running them [22, 23]. Additionally, individual privacy needs to be taken into account. It is risky to share users' data by default without their permission because they might object to efforts for managed charging.

Potential privacy issues, security concerns, and cyber threats in autonomous cars were noted by [24]. In addition to highlighting data collection points, security issues, and cyberattacks, these researchers also suggested a potential countermeasure to lessen and fight against these dangers. Traffic flow attacks, platooning, carpooling, and parking attack situations are a few examples of attacks that have been studied. To emphasize energy trends, technological needs, and cyber security concerns, performed a systematic review of the abrupt change in the transportation sector [25]. The article highlights global energy crisis scenarios, integrates EVs with renewable energy sources, and addresses open issues. The cybersecurity concerns of autonomous vehicles were covered in [26] by illustrating potential attack scenarios. It emphasized possible security holes and weaknesses that could be exploited and impact motorist safety. Also, a research path for using AI and machine learning techniques to defend against specific EV attacks was offered.

In numerous works, the literature has addressed attacks on or through the EV ecosystem against users and the power grid. Attackers who take over the EV's battery management system through hacked online services or malware installed on the vehicle's systems can seriously harm the vehicle itself. In [27, 28], there are discussions of the potential harm the attackers could inflict on the EVs. They present a harmful threat to coordinated charging. By altering the charging current and evading the security precautions, EV batteries can be overcharged. Attacks on users, however, are viewed as being outside the purview of this effort.

2. State of the Art (Literature Review) Cont.

The authors in [29] presented an EV attack formulation that would destabilize the Manhattan power grid by only using data that was readily accessible to the public. Their approach entails modeling the power system as a feedback control system and the EV as the system's feedback gain to calculate the necessary number of EVs. According to their research, even though Manhattan does not have enough EVs at the moment to launch such an attack, the increase in EV sales will eventually create a surface big enough to enable it.

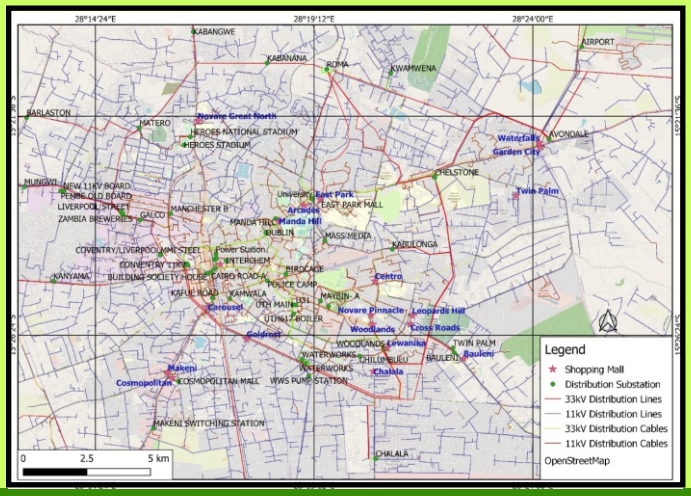
3. Site Selection and Data

Lusaka boasts numerous shopping malls, with the majority experiencing heavy traffic from both Zambian and non-Zambian visitors. Fortunately, these malls have ample room for installing controlled electric vehicle (EV) charging stations, allowing for easy monitoring of loading and preventing overloading. A study focused on one of Lusaka's shopping malls, located near the central business area of the town/province, has led to the decision to install controlled EV charging stations at this mall soon.

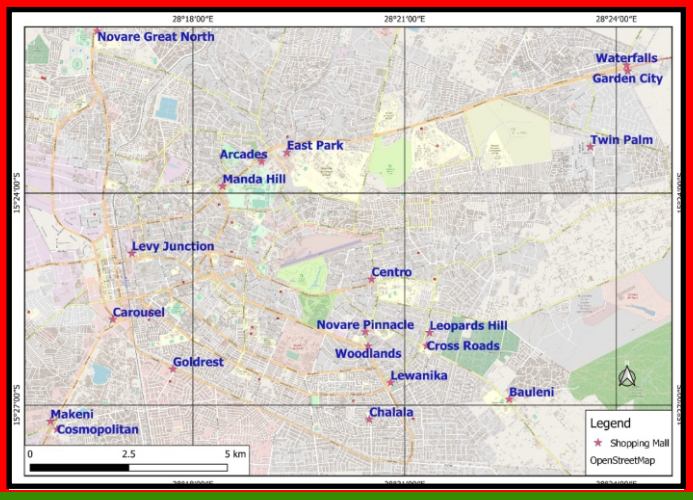
ZEMIA

3. Site Selection and Data Cont.

MALLS IN LUSAKA WITH GRID LINES



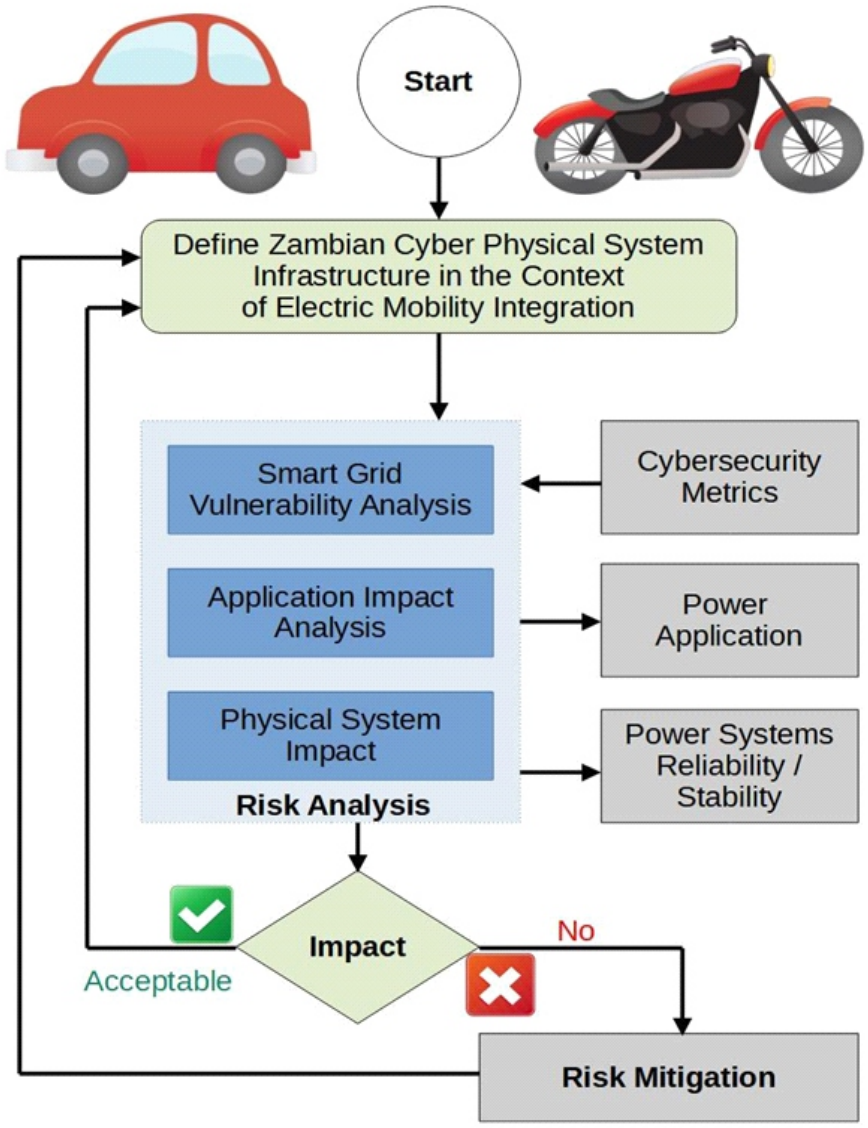
MAP OF MALLS IN LUSAKA



ARIAL VIEW OF LEVY MALL

4. Methodology

The methodology that was used to study the impact of cyber-attack-induced uncontrolled charging is shown in Figure 1.



ZEMIA

4. Methodology Cont.

Figure 1. Methodology encompassing cybersecurity threats.

4.1. Cyber Security Vulnerability Assessment

The cyber security vulnerability assessment is done in Figure 1 and Figure 2.

