Assessing the Cyber Threat Landscape for Virtual Power Plants

ARTICLE HISTORY

Received 10 March 2022
Accepted 02 May 2022

George Gkoktsis
Cyber-Physical Systems Security
Fraunhofer SIT
Darmstadt, Germany
george.gkoktsis@sit.fraunhofer.de

"Assessing the Cyber Threat Landscape for Virtual Power Plants",
Latin-American Journal of Computing (LAJC), vol. 9, no. 2, 2022.
G. Gkoktsis,

Assessing the Cyber Threat Landscape for Virtual Power Plants

George Gkoktsis
Cyber-Physical Systems Security
Fraunhofer SIT
Darmstadt – Germany
george.gkoktsisgvidal@sit.fraunhofer.de

Abstract— Virtual Power Plants (VPPs) aggregate and coordinate Distributed Energy Resources (DER) as a single entity aiding in the decarbonization of the energy generation mix. The infrastructure of VPPs relies heavily on the rigorous and accurate exchange of information between the DER and the VPP, as well as other grid entities. This exposes them to possible cyber threats that impede their functions and can have negative impacts on the stability and reliability of the grid. This paper evaluates the threat landscape against threats that affect VPPs. A heuristic method of assessing the impact and likelihood of attacks is constructed based on a) proposed methods in the literature, b) standardization bodies, and c) in relation to a VPPs security profile. Our findings indicate that False Data Injection attacks pose the greatest risk, competing with disruption of their functions due to Denial of Service.

Keywords— *Virtual Power Plants, Cyber-Physical Security, Smart Grid Security*

I. INTRODUCTION

Renewable generation is promoted as decarbonization plans are followed through all over the globe in an effort to reduce CO2 emissions. Renewables are constructed where their potential is harnessed, for example, wind generators are installed on mountaintops or offshore. They are referred to as Distributed Energy Resources (DER). Energy dispatch scheduling is performed based on load curve forecasts. Periodically, daily, monthly etc., the expected consumption is calculated, and generation is scheduled accordingly to satisfy the load. DER have small generation capacity in general, 2-3 orders of magnitude smaller than fuel-based generators and are numerous. Thus, including them in dispatch scheduling individually is mostly inefficient. Their very fast connection to the grid capability, however, enables them to participate in demand response, i.e., the dynamic grid generation and load management. Due to these reasons, Virtual Power Plants (VPPs) are created to aggregate DER generation, optimize control, and interact with the market in a coordinated and profitable manner.

There are many definitions in the literature about VPPs. This paper defines a VPP as: "A portfolio of DERs, which are connected by a control system based on information and communication technology (ICT). The VPP acts as a single visible entity in the power system, is always grid-tied and can be either static or dynamic" [1]. In the Smart Grid Architecture Model [2]Integrity and Availability, VPPs are loosely described as "aggregation of DER". However, they have the potential to substantial aggregate amounts of generation capacity, reaching GW of output, and thus comparable to Steam units so they can be considered critical infrastructure.

In the absence of standardized architectures, implementations of VPPs are based on the vision of individual organizations, where software solutions are used to control and dispatch DER. The "control system" aspect of the definition is usually an amalgamation of interoperable firmware and proprietary software capable of interfacing the VPP management platform and responding to market signals. Moreover, due to the topological distribution of participating generation, it is hard, if not impossible, for critical communication channels to avoid being implemented over the wider internet.

Energy systems are engineered to provide safe, reliable, and robust energy generation and delivery. Cyber threats against them can cause instabilities, which can lead to instigation of cascading failure events [3], [4]. Attackers may exploit weaknesses in the architecture to cause blackouts [5] or invalidate safety equipment [6].

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762928

An additional difficulty in VPP cybersecurity is the plurality of stakeholders participating in the structure. The VPP operator may not be the owner of the DER but act only as a mediator between generating entities and the energy market. DER are electrically connected to Distribution System Operator's (DSO) infrastructure. Jurisdiction and liability for security policy creation and enforcement are not trivial in an environment rich with cyber-physical dependencies between different legal entities. The dependence on third-party assurances in the form of trustworthy software and hardware complicates further the situation. For example, a smart inverter operating on third party software can be attacked [7]converting electric power and energy into several forms and magnitudes. Power electronics also facilitate the control of distributed generation and storage assets. Inverters are prominent power electronics found in many customer premises because of their pertinence in converting electricity from DC to AC. Smart inverters go beyond basic conversion and have the potential to support the utility system. The additional grid support function creates some cyber security vulnerabilities, especially when the grid relies on inverter-dependent DER in high proliferation areas. In California., the Smart Inverter Working Group (SIWG by exploiting a design flaw in the software. Changing the settings will affect the power output of the DER, possibly creating system instability in the process. This affects both the VPP, as well as the general grid. It may be challenging to determine who bears responsibility for securing the infrastructure and who is liable for the damages.

