Intrusion Resilience for PV Inverters in a Distribution Grid Use-Case Featuring Dynamic Voltage Control

BooJoong Kang[1], David Umsonst[2], Mario Faschang[3], Christian Seitl[3], Ivo Friedberg[4],
Friederich Kupzog[3], Henrik Sandberg[2] and Kieran McLaughlin[1]

[1] Queen's University Belfast, UK
[2] KTH Royal Institute of Technology, Sweden
[3] AIT Austrian Institute of Technology GmbH, Austria
[4] Austrian Power Grid AG, Austria
b.kang@qub.ac.uk

Abstract. ICT-enabled smart grid devices, potentially introduce new cyber vulnerabilities that weaken the resilience of the electric grid. Using real and simulated PV inverters, this work demonstrates how cyber-attacks on IEC 61850 communications to field devices can force an unstable state, causing voltage oscillations or overvoltage situations in a distribution grid. An automated resilience mechanism is therefore presented, combining intrusion detection and decentralised resilient controllers, which is demonstrated to assure stable operation of an energy system by counteracting cyber-attacks targeting embedded PV inverters.

Keywords: Cyber Security, Smart Grids, Resilient Control, Intrusion response.

1 Introduction

This work investigates a novel protection scheme against cyber-attacks, based on domain-specific modelling of the physical features of an electrical distribution system where embedded PV inverters are dynamically controlled to manage power and voltage outputs. Many cyber-physical infrastructures use the well-established Supervisory Control and Data Acquisition (SCADA) paradigm, with a central control instance and numerous logical connections to field devices. This work focuses on power grid infrastructure, which is a typical example for that paradigm. With the introduction of participants such as renewable energy generators, new connections to participants are being deployed, and an emerging concern is the rapid increase in field devices that require communications. At the very least, this is required for remote monitoring, but it is also highly desirable to support parameter configuration to enable a range of grid management applications. However, integrating such capabilities increases the cyber-attack surface, presenting a risk that controls may be tampered with, resulting in instabilities.

In this work, a use-case is considered where photovoltaic (PV) inverters are remotely controlled via IT network connections to a central distribution system operator (DSO) system. The controller in this case aims to facilitate improved voltage management for distribution lines that have a high proportion of distributed embedded generation. The components of the control loop are thus distributed across subsystems, interlinked via SCADA communications. The specific problem investigated is to enable this control system to detect a cyber-attack, and automatically react to mitigate physical effects in the electrical grid. For this scenario, a resilient controller (RC) is developed that protects the field devices from malicious parameter changes. In parallel, a domain specific SCADA intrusion detection system is developed that uses deep packet inspection to detect manipulated device communications. A realistic physical laboratory demonstration environment is used to show how a novel combination of these two approaches can be integrated to ensure system stability during a set of cyberattack scenarios. The main research contributions of this work are as follows:

- Resilient control theory is deployed in a real environment, supporting decision making for real-time response.
- An active intrusion response mechanism integrates with physical system controls in real-time, going beyond previous passive SCADA IDS approaches.
- Validation in a realistic testbed, comprising hardware linked to a simulated grid environment, interconnected via IT.

2 Related Work and Motivation

Previous work investigating cyber-attacks in cyber-physical systems often models or demonstrates physical effects caused by deliberate interference in the cyber domain. However, research gaps remain regarding: 1) detailed system implementations demonstrating specific cyber-attacks executed to cause direct physical effects; 2) attack mitigation methods to respond to cyber-attacks.

Regarding the first gap, the literature typically addresses the problem from a system modelling perspective [1]. In doing so, it is possible to reveal detail about the impact on electrical parameters across a grid model, such as the IEEE *n* bus system models [2]. However, such studies primarily reveal effects and constraints pertaining to grid stability, with the issue of cyber security being a motivation, rather than part of the experiments. A few papers take this further by investigating attacks via software/hardware co-simulation. E.g., Hahn [3] introduces a testbed to explore vulnerabilities and physical effects, showing how voltages, flows, and generation could be adversely affected by simple DoS attacks. Such studies remain focused on problem identification.