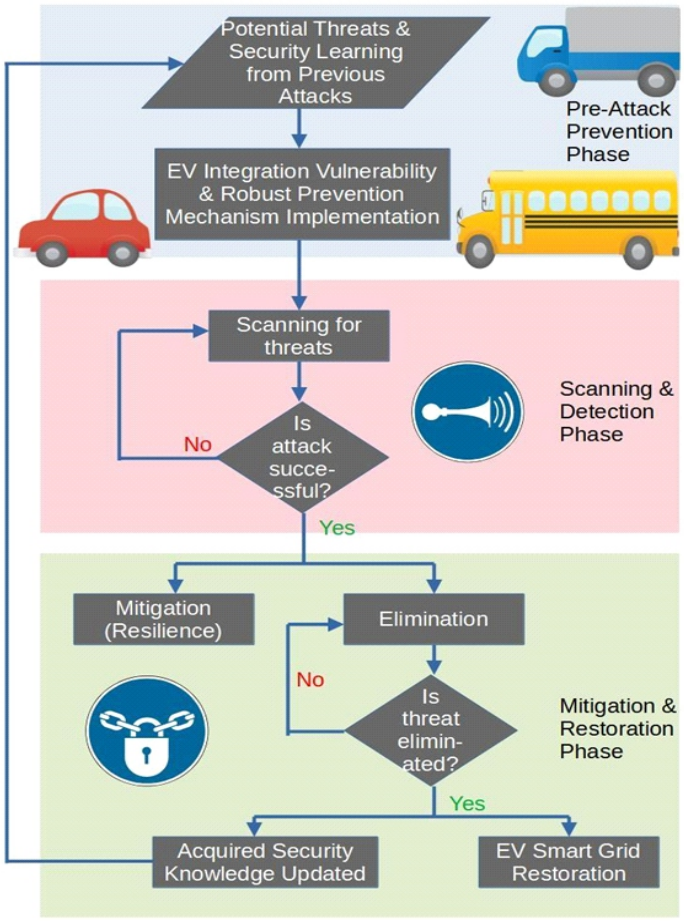


Figure 2. Methodology with cyber security consideration for EV hosting Capacity.

The proper functioning of substations located in various places is vital to the cyber-physical infrastructure of a distribution network. These substations are responsible for supplying energy to shopping malls and EV charging stations.

Figure 1 depicted the evaluation of cyber security maintenance and controlled charging operations. If a cyber attack occurs, uncoordinated charging can result, allowing any customer connected to a charging point to charge their EV. This represents a shift from controlled to uncontrolled charging, with charging occurring at either slow or fast speeds.

Charging that involves only a few simultaneous actions would remain within the limits of the cables and transformers. However, the immediate transition to simultaneous, uncontrolled charging could affect the loading voltage levels, leading to situations of overloading and Undervoltage. Both factors may trigger protection relays, which can cause disruptions to the supply of energy to the shopping mall.

4. Methodology Cont.

A flow chart to counter and mitigate the attacks is proposed in Figure 2. There are three layers in Figure 2, namely: Pre-attack prevention, scanning and detections, and mitigation leading to restorations.

4.1.1. Pre-Attack Prevention

The Identify feature may be the most important because it evaluates the organization's cybersecurity risk. The likelihood and effect of a specific cybersecurity event are multiplied to determine risk. The sum of all potential cybersecurity events represents the organization's danger. The first difficulty in calculating risk is creating an inventory of every scenario. The traditional strategy involves segmenting the issue into various categories of desired security properties, such as the well-known CIA triad: confidentiality, integrity, and availability. Unfortunately, no method can be guaranteed to be comprehensive.

Data confidentiality is a fundamental security feature for protecting data. This is particularly important in cloud computing due to several factors that increase the risk of data breaches. These include remote data storage, the lack of a network perimeter, the use of third-party cloud service providers, multitenancy, and extensive infrastructure sharing. Given these risks, offering data confidentiality as part of cloud computing services is crucial.

Furthermore, since cloud computing combines old and new technologies, it inevitably creates new security risks due to implementation and system design flaws. Balancing data security with usability, system scalability, and dynamics presents challenges in providing adequate security assurance, especially regarding data confidentiality [30].

Integrity models shield system data from unauthorized or unintentional changes, maintaining the accuracy and reliability of the data [30]. Virtue models aim to prevent unauthorized users from changing applications or data and stop improper or unauthorized

changes from being made by approved users. Ensure that data and initiatives are consistent both internally and externally. Balancing a collection of transactions to ensure that all the data is present and correctly accounted for is an illustration of an integrity check [30].

ZEMIA

4.Methodology Cont.

Data and resources are kept accessible for authorized use by availability models, particularly in times of crisis or catastrophe. Information security professionals typically address three typical availability issues: Denial of service (DoS) brought on by malicious assaults or by implementation flaws that have not yet been found (for example, a program written by a programmer who is unaware of a flaw that could crash the program if a certain unexpected input is encountered) loss of information system capabilities brought on by human error or natural catastrophes (such as fires, floods, storms, or earthquakes) (bombs or strikes) equipment fails while being used normally [30].

Granting access only to authorized personnel, encrypting data being sent over the Internet or stored on digital media, testing computer system security regularly to find new vulnerabilities, building software defensively, and creating a disaster recovery plan are some actions that preserve confidentiality, integrity, and/or availability [31].

Given the wide distribution of the attack surface, it is a herculean job to detect cyber threats against electric vehicles and the infrastructure [32].

4.1.2. Scanning and Detection

Operational planning is essential for integrating cyber-security into an infrastructure that is both present and evolving. Cyber ranges can be utilized from a human viewpoint to simulate a representative infrastructure and related cyber-attacks against the power grid to test and train operators to recognize, detect, and react quickly. It is crucial from the end-user viewpoint to inform users of various risks that are still to be discovered. (e.g.Connecting a vehicle to open wireless hotspots in the vicinity of charging stations).

From a technological perspective, EVs and the grid must include a variety of conventional safeguards and defense mechanisms, including firewalls, intrusion detection and prevention systems, disabling default credentials, and communications encryption. Cyber-deception or digital twinning, which monitors the system's status, can also be used to give the attacker the impression that they are interacting with a real system while giving them false information. Cyber-deception also permits information collecting for the recovery phase with a low false positive rate and modus operandi.

4. Methodology Cont.

4.1.3. Mitigation and Restoration

A Security information and event management (SIEM) system should be used to combine data from the different cyber-security tools so that a security operator can analyze it. In addition to deploying cyber-security components, it is important to analyze the tactics, techniques, and procedures (TTPs) used by attackers and take lessons from prior attacks.

Currently, utilities build and manage generating stations, substations, transmission, and distribution networks with varying degrees of contingency design to guarantee service continuity. The goal of a contingency design is to guarantee that, if one or more components fail up to a preset design level, neither the remaining equipment in use will stop serving customers nor will it operate above its intended working specifications or ratings. Instead of multiple pieces of equipment being damaged at one location or even losing multiple important facilities, utilities typically create contingency plans based on the failure of a single piece of equipment or a common support structure. (like a common transmission tower). However, such N-1 or N-2 design criteria are probably not sufficient to guarantee continued operation in the event of a carefully planned terrorist attack.

Utilities and electric vehicle service equipment operators must therefore create emergency response strategies. The planning and drill process is invaluable in developing a capability to react to actual events because it provides a fundamental framework and foundation, even though it is impossible to cover all potential emergency scenarios. Manufacturers can reduce the risks of cyberattacks on connected and automated vehicles (CAVs) by: Switching to a safe operational mode if inaccurate sensor data is discovered, such as alerts and driver intervention with automation levels 1 through 3

Implementing systems for instruction detection and prevention, such as firewalls, secure shells that verify the network and the device, key management, private access point names, and password encryption; and using secure communication infrastructure, such as dedicated short-range communication (DSRC) on a system like the U.S. Department of Transportation (DOT's) Security Credential Management System (SCMS).

Using network segmentation, encryption, secure authorization, and authentication for OTA updates and safety-critical messages in modern vehicles [33].

ZEMIA

4. Methodology Cont.

4.2. EV Charging Impact Assessment

The sustained attack on cyber security and loss of control led to the uncontrolled charging of EVs. There is a need to assess this impact. The impact of the slow and fast charging is assessed using the flowchart in Figure 3.

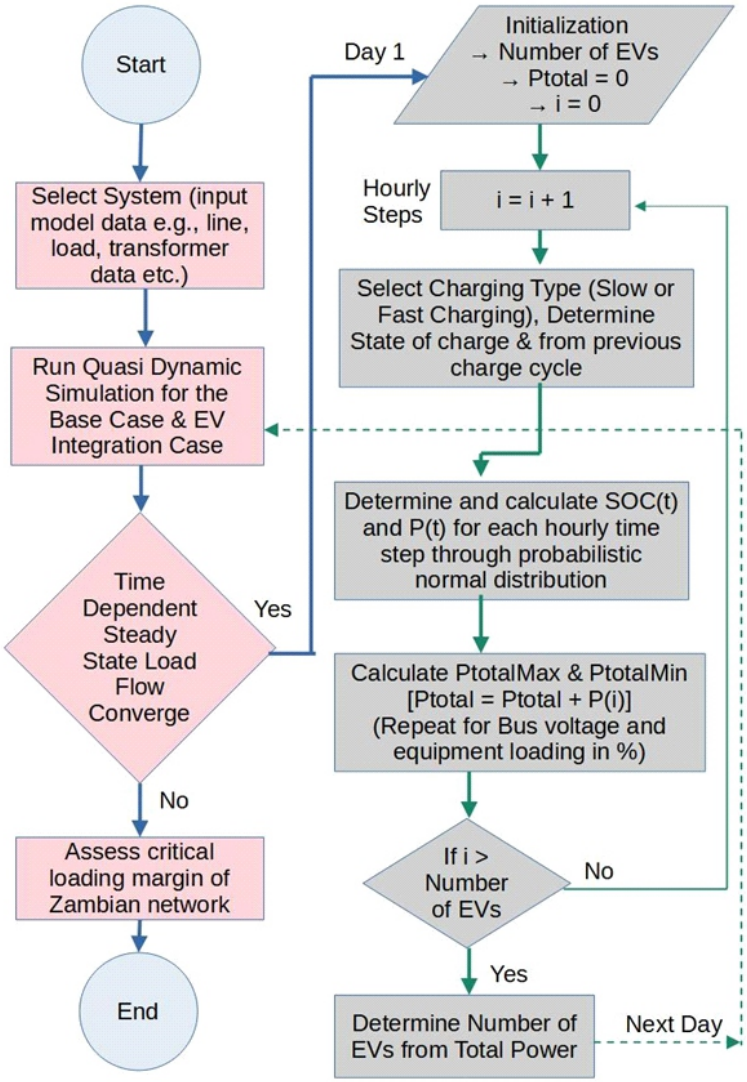


Figure 3. Overall study methodology.

