Who Controls Your Power Grid? On the Impact of Misdirected Distributed Energy Resources on Grid Stability

Niklas Goerke
goerke@fzi.de
FZI Research Center for Information Technology
Karlsruhe, Germany

Alexandra Märtz
alexandra.maertz@kit.edu
Chair of Energy Economics, Institute for Industrial Production, Karlsruhe Institute of Technology
Germany

Ingmar Baumgart
baumgart@fzi.de
FZI Research Center for Information Technology
Karlsruhe, Germany

ABSTRACT

The power grid is a critical infrastructure that is becoming increasingly indispensable due to rising electrification. Depending on their size, failures in the power grid are accompanied by considerable disruption to society. It is imperative to understand the vulnerabilities that exist within this intricate network, as attacks on the power grid have the potential to wreak havoc on a national and even global scale. With the growing trend of smart grid technologies, the attack surface has expanded, making it easier for malicious actors to compromise multiple entry points.

Therefore, quantifying the number of devices required for an attack is a critical aspect of grid security. This underlying paper underscores the importance of identifying vulnerabilities within the power grid's control systems, understanding potential attack vectors, and implementing robust security measures.

Our results reveal a concerning reality: malicious actors with a relatively limited degree of control over the technologies mentioned above have the ability to exert a profound influence o n t he balance of the power grid, especially with regard to the vital frequency containment reserve. By illuminating these potential points of influence, we aim to create a deeper understanding of the multi-layered threats that can compromise the resilience of our power grids.

KEYWORDS

power grid, stability, blackout, cyberattack, ENTSO-E, Electric Vehicle, Building Heat Pump, Battery Energy Storage System, Photovoltaic Inverter

1 INTRODUCTION

An uninterrupted and stable power supply is increasingly important in the context of the transformation of the energy system. However, due to the increase of renewable energy sources, electricity production cannot always follow demand; instead, demand must be steered to match the available supply to support the stability of the power grid. Multiple mechanisms exist that enable high-wattage devices in the household to automatically shift their energy demand to times of high supply, ideally without impacting convenience for the users. These mechanisms depend on communication infrastructure and correctly communicated data.

Research shows that misdirecting relevant devices can put additional stress on the power grid [24]. Attackers have in the past attacked power grids with the explicit goal of interrupting energy supply [7, 25]. Internet of Things (IoT) devices often show security flaws that have previously been exploited by attackers, e.g. to build the Mirai botnet consisting of up to 600,000 devices [3]. Employing high-wattage, always-connected devices such as Electric Vehicles (EVs), Building Heat Pumps (BHPs), Photovoltaic Inverter (PV-I) or Battery Energy Storage Systems (BESSs) to support grid stability thus also brings new risks to the system.

In the presented work, we address this topic by analyzing the effect on grid stability that cyberattacks on Distributed Energy Resource (DER) could have. The paper addresses the following research questions

- How many DERs must be misdirected in order to destabilize the power grid?
- How do these amounts compare to the predicted pervasion of DERs in the future?
- Which ways can an attacker use to gain the influence to perform this misdirection?

The results can be used to identify weak points and to improve the resiliency of energy system. They also highlight the increasing risk by the rise of digitization.

1.1 Motivation for Adversaries

There is a variety of reasons for attackers to target the power grid. We present two examples to show that these attacks are a relevant threat that needs to be addressed.

1.1.1 Terrorism. Attackers can attack the power grid with the explicit goal of causing damage to the grid itself and people, institutions and society that depend on it. Such an attack might be performed by terrorist actors or enemy countries as part of a (cyber-) war. In this case, it can be assumed that it is the attackers' goal to destabilize the power grid over a prolonged period or to cause long-term damage to prevent a quick recovery. Attacks of this kind have been performed against the Ukrainian power grid in 2015 and 2016 [7, 25].

1.1.2 Extortion and Blackmailing. Attackers with a financial motivation might see a lucrative target in the power grid. If they manage to gain control of (a part of) the power grid, they are able to demonstrate this power without causing long-term damage and without losing their control. Based on such a demonstration of power, e.g. a destabilization of a geographical region of the grid, they might then try to extort relevant actors such as companies or the government for ransom to not attack the power grid again. Extortion using digital assets is a common threat, especially in ransomware and distributed Denial-of-Service (DDos) attacks. Due to the availability of (semi-) anonymous cryptocurrencies that allow attackers to receive funds without giving up their location and identity, this kind of attack is also relevant to the power grid.

2 OUR CONTRIBUTION

In this work, we analyze the threat that high-wattage devices in the household pose to the power grid if they are under the control of an attacker. To do so, we use projections for the amount of Electric Vehicles (EVs), Building Heat Pumps (BHPs), Photovoltaic Inverters (PV-Is) and Battery Energy Storage Systems (BESSs) in 2030 and 2040 in Germany and show that attackers only need to control a small share of these devices to impact the power grid's stability. We describe the influences on each of these device types that an attacker could use to change their behavior.

3 RELATED WORK

One of the first works on IoT based attacks on the power grid was presented by Soltan et al. [24]. The authors identified a new class of attack called MadIoT (Manipulation of demand via IoT) and show the potential impact on the WSCC 9-bus simulated grid. Huang et al. [18] have performed a similar analysis on the North American power grid.

Kern et al. focused their work on EVs and how an attacker might be able to impact the power grid by applying different charging strategies [19]. They validated their results in a simulation on a local transmission system and the polish power grid. Similarly, Zhdanova et al. simulated a local power grid and show that in a typical European low voltage grid of 170 Households, a local blackout can be caused if only 68 EVs are miscontrolled [27].

