Impact of cyberattacks targeting distributed photovoltaic inverters

Marta Gomis Domènech, Yassine Naimi, Xavier Le Pivert

Impact of Cyberattacks Targeting Distributed Photovoltaic Inverters

Marta Gomis Domènech
Univ. Grenoble Alpes, CEA, Liten
Campus INES 73375
Le Bourget du Lac, France
marta.gomisdomenech2@cea.fr

Yassine Naimi
Univ. Grenoble Alpes, CEA, Liten
Campus INES 73375
Le Bourget du Lac, France
yassine.naimi@cea.fr

Xavier Le Pivert
Univ. Grenoble Alpes, CEA, Liten
Campus INES 73375
Le Bourget du Lac, France
xavier.lepivert@cea.fr

***Abstract*—Smart grid technologies increase the power grid vulnerability to cyberattacks. This study analyses the impact on voltage profiles of cyberattacks against photovoltaic (PV) inverters. Their capability to support the grid through ancillary services enlarges their attack surface. In particular, their reactive power capability is considered in order to evaluate whether the related cybersecurity threats constitute a risk of voltage collapse. The study case network, which can be used as a benchmark, represents the distribution of a small city. The voltage regulation consists of an On-Load Tap Changer (OLTC) and the reactive power control of distributed inverters. Under cyberattack, the inverters start absorbing reactive power in undervoltage conditions. The metrics are the minimum voltage of the network and the loading of equipment. A domino effect on the attack activation is observed. The cyberattacks degrade the network voltage, but the voltage stability in terms of collapse is not endangered, thanks to the support of the OLTC.**

***Index Terms*—Distributed PV inverters, reactive power capability, smart grid cybersecurity, voltage collapse risk, voltage regulation**

I. Introduction

Smart grid technologies will play a fundamental role in the operation of the power grid, especially with the spread of renewable distributed energy resources [1]. The intermittence of these resources makes the balance between generation and consumption more complex [2]. Smart grid technologies rely on data acquisition and communication systems integrated to the power system, as well as on the interoperability among grid components, as tackled by the IEEE Std 2030. They make it possible for grid operators to monitor and remotely control grid components in order to compensate for the instantaneous power unbalances. The communication layer entails a cybersecurity risk [3], [4], which is particularly critical, because (a) the power grid provides an essential service in which the cyber system acts on the physical system, and (b) the power grid is operated at increasingly stressed conditions.

The renewable distributed energy resources tacked in this study are the PV installations. During their initial deployment, the inverters interfacing them with the grid were operated at unity power factor (IEEE P1547 Standard), therefore exclusively injecting active power. Shortly after, Grid Codes were revised to allow PV ancillary services (i.e. to exploit their flexibility in order to support the grid); in particular, the inverters' reactive power capability for voltage regulation [5], [6].

This work has been realized by members of INES.2S and received funding from the French State under its investment for the future programme with the reference ANR-10-IEED-0014-01.

This study assesses the risk of voltage collapse of the distribution power grid caused by a cyberattack targeting the voltage control of the distributed PV inverters (that is, their Q(V) characteristic), given the reactive power limit of the distribution network in both medium voltage (MV) and low voltage (LV). With this objective, the voltage profiles at the most critical nodes of the network are analysed, as the first effect of such cyberattack is local. Two low voltage thresholds are considered: 0.9 pu for normal operation and 0.85 pu for PV disconnection, which may be critical for the grid in the case of high PV penetration.

II. Study case network

The comprehensive and representative study case network represents the distribution of a small city. It is modelled using PowerFactory and it is composed of existing test networks: the American IEEE 13-bus and 37-bus MV feeders [7], assembled with the European LV network, presented in [8]. Its overview is shown in Fig. 1 left. The HV/MV substation is supplied by an external network with a short-circuit power of 150 MVA. The network has a radial topology, and it is composed of 157 nodes, including 57 distributed PV installations in both MV and LV. The original feeders and network are modified in order to (a) be assembled in a coherent and realistic manner, and (b) achieve the desired level of distributed PV generation.