The steps taken for the Quasi-Dynamic impact study are summarised in Figure 3. The modeling of the study was done in DigSilent Power Factory. A quasi-dynamic model was implemented in the developed model. It is explained in Section 4.2.1.

In the quasi-dynamic simulation (QDS), the Electric Vehicle model will start charging within a given time range between the earliest and the latest time of arrival (specified by the user, parameters "EarliestArrival" and "LatestArrival").

ZEMIA

4. Methodology Cont.

Using a uniform distribution, the model chooses the starting time for each new day within the specified time range.

The user can define if the charging station supports fast charging (parameter "fast-charging") and specify the corresponding power flow (parameters "maxP" for fast charging and "lowP" for normal charging). The energy size of the EV's battery is provided by the parameter "Eini" in MWh. The state of charge (SOC) at the start of charging is drawn randomly to represent varying driving distances per day and vehicle. If the maximum allowed SOC is reached (SOC is at the value of parameter "SOCmax"), i.e. if the EV is fully charged, the SOC will remain at this SOC level internally. On the following day, the SOC is again drawn randomly at the time of arrival (which is within the specified time range).

The first part of the study is modeling the distribution network supplying Levy Shopping Mall in DigSilent Power Factory Software. The distribution network of cables is from the UTH substation to the Levy Shopping Mall substation with its transformers (T1-T5).

The base case, without EV charging, is obtained through the initial simulation and comparison with the measurement at the substation for verification. After the verification, the controlled EV charging was studied.

The cyber attack and loss of control lead to uncontrolled charging. The impact of slow and fast uncontrolled/uncoordinated charging is studied. It follows the flow chart presented in Figure 3. The charging profiles implemented are discussed in Section 4.2.1.

4.2.1. Fast and Slow Charging Profiles

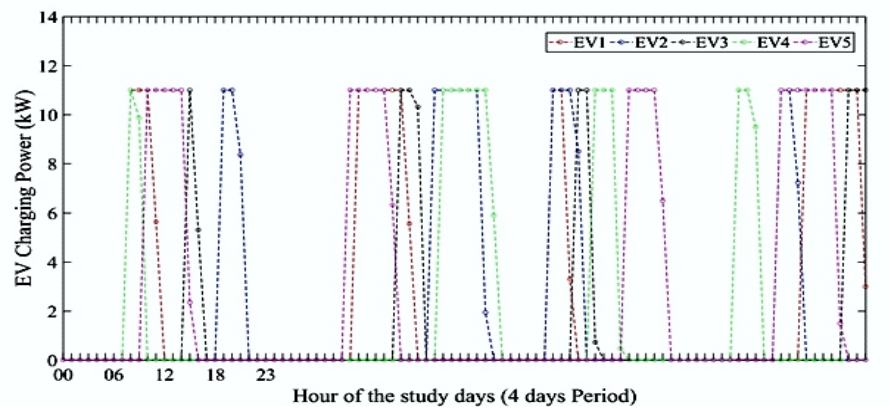
The study has adopted slow and fast charging profiles, utilizing charging powers of 3.7 kW, 11 kW, and 22 kW. To benchmark the charging times for the EVs, the battery capacity in the quasi-dynamic model was assumed to be 100 kWh for generic EV loads and 80 kWh for EVs connected to Charging Station (1). According to the simulation results, assuming the battery is at 25% state of charge (SOC), it would take approximately 20 hours for a 3.7 kW charger to reach a full charge for the generic EV loads. On the other hand, an 11 kW charger would only take 6.8 hours for the same generic EV loads. In the case of EVs connected to Charging Station (1), an 11 kW charger would take approximately 5.45 hours to reach a full charge from the initial 25% SOC. For faster charging, the 22 kW fast charger was found to be more efficient, taking only 2.7 hours to attain a full charge from the same initial 25% SOC. These results are consistent with previous studies on EV charging profiles, where fast charging is more efficient and effective in reducing charging times.

Figures 4 (a) and (b) show the fast and slow charging profiles applied in the model. The uncontrolled charging makes any of the EVs able to charge without any associated control.

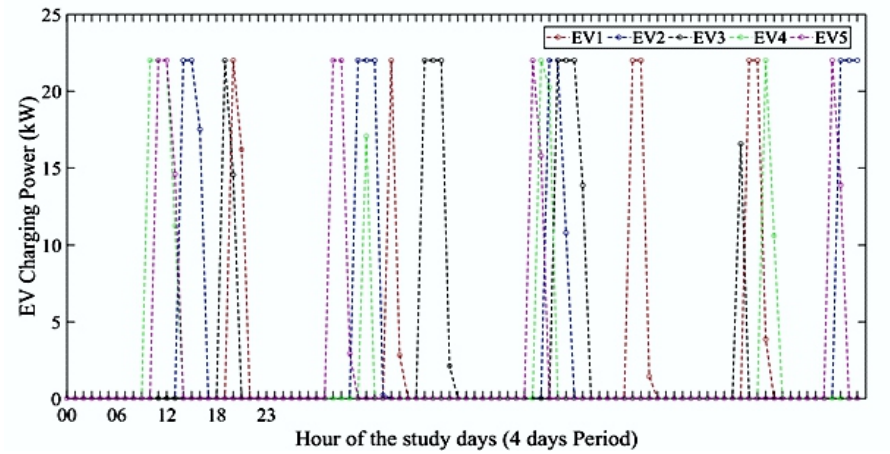
ZEMIA

4. Methodology Cont.

Figures 4 (a) and (b) show the fast and slow charging profiles applied in the model. The uncontrolled charging makes any of the EVs able to charge without any associated control.



(a) The EV's charging cycles for fast charging and durations during study hours.



(b) The EV's charging cycles for fast charging and durations during study hours.

Figure 4. The slow and fast charging cycles of Electric Vehicles (EVs) at Levy Shopping Mall.

ZEMIA

5. EV Integrated Results

5. EV Integration Results

The results of the EV Charging integration started with coordinated and controlled EV charging. After that, for uncoordinated/uncontrolled charging results, impact on voltage level and loading are obtained.

5.2. Controlled and Coordinated EV Charging

The supply cable has a capacity of 30 MW. The transformers connected downstream and supplying the mall are 12 MW (T1) and 1 MW (T2-T5).

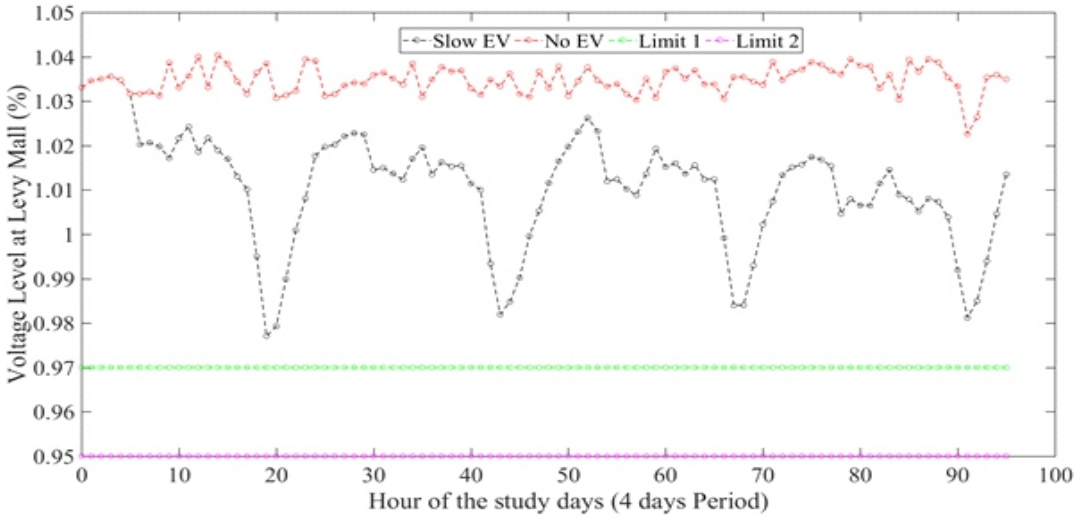
The coordinated and controlled EV charging within the cyber security space entails mitigation of exceeding the limits of the supply cable and transformers. The simulated study for the intended installation showed no violation of limits. The operation of the installation in a coordinated and controlled way is essential for the shopping mall studied.