In [1, 22], the authors present in detail the effect that synchronized start and stop of charging operations can have on the New York and Manhattan power grid. The authors of [12] show that an attacker with knowledge about the details of the power grid can perform even stronger attacks.

Multiple authors have presented attacks on end-user controlled devices. Baumgart et al. show that BESS contain fundamental security flaws, rendering them vulnerable to cyberattacks [5]. El Hussini et al. analyzed the attack vectors on EV charging stations and show how an attacker can use these to perform surge-in-demand and other attacks [13].

Multiple authors have previously presented work on the impact a coordinated attack can have on power grids. Krause et al. analyzed the communication infrastructure of power grids [20]. Based on this, the authors derived fundamental cyber security challenges of power grids and identified multiple attack scenarios that pose a potential security challenge to the power grid.

The authors of [26] reviewed existing studies on the impact of false data injection attacks on power systems from three aspects. In this context, a distinction is made between impairing economic planning through incorrect data injection, incorrect data for estimating the state of the electricity grid and how injection of incorrect data can affect the distributed control of distributed generators or microgrids and create an imbalance between supply and demand.

Dabrowski et al. developed attacks violating the grid maintaining conditions and investigated their impact on power grid operation [10]. In addition, the authors assessed their feasibility for today's adversaries.

Most of the works presented focus on one kind of DER (e.g. EVs), concern the U.S. or a simulated power grid or focus on how the DERs need to be miscontrolled to achieve the highest impact. This work closes a gap by considering all kinds of DERs and the amounts of each of them that an attacker would need to control to be able to impact the European Network of Transmission System Operators for Electricity (ENTSO-E) grid or a typical distribution grid.

4 IMPACTS ON THE POWER GRID

In the course of the energy transition, the power generation sector is undergoing fundamental changes. With the aim of reducing emissions and creating a secure and environmentally compatible energy supply for the future, the expansion of decentralized and renewable energy plants is being strongly promoted.

4.1 ENTSO-E Power System

The European Network of Transmission System Operators for Electricity (ENTSO-E) is the pan-European power grid connecting most European national grids. The connection implies that energy can and does flow in between them and that there is a uniform AC frequency of 50 Hz. The frequency closely follows any imbalance in power generation to consumption: if too little energy is provided to cover the demand, the frequency drops. Conversely, if too much energy is being provided, the frequency increases. Positive or negative deviations of max. 200 mHz are acceptable in ENTSO-E; any larger deviation activates emergency measures such as rolling blackouts. The Transmission System Operators (TSOs), who are responsible for system security, procure operational reserve that can be called up in the event of a deviation between generation and consumption, in order to balance the power supply.

In ENTSO-E, this operational reserve is organized in three tiers: frequency containment reserve (FCR), automatic frequency restoration reserve (aFRR) and manual Frequency Restoration Reserve (mFRR). In case the frequency deviates from the allowed range, usually in between 49.99 and 50.01 Hz, the FCR automatically activates positive or negative balancing power, proportional to the deviation, in order to stabilize the frequency back to the allowed range. The FCR is procured by the TSO and usually provided by batteries and other techniques that are extremely flexible and can react quickly. Any provider of FCR needs to be able to react automatically to frequency deviations and to ramp up to full power within 30 seconds. Currently, 3,000 MW of FCR are being provided that will ramp-up to full power in a range of 200 mHz around the nominal frequency [8].

The aFRR is activated to support the FCR in cases where the reserve is needed over a prolonged period. Whilst the FCR activates within seconds, the aFRR has a lead-time of up to 30 seconds until the first reaction and a ramp-up time of 5 minutes until the full balancing power needs to be provided. Due to the lead-time, the aFRR cannot be relied on for any surge or drop in demand or supply that happens within 30 seconds. The aFRR can be supported by the mFRR in cases where demand and supply deviate for even longer periods. The mFRR has an even longer lead-time of 5 minutes.

Any sudden surge or drop in load of more than 3,000 MW will result in frequency deviations of more than 200 mHz that cannot be compensated by the FCR. The effect, that frequency deviations have depends on the size of the deviation. The European Regulation defines, that load shedding should be performed if the frequency drops to 49 Hz [9].

Attackers can exploit the sensitive equilibrium between generation and consumption. Dabrowski et al. modeled that, depending on the current load in ENTSO-E, attackers who perform static or dynamic load attacks only need to control 4,500 MW to push the frequency below 49 Hz [10].

4.2 Low voltage distribution grid

Electrical energy is transmitted from power plants to different regions and then via distribution grids to local end customers. In Europe, low voltage distribution grids usually have a voltage of 400 V and are fed from the medium voltage grid using transformers with ratings of 250 kVA - 1000 kVA. The low voltage grid faces additional challenges due to the paradigm shift in the electricity system and the associated increasing penetration of DERs (Electric Vehicles (EVs), Building Heat Pumps (BHPs), Photovoltaic Inverters (PV-Is), Battery Energy Storage Systems (BESSs)) [27]. The consequences of overloading a transformer are strongly dependent on the duration of the overload. As described by Zhdanova et al. [27], an overload of a factor 1.5 of the nominal power for 90 minutes will not lead to a failure. However, a 2.8-fold overload of the nominal power can lead to a blackout in only 3 to 5 minutes. For further calculations, we assume a typical 400 kVA transformer that is commonly used to supply a number of 110 up to 230 households. We use a typical energy conversion efficiency factor of 0.9, which indicates the ratio between the nominal power and the net output of the transformer. We perform calculations for both 110 and 230 households to show results for the plausible range of households connected. The fuses of this transformer will typically trip at 1008 kW within a few minutes ($400\ kVA \times 2.8 \times 0.9 = 1008\ kW$). Transformers are commonly operated with a maximum work factor of 60 %, thus Distribution Grid Operators (DGOs) choose the transformer dimension in a way that it will have a maximum load of 60 % according to the expected power demand by the connected households. Analyzing the Standard Load Profile for German Households[1], we find that it is modeled that households never draw less than 18 % of their maximum demand. Thus a transformer that is planned to operate at a maximum of 60 % load should never operate below $60\% \times 18\% = 10.8\%$ of its maximum capacity. For the assumed 400 kVA transformer, we can thus assume that it always operates at a minimum of $400kVA \times 0.9 \times 10.8\% = 38.9kW$. An attacker would thus need to add another 969.1 kW in order to reach the critical load of 1008 kW.