With the objective to assess the risk of voltage collapse, the study case is a Saturday in winter, since it is the worst-case scenario in terms of peak consumption. For the same reason, the analysis focuses on the two daily periods of high demand: early afternoon and evening.

A. PV generation

The PV generation is modelled according to the location and to the day of the year, assuming sunny weather. The rating of the inverters is the sum of peak powers of all connected panels, the difference with the actual generation gives some margin for the injection or absorption of reactive power without oversizing. The total capacity is 585 kWp (210

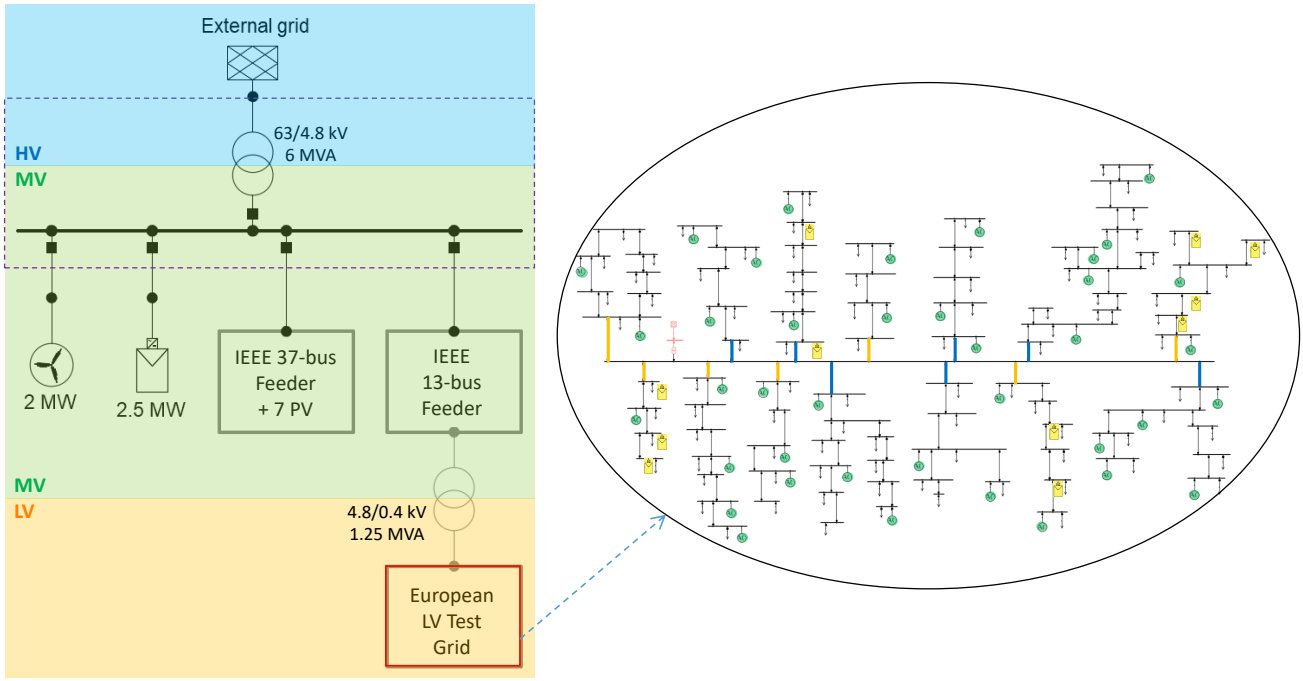

Fig. 1. Left: study case network overview; highlight of the HV/MV substation (purple dashed line), and of the three voltage levels: HV (63 kV, in blue), MV (4.8 kV, in green) and LV (400 V, in yellow). Right: zoom on the LV network; highlight of the distributed PV units (green) and of the two feeder types: urban (blue) and suburban (yellow).

kWp in MV and 375 kWp in LV), which corresponds to around 10% of the total peak consumption. The actual maximum power generated by the PV installations is around 40% of the installed capacity, i.e. 4% of the total peak consumption.