5.3. Uncontrolled and Uncoordinated EV Charging

Cyber attacks and loss of control influence the system parameters. The results obtained are given in Section 5.2.1 to Section 5.2.3.

5.2.1. Levy Shopping Mall Voltage Profile

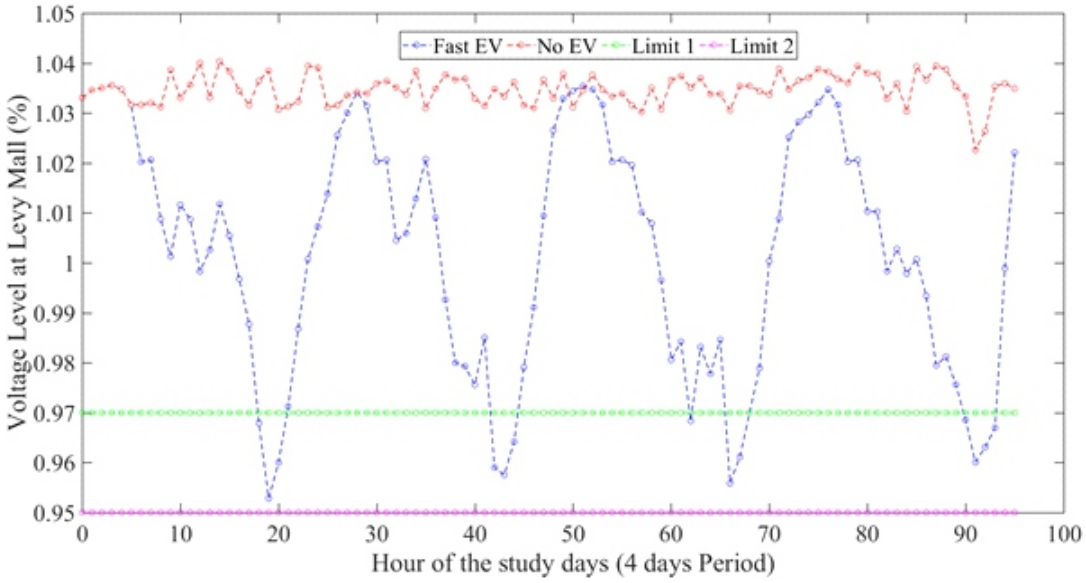
The results for the voltage level and profile for the quasi-dynamics study for the days are shown in Figure 5.



(a) The EV's slow charging impacts the voltage level.

ZEMIA

5. EV Integrated Results Cont.



(b) The EVs fast charging impact on the voltage level.

Figure 5. The slow and fast charging of Electric Vehicles (EV) effect on the voltage level at Levy Shopping Mall.

The impact of the slow and fast charging at the shopping mall is shown in Figures 5 (a) and 5 (b). In both EV charging, there is a cyclic impact of the voltage level and profile. The effect is severe for fast charging (see (b).

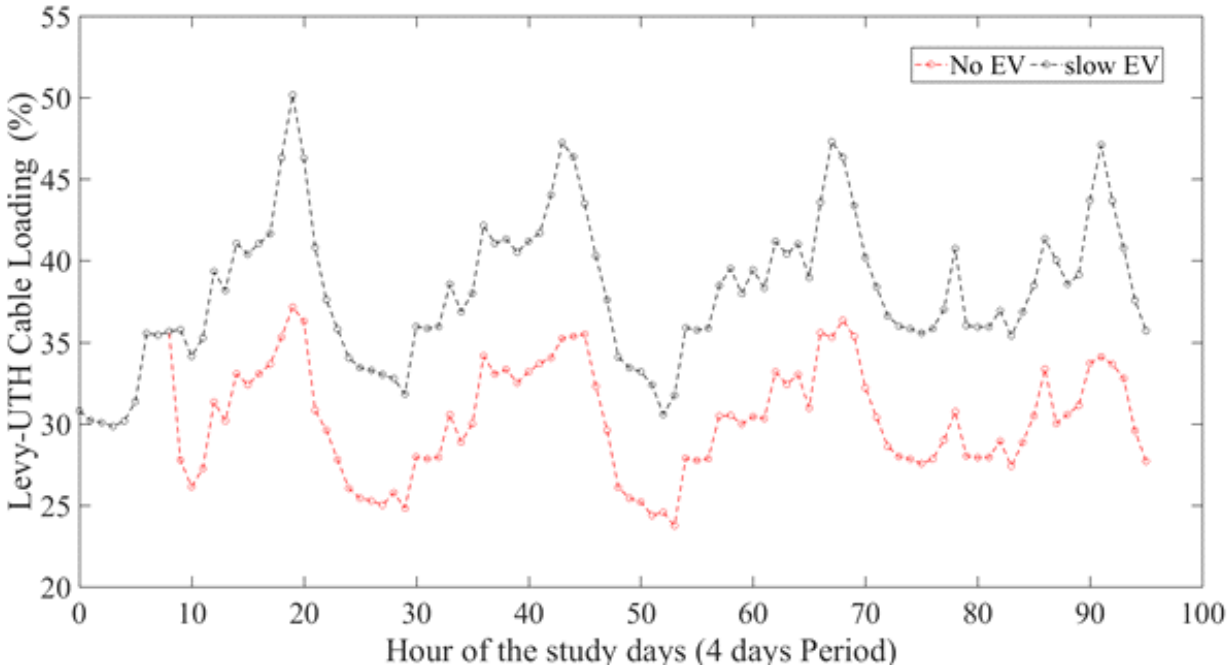
In Figure 5 (a), the 3% and 5% limits are not exceeded. There is an indication of Undervoltage Undervoltage times. The planning aspect expects the voltage not to go beyond the 3% limit level. The power quality needs to be within 5% of the nominal value. The fast charging cycles impacted the voltages worse than the slow charging cycles. The voltage level and profile exceed the planning level at various times. The power quality level of 95% (-5%) is not exceeded. At a certain point, there is a high likelihood of getting closer to the 5% limit.

ZEMIA

5. EV Integrated Results Cont.

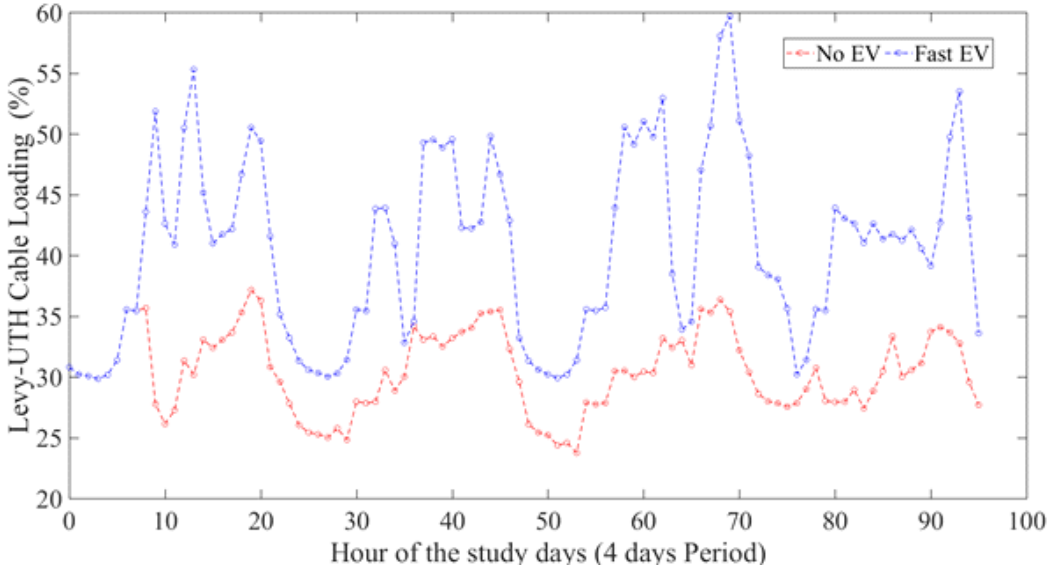
5.2.2. UTH-Levy Shopping Mall Cable Loading Levels

The cable connection between UTH and Level Mall can carry 30 MW of the load. The base results, slow and fast EV charging impact on the loading level, are shown in Figure 6.



(a) The changes in the loading level due to EV's slow charging.

5. EV Integrated Results Cont.



(b) The changes in the loading level of the supply cable due to EVs fast charging.

Figure 6. The changes in the UTH-Level Shopping Mall cable loading level due to the slow and fast charging of Electric Vehicles (EV).

The margin between the base load and the maximum capacity of the supply cable varied between 63% and 76%. The margin is larger than 50% of the capacity.