5 CONTROLLING RELEVANT DEVICES

In this work, we consider four different types of DER: Electric Vehicles (EVs), BHPs, Photovoltaic Inverters (PV-Is) and Battery Energy Storage Systems (BESSs). This choice was made as these four have been prominently discussed in a German legislative procedure and are listed in the final version of the recently changed German §14a EnWG as controllable (power) consumption devices[2].

Installed in a typical household, they are interconnected with influential entities and receive direct commands or input data (e.g. energy prices) from them. These influential entities can be split into two groups: *central* and *local* entities:

Central entities are operated by a central operator and influence a large amount of DERs. This could be a cloud service that all BHPs made by one specific manufacturer are connected to.

Local entities are installed in the local household and influence only a very limited amount of DERs. This could be an Energy Management System (EMS) installed in a private household that influence only one BHP and one EV. DERs themselves are also considered local entities as they can (only) influence themselves.

Communication Channels are required to transport information from and to the devices.

The concrete list of influential entities is dependent on the type of DER, the manufacturer and the specific setup it is operated in. Different manufacturers implement different functionalities and not all customers activate all functions.

An overview of possible influences on the different DERs is given in table 1. The influence on EVs is shown in figure 1.

5.1 Attacking central entities

Central entities can influence a large amount of DERs. If an attacker manages to take control of them, they can influence the behavior of the depending DERs.

5.1.1 Distribution Grid Operators (DGOs). The distribution grid is fed via transformers with a maximum capacity that must not be overloaded (see section 4.2). It is thus for the DGOs to keep the balance of demand, supply and the maximum power each transformer can provide. In Germany, it is planned to enable DGO to be able to

[1] Bundesverband der Energie- und Wasserwirtschaft, https://www.bdew.de/energie/standardlastprofile-strom/

[2] German: "Steuerbare Verbrauchseinrichtungen", See §14a III EnWG.

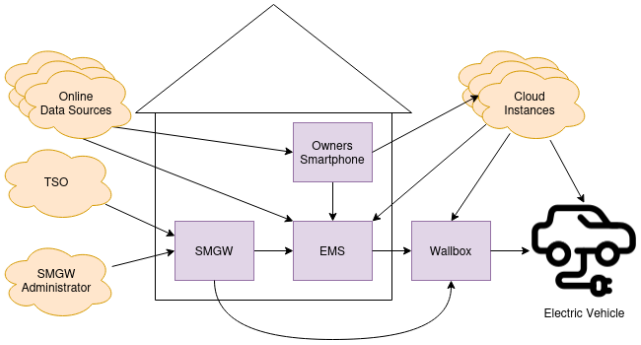

Figure 1: Influences on EVs. Central entities are displayed in orange cloud shaped style; local entities are displayed as purple rectangles.

Table 1: Influential entities on the different DERs.

	central / local	EVs	BHPs	PV-Is	BESSs
Distribution Grid Operator (DGO)	central	✓[wb]	✓	✓	✓
Cloud instances	central	✓[ii]	✓[ii]	✓[ii]	✓[ii]
SMGW Administrator	central	✓[ii]	✓[ii]	✓[ii]	✓[ii]
Online Data Sources	central	✓[ii]	✓[ii]	✓[ii]	✓[ii]
Device itself	local	✓	✓	✓	✓
EMS	local	✓[ii,wb]	✓[ii]	✓[ii]	✓[ii]
Owners Smartphone	local	✓[ii]	✓[ii]	✓[ii]	✓[ii]
Smart Meter Gateway (SMGW)[2]	local	✓[wb]	✓	✓	✓
Wallbox	local	✓	–	–	–
Communication Channels	both	✓	✓	✓	✓

[ii] if implemented. Most manufacturers provide this, but it is not strictly necessary for the DER to operate [wb] via the wallbox
[2] See Section 5.2.4 for details

use variable charges and surcharges on the energy prices and even be able to set consumption limits on DERs[3]. These measures are meant to incentivize consumers to shift their energy consumption towards times of high supply. Current and future energy prices as well as consumption limits are planned to be communicated from the DGO to the Smart Meter Gateway (SMGW) that will then forward them to the relevant devices in the household. An attacker who manages to take over the relevant systems at the DGO will thus be able to issue energy prices as well as set and lift consumption limits. Pervasive attacks against companies are common and even attacks against completely isolated systems have been recorded in the past [14].

5.1.2 Cloud instances. are often run by the manufacturer of a DER, EMS, wallbox or another local device. They are commonly used to provide information to the owner of the device and enable him or her to issue commands to it. To do so, the cloud service must be accessible from the internet. Attackers can thus also reach the cloud service and attack it. If they succeed in gaining control over relevant parts of the cloud service, they can act on its behalf and issue manipulated information to the user, to the connected DERs or other devices. They can also issue commands to those devices and thus make all connected devices simultaneously perform actions such as drawing energy from the power grid or stopping to supply energy to the grid.

5.1.3 SMGW Administrators. are a kind of cloud infrastructure set up specifically for administrating the SMGWs. They are specifically designed to perform administrative tasks such as changing the configuration or updating the firmware of connected SMGWs. A successful attack on a SMGW administrator could enable an attacker to misconfigure SMGWs.