B. Loads

As opposed to the MV level, the LV network (Fig. 1 right) is particularly heterogeneous in terms of demand profiles: coherent to the urban and suburban nature of the feeders, which supply residential, commercial and agricultural loads. The loads sizing process consists in the assignment of:

1) Peak consumption values (directly obtained from the original values in MV, and assumed from the French power subscription options in LV)
2) Power factors assumed constant (between 0.75 and 0.9 in MV, 0.93 in LV)
3) Standard consumption profiles from [8], depending on the load category
4) Sets of ZIP coefficients from [9] (LV) and [10] (MV), to account for loads' voltage sensitivity (a total of 11 and 3 sets are used in LV and in MV, respectively)

The loads sizing is validated by checking the loading of equipment, in a bottom-up manner: first the LV lines, then the MV/LV transformer, and finally the MV lines. In accordance with the objective of the study, the final network is considerably highly loaded, without reaching a critical state.

Without considering the voltage sensitivity of loads (i.e. considering constant PQ loads), the peak power of the LV network is 1.1 MW in the evening, and each MV feeder supplies around 2.4 MW. The total peak consumption is therefore almost 6 MW. The replacement of PQ loads with ZIP loads reduces the maximum voltage drop of the network by 3%. It also reduces the loading of the distribution transformer by 14%. More illustrative is the fact that with PQ loads, all the 91 LV nodes reach minimum voltages lower than the PV disconnection threshold; while with ZIP loads, it is the case of only 17 terminal nodes (distributed among the 14 feeders).

III. Voltage Control Equipment

Two voltage regulation mechanisms are modelled: the OLTC of the HV/MV transformer, and the reactive power control of distributed PV installations. The OLTC has 11 positions (±5 taps), centred in the voltage setpoint of 1.032 pu. Each tap entails a voltage change of 1.5%, the lower and upper voltage bounds are 1.022 pu and 1.042 pu, respectively. These parameters are adjusted so that in normal operation, all nodes keep acceptable voltage levels during the whole day. The Q(V) control of the inverters consists of a conventional droop with a dead band. The droop value is 2% (the quickest within the commonly used range of 2% to 10% [11]); the lower dead band limit is 0.965 pu. The upper dead band limit is not of interest because the focus is on high demand conditions. The voltage control with the mentioned parameters is referred to as the "base case" in the rest of the article.

The black characteristic in Fig. 2 shows a generic, not to scale droop characteristic. The power limitation of inverters (Q_{max} and Q_{min}) from the technological point of view is related to their nominal apparent power. However, the reactive power absorption and injection limits are set to 60% of the nominal power, regardless of the actual active power injection.

This limit is obtained from their usual adjustable power factors of 0.8 inductive to 0.8 capacitive, which results in ±3 kVar, ±6 kVar and ±18 kVar for the installations in LV urban, LV suburban and MV feeders, respectively. Due to the voltage levels in the network, the voltage control is only activated in the LV inverters, which inject reactive power in order to support the network voltage.

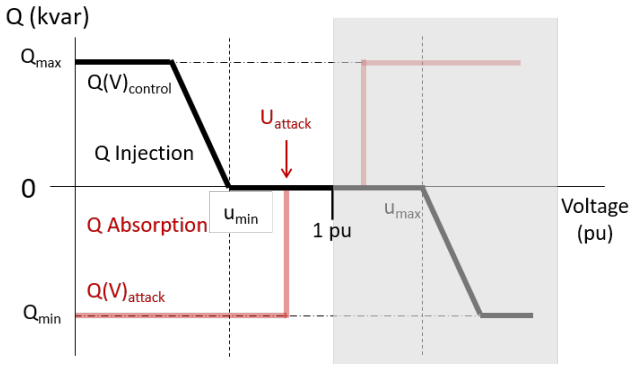

Fig. 2. Q(V) control of the distributed PV inverters (black curve) and activation rule of the modelled cyberattack (red curve). The voltage range of interest is lower than 1 pu, which corresponds to high demand conditions.