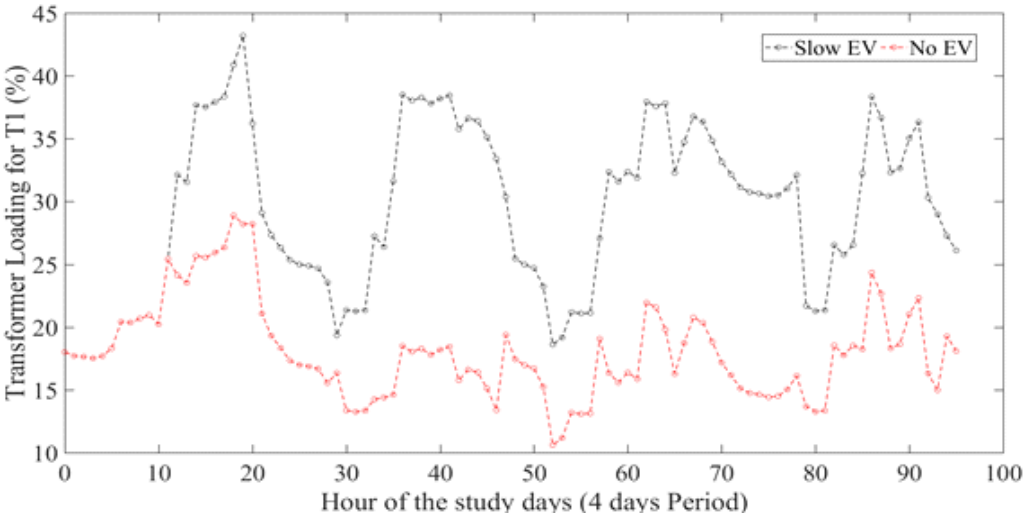
In Figure 6 (a), the maximum loading with slow, fast charging is at the 50% mark. For fast charging, it is at the 60% mark. The increase in load with slow and fast charging is not larger than 60% of the cable carrying capacity.

5.2.3. Transformer T1-T5 Loading Levels

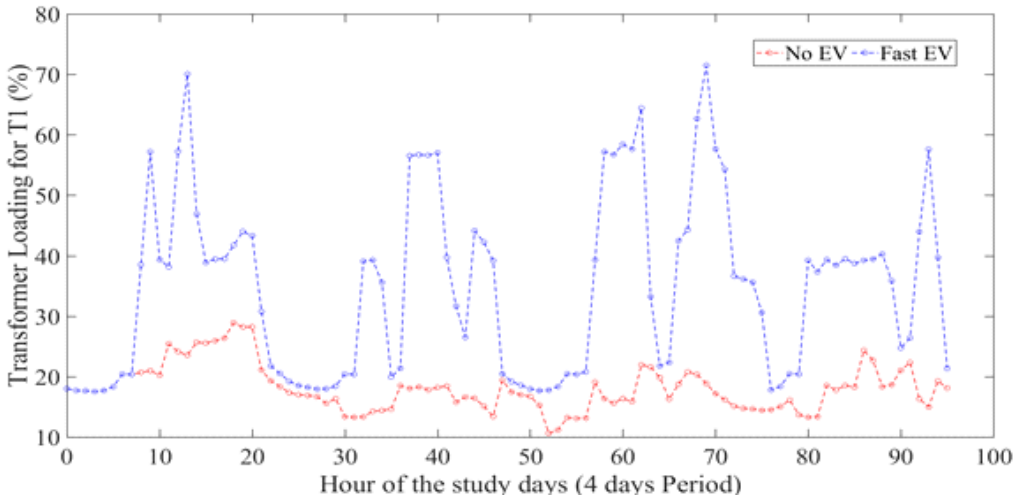
ZEMIA

5. EV Integrated Results Cont.

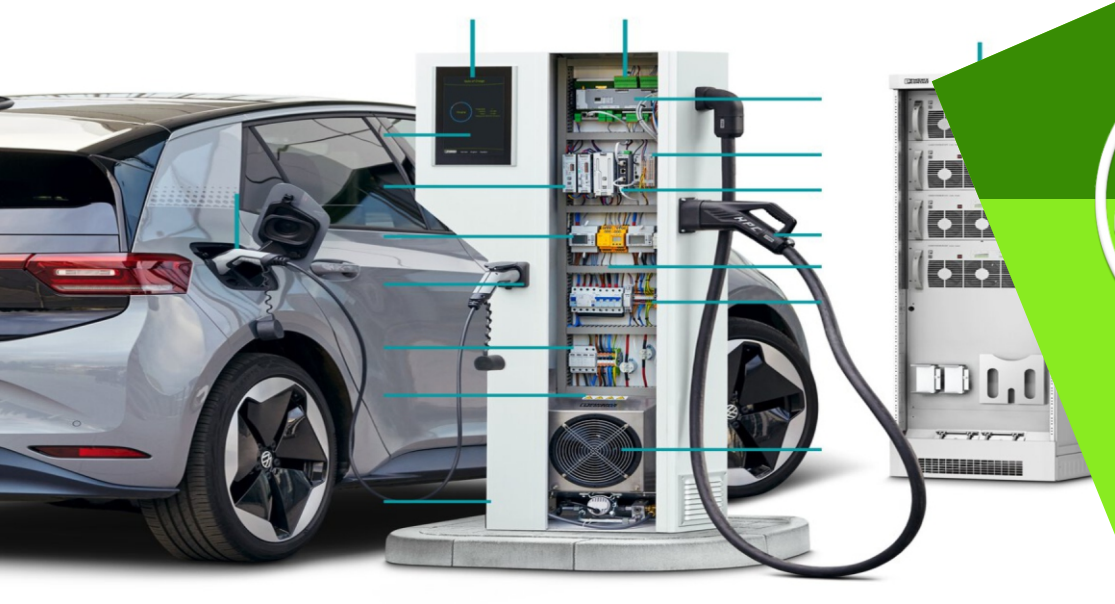
The transformer supply is via the receiving T1 with the technical specifications of 12 MVA 33/11 kV. The loading level of the base, with slow and fast EV charging, is given in Figure 7.



(a) The Transformer T1 loading level changes because of slow charging.

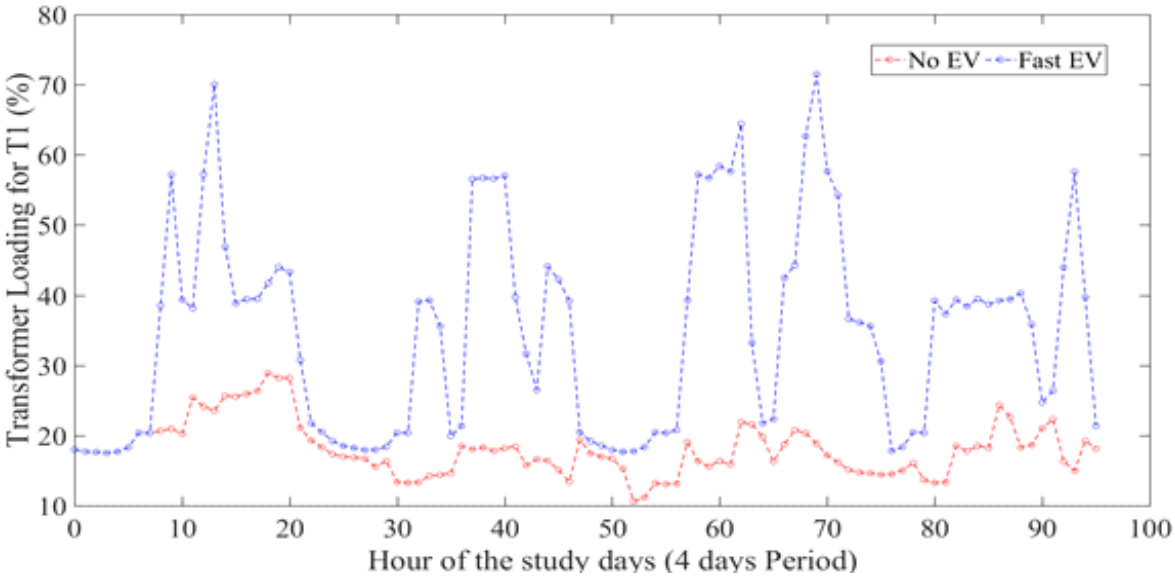


(b) The Transformer T1 loading level changes because of fast charging.



ZEMIA

5. EV Integrated Results Cont.



(b) The Transformer T1 loading level changes because of fast charging.

Figure 7. The changes in Transformer-T1 loading level due to the slow and fast charging of Electric Vehicles (EV).