Assessing the threat landscape for VPPs is of vital importance for most of their cyber security activities. For security management, it enables accurate estimation of risk [8]. It assists threat modelling in identifying the threat actors that need to be tracked, as a result augmenting detection of their activities. Then, response and remediation plans and playbooks can be designed and implemented, supporting cyber resilience. The field is relatively immature, and, in our opinion, it is important to take the physical system into consideration while performing this exercise.

To avoid the aforementioned complications and in an effort to preserve the generality principle, in this paper, a VPP is abstracted to three functions that must be fulfilled, as per the accepted definition, and the threat landscape is assessed against any adversarial effort to invalidate these functions. They are:

1. Interaction with the energy market and demand response,
2. Supervision and control of participating DER,
3. Safe operation of DER.

This paper aims to contribute in the following ways: i) illuminate the unique security threats and requirements of VPPs, and ii) propose a heuristic impact and likelihood evaluation method within the scope and definitions of VPPs.

II. RELATED WORK

In this section, an overview of relevant research to smart grid threat landscape and VPP security is presented. First, the threat landscape itself is presented and then research specific to VPP cybersecurity.

In [9], the European Union Agency for Cybersecurity (ENISA) presents the cyber threats related to the smart grid while taking into consideration possible physical attacks that may be relevant. The necessity for developing threat intelligence in the form of attack scenarios is showcased, as well as the gap in the criticality assessment of smart grid assets and processes. Considering the rapidly evolving threat environment for critical infrastructures, it would be considered outdated.

The National Electric Sector Cybersecurity Organization Resource (NESCOR) described a plethora of attack scenarios against the smart grid in [10], [11], organized into 6 categories. Two of those are closely relevant to VPPs, namely DER and Wide Area Monitoring, Protection and Control (WAMPAC). Amongst others, a threat model and 16 threat impact evaluation criteria are being presented to facilitate a risk representation of scenarios tailor-made for the smart grid. In order to generate threat intelligence, these scenarios need to be tested, and use cases constructed, as attempted in various research efforts, like [12]–[14]. To our knowledge, no use case was constructed for VPP structures.

Within the CYBER-TRUST project [15], a threat landscape for Trusted Internet of Things was constructed, with a section devoted solely to threats against the smart grid. The alleviating effect of our state-of-the-art security practices, like the presence of firewalls, IPS, anti-malware, the existence of security policies etc., is then estimated. However, according to their analysis, these countermeasures have little to no effect on mitigating the smart grid-specific threats. Considering the characteristics of VPPs, this problem is further exacerbated by the fact that critical communications can be utilized in home-area networks, wired or wireless, which are intrinsically unsafe.

In [16], Sandia National presents a design and evaluation of secure VPPs. While taking into consideration all aforementioned hurdles, the viability of signal correlations for Intrusion Detection Systems is showcased, and a network segmentation strategy, which is performed with topological-operational considerations, is suggested. Attacks are simulated in PowerWorld, and the system's response is then correlated with attack-free conditions. The attack scenarios themselves involve malicious disconnections of VPP elements and malicious generation manipulation, like ramping up/down active/reactive power output of DER. For our paradigm, these scenarios only address the third function of a VPP, the safe operation of DER. Their adversarial model assumes one action of the attacker, which is also a limiting factor. Additionally, it is unclear whether the effects can be uniquely caused by adversarial activity or due to faulty operation.

Hussain et al. [17] explain the adoption of the IEC 62351 standard for IEC 61850 communication channels. Its relevance to VPPs lies in the analysis of routable IEC 61850 protocols for DER coordination, like IEC 60870-104 and derivatives, R-GOOSE and R-SV, and MMS. Even though IEC 62351 is an improvement of the inherent weaknesses of R-GOOSE and R-SV, Quality of Service requirements limits the applicable integrity and source authentication mechanisms to the use of HMACs, without consideration of confidentiality. However, when routed over untrusted networks, confidentiality becomes a requirement, as the messages may contain sensitive information, such as the financial information of the DER. Furthermore, authentication of DER equipment has embedded certificates for Digital Signature schemes, which are hard coded in the Intelligent Electrical Devices (IEDs) and lack the ability to be revoked when compromised.