The Low Voltage Ride Through (LVRT) characteristics of the distributed PV units are not modelled. However, the last recovery voltage level of 0.85 pu in Europe [12] is considered as the critical low voltage threshold, as mentioned above.

IV. Cyberattack Modelling

Since the focus of the study is on the physical impact of cyberattacks, their implementation from the ICT (Information and Communication Technology) point of view is out of scope. The cyberattack model assumes that a malicious code has previously infected all the distributed PV inverters.

The attacked inverters start absorbing reactive power in undervoltage conditions, responding to an activation rule based on their local voltage measurement (similar to the activation of the voltage regulation described above). The red curve in Fig. 2 shows the attack activation rule, compared to the voltage regulation characteristic (black curve). The low voltage dead band limit for attack activation is 0.95 pu; and the droop value is $10^{-5}\%$, so that the reactive power saturation limits are reached in a single simulation step. As in the base case, only the LV inverters are activated, but this time absorbing reactive power and therefore worsening the stressed state of the network in terms of voltage. This scenario is referred to as Cyberattack 1. It allows studying the behaviour of the OLTC under attack.

A second cyberattack scenario is modelled blocking the action of the OLTC, in order to determine its capacity to limit the attack consequences. The low dead band limit of the LV inverters has been adapted to the more degraded voltages, in order to allow for comparison: the dead band limit in LV is 0.885 pu for this scenario, while 0.95 pu is kept in MV. This scenario is referred to as Cyberattack 2.

V. Results and Discussion

The time step of the quasi-dynamic and balanced simulations is one second. In this section, an overview of the inverters' behaviour is shown in the first place. The attack activation in the evening high demand period is then analysed. Finally, the minimum voltage of the network and the maximum loading of the equipment are assessed.

A. Reactive power capability of inverters

Fig. 3 shows the reactive power of the 50 LV inverters, for the base case scenario of voltage support by reactive power injection (top), and for the Cyberattack 2 with reactive power absorption (bottom). During the daily periods of high demand, one observes two reactive power saturation limits due to the different ratings of the PV installations in LV for urban (red and orange curves) and suburban areas (blue and purple curves). The figure illustrates the quick activation of the attacks (bottom) compared to the slower reaction of the voltage control (top), due to the difference between the droop values.

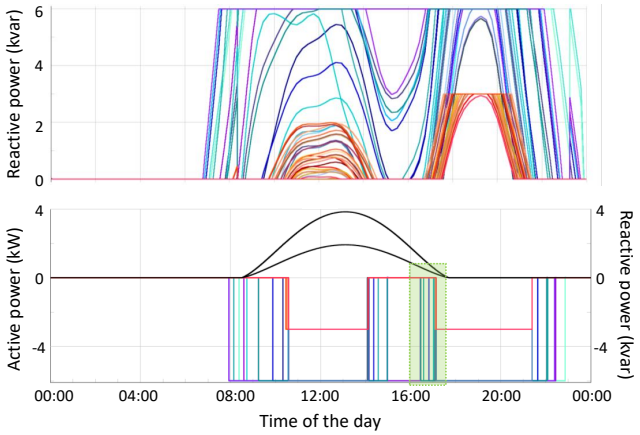

Fig. 3. Power transfered by the LV inverters. Top: reactive power injection in the base case. Bottom: reactive power absorption in the Cyberattack 2, and active power generation for the two different installations ratings (in black). The active power generation has not been included in the top figure for the sake of clarity and for redundancy avoiding, since it is identical to that of the bottom figure.

B. Cyberattack activation

The evening activation of the Cyberattack 2 (highlighted in green in Fig. 3, bottom) is further analysed in Fig. 4. In particular, the focus is on the interaction among attacked inverters, as well as on the immediate impact on the voltage.