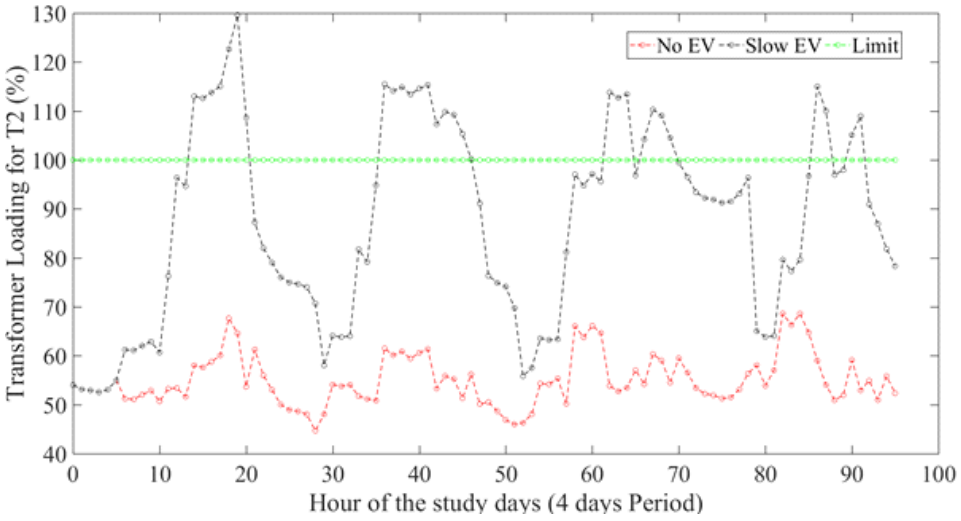
The transformer T1 will limit EV charging at the shopping mall. The margin of the base load is 56% minimum and a maximum of 82% in a cyclic manner. The number of EV charging at a minimum load margin is 1,816 (3.7 kW), 610 (11 kW), and 305 (22 kW) downstream of the transformer T1. When the maximum margin is considered, the number of EVs can increase by 46% that of the minimum margin.

The connection of slow charging downstream shows a maximum margin reduction from 82% to 55%. The transformer thermal limit is not exceeded. Similarly, the margin reduces from 56% to 30% for fast charging cycles. More uncoordinated and uncontrolled EV charging can take place downstream for transformer T1.

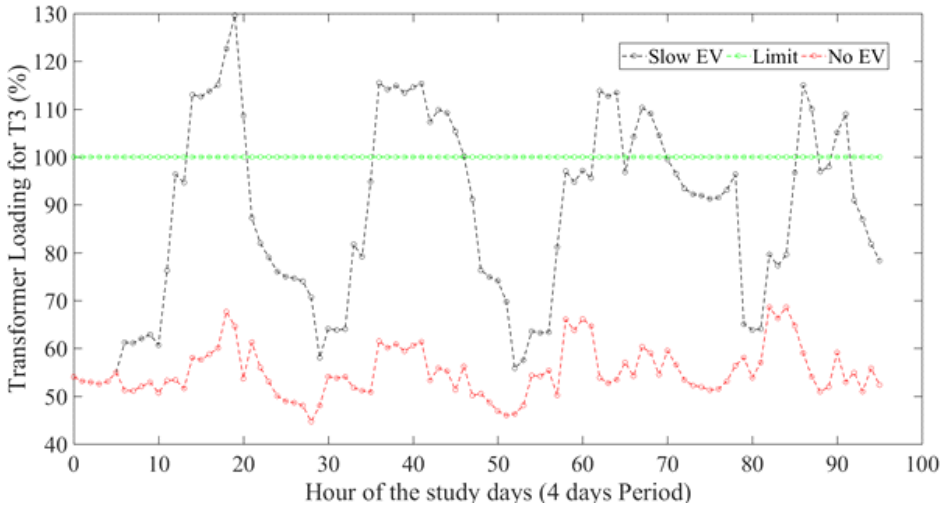
The next challenge is on the 11/0.4 kV transformers with 1 MW each. The results of the impact of EV charging are given in Figures 8 (a) to (d).

ZEMIA

5. EV Integrated Results Cont.



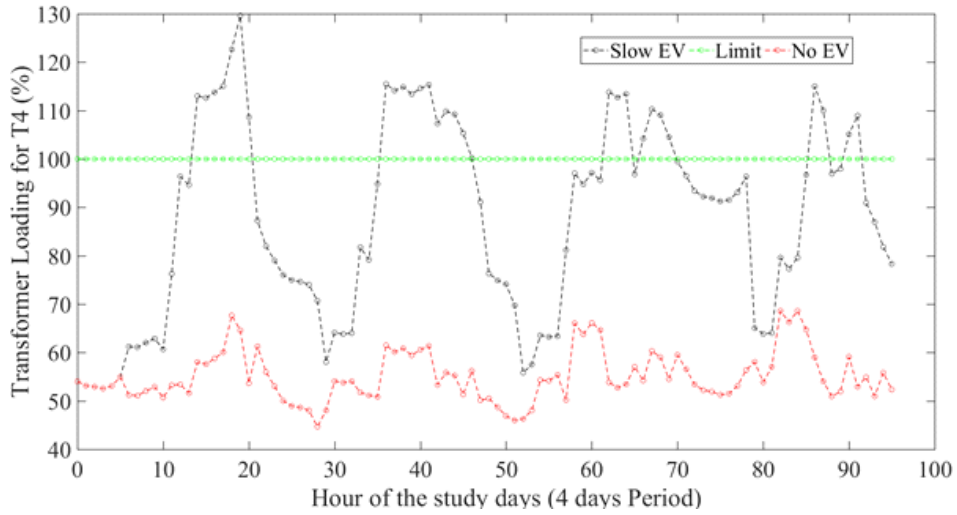
(a) The Transformer T2 loading level changes because of slow charging.



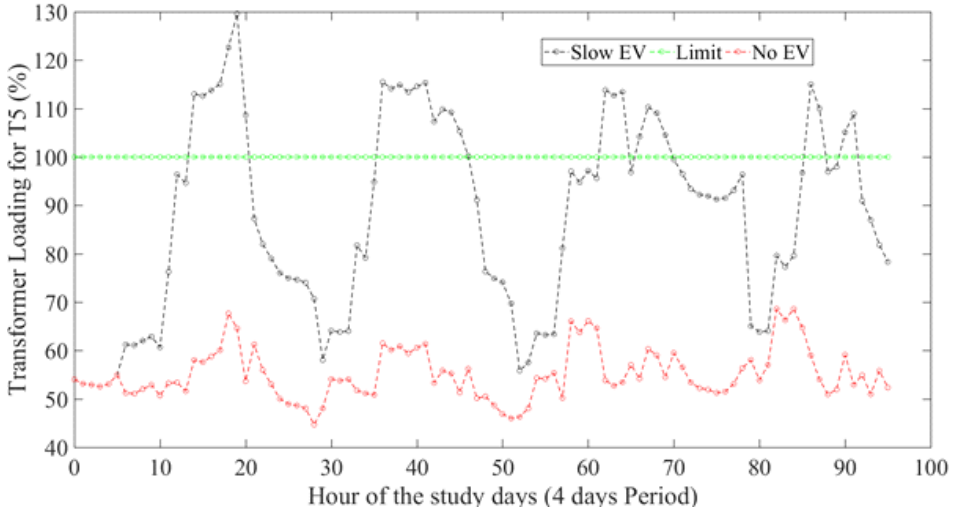
(b) The Transformer T3 loading level changes because of slow charging.

ZEMIA

5. EV Integrated Results Cont.



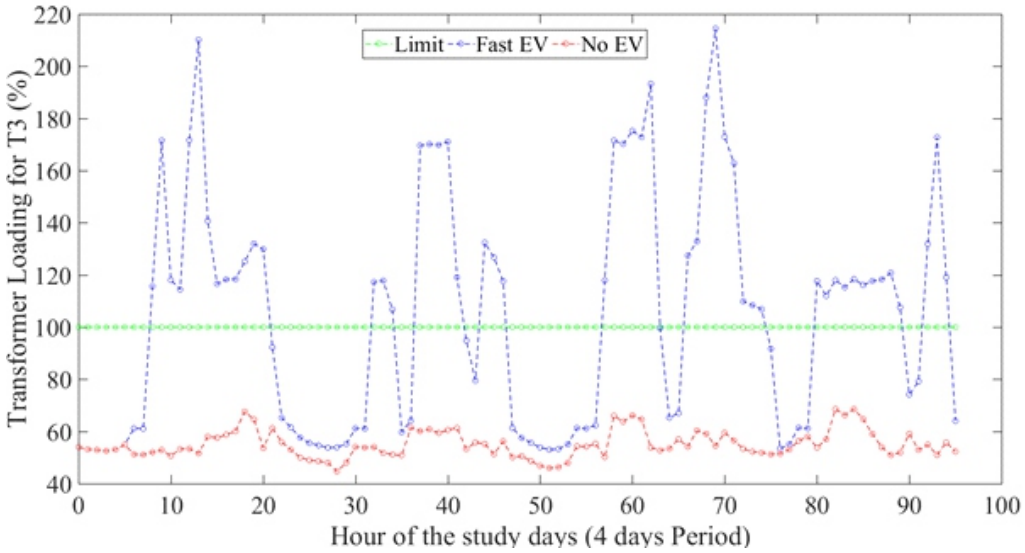
© The changes in the Transformer T4 loading level because of slow charging.