5.1.4 Online Data Sources. can be used by DERs or other local devices to receive information relevant to them. This could be a weather service that helps an EMS predict the energy yield from photovoltaics or a similar public data source. A private data source could be the online-hosted calendar of the owner that gives an EMS information about the demand for a fully charged EV in the morning. Another example is the day-ahead energy price for the owner's energy-contract that an EMS might use to plan charging and discharging of an EV or BESS.

5.2 Attacking local entities

Local entities influence only a very limited amount of DERs. They are commonly installed in the owner's household and most of them are mass-produced devices that are installed in an identical configuration in a large number of households. An attacker can easily purchase one of these devices to analyze it and possibly find exploitable security vulnerabilities. If he or she manages to discover a security vulnerability that can be used to compromise one device, the same vulnerability can - in most cases - be used to compromise similar devices. Many devices are based on standard hard- and software components such as open-source software libraries. If a relevant vulnerability in one of those components is found, it may be exploitable on a multitude of different devices with a large number of instances each. It depends on the type of vulnerability found, if and how an attacker can use it to compromise large amounts of local entities. Successful attacks on large amounts of local IoT devices have been seen by the Mirai Botnet [3].

5.2.1 Distributed Energy Resources. DERs are also considered local entities, as attackers who compromise them can (only) influence their behavior. In most cases, they will be connected to the internet. In Germany, it is still unclear if this internet connection must go through the SMGW [15, Chapter 6]. Previous research on BESS has shown that DERs can be vulnerable similar to other IoT devices [5].

5.2.2 Energy Management Systems. Energy Management Systems (EMSs) are designed to supervise and control the energy consumption of the connected DERs in order to optimize consumption for parameters such as energy prices during the day. To do so, they are able to influence the behavior of the DERs. An attacker who is able to control an EMS can thus use it to manipulate the behavior of the connected devices such as EVs, wallboxes, BHPs and BESS.

[3] A recent change of §14a of the German Law (*Energiewirtschaftsgesetz (EnWG)*) allows a limit of 4.2 kW per DER to be set.

5.2.3 Owners Smartphone. Many DERs can be configured or controlled via a smartphone app. This implies that an attacker, who manages to completely or partly compromise a smartphone, can use this to exercise control over the connected DERs.

5.2.4 Smart Meter Gateways. are the central element to enable secure data transfer from smart energy meters and possibly DERs to central entities on the Internet in Germany. They are strictly standardized and must comply with a Common-Criteria Protection Profile designed by the German Federal Office for Information Security (BSI)[4]. In the future, SMGWs will be mandatory for all households in Germany. An attacker who is able to control an SMGW is in some cases able to manipulate the communicated information itself and can prevent communication of relevant devices to external parties. See section 5.3 for a discussion on attacks on communication channels.

5.2.5 Wallboxes. Wallboxes can directly limit the power an EV is able to draw. An attacker who is able to control a wallbox can thus influence the power a connected EV is able to draw.

5.3 Attacking communication channels

DERs depend on receiving instructions or information from other entities. Attacks on communication channels that are used to transport them, can be performed locally (e.g. in the household) thus affecting few DERs or close to central entities thus affecting large numbers of DERs. If an attacker is only able to read from the communication channel, he or she can learn the fact that communication is taking place or, if security mechanisms such as Transport Layer Security (TLS) are not used, learn the actual instructions or information communicated. More powerful Machine-in-the-Middle (MITM) attackers are additionally able to manipulate the contents of the communication if standard security mechanisms such as TLS are not applied. If the contents of the communication are protected, MITM attackers can still interrupt the communication thus preventing DERs from receiving the information they depend on. The affected DERs must then resort to pre-configured default behavior that might be identical for all DERs of a specific type, which an attacker could abuse to make all DERs behave identically.

6 CONTROLLING RELEVANT AMOUNTS OF DEVICES

In this section, we show the amount of DERs A_{DER} of each type an attacker needs to control to be able to impact the power grid as described in section 4. This is generally given by:

$$A_{DER} = \frac{P_{imp}}{P_{DER}} \tag{1}$$

With P_{imp} being the Power needed to impact the grid and P_{DER} the amount of Power a device is able to draw from the grid.

6.1 Electric Vehicles

As described in section 5, there are multiple ways an attacker can take to control the charging behavior of an EV. He or she must consider the time of day at which to perform an attack in regards to the amount of EVs being connected to the power grid. A study of 673 British EV users found that in 2017 and 2018 a maximum of 20 % of EVs are being charged simultaneously in the late afternoon / early evening on weekdays [11]. The attacker would thus need to gain control over 5 times the amount of EVs required to perform the attack.

Table 2: Distribution of charging power of private wallboxes

		2030	2040
Charging power	3.7 kW	10 %	0 %
	11 kW	60 %	65 %
	22 kW	30 %	35 %
Weighted average		13,6 kW	15 kW

6.1.1 Situation in Germany. There are multiple sources ([2, 17, 28]) that estimate the amount of EVs in Germany in 2030 and 2040. Based on them, we estimate that there will be 7 Mio. EVs in Germany by 2030 and 20 Mio. in 2040. Based on the same literature, we estimate that the power available at each private charging point in Germany is averaging at 13.6 kW in 2030 and 15 kW in 2040 as shown in table 2.