III. THREAT EVALUATION CRITERIA

This section presents the methodology employed for threat assessment. Each threat was examined towards its relevance to the security profile of a VPP. A qualitative assessment of the impact by adapting the NESCOR impact evaluation scales, was performed. Similarly, the likelihood assessment adapted the relevant scales while taking into consideration published literature and vulnerability databases. The scoring of each criterion is also influenced by CEN-CELEC-ETSI and NIST recommendations.

A. VPP CYBERSECURITY PROFILE

The US National Institute of Standards and Technology (NIST), in their Technical Note 2051 [18], introduces the cybersecurity profile for the Smart Grid. It assists with cybersecurity management of organizations participating in the energy infrastructure with heavy penetration of DER and consists of five high-level security categories, namely: Identify, Protect, Detect, Respond, Recover. These consist of 108 subcategories such as Asset Management, Risk Assessment, Identity Management, Access Control etc. Together they form the Core of a Cybersecurity profile. Business objectives, cybersecurity requirements and the technical environment is given as an input to the profile, and operating methodologies are the output.

In order to form a basis for the threat assessment for VPPs, a high-level security profile for them was created. It was used as a tool to examine the relevance of a particular threat to the high-level security objectives of VPPs. Fig. 1 shows a diagram of the process used to create the VPP profile. In Step 1, the operational functions of the VPP are defined as business mission objectives. Thus, sets of the core functions are created for every objective.

Eventhough the maintenance of safety, reliability, resilience, and support for grid modernization is described as business objectives in the Technical Note, we opted to input them to the profile as requirements, as there are legal requirements for their maintenance when part of the critical infrastructure. This is given as input to the core of the profile in Step 2. At the end of Step 2, for every mission objective, the security requirements are deduced.

Step 3 is the threat modelling part of the process. Here, the threat landscape is mapped to each business objective and classified per security requirement. Security gaps, like protocol weaknesses, or possible legacy equipment, are also taken into consideration as system vulnerabilities and are mapped alongside the known threats. For example, an adversary attempting to alter the power setpoint of a DER threatens the reliability requirement of the secure DER operation objective. The threat is examined on how the threat should be identified, responded to, and mitigated. Failure to do so produces the impacts that are then evaluated by the assessment criteria.

The output of the profile is the mitigations of each threat based on the aforementioned analysis. These can be either technical controls or policies, depending on the function that is invalidated. In the above example, source authentication and access management policy creation are possible countermeasures. In this paper, however, this part is omitted, as a resilient response to attacks and disturbances for VPPs is a future goal of our research.

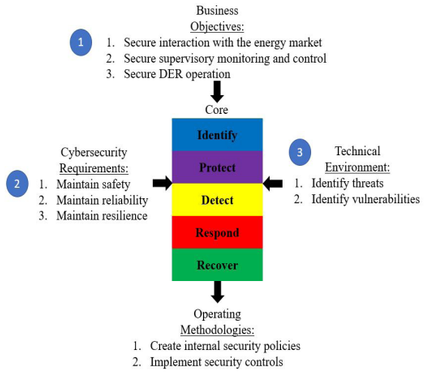

Fig. 1 Security Profile of a VPP creation process

B. IMPACT ASSESSMENT CRITERIA

To estimate the effects of successful attacks, we adapted and scaled the NESCOR impact criteria [10] to fit the VPP paradigm, summarized in Table I.

The final impact score of an attack was calculated as the mean average of the score of each criterion. A more precise approach would be to calculate a weighted average of the scores, as they scale at different rates, and their relative value is difficult to quantify. Specifically, the safety ranking and the ecological concerns (which are omitted in this analysis, as VPPs are mostly comprised of DER and generation is assumed to not involve chemical, radioactive, or kinetic processes), are problematic as in this evaluation, the loss of human life is of equal importance as the instigation of system instabilities. The exercise of accurately quantifying them, however, is out of scope of this research.

To mitigate this imbalance, two additional rules were used. If a threat is scored 9 at the safety criterion, it is automatically considered critical, regardless of other scores. If a threat scores 9 in at least two other categories, it is considered critical.

TABLE I. Impact Assessment Criteria

Criterion	Scoring	
	Minimum Score	Maximum Score
System scale	0: single DER affected	9: All DER affected
Safety	0: none	9: 1 possible death
Financial Impact on VPP	0: petty cash	9: >5% of revenue
Negative impact on generation capacity	0: none	9: >10% for more than 8 hours
Negative impact on the energy market	0: None	9: Loss of market participation
Negative impact on transmission system	0: None	9: Instigation of instabilities
Negative impact on billing functions	0: None	9: widespread loss of accurate power usage data
Privacy Loss	0: None	9: All stakeholder private data leaked

C. LIKELIHOOD ASSESSMENT CRITERIA

Keeping consistency with the impact assessment criteria, the likelihood assessment criteria are adapted and scaled NESCOR criteria to VPPs. Table II summarizes them.