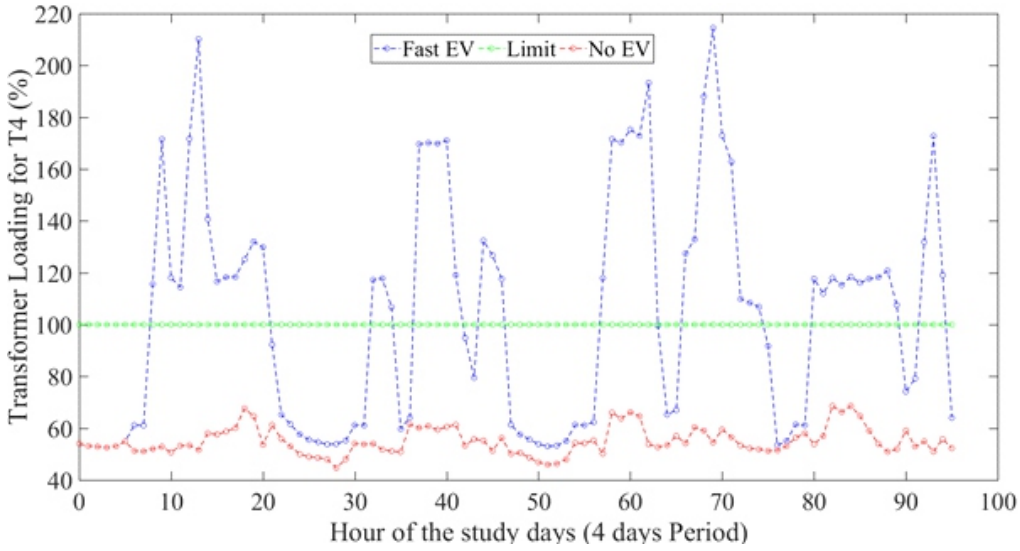
(a) The Transformer T2 loading level changes because of fast charging.

ZEMIA

5. EV Integrated Results Cont.



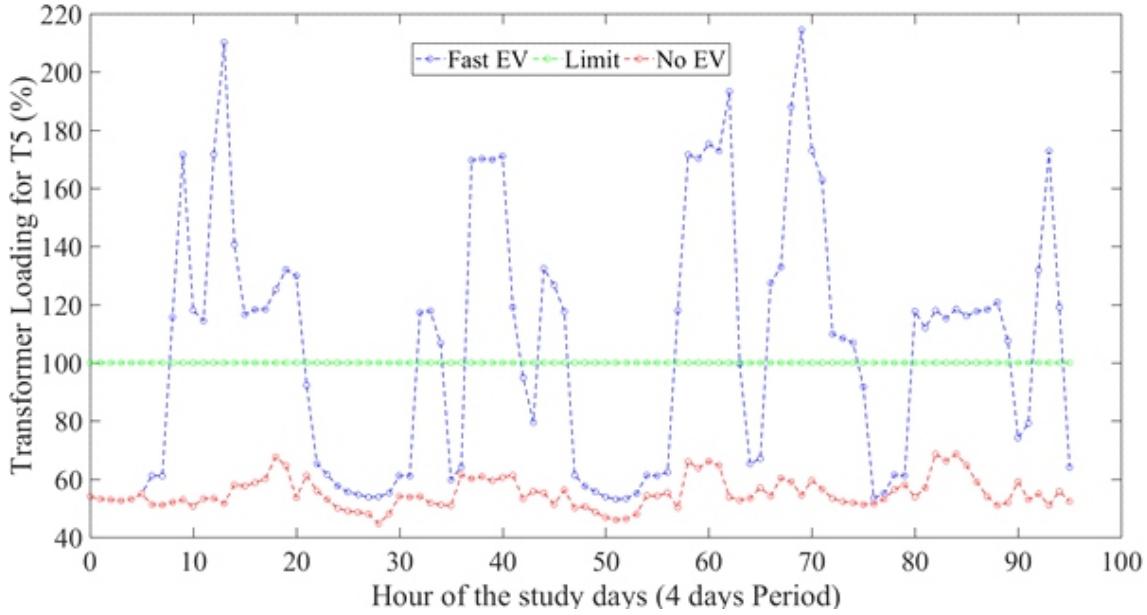
(b) The Transformer T2 loading level changes because of fast charging.



(c) The Transformer T2 loading level changes because of fast charging.

ZEMIA

5. EV Integrated Results Cont.



(d) The Transformer T2 loading level changes because of fast charging.

Figure 9. The changes in Transformer-T2 to T5 loading level due to the fast charging of Electric Vehicles (EV).

The impact of fast charging is severe for the transformers T2-T5. There will be overloading and loss of supply. The thermal limit is exceeded for each of the parallel transformers. Both slow and fast charging would be a problem for the downstream transformers.

ZEMIA

6. Discussion

This study examined the impact of cyber security on coordinated and controlled EV charging in public places such as shopping malls. The findings demonstrate that maintaining cyber security is crucial to regulating the charging cycles at public charging stations with multiple charging points. Previous research in the literature supports the importance of cyber security in the functioning of electric vehicles, as any cyber attack or breach can lead to uncoordinated charging, causing chaos and disruption.

The power supply cable and main transformer for the Levy shopping mall were planned and designed by the utility company, ZESCO, to consider future growth in loads. The last mile transformer (11/0.4 kV) was identified as the bottleneck for adding many EV charging stations. Four last-mile transformers were installed in parallel at the shopping mall, with each operating at a manageable load. However, if all transformers were to operate as a unit, the load would increase by 17% for slow EV charging and 36% for fast EV charging, which is allowable for all transformers in operation. Nevertheless, an overloading condition would occur if 2-3 transformers are lost.

The analysis results in Section 5 revealed the development of an Undervoltage problem due to slow and fast charging. While Undervoltage is not the main issue in public places, overloading is the most significant challenge. Thermal limits, including the thermal limits of lines, cables, transformers (larger than 11 kV), and last mile transformers (11/0.4 kV), must be considered for the rollout of EV charging points in public places, malls, and residential areas. The findings of this study highlight the need for improved planning and management of public charging stations to ensure safe and reliable charging infrastructure that is resilient to cyber-attacks.

ZEMIA

7. Conclusion

This paper presents a detailed quasi-dynamic EV integration study, including an analysis of uncoordinated charging induced by a cyber-attack on controlled charging. The study reveals that the bottleneck for integrating EV charging points in public places will be overloading lines, cables, and transformers. It is recommended that cyber security for public charging stations be enhanced with top-notch coordination and control.

The paper successfully proposes a framework for simulating and analyzing the impact of electric vehicles on the distribution network in Lusaka-Zambia, specifically targeting shopping malls as the perceived first level of EV charging for potential future adopters. The study analyses various scenarios with different rated charging powers and increasing penetration levels and presents comprehensive analyses of the impact of cyber-attack-induced uncontrolled EV charging on the voltage level, supply cable, and transformer loading at shopping malls.

Furthermore, the paper presents recommendations for addressing key challenges for Zambia's efficient, effective, and sustainable integration of uncoordinated EV charging infrastructure. Implementing this framework will aid in analysing case studies showing the impact of different scenarios during a cyber-attack, fulfilling the study's objectives. Overall, this paper contributes significantly to the literature and provides valuable insights for policymakers and stakeholders in the electric vehicle industry.