Regarding the second gap, proposed solutions typically focus solely on cyber or physical aspects. One approach is to reduce the problem of intrusion detection to an “anomaly detection” problem [4]. This often happens in isolation from the cyber domain, and the practicalities of real-time deployment are not generally considered. A weakness is that whereas alerts can be generated, it is difficult to map alerts to consequences in the physical domain. The question arises, how to translate alerts into mitigation actions in the physical domain? To address these issues, this paper investigates a combination of two main components: resilient control and intrusion detection.

Resilient control has gained a lot of interest in recent years. Research on the topic is conducted in different areas, such as control theory, power systems, and security. Resilient control systems can achieve an acceptable level of operational performance and state awareness in the presence of random, malicious, or unexpected disturbances [5]. Urbina et al. [6] define a common taxonomy for the different areas in the field of resilient control. This discussion will focus on power systems. On the substation level, Isozaki et al. [7] show how an adversary can manipulate a centralised tap changer control in the substation to cause voltage violations or to reduce the output power of PVs. Furthermore, they present a detection algorithm, which increases the resilience of the system by improving the operational performance during an attack. At a lower level of the power grid, Teixeira et al. [8] show how a microgrid with a quadratic voltage droop control for PVs can be attacked but no mitigation methods are proposed. The resilient control strategies introduced in this paper are active on the PV level, but in contrast to [8] the commonly used piecewise linear voltage droop control is considered. Furthermore, PVs are protected against attack on the droop law setpoints.

From a cyber-security viewpoint, Genge et al. [9] whitelist allowed traffic and detect prohibited connections based on general information such as IP address, port number and protocol. However, such traditional techniques cannot interpret application layer data to provide information about physical system states. Yang et al. [10] introduce model based detection methods for IEC61850. Caselli et al. [11] adopt discrete-time Markov chains to detect anomalies, and Yoo et al. [12] use one-class support vector machines to learn normal behaviours. However, most research focuses on how to detect attacks, with less attention on how to apply the results to provide mitigation. Recent work has emerged investigating intrusion response systems (IRS) whereby automated actions are applied to mitigate detected attacks. Literature on IRS focuses mainly on traditional IT [13], while IRS in cyber-physical use-cases are broadly unaddressed. He et al. [14] demonstrated that an automated IRS could significantly improve the reliability of cyber-physical systems. Qi et al. [15] investigate distributed energy installations that operate smart inverters and propose mechanisms to automatically respond to cyber-attacks, but the proposal is not supported by an implementation. Li et al [16] propose algorithms for identifying optimal solutions against cyber-attacks, but mainly focus on how to make a decision (as a response) for cyber-attack(s).

3 Selection of the Smart Grid Scenario

Three broad types of control loop are present in today's digitalised distribution system:

1. Local loops with sensor, controller and actuator in close proximity. E.g., maximum power control of an inverter, or substation voltage control with on-load tap changer. Such loops are common and operate autogenously. Changes must be made on-site.
2. Local control loops with interfaces for remote configuration and monitoring. E.g., communication interfaces to distribution-level generators above a certain power rating. The number of control loops in this category will increase in the coming years.
3. Remote control loops, with dedicated sensor-controller / controller-actuator telecommunications. Due to their time-critical nature these are usually avoided.

The second category is chosen for further study in this work, as it is expected to be the most widely applied concept in future and is widely representative. The scenario that is now developed focuses on residential inverters. To avoid grid congestion, distributed energy resources such as PV and battery systems are required to provide so-called ancillary services to the power system. In a distribution grid scenario, the most relevant ancillary service is voltage control, with the aim to maintain line voltages within the technical specifications EN50160. For example, the use of PV inverters to provide a voltage control service is realised using droop control, with the voltage at the connection point used as input and a droop law changing the unit's reactive power as shown in Fig. 1, based on the voltage at the feeding point (see also EN50438:2013).

The configuration of the droop law is typically done on installation of the unit. However, it is proposed that the four supporting points of the droop law shown in Fig. 1 are updateable remotely using an IP-based communication network. In this scenario a controller is placed in a secondary substation, which supports communication using the IEC 61850 protocol. The controller uses measurements from the low voltage grid to gain the voltage level and variations. It is able to adjust the voltage level using an on-site MV/LV on-load tap changer transformer. However, its relevant functionality in this context is that it also updates the settings for reactive power control for the PV inverters. It does this on a regular basis by transmitting a $Q(U)$ function, via IEC 61850, consisting of four support vectors (see Fig. 1). This function defines the control gain of the proportional reactive power controller implemented in the inverters. Malicious changes in this gain can result in significant voltage limit violations or oscillations.