TABLE II. Likelihood Assessment Criteria

Criterion	Scoring	
	Minimum Score	Maximum Score
Skill required	0: Deep domain knowledge and ability to create custom attacking tools	9: Basic domain understanding and computer skills
Accessibility	0: Air-gapped, solid access controls	9: Internet facing, no access controls
Attack Vector	0: Theoretical	9: Multiple widely exploited techniques
CVE	0: None known	9: Known, commonly used CVEs in unsupported and/or legacy assets

By combining the impact and likelihood criteria and by cross-examination with the security profile for relevance, a high-level risk representation of threats was performed. The next section describes our preliminary findings.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762928

IV. CRITICAL THREATS AGAINST VPPS

In this section, our findings of VPP threats will be presented, after examining the threat landscape. The context of each threat is first examined, a risk representation is then presented, alongside with possible attack vectors that can manifest the threat and, finally an example scenario is described.

A. OBSTRUCTION OF INTERACTIONS BETWEEN THE VPP AND THE ENERGY MARKET

The physical electricity grid consists of various parts with distinct roles. Generation is where electrical energy is transformed from other energy sources; transmission is the part of the system that transfers the energy from one point to another, distribution is the part of the system responsible for distributing the energy to the consumers and, finally, consumption is the part where electrical energy is converted to other forms of energy. Depending on their generation capacity, DER is usually physically connected to the distribution part of the grid.

The energy market then consists of the producers, who generate electrical energy and sell it to the consumers, the Transmission System Operators (TSOs), who are responsible for the grid's stable and reliable transfer of energy over long distances, the Distribution System Operators (DSOs), who are paid to deliver the energy to the consumers, and the regulating authorities, who monitor and regulate the market.

Even though a VPP can participate in the retail market, there is little adversarial activity to jeopardize it, and we deem it out of the scope of our study. We focus on the VPPs participation in the wholesale market, which consists of the following parts:

- The forward market, where contracts can be weeks or years in the future,
- The day-ahead market,
- The intraday market, or spot market,
- The ancillary services market, which offers demand response and compensation services.

Considering the operation of a VPP within the energy market, their role is crucial for coordinating DER generation and dispatch. As aggregators of multiple DER, they participate in the day-ahead, intraday, and ancillary services markets. Since the cost of production is minimal to zero, due to the renewable nature of most of the aggregated DER, and in combination with the prioritization of renewable generation in scheduling, the ability of the VPP to securely interact with the energy exchange, as well as direct market sellers, by nature of bilateral contracts, is mission critical for the economic stability and profitability of the VPP.

From the entirety of the grid point of view, VPPs can and do exceed 1000MW of generation capacity. This makes them comparable to thermoelectric and nuclear power plants. Unlike those power plants, the economic strategies of VPPs are based on accurate weather forecasting and optimal dispatch scheduling. Interruption of these information flows can deprive the system of gigawatts of power, and since DER interact with load curve calculations by "shaving" the load curve, manifest unexpected load peaks that can congest the transmission system or create system instabilities.

There are two possible ways that an adversary can threaten this VPP mission objective. Firstly, interruption of communication is possible in cases where custom software is being used to facilitate this interaction. This interface is usually provided to the VPP operator as Software-as-a-Service, which would then classify these software solutions as part of the supply chain for the VPP. Standard Denial-of-Service techniques, such as flooding and Distributed Denial of Service (DDoS) against the software provider or the VPP can induce delays and interruptions that can impact the ability of the VPP to offer ancillary services, as well as interacting with intraday markets. Secondly, data tampering vectors can prove just as devastating, as the VPP operator is deprived of their ability to make correct decisions. These can take the form of falsified load forecasts, system state estimation, grid measurements, market pricing forecasts etc.

Table III and Table IV summarize the impact and likelihood assessment of the threat as follows:

TABLE III. Impact Assessment of Market Interruption Threat

Criterion	Assessment	
	Score	Comments
System scale	9	A Shutdown of the market interface affects the operation of the entirety of the VPP, so every DER is affected.
Safety	0	No expected physical impacts that create hazardous conditions are expected.
Financial Impact on VPP	1	Assuming that the VPP partakes in the day ahead, ancillary market and spot market, the attack can disrupt the operation of the VPP for up to a few days. This will represent less than 1% of yearly revenue.
Negative impact on generation capacity	0	Generation functions are not impeded without presence of further faults.
Negative impact on the energy market	9	This is the target of the threat; total market disconnection is expected.
Negative impact on transmission system	2	Some transient effects if DER are automatically disconnected.
Negative impact on billing functions	0	Power usage data are not expected to be affected.
Privacy Loss	0	Vectors examined do not include data exfiltration techniques.
Total Score	2,62	