In order to impact the power grid as described in section 4, an attacker would need to control $P_{imp} = 4500MW$. Applying equation 1 for 2030, the attacker would need to control the charging operation of

$$\frac{4500MW}{13.6kW} \approx 331,000\ EVs \tag{2}$$

For 2040, due to the rise in charging power per charging port, this number would go down to $\approx 300,000$ EVs. In relation to the amount of EVs estimated for Germany for these years, the attacker would need to control the charging operation 4.7 % of all EVs in 2030 and 1.5 % in 2040. This numbers must be corrected to 23.6 % and 7.5 % respectively to compensate for the fact that (at least for 2017 and 2018) at most, 20 % of all EVs are being connected to the power grid simultaneously.

6.1.2 Situation in the distribution grid. The Federal Statistical Office of Germany predicts 42 Mio. households for 2030 and 42.1 Mio for 2040[5]. Using these numbers to scale down the amount of EVs to our model distribution grid (see section 4.2), we predict that in 2030 there will be in between 18 to 38 EVs per 400 kVA transformer, depending on the amount of households connected. These numbers grow to 52 to 109 in 2040, see table 3.

In order to impact the distribution grid as described in section 4.2, an attacker would need to control $P_{imp} = 969,1kW$. Applying equation 1 for 2030, the attacker would need to control the charging operation of

$$\frac{969,1kW}{13.6kW} \approx 71EVs \tag{3}$$

For 2030, this is more than the prediction for EVs connected to a transformer, even if 230 average households are being supplied. Due to the predicted rise in average private charging power, this number will go down to 65 EVs for 2040, which is in the range of

[4] BSI-CC-PP-0073

[5] The Federal Statistical Office of Germany presents two predictions for the amount of households for each year. We averaged them to 42 Mio for 2030 and 42,1 Mio for 2040, see https://www-genesis.destatis.de/genesis/online?sequenz=tabelleErgebnis&selectionname=12421-0100, accessed July 24, 2023

predicted EVs per 400 kVA transformer (see table 3). These numbers roughly match the results form [27], where the authors found that a local blackout could be caused by 68 EVs.

On the one hand, this numbers must be corrected to 356 EVs for 2030 (323 for 2040) to compensate for the fact that at most 20 % of all EVs are being charged simultaneously. This is more EVs than can be expected to be commonly supplied by a 400 kVA transformer, which would imply that there should be no risk for overloading the transformer. On the other hand, in lack of more detailed statistics, we scaled the amount of EVs per transformer by the amount of households, thus assuming average households per transformer. This method does not account for special situations, e.g. prosperous urban areas with more than average EVs per household.

6.2 Building Heat Pumps

BHPs must be chosen so that they are able to supply enough energy for the building on the coldest day of the year. Thus, for most days of the year, they are operating far below their maximum power, e.g. only providing warm water in summer. The heat pumps in single-family houses analyzed in [23] have a nominal electrical capacity of 1.9 or 3 kW and operate "almost constant around 180 W" in summer. This is also supported by a Fraunhofer Study [16] of single-family and small multi-family houses, which found a median electrical Energy demand of 1 $kWh/d \approx 130\ W$ of constant load per inhabited unit[6]. We thus conservatively estimate that BHPs have an average usage factor of 0.1 in summer.

6.2.1 Situation in Germany. Based on multiple sources of literature [4, 17, 28], we estimate the amount of BHPs for 2030 to 2 Mio. and for 2040 to 5 Mio. as a lower bound, with an average peak power of 6.5 kW. There thus is a minimum flexibility of $(1 - 0.1) * 6\ .5kW = 5.85kW$ per heat pump that an attacker can switch on if he or she is able to control it. In order to reach the required $P_{imp} = 4,500\ MW$, an attacker would thus need to control

$$\frac{4,500MW}{5.85kW} \approx 769,000\ heat\ pumps \tag{4}$$

This is equivalent to 38.5 % of the installed devices in 2030 and 15.4 % of the installed devices in 2040.

6.2.2 Situation in the distribution grid. Scaling these numbers to the typical 400 kVA transformer using the amount of households (analogous to section 6.1.2 on EVs), it is predicted that that in 2030 there will be in between 5 to 11 heat pumps per 400 kVA transformer, depending on the amount of households connected. These numbers grow to 13 to 27 in 2040, see table 3. In order to impact the distribution grid as described in section 4.2, an attacker would need to control $P_{imp} = 969,1kW$ which, using equation 1, transfers to 166 heat pumps.

For both 2030 and 2040, this is more than can be assumed to be connected to an *average* 400 kVA transformer. A risk might still arise in special situations, e.g. in prosperous newly built single-family-house urban areas where more than 166 houses equipped with heat pumps might be connected to a 400 kVA transformer.

[6]A constant load is a conservative estimate, in reality an attacker could pick a time of day with an even lower load.

6.3 Photovoltaic Inverters

Photovoltaic Inverters (PV-Is) used in on-the-roof installations in households currently have a median peak power of $8kWp$[7]. Attackers who are able to control a PV-I can reduce the power or switch it off completely thus cutting of the power supplied by it.

6.3.1 Situation in Germany. A recent study describes a realistic scenario for future photovoltaic installations [21]["Hauptszenario"]. The authors assume 116 GW of rooftop photovoltaic installations for 2030 and 188 GW for 2040[8]. This translates to 14.5 Mio. installations in 2030 and 23.5 Mio. installations in 2040.

In order to reach the required $P_{imp} = 4,500\ MW$, an attacker would need to control

$$\frac{4,500MW}{8kW} \approx 563,000\ PV - I \tag{5}$$

This is equivalent to 3.9 % of the installed devices in 2030 and 2.4 % of the installed devices in 2040.

6.3.2 Situation in the distribution grid. Scaling these numbers to our model distribution using the amount of households (analogous to section 6.1.2 on EVs), it is predicted that that in 2030 there will be in between 38 (for 110 households) to 79 (for 230 households) PV-I per 400 kVA transformer. These numbers grow to 61 to 128 in 2040, see table 3. In order to impact the distribution grid as described in section 4.2, an attacker would need to control $P_{imp} = 969,1\ kW$ which, using equation 1, transfers to 121 PV-I.