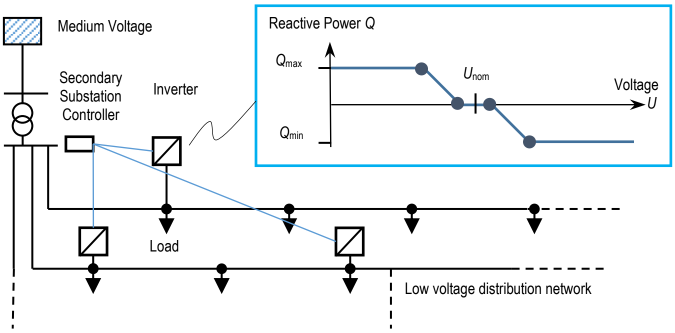

Fig. 1. Low voltage grid scenario and $Q(U)$ of PV inverters to support the local line voltage.

4 Automated Intrusion Resilience

A unified mechanism is now proposed for automated intrusion resilience. The proposed approach assumes that intrusions are possible, thus shifts the emphasis towards resilience of the underlying control loops and system behaviour. Note that the emphasis is on protecting the physical operation of the grid compared to traditional IRS approaches that focus on mitigation in the cyber domain [13]. Therefore, section 4.1 identifies the physical properties and models of the investigated scenario that can be used to verify that a new droop law yields a stable grid operation and to mitigate effects of malicious changes. Section 4.2 describes a custom intrusion detection approach to interact with resilient control components and how each component interoperates.

4.1 Resilience Control

A resilient controller (RC) is proposed to increase the robustness, safety, and security of local controllers with remote action interfaces. Hence, each PV inverter has a local resilient control module, which checks the commands. Although the module increases the inverter's resilience towards attacks and faults, it also limits the remote controllability. Therefore, the module must be designed so the control centre can achieve its control requirement and simultaneously reduce potential damage.

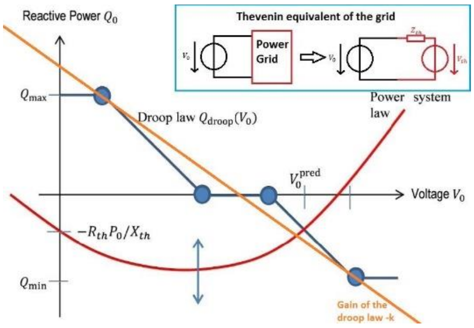

Fig. 2. Intersection between droop and power system law.

The PV has an anti-islanding system [17] that obtains a Thévenin equivalent of the grid from the PV's local perspective. The Thévenin equivalent consists of a constant voltage source V_{th} and total grid impedance $Z_{th} = R_{th} + jX_{th}$ (see upper right corner of Fig. 2). The model of [18] for the PV inverter is adopted and it is assumed that the voltage at the Point of Common Coupling $V_0 < \theta$ is close to the Thévenin voltage $V_{th}\angle 0$, i.e. $V_0 \approx V_{th}$, $\sin\theta \approx \theta$ and $\cos\theta \approx 1$.

Hence, it is verified that the droop law received from the control centre yields a steady state voltage, which is inside the allowed voltage range. Moreover, it is also verified that the new droop law is stabilising, i.e. it does not induce oscillations of the reactive power. This leads to two resilient control rules:

Rule 1 (Voltage Prediction with the Thévenin equivalent): With the Thévenin equivalent the relationship between the reactive power Q_0 injected in the grid and the PV voltage V_0 of the PV under the active power injection P_0 is expressed as

$$Q_0 \approx \frac{1}{X_{th}}(V_0 - V_{th})V_0 - \frac{R_{th}}{X_{th}}P_0$$

This power system law is used to predict the steady state voltage V_0, called V_0^{pred} by finding the intersection with the new remotely commanded droop law (see Fig. 2). After finding V_0^{pred} a range check is performed to see if the new droop law yields an acceptable steady state voltage: $V_{\min} \leq V_0^{\text{pred}} \leq V_{\max}$. If not, the new droop law is disregarded. Note, for applying this rule it is assumed that the droop law yields stable dynamics, which is checked by the following rule.