TABLE IV. Likelihood Assessment of Market Intruption Threat

Criterion	Assessment	
	Score	Comments
Skill required	9	Attacks against web-facing IT infrastructure are very common and tools for performing the attack are widespread (even legitimate offensive security tools).
Accessibility	9	Internet facing interface.
Attack Vector	9	Multiple, widely exploited and well documented techniques.
CVE	9	We expect them to be present due to legacy equipment.
Total Score	9	

CVEs are expected to be present and exploitable since operational data from the DER is essential to the operation of the VPP and patching of CVEs, if possible, on legacy equipment, requires intensive preparation and can only happen during scheduled maintenance windows.

While there are no recorded attacks against this function, incidents like the partial decoupling of the market in June 2019 [19] are indicative of such possible impacts. A corrupted file was the root cause of a series of events that led to partial decoupling. Similar effects can be caused through adversarial means.

B. FALSE DATA INJECTION IN THE SUPERVISORY AND CONTROL LAYER

False Data Injection attacks have been thoroughly studied in the past years. From GOOSE poisoning attacks [20], Load Redistribution Attacks [21]the focus in the LAA literature has been only on static load altering attacks, where the attack is mainly concerned in changing the volume of the load. In contrast, in this paper, we address dynamic load altering attacks (DLAAs, attacks against inverters [22] and in-state estimation [23]. The intention of these attacks is to insert realistic data into a communications channel with the intention of forcing cyber-physical elements to diverge from their intended operation. They can take the form of either spoofing data, or tampering, by capturing and altering legitimate traffic.

Information about the operational status of the DER is generated by a third-party software specific to the installed manufacturer or maintainer. Communication protocols are assumed to be standard industry-specific, IEC 61850 MMS/GOOSE, DNP3, Modbus at substations. Communication between the third-party software and the platform is assumed to not be fully air-gapped due to the topological distribution of DER and the lack of proprietary communication infrastructure. The load's state and general substation characteristics, like bus voltages and angles, are communicated to VPP operators by DSOs. These protocols have known weaknesses that are difficult to mitigate, partly because their design did not include cyber-security, or their operational reliability requirements hinder them from performing security functions due to constraints of the operational environment.

VPPs have unique supervisory and control environments that differentiate themselves from traditional SCADA infrastructures. They are, however, required to interoperate with DSO SCADA systems. As a result, when considering threats against this function, they may be case-specific to the implementation of each VPP. It is implied in the implementation of the aforementioned protocols that they are operating in trusted network segments.

Attack vectors that can enable the threat, among others, can be: supply chain compromise, remote service exploit, unauthorized command message injection, masquerading attacks, and blind false traffic injection [24].

Table V and VI summarize our evaluation impact and the likelihood of the threat.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762928

TABLE V. Impact Assessment of FDI attacks

Criterion	Assessment	
	Score	Comments
System scale	9	A compromise of the Supervisory monitoring and Control Platform has the potential to affect all DER connected to the VPP
Safety	7	Unsafe conditions are possible, due to stress to transformers and faulty breaker operation
Financial Impact on VPP	1	Assuming that the VPP partakes in the day ahead, ancillary market and spot market, the attack can disrupt the operation of the VPP for up to a few days. This will represent less than 1% of yearly revenue.
Negative impact on generation capacity	9	Disturbance expected to affect more than10% of generation for more than 8 hours´.
Negative impact on the energy market	5	The VPP can participate in the market, but DER optimization can be severely impeded.
Negative impact on transmission system	9	Instigation of instabilities is possible in unplanned DER connection and disconnection, as well as inability to provide ancillary services.
Negative impact on billing functions	0	Power usage data are not expected to be affected.
Privacy Loss	0	Vectors examined do not include data exfiltration techniques.
Total Score	5	

TABLE VI. Likelihood Assessment of FDI attacks

Criterion	Assessment	
	Score	Comments
Skill required	9	Attacks against web-facing IT infrastructure are very common and tools for performing the attack are widespread (even legitimate offensive security tools).
Accessibility	9	Internet facing interface.
Attack Vector	9	Multiple, widely exploited and well documented techniques.
CVE	9	We expect them to be present due to legacy equipment.
Total Score	9	

An example of this scenario is an adversary changing the maximum power setpoint of inverters in PV installations. VPPs naturally change this setpoint as a response to market signals. A malicious alteration by means of an unauthorized command message injection can lead to shut down of the inverter [13]. By extension, such a command sent to multiple inverters at the same time can shut down multiple DER at once.