For 2030, this is more than can be assumed to be connected to an average 400 kVA transformer. For 2040, the numbers indicate that 128 PV-Is could be connected to a 400 kVA transformer in some cases, but it must be taken into account that if more households are connected to a transformer, they will most likely be in multifamily residential houses which have proportionally less roof area and thus proportionally less PV power installed. Thus, for both 2030 and 2040 it seems implausible, that enough PV-Is are connected to a transformer in a distribution grid to perform an attack like this.

6.4 Battery Energy Storage Systems

Attackers who are able to control the behavior of a BESS can not only start or stop charging it, but also start or stop discharging it into the power grid. Analyzing the German *Marktstammdatenregister* [6], we found that BESS have a median power of 4.6 kW[9]. Attackers could potentially switch BESS from discharging into the power grid at 4.6 kW to charging from the power grid at 4.6 kW, we thus model BESS at an average controllable power of 9.2 kW each.

6.4.1 Situation in Germany / ENTSO-E. In order to reach the required $P_{imp} = 4,500MW$, an attacker would thus need to control

$$\frac{4,500MW}{9.2kW} \approx 489,000\ BESS \tag{6}$$

[7]Data taken as of 15.02.2023 from https://www.marktstammdatenregister.de [6] a compulsory registry containing all PV-Is. We included all PV-I that are connected at household level and are labeled as "rooftop mounted, building, facade". As this is a long-tailed distribution with some unrealistically high values, (e.g. 144 MWp), we use the median.

[8]Data for rooftop installation is only given for 2030 and 2045, so the value for 2040 is an interpolation from the two

[9]We included all BESS that are connected at household level. As this is a long-tailed distribution with some unrealistically high values, (e.g. 295 MW BESS), we use the median. Data taken as of 15.02.2023 from https://www.marktstammdatenregister.de

Table 3: Overview of the amounts of DERs predicted for 2030 and 2040 in comparison to the amounts an attacker needs to control in order to impact the power grid and the proportion of those numbers. Given for Germany / ENTSO-E and a model distribution grid supplied by a 400 kVA transformer as described in section 4

		2030			2040		
		Germany	400 kVA transformer		Germany	400 kVA transformer	
			110 households	230 households		110 households	230 households
Critical Power[I]		4500 MW	969,1 kW	969,1 kW	4500 MW	969,1 kW	969,1 kW
EVs	Predicted amount	7 Mio.	18	38	20 Mio.	52	109
	Critical amount	331,000	71	71	300,000	65	65
	Proportion	4.7 % / 23.6 %[c]	389 % / 1943 %[c]	186 % / 929 %[c]	1.5 % / 7.5 %[c]	124 % / 618 % [c]	59 % / 296 %[c]
Heat pumps	Predicted amount	2 Mio.	5	11	5 Mio.	13	27
	Critical amount	769,000	166	166	769,000	166	166
	Proportion	38.5 %	3163 %	1513 %	15.4 %	1268 %	606 %
PV-I	Predicted amount	14.5 Mio.	38	79	23.5 Mio.	61	128
	Critical amount	563,000	121	121	563,000	121	121
	Proportion	3.9 %	319 %	153 %	2.4 %	197 %	94 %
BESS	Predicted amount	2.9 Mio.	8	16	4.8 Mio.	13	26
	Critical amount	489,000	105	105	489,000	105	105
	Proportion	16.6 %	1387 %	663 %	10.2 %	840 %	402 %

[I] The Power an attacker needs to control in order to be able to impact the power grid at the described level. See section 4 for details.
[c] EVs can only be charged when connected to the power grid. At most, 20 % are being connected at once. See section 6.1 for details

Currently, there are 433,734 BESS and 2,135,712 photovoltaic power systems installed at household level on the roof in Germany [6], thus about 20 % of all photovoltaic power systems are equipped with a BESS. Taking the amount of PV-Is as described in 6.3, and assuming that this quota will stay the same for 2030 and 2040, we can estimate 2,900,000 and 4,800,000 BESSs 2030 and 2040, respectively. Thus, an attacker would need to control 16.9 % of the installed devices in 2030 and 10.2 % of the installed devices in 2040.

6.4.2 Situation in the distribution grid. Scaling these numbers to our model distribution grid using the amount of households (analogous to section 6.1.2 on EVs), it is predicted that that in 2030 there will be in between 8 to 16 BESS per 400 kVA transformer, depending on the amount of households connected. These numbers grow to 13 to 26 in 2040, see table 3. In order to impact the distribution grid as described in section 4.2, an attacker would need to control $P_{imp} = 969,1\ kW$ which, using equation 1, transfers to 105 BESS.

For both 2030 and 2040, this is more than can be assumed to be connected to an average 400 kVA transformer. A risk might still arise in special situations, e.g. in prosperous newly built single-family-house urban areas where more than 105 houses equipped with BESS might be connected to a 400 kVA transformer.

7 DISCUSSION

Our calculations show, that in order to impact the stability of ENTSO-E a far lower share of DERs needs to be miscontrolled than to impact the distribution grid. Taking the example of EVs, an attacker only needs to control the behavior of $\approx 331,000\ EVs$ to impact the stability of ENTSO-E.

According to the Federal Motor Transport Authority in Germany[10], in January 2023, there were 23 manufacturers with more than 331,000 vehicles currently registered in Germany.