A domino effect on the attack activation among nearby inverters is observed: there is a significant overlapping among the 50 curves (Fig. 4, top), which shows that the attack is activated in several inverters at the same simulation time step. This is especially true in LV (red and orange curves), since the voltages at the inverters' terminals are more similar. The voltage in the terminal nodes of the three critical LV feeders shows sudden drops when the attack in several inverters is activated (Fig. 4, bottom), for example between 17:05 and

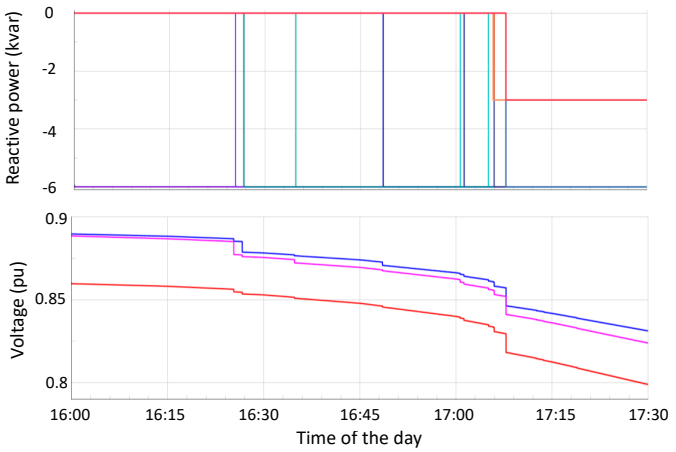

Fig. 4. Evening activation of the cyberattack 2. Top: reactive power absorption of LV inverters, bottom: voltage of three critical LV terminal nodes.

17:10. The total impact in these nodes, removing the natural variation of the voltage due to the demand variation, is around 3% for the chosen activation rules and reactive power limits of the inverters.

It has to be noted that the reaction time of the inverters' controllers, including the reactive power setpoint calculation, is smaller than the simulation time step.

C. Minimum voltage of the network

Up until now, the base case scenario has been compared with the Cyberattack 2 (OLTC deactivated), in order to better visualize the inverters' behaviour and the maximum possible impact of the attack on the voltages. In this subsection, the results are discussed considering the Cyberattack 1 as well, i.e. with the OLTC activated. Keeping the point of view of the voltage collapse risk, the main indicator is the minimum voltage in the network, which is summarized in Table I.

TABLE I
MINIMUM VOLTAGE OF THE NETWORK, TIME AT WHICH IT IS REACHED, AND FEEDER TYPE OF THE CONCERNED NODE

Case	**A**	**B**	**C**	**D**	**E**
V_{min} **(pu)**	0.791	0.870	0.887	0.851	0.755
Hour	19:15	18:14	19:30	19:30	19:15
Feeder type	Suburban residential		(Suburban) agricultural		Suburban residential

Cases A, B and C correspond to the three modelling stages of the voltage regulation equipment: no regulation (A), regulation by the OLTC only (B), and regulation by the OLTC and inverters as the base case (C). Cases D and E correspond to the Cyberattack 1 and 2 presented above, respectively. The results prove the complexity to conclude about the most critical time and feeder in terms of minimum voltage, and therefore the suitability of the simulation approach for the voltage collapse risk assessment carried out in this study.

Fig. 5 shows the voltage at the three critical LV nodes during the evening high demand, comparing the base case (case C) with the Cyberattack 1 (case D). The dashed line corresponds to the PV disconnection voltage threshold. For the base case (Fig. 5, top), the voltage in the two most critical nodes goes slightly under the normal operation threshold, but there is still some margin with the disconnection threshold. The Cyberattack 1 (Fig. 5, bottom) causes a voltage dip that degrades the network voltage, and the regulatory low voltage threshold corresponding to normal operation is not respected. The OLTC acts around one hour after the attack activation, significantly limiting the consequences: the voltage stability in terms of collapse is not endangered. However, there is a very small margin with the disconnection threshold between 18h and 20h.