C. DENIAL OF SERVICE OF CONTROLLED ELEMENTS

Electrically, DER are connected to the distribution network, either in the Medium or Low Voltage substations. For DSOs SCADA needs, DER provide communication links to the respective substation to provide electrical measurements, like voltages, current values, power output, power factor etc., as well as establish communications with the VPP operator. Interoperability and backwards compatibility of equipment is paramount to establish a functioning and reliable communication link. They can be wired, through twisted pair cables, optic fiber, power cables, or wireless, through ZigBee, WLAN, GSM, or Z-wave. Topologically, they are connected on a star or mesh grids with the VPP operator. Communication protocols that are used to implement supervisory and control functions are:

- IEC 60870-104 and their derivatives, like DNP3
- Modbus
- IEC 61850, GOOSE and SV for substation automation, MMS, or XML for DER-VPP communication.

The design of IEC 61850, being object oriented and providing interoperability and backwards compatibility options, is gaining traction on becoming the de facto protocol of choice for Smart Grid implementations, especially in Europe. IEC 62351 is the relevant security standard for securing IEC 60870-104 and derivatives, as well as IEC 61850 protocols. However, due to the performance requirements of IEC 61850, modern encryption implementations are sometimes not possible. Even with the augmentations of IEC 62351, these protocols are not fully protected, e.g., the trust architecture is based on embedded X.509 certificates on equipment, which cannot be revoked [25], RSA 1024 used for digital signatures deemed unsafe by NIST, HMAC schemes requiring pre-shared keys. In particular, the fact that certificates are hard embedded in equipment makes physical security of the infrastructure crucial, which is then obstructed by the fact that DER can be located in hard to reach and monitor locations. A motivated adversary could physically access equipment and extract the keys directly from the circuitry of the equipment.

Apart from these inherent weaknesses, these

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762928

protocols are often mapped to the TCP/IP protocol below the transport layer of OSI, which implies they are susceptible to common flooding and distributed DoS attack vectors. DoS, however, can manifest through FDI vectors as well, when the attack locks the equipment in reboot loops, activates test operation (which is a misconfiguration option), or locks them in update mode. Subtler and more specific vectors can include timing violations, such as withholding packets over the TAL (Time Allowed to Live) threshold or changing the time parameter of the packets, which effectively makes the equipment inoperable.

Performing a dependency analysis on the threat scenario, we also identified that Byzantine failure state induction is also possible. Due to the inherent statistical discrepancies of Smart Grid data, the possibility of Byzantine sensors, IEDs and data [26] is possible. Byzantine state in the VPP setting can take three forms:

1. Equipment compromised and intentionally misconfigured,
2. Failed equipment, where status is being denied or disrupted from being communicated, e.g., alarm suppression
3. Hidden failure that has been intentionally or unintentionally induced.

In a trusted environment, as described above, it is particularly challenging to identify the compromised equipment and reestablish normal operation and the root of trust. When protective equipment is involved or directly targeted, like the TRISIS malware [6], hazardous conditions can be present, including the danger of electrocution. Apart from human safety hazards, Safety Instrumentation Systems (SIS) in a Byzantine state may fail in the presence of non-adversarial faults, causing damage to the infrastructure or interrupt operation without any faults present, causing financial losses.

Table VII and VIII summarize our ratings for impact and likelihood assessment.

TABLE VII. Impact Assessment of DoS attacks on controlled elements

Criterion	Assessment	
	Score	Comments
System scale	0	This is a targeted attack against specific DER.
Safety	9	Byzantine failure state of protective equipment can cause electrocution.
Financial Impact on VPP	3	Physical damage can exceed 1% of yearly revenue.
Negative impact on generation capacity	1	Expected to impact less than 3% of generation capacity.
Negative impact on the energy market	0	The VPP can participate in the market, DER optimization can be slightly impacted.
Negative impact on transmission system	9	Instigation of instabilities is possible in unplanned DER connection and disconnection, as well as inability to provide ancillary services.
Negative impact on billing functions	0	Power usage data are not expected to be affected.
Privacy Loss	2	Data can be exfiltrated, limited to target DER.
Total Score	3	

TABLE VIII. Likelihood Assessment of DoS attacks on controlled elements

Criterion	Assessment	
	Score	Comments
Skill required	2	Substantial domain knowledge needed, ability to adapt existing offensive tools.
Accessibility	9	Internet facing interfaces possible.
Attack Vector	3	Exploited by high profile threat groups.
CVE	9	We expect them to be present in legacy equipment.
Total Score	5,75	

Communication delay between elements of the VPP will further be examined. Time delays on electrical measurements can adversely impact system stability [27]the paper presents a power system model based on delay differential algebraic equations (DDAE, as well as induce oscillations in the power output of the VPP [28]. These can have subsequent impacts on other subsystems of the VPP, like the pitch angle control of wind generators.