There were over 10 Mio. vehicles registered that were manufactured by Volkswagen without its subsidiaries. It is thus plausible, that also with rising amounts of EVs some manufacturers will dominate in such a way that an attacker who is able to perform a successful attack on the cloud infrastructure of one of these manufacturers might be able to influence enough vehicles to impact grid stability. This implies that, depending on the architecture used in the cloud, the EV manufacturer cloud systems could be considered a single point of failure to the power grid. As described in section 6.1, a study of EV usage in Britain in 2017 and 2018 found, that at most, 20 % of all EVs are connected to the power grid at the same time. This must be taken into account and the amount of EVs an attacker needs to control should be corrected to 1,654,000. On the other hand, it must be considered that EVs are a rather new technology and user behavior might change in the future. For example to be able to use the benefits of bidirectional charging, EVs must be connected to the power grid more often and for longer periods. Attackers might thus need to control fewer EVs in the future than can be predicted based on today's studies.

Based on our calculations (see table 3), using DERs to overload distribution grid transformers is an implausible attack vector. It must be taken into account though, that due to the rather small amount of available data on the situation and load in the distribution grid, we based our calculations on defensive assumptions. There are multiple options for attackers to tip the odds in their favor, e.g. they could choose a time of higher transformer base load to perform their attack.

[10] Statistics taken from https://www.kba.de/DE/Statistik/Fahrzeuge/Bestand/Jahrebilanz_Bestand/fz_b_jahresbilanz_node.html, accessed July 24, 2023

8 CONCLUSION AND FUTURE WORK

Based on projections from existing literature in the context of Germany, we quantify the amount of DER an attacker needs to influence in order to be able to impact the power grid stability in scenarios for the years 2030 and 2040. Our in-depth analysis shows that an attacker needs to control, for example only 3.9 % of all PV-I in 2030 in order to be able to impact the stability of the European ENTSO-E power grid. This influence can be achieved in multiple ways, either by attacking the devices directly, by attacking local entities (such as wallboxes, or EMS) or central entities (e.g. manufacturer cloud systems).

To support the validity and relevance of our findings, we present realistic attacker models that show why attackers might be interested in performing attacks on the power grid. Based on the numbers derived, we discuss that the proportion of devices an attacker needs to misguide to impact the grid stability in ENTSO-E is relatively small. Our analysis highlights multiple single points of failure that can be exploited by an attacker to destabilize the grid on this level. Calculations for an exemplary 400 kVA transformer show that the danger for the grid on distribution level is significantly lower.

The key point of our research underscores the urgency to strengthen security measures and develop comprehensive safeguards for these household devices, as well as the central role that proactive cybersecurity strategies and management play in ensuring the essential stability of power grids.

In the future, the research presented could be extended to different power grid levels, such as bigger cities. In addition, the calculations shown need to be updated regularly to stay in line with the most recent data and newer predictions on the amount of DER. Our findings for the distribution grid could are based on conservative estimates that could be refined by performing in-depth measurements of exemplary neighborhoods with high DER pervasion. Further research is also required on measures that can be employed to systematically prevent central entities such as manufacturer cloud services from becoming single points of failure to the power grid.

ACKNOWLEDGMENTS

This work has been partly funded by the German Federal Ministry for Economic Affairs a nd C limate A ction i n P roject SynergieQuartier Walldorf.

REFERENCES

[1] Samrat Acharya, Yury Dvorkin, and Ramesh Karri. 2020. Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable? *IEEE Transactions on Smart Grid* 11, 6 (Nov. 2020), 5099–5113. https://doi.org/10.1109/TSG.2020.2994177

[2] Regulatory Assistance Project (RAP) Agora Verkehrswende, Agora Energiewende. 2019. *Verteilnetzausbau für die Energiewende - Elektromobilität im Fokus.* Technical Report. Agora Verkehrswende, Agora Energiewende, Regulatory Assistance Project (RAP).

[3] 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. 2017. Understanding the Mirai Botnet. In *26th USENIX Security Symposium (USENIX Security 17).* USENIX Association, Vancouver, BC, 1093–1110. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[4] Karl-Heinz Backhaus, Hendrik Ehrhardt, André Jacob, Barara Kaiser, Lars Petereit, Björn Schreinermacher, Alexander Sperr, Egbert Tippelt, and Volker Weinmann. 2020. *Branchenstudie 2021: Marktanalyse - Szenarien - Handlungsempfehlungen.* Technical Report. Bundesverband Wärmepumpe (BWP) e. V.

[5] Ingmar Baumgart, Matthias Borsig, Niklas Goerke, Timon Hackenjos, Jochen Rill, and Marek Wehmer. 2019. Who Controls Your Energy? On the (In)Security of Residential Battery Energy Storage Systems. In *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm).* IEEE, Beijing, China, 1–6. https://doi.org/10.1109/SmartGridComm.2019.8909749

[6] Bundesnetzagentur. [n. d.]. *Marktstammdatenregister.* Bundesnetzagentur. https://www.marktstammdatenregister.de

[7] CISA. 2016. *ICS Alert Cyber-Attack Against Ukrainian Critical Infrastructure.* Technical Report IR-ALERT-H-16-056-01. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01

[8] The European Commission. 2017. establishing a guideline on electricity transmission system operation. https://eur-lex.europa.eu/eli/reg/2017/1485/oj

[9] The European Commission. 2017. establishing a network code on electricity emergency and restoration. https://eur-lex.europa.eu/eli/reg/2017/2196/oj

[10] Adrian Dabrowski, Johanna Ullrich, and Edgar R. Weippl. 2017. Grid Shock: Coordinated Load-Changing Attacks on Power Grids: The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well. In *Proceedings of the 33rd Annual Computer Security Applications Conference* (Orlando, FL, USA) *(ACSAC '17).* Association for Computing Machinery, New York, NY, USA, 303–314. https://doi.org/10.1145/3134600.3134639