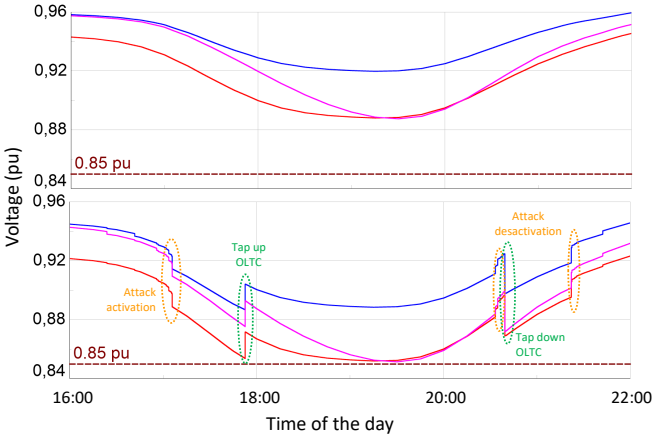

Fig. 5. Voltage of the three critical LV nodes for the base case (C, on top) and the cyberattack 1 (D, at the bottom), with highlight of the impact of the attack on the voltage (in orange) and of the OLTC tap changer (in green).

Without the OLTC action (case E), the minimum voltage in the network is not acceptable (0.755 pu), and the voltage in all LV nodes goes under 0.85 pu. Some of them stay under this value for a considerably long period. All distributed PV in LV would therefore disconnect, and so would do the LV loads with undervoltage protections. These protections are not modelled in the study. Further studies should be done in order to assess the impact of such disconnection. Instinctively, the PV units disconnection in the evening would reduce the impact of the attack. However, if the inverters provide other ancillary services to the grid, or if they are injecting active power from a battery storage system, the overall impact of the disconnection could be harmful. On the other hand, the inverters disconnection during the daylight (due to the morning activation of the attack) would prevent both the absorption of reactive power and the injection of the active power generated by the PV. The consequences would therefore depend on the grid state and the number of installations implied, but in any case, unless a battery stored the power generated by the panels, such renewable generation would be lost.

D. Maximum loading of the equipment

The loading of grid equipment has an impact on the network losses. The loading of the two transformers and of the most

critical line are compared in Table II for the base case and for the two cyberattacks, during the evening high demand period as the worst-case scenario in terms of losses. The critical line is the MV feeder from the HV/MV substation to the 13-bus feeder (which supplies the LV network). As expected, the maximum loading conditions coincide in time with the minimum voltage conditions assessed above.

TABLE II
TRANSFORMERS AND CRITICAL LINE LOADING DURING THE EVENING HIGH DEMAND FOR THE BASE CASE (C) AND FOR THE TWO CYBERATTACKS (D AND E)

Equipment	Loading indicator	C	D	E
HV/MV transformer	Max. loading (%)	101	108	102
	Over-loading duration (min)	55	67	70
MV/LV transformer	Max. loading (%)	94	108	115
	Over-loading duration (min)	-	61	151
Critical line	Max. loading (%)	75	78	82
	Time over 75% loading (min)	-	124	160

The maximum loading values are acceptable in the base case (C), while they are significantly higher under cyberattack (D and E). This is especially true regarding the transformers; even though the critical line follows the same trend, it keeps acceptable loading levels in all cases. In the Cyberattack 1 (D), the two transformers share the loading increase. In the Cyberattack 2 (E), the distribution transformer bears the consumption increase up to a 115% loading, which is not acceptable: the related overheating would result in a decreased life expectancy of the transformer.

CONCLUSION

The modelled cyberattacks reduce the terminal network voltage by around 3%. The study shows that the OLTC plays a crucial role in limiting the cyberattack impact: it reduces the voltage dips, avoiding the disconnection of distributed PV units in LV, as well as that of some loads. With the OLTC under normal operation, some voltages reach levels very close to the disconnection threshold. Besides, the voltage in a large part of the LV network stays below the normal operation threshold during a few hours, but the situation is still stable. Without the OLTC, on the contrary, the whole LV network reaches voltages under 0.85 pu. The voltage in MV is just slightly impacted by the cyberattacks, thanks to the proximity to the OLTC (and its setpoint being higher than the nominal level).

The cyberattack could go unnoticed and be recurring during a long period. This would increase the wear and tear of the transformer tap changer in the substation, as it has been shown that the number of tap changes increases under attack, with the tap changer trying to compensate the degraded voltages. Besides, the distribution transformer and the lines would also be affected, due to the increase of their loading in high demand conditions.