V. CONCLUSIONS

Threat assessment in Smart Grid environments is nontrivial but a critical part of risk assessment. In the case of VPPs, this is further exacerbated by the distributed, non-standardized patchwork of different technologies, operating environments, and communication implementations. Diverse ownership of DER, interoperability requirements, Quality of

Service requirements increase the complexity of the system and allow for security gaps to be overlooked.

In order to overcome these problems, we constructed a generalized security profile for VPPs, elected and scaled evaluation criteria, and examined the threat landscape as it translates to VPP environments.

Taking into consideration the inherent gaps in security for Smart Grid communications and implementation, our preliminary findings suggest that FDI attacks remain a prominent threat for VPPs and can affect them in all their operational functions. The trust architecture of VPPs relies greatly on third-party trust relationships between the VPP, DER and third-party implementation solutions. VPP operators are left with no choice but to replace compromised equipment, as it cannot be reinstated in a trustworthy state. DoS attacks are also prominent, as a successful attack may threaten grid stability as well as impact the generation capacity of VPPs. Finally, compromising the interaction between VPP and energy markets can endanger market functions as a whole.

VI. FUTURE WORK

The next stage of our work will focus on expanding on scenarios revolving around the identified threats, by utilizing attack-fault trees to include physical errors that can be induced by the execution of each scenario. An attempt to create correlations between these reactions and anomalous behavior of IT elements will be made and Indicators of Compromise that take into consideration physical system responses and measurements will be constructed.

ACKNOWLEDGMENTS

This publication is partly a result of SecDER project, funded by the German Federal Ministry for Economic Affairs and Energy (BMWi).

REFERENCES

[1] G. Plancke, K. De Vos, R. Belmans, and A. Delnooz, “Virtual power plants: Definition, applications and barriers to the implementation in the distribution system,” Int. Conf. Eur. Energy Mark. EEM, vol. 2015-Augus, 2015, doi: 10.1109/EEM.2015.7216693.

[2] CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids, “CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Information Security,” no. November, pp. 1–107, 2012, [Online]. Available: ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf.

[3] J. Guo, Y. Han, C. Guo, F. Lou, and Y. Wang, “Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties,” Energies, vol. 10, no. 1, pp. 1–21, 2017, doi: 10.3390/en10010087.

[4] X. Gao, X. Li, and X. Yang, “Robustness assessment of the cyber-physical system against cascading failure in a virtual power plant based on complex network theory,” Int. Trans. Electr. Energy Syst., no. June, pp. 1–27, 2021, doi: 10.1002/2050-7038.13039.

[5] Robert M. Lee, Michael J. Assante, and Tim Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case,” Ics.Sans.Org, pp. 2–11, 2016, [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[6] Dragos Inc., “TRISIS Malware,” pp. 1–19, 2017, [Online]. Available: https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=40B2ED59-D34E-47C3-B9E2-1E8D030C5748.

[7] O. T. Soyoye and K. C. Stefferud, “Cybersecurity Risk Assessment for California’s Smart Inverter Functions,” 2019 IEEE CyberPELS, CyberPELS 2019, 2019, doi: 10.1109/CyberPELS.2019.8925257.

[8] M. Touhiduzzaman, S. N. G. Gourisetti, C. Eppinger, and A. Somani, “A Review of Cybersecurity Risk and Consequences for Critical Infrastructure,” Proc. - 2019 Resil. Week, RWS 2019, pp. 7–13, 2019, doi: 10.1109/RWS47064.2019.8971975.

[9] L. Marinos, “European Union Agency for Network and Information Security Smart Grid Threat Landscape and Good Practice Guide Smart Grid Threat Landscape and Good Practice Guide About ENISA Smart Grid Threat Landscape and Good Practice Guide,” no. December, 2013.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762928

[10] NESCOR, “Electric Sector Failure Scenarios and Impact Analyses – Version 3.0,” no. December, 2015, [Online]. Available: http://smartgrid.epri.com/doc/NESCOR Failure Scenarios v3 12-11-15.pdf.

[11] E. P. R. I. (EPRI), “Analysis of Selected Electric Sector High Risk Failure Scenarios National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1 First Version,” no. September, 2013.

[12] W. G. Temple, Y. Li, B. A. N. Tran, Y. Liu, and B. Chen, “Railway system failure scenario analysis,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10242 LNCS, pp. 213–225, 2017, doi: 10.1007/978-3-319-71368-7_18.