[11] Western Power Distribution. 2019. *Summary of the findings of the Electric Nation smart charging trial.* Technical Report. Distribution, Western Power. https://electricnation.org.uk/2019/07/17/electric-nation-smart-charged-conference-review/

[12] Yury Dvorkin and Siddharth Garg. 2017. IoT-enabled distributed cyber-attacks on transmission and distribution grids. In *2017 North American Power Symposium (NAPS).* IEEE, Morgantown, WV, 1–6. https://doi.org/10.1109/NAPS.2017.8107363

[13] Hossam ElHussini, Chadi Assi, Bassam Moussa, Ribal Atallah, and Ali Ghrayeb. 2021. A Tale of Two Entities: Contextualizing the Security of Electric Vehicle Charging Stations on the Power Grid. *ACM Transactions on Internet of Things* 2, 2 (May 2021), 1–21. https://doi.org/10.1145/3437258

[14] Nicolas Falliere, Liam O Murchu, and Eric Chien. 2011. W32. stuxnet dossier. *White paper, symantec corp., security response* 5, 6 (2011), 29.

[15] Bundesamt für Sicherheit in der Informationstechnik (BSI). 2022. *Technische Eckpunkte für die Weiterentwicklung der Standards für die Digitalisierung der Energiewende.* Technical Report. Bundesamt für Sicherheit in der Informationstechnik (BSI). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/technische_eckpunkte.pdf

[16] Danny Günther, Jeannette Wapler, Robert Langner, Sebastian Helmling, Marek Miara, David Fischer, Dirk Zimmermann, Tobias Wolf, and Bernhard Wille-Hausmann. 2020. *Wärmepumpen in Bestandsgebäuden.* Technical Report. Fraunhofer ISE., Freiburg. https://www.ise.fraunhofer.de/de/forschungsprojekte/wpsmart-im-bestand.html

[17] Deutsche Energie-Agentur GmbH (Hrsg.). 2021. *dena-Leitstudie Aufbruch Klimaneutralität.* Technical Report. Deutsche Energie-Agentur GmbH (Hrsg.).

[18] Bing Huang, Alvaro A. Cardenas, and Ross Baldick. 2019. Not Everything is Dark and Gloomy: Power Grid Protections Against IoT Demand Attacks. In *28th USENIX Security Symposium (USENIX Security 19).* USENIX Association, Santa Clara, CA, 1115–1132. https://www.usenix.org/conference/usenixsecurity19/presentation/huang

[19] Dustin Kern and Christoph Krauß. 2021. Analysis of E-Mobility-based Threats to Power Grid Resilience. In *Computer Science in Cars Symposium.* ACM, Ingolstadt Germany, 1–12. https://doi.org/10.1145/3488904.3493385

[20] Tim Krause, Raphael Ernst, Benedikt Klaer, Immanuel Hacker, and Martin Henze. 2021. Cybersecurity in power grids: Challenges and opportunities. *Sensors* 21, 18 (2021), 6225.

[21] Mario Ragwitz, Anke Weidlich, Dirk Biermann, Julian Brandes, Tom Brown, Célia Burghardt, Elisabeth Dütschke, Berit Erlach, Manfred Fischedick, Sabine Fuss, Oliver Geden, Jörn Gierds, Ulrike Herrmann, Patrick Jochem, Christoph Kost, Gunnar Luderer, Karsten Neuhoff, Mirko Schäfer, Kurt Wagemann, Frauke Wiese, Jenny Winkler, Bastian Zachmann, and Lin Zheng. 2023. *Szenarien für ein klimaneutrales Deutschland. Technologieumbau, Verbrauchsreduktion und Kohlenstoffmanagement.* Technical Report. acatech - Deutsche Akademie der Technikwissenschaften. 224 pages. https://doi.org/10.48669/ESYS_2023-3

[22] Mohammad Ali Sayed, Ribal Atallah, Chadi Assi, and Mourad Debbabi. 2022. Electric vehicle attack impact on power grid operation. *International Journal of Electrical Power & Energy Systems* 137 (May 2022), 107784. https://doi.org/10.1016/j.ijepes.2021.107784

[23] Marlon Schlemminger, Tobias Ohrdes, Elisabeth Schneider, and Michael Knoop. 2022. Dataset on electrical single-family house and heat pump load profiles in Germany. *Scientific Data* 9, 1 (Feb. 2022), 56. https://doi.org/10.1038/s41597-022-01156-1

[24] Saleh Soltan, Prateek Mittal, and H. Vincent Poor. 2018. BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. In *27th USENIX Security Symposium (USENIX Security 18).* USENIX Association, Baltimore, MD, 15–32. https://www.usenix.org/conference/usenixsecurity18/presentation/soltan

[25] Julia E. Sullivan and Dmitriy Kamensky. 2017. How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *The Electricity Journal* 30, 3 (April 2017), 30–35. https://doi.org/10.1016/j.tej.2017.02.006

[26] Yan Xu. 2020. A review of cyber security risks of power systems: from static to dynamic false data attacks. *Protection and Control of Modern Power Systems* 5, 1 (2020), 19.

[27] Maria Zhdanova, Julian Urbansky, Anne Hagemeier, Daniel Zelle, Isabelle Hermann, and Dorian Höffner. 2022. Local Power Grids at Risk – An Experimental and Simulation-based Analysis of Attacks on Vehicle-To-Grid Communication. In *Proceedings of the 38th Annual Computer Security Applications Conference*. ACM, Austin TX USA, 42–55. https://doi.org/10.1145/3564625.3568136

[28] Übertragungsnetzbetreiber. 2022. *Netzentwicklungsplan 2035*. Technical Report.