There is a clear interaction between the cyberattack conditions and the OLTC operation. This equipment succeeds in either avoiding the activation or directly deactivating the attack in some inverters (even if it may be activated again later, depending on the demand evolution). There is also an interaction among the inverters under attack: even if the simulation step is longer than the reaction time of the inverters' controllers, the analysis proves a domino effect among the nearby inverters, which is more noticeable in the evening, when the rate of demand increase is more pronounced.

Further studies could include the disconnection protections, replace the considered reactive power limit by only limiting the apparent power, or consider other days of the year and other types of cyberattacks. Efforts should be done to make the power grid more resilient to cybersecurity threats.

REFERENCES

[1] *Flexibility for Resilience: how can flexibility support power grids resilience?* European Comission. Directorate General for Energy. LU: Publications Office, 2022. Accessed: 16 January 2023. [Online]. Available: https://data.europa.eu/doi/10.2833/676635.

[2] R. W. Kenyon, M. Bossart, M. Marković, K. Doubleday, R. Matsuda-Dunn, S. Mitova, S. A. Julien, E. T. Hale, and B.-M. Hodge, "Stability and control of power systems with high penetrations of inverter-based resources: An accessible review of current knowledge and open questions," *Solar Energy*, vol. 210, pp. 149–168, Nov. 2020. doi: 10.1016/j.solener.2020.05.053.

[3] L. Zanni, "SHAPING THE FUTURE OF THE SWISS ELECTRICAL INFRASTRICTURE," activity report, Swiss Competence Centers for Energy Research, Lausanne, Mar. 2021. [Online]. Available: http://www.pvtest.ch/Dokumente/Publikationen/283_Activity_Report_2017-2020_14.03.2021_JP.pdf.

[4] "Power grid cyberattack in Ukraine (2015)," June 2021. Accessed: 6 July, 2022. [Online]. Available: https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015).

[5] Q. Zheng, J. Li, X. Ai, J. Wen, and J. Fang, "Overivew of grid codes for photovoltaic integration," in *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, (Beijing), pp. 1–6, IEEE, Nov. 2017. doi: 10.1109/EI2.2017.8245501.

[6] A. Teymouri, A. Mehrizi-Sani, and C.-C. Liu, "Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, pp. 2872–2877, Oct. 2018. doi: 10.1109/IECON.2018.8591583.

[7] "Resources – IEEE PES Test Feeder." Accessed: 11 May 2022. [Online]. Available: https://cmte.ieee.org/pes-testfeeders/resources/.

[8] A. Traupmann and T. Kienberger, "Test Grids for the Integration of RES—A Contribution for the European Context," *Energies*, vol. 13, p. 5431, Jan. 2020. doi: 10.3390/en13205431.

[9] A. Bokhari, A. Alkan, R. Dogan, M. Diaz-Aguilo, F. de Leon, D. Czarkowski, Z. Zabar, L. Birenbaum, A. Noel, and R. E. Uosef, "Experimental Determination of the ZIP Coefficients for Modern Residential, Commercial, and Industrial Loads," *IEEE Transactions on Power Delivery*, vol. 29, pp. 1372–1381, June 2014. doi: 10.1109/TPWRD.2013.2285096.

[10] M. Diaz-Aguiló, J. Sandraz, R. Macwan, F. de León, D. Czarkowski, C. Comack, and D. Wang, "Field-Validated Load Model for the Analysis of CVR in Distribution Secondary Networks: Energy Conservation," *IEEE Transactions on Power Delivery*, vol. 28, pp. 2428–2436, Oct. 2013. doi: 10.1109/TPWRD.2013.2271095.

[11] "Reactive Power Capability and Interconnection Requirements for PV and Wind Plants." Accessed: 30 May 2022. [Online]. Available: https://www.esig.energy/wiki-main-page/reactive-power-capability-and-interconnection-requirements-for-pv-and-wind-plants/.

[12] "COMMISSION REGULATION (EU) 2016/ 631 - of 14 April 2016 - establishing a network code on requirements for grid connection of generators," p. 68.