8. Acknowledgments

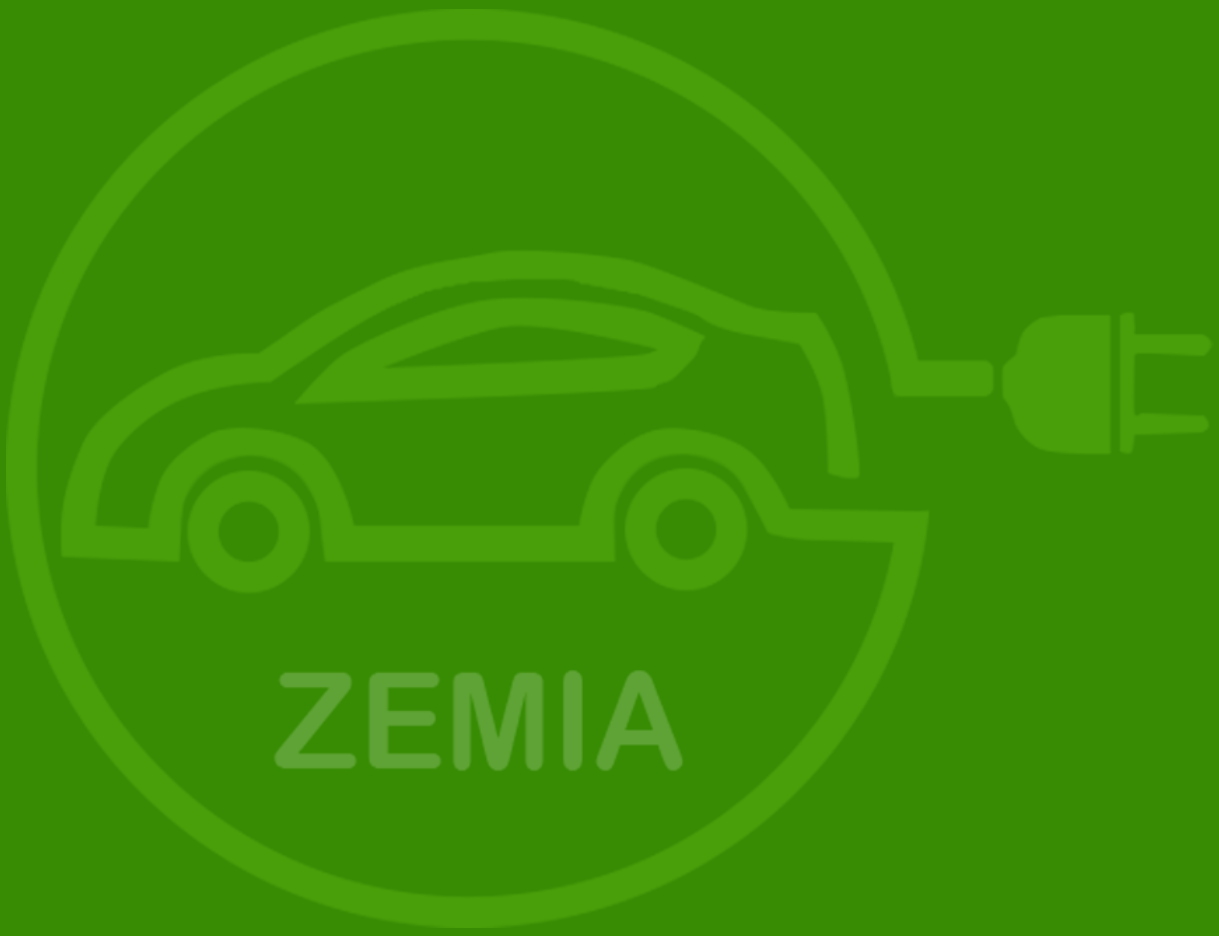
The work was done during the Energiforsk (Sweden) funded project on Methods for estimating the hosting capacity at the Luleå University of Technology, Skellefteå-Sweden, in Collaboration with ZESCO (Utility company) and the University of Zambia (UNZA) in Zambia.

9. References

1. [1] IEA. (2022). *Electric cars fend off supply challenges to more than double global sales*. Available: https://www.iea.org/commentaries/electric-cars-fend-off-supply-challenges-to-more-than-double-global-sales
2. [2] M. Surin. (2022). *Global sales of EVs rose to a record high of 6.6 million in 2021, says IEA*. Available: https://www.theedgemarkets.com/article/global-sales-evs-rose-record-high-66-million-2021-says-iea
3. [3] IEA, "Net Zero by a 2050-A roadmap for the Global Energy Sector," International Energy Agency (IEA), Paris, France, 2021.
4. [4] Virta Ltd. (2022). *"The Global Electric Vehicle Market in 2022 – Virta." Virta Global,* Available: https://www.virta.global/en/global-electric-vehicle-market
5. [5] Clean Energy Ministerial (CEM), "Global EV Outlook 2021," International Energy Agency (IEA), 2022.
6. [6] Dezan Shira & Associates, "China Considers Extending its EV Subsidies to 2023," in *China Briefing*, ed. Beijing, China: China Briefing, 2022.
7. [7] Joshua Jere. (2018). *Zambia Launches First Electric Cars*. Available: https://www.znbc.co.zm/news/zambia-launches-first-electric-cars/
8. [8] Autoworld Zambia. (2021, March). *Electric-powered vehicles in Zambia?* Available: https://www.autoworldzambia.com/blog/electric-powered-vehicles-in-zambia
9. [9] Lusaka Times. (2022, December). *ERB prepares for Electric vehicle deployment*. Available: https://www.lusakatimes.com/2022/05/27/363311/
10. [10] J. Mututwa and S. Manchishi. (2022, December). *How Can Zambia Benefit from the Electric Vehicle Market?* Available: https://zipar.org.zm/how-can-zambia-benefit-from-the-electric-vehicle-market/
11. [11] Atlas Copco Zambia. (2022, December). *The lightweight, electric future of cars*. Available: https://www.atlascopco.com/en-zm/itba/industry-solutions/automotive-entry/electricvehicles
12. [12] D. Whitehouse. (2022, November). *Zambia's copper can drive the global shift to electric cars*. Available: https://www.theafricareport.com/181236/zambias-copper-can-drive-global-shift-to-electric-cars-zanaco-executive-says/
13. [13] K. J. Nyoni, "Electric Mobility Rollout Potential in Zambia," *Zenodo,* pp. 1-18, 2022.
14. [14] Dmitry Sklyar, "Remotely controlled EV home chargers – the threats and vulnerabilities," Kaspersky and SecureLine, 2018.
15. [15] H. Xiao, Y. Huimei, W. Chen, and L. Hongjun, "A survey of the influence of electric vehicle charging on the power grid," in *9th IEEE Conference on Industrial Electronics and Applications*, 2014, pp. 121-126.
16. [16] R. A. Verzijlbergh, M. O. W. Grond, Z. Lukszo, J. G. Slootweg, and M. D. Ilic, "Network Impacts and Cost Savings of Controlled EV Charging," *IEEE Transactions on Smart Grid,* vol. 3, pp. 1203-1212, 2012.
17. [17] K. M. Tan, V. K. Ramachandaramurthy, and J. Y. Yong, "Integration of electric vehicles in smart grid: A review on the vehicle to grid technologies and optimization techniques," *Renewable and Sustainable Energy Reviews,* vol. 53, pp. 720-732, 2016/01/01/ 2016.
18. [18] W. S. Tounsi Fokui, M. Saulo, and L. Ngoo, "Controlled electric vehicle charging for reverse power flow correction in the distribution network with high photovoltaic penetration: the case of an expanded IEEE 13 node test network," *Heliyon,* vol. 8, p. e09058, Mar 2022.
19. [19] F. G. Dias, D. Scoffield, M. Mohanpurkar, R. Hovsapian, and A. Medam, "Impact of controlled and uncontrolled charging of electric vehicles on a residential distribution grid," in *2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, 2018, pp. 1-5.
20. [20] C. B. Jones, M. Lave, W. Vining, and B. M. Garcia, "Uncontrolled Electric Vehicle Charging Impacts on Distribution Electric Power Systems with Primarily Residential, Commercial or Industrial Loads," *Energies,* vol. 14, p. 1688, 2021.
21. [21] Z. Muhammad, Z. Anwar, B. Saleem, and J. Shahid, "Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental Sustainability," *Energies,* vol. 16, p. 1113, 2023.
22. [22] SAE International, *SAE J3061-Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*: SAE International, 2016.
23. [23] M. Steger, M. Karner, J. Hillebrand, W. Rom, and K. Römer, "A security metric for structured security analysis of cyber-physical systems supporting SAE J3061," in *2016 2nd International Workshop on Modelling, Analysis, and Control of Complex CPS (CPS Data)*, 2016, pp. 1-6.
24. [24] M. Hataba, A. Sherif, M. Mahmoud, M. Abdallah, and W. Alasmary, "Security and Privacy Issues in Autonomous Vehicles: A Layer-Based Survey," *IEEE Open Journal of the Communications Society,* vol. 3, pp. 811-829, 2022.
25. [25] M. Bharathidasan, V. Indragandhi, V. Suresh, M. Jasiński, and Z. Leonowicz, "A review on electric vehicle: Technologies, energy trading, and cyber security," *Energy Reports,* vol. 8, pp. 9662-9685, 2022/11/01/ 2022.
26. [26] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defence," *Computers & Security,* vol. 103, p. 102150, 2021/04/01/ 2021.
27. [27] F. Sagstetter, M. Lukasiewycz, S. Steinhorst, M. Wolf, A. Bouard, W. R. Harris, *et al.*, "Security challenges in automotive hardware/software architecture design," in *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2013, pp. 458-463.
28. [28] M. Brandl, H. Gall, M. Wenger, V. Lorentz, M. Giegerich, F. Baronti, *et al.*, "Batteries and battery management systems for electric vehicles," in *2012 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2012, pp. 971-976.
29. [29] S. Acharya, Y. Dvorkin, and R. Karri, "Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?," *IEEE Transactions on Smart Grid,* vol. 11, pp. 5099-5113, 2020.
30. [30] B. Lundgren and N. Möller, "Defining Information Security," *Science and Engineering Ethics,* vol. 25, pp. 419-441, 2019/04/01 2019.
31. [31] A. Al Ghazo, "A framework for Cybersecurity of Supervisory Control and Data Acquisition (SCADA) Systems and Industrial Control Systems (ICS)," Iowa State University, 2020.
32. [32] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, "Cybersecurity in Power Grids: Challenges and Opportunities," *Sensors,* vol. 21, p. 6225, 2021.
33. [33] X. Sun, F. R. Yu, and P. Zhang, "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)," *IEEE Transactions on Intelligent Transportation Systems,* vol. 23, pp. 6240-6259, 2022.

10. Disclaimer/Publisher's Note:

The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s)



www.zemia.org