[13] B. J. Kang et al., “Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations,” IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA, vol. 2015-Octob, 2015, doi: 10.1109/ETFA.2015.7301457.

[14] S. Jauhar et al., “Model-Based Cybersecurity Assessment with NESCOR Smart Grid Failure Scenarios,” Proc. - 2015 IEEE 21st Pacific Rim Int. Symp. Dependable Comput. PRDC 2015, pp. 319–324, 2016, doi: 10.1109/PRDC.2015.37.

[15] Cyber Trust, “D2 . 1 Threat landscape : trends and methods,” no. 2018, p. 250, 2020.

[16] J. Johnson, J. Flicker, A. Castillo, and C. Hansen, “Design and Implementation of a Secure Virtual Power Plant,” no. September, pp. 243–287, 2017, doi: 10.13140/RG.2.2.36603.62244.

[17] S. M. S. Hussain, T. S. Ustun, and A. Kalam, “A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges,” IEEE Trans. Ind. Informatics, vol. 16, no. 9, pp. 5643–5654, 2020, doi: 10.1109/TII.2019.2956734.

[18] J. Marron, A. Gopstein, N. Bartol, and V. Feldman, “Cybersecurity framework smart grid profile,” p. 142, 2019, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2051.pdf.

[19] NEMO Commitee, “SDAC report on the ‘partial decoupling’ incident of June 7th 2019,” 2019.

[20] N. Kush, E. Ahmed, M. Branagan, and E. Foo, “Poisoned GOOSE: Exploiting the GOOSE protocol,” Conf. Res. Pract. Inf. Technol. Ser., vol. 149, pp. 17–22, 2014.

[21] S. Amini, H. Mohsenian-Rad, and F. Pasqualetti, “Dynamic load altering attacks in smart grid,” 2015 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT 2015, pp. 1–5, 2015, doi: 10.1109/ISGT.2015.7131791.

[22] T. O. Olowu, S. Dharmasena, H. Jafari, and A. Sarwat, “Investigation of False Data Injection Attacks on Smart Inverter Settings,” 2020 IEEE CyberPELS, CyberPELS 2020, no. January 2021, 2020, doi: 10.1109/CyberPELS49534.2020.9311541.

[23] R. Lin et al., “False Data Injection Attacks against State Estimation in AC-DC Hybrid Power System,” Chinese Control Conf. CCC, vol. 2020-July, pp. 4302–4306, 2020, doi: 10.23919/CCC50068.2020.9189440.

[24] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, “Smart grid data integrity attacks: Characterizations and Countermeasures,” IEEE Trans. Smart Grid, vol. 4, no. 3, pp. 1244–1253, 2013, doi: 10.1109/TSG.2013.2245155.

[25] J. G. Wright and S. D. Wolthusen, “Limitations of IEC62351-3’s public key management,” Proc. - Int. Conf. Netw. Protoc. ICNP, vol. 2016-Decem, no. HotPNS, pp. 1–6, 2016, doi: 10.1109/ICNP.2016.7785322.

[26] A. Vempaty, L. Tong, and P. K. Varshney, “Distributed inference with Byzantine data: State-of-the-art review on data falsification attacks,” IEEE Signal Process. Mag., vol. 30, no. 5, pp. 65–75, 2013, doi: 10.1109/MSP.2013.2262116.

[27] F. Milano and M. Anghel, “Impact of time delays on power system stability,” IEEE Trans. Circuits Syst. I Regul. Pap., vol. 59, no. 4, pp. 889–900, 2012, doi: 10.1109/TCSI.2011.2169744.

[28] M. Elkhatib, J. Johnson, and D. Schoenwald, “Virtual Power Plant Feedback Control Design for Fast and Reliable Energy Market and Contingency Reserve Dispatch,” pp. 2969–2974, 2018, doi: 10.1109/pvsc.2017.8366393.

AUTHORS

George Gkoktsis

George Gkoktsis received his Diploma on Electrical and Computers Engineering with specialization field Electrical Energy from Aristotle University of Thessaloniki, Greece in 2015 and his MSc on Information Security from University of London in 2020.
He is currently working as a researcher at Fraunhofer SIT in Germany, in the department of Cyber-Physical Systems Security and affiliated with the National Research for Applied Cybersecurity ATHENE. His research focuses on Electrical Energy System's cybersecurity, Cyber-resiliency for the energy sector and threat modeling for Critical Infrastructures.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762928

G. Gkoktsis,
"Assessing the Cyber Threat Landscape for Virtual Power Plants",
Latin-American Journal of Computing (LAJC), vol. 9 no. 2, 2022.