Rule 2 (Stability of the droop law): If the gain *k* of the droop law (slope of the orange line in Fig. 2) exceeds a certain critical gain k_{crit} the droop law destabilises the grid. Unstable here means that the reactive power starts to oscillate between the maximum and minimum reactive power possible. This might damage the PV inverter over a longer period of time. To avoid instability the gain of the new droop law is compared with the critical gain and if $k>k_{crit}$ the droop law is rejected.

The crux is to find k_{crit}. Here two methods are presented to obtain estimates of the critical gain. The first method uses the Thévenin equivalent and is a conservative version of the circle criterion [19]. The critical gain is obtained as

$$k_{\text{crit}} = \frac{V_{th} X_{th}}{R_{th}^2 + X_{th}^2}$$

and it has the advantage of being locally available, i.e. the Thévenin equivalent is obtained at the PV level without any other information. This critical gain is a heuristic value because the dynamics of all other PVs are disregarded by using the steady-state Thévenin equivalent of the grid and a conservative version of the circle criterion.

The second method uses the multivariate circle criterion [19]. Here, the Thévenin equivalent is not used, but the grid as a whole. After linearizing the grid equations of the reactive power and voltage, the multivariate circle criterion is used to obtain an estimate of the critical gain for all PVs. The advantage is that an estimate with a more solid theoretical foundation is obtained, but it is not possible to obtain the estimate in a completely decentralised fashion, since some knowledge of the whole grid is required. In the experiments in Section 5, the first method to estimate the critical gain is used.

4.2 Intrusion Detection and Resilience

The proposed IDS is custom-designed for IEC61850 based SCADA communications, and consists of two layers: local intrusion detection and global intrusion detection. Local units are placed at strategic points to monitor network traffic as shown in Fig. 3. These units apply whitelist, signature detection, and stateful analysis approaches. This is motivated due to the common use of legacy devices, unencrypted communications, and unauthenticated devices typically found in power systems in real-world.

Whitelist defines authorised connections and allowed operations, so any unauthorised connection or operation can be detected. Signature detection is used to detect known cyber-attacks at an individual packet level. Stateful analysis investigates traffic over the time by inspecting flows rather than packet-by-packet analysis. As an IEC

61850 interpreter is implemented in our IDS, the IDS can inspect application data and store the status information. The IDS will alert if a violation has been detected. Local units provide alerts and the status information to the global centre. The global centre provides high-level intrusion detection based on alerts and reports collected across all units. The global centre can identify inconsistencies by applying stateful analysis and anomaly detection on the global view of the network. The global centre can identify:

1) Man-in-the-middle attacks (MITM): packets are diverted to a wrong destination,
2) Manipulation: inconsistency or data change in a packet at a point of the network,
3) Injection: packet identified that is not at the closest local unit of the originator,
4) Drop: if any packet has failed to arrive at the closest local unit of the destination.

The global centre also provides additional information such as original data that are manipulated, what devices are under attack, status of interested devices, etc. Intrusion resilience is enabled by integrating intrusion detection and resilient control, which interact to share information as shown in Fig. 3. The RCs are placed alongside devices to verify commands and are responsible for device protection. IDS alerts allow RCs to define and enact fine-grained policies against attacks and failures.

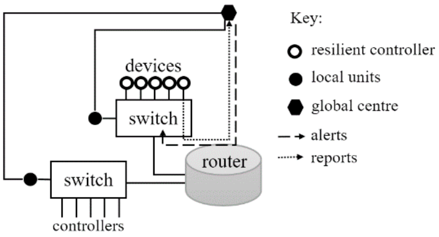

Fig. 3. Intrusion detection and resilience

Table 1. IDS alerts and RC actions.

Attacks		IDS (Alert to RC)	RC (Action)
Illegal Connection	Connection	Timestamp, IP/Port	Reject commands and disconnect the connection (if possible)
	Commands	Timestamp, IP/Port, Commands	Reject commands
	Disconnection	Timestamp, IP/Port	Apply normal rules
Man-in-the Middle (MITM)	Start	Timestamp, IP/Port/MAC	Disconnect the connection (if possible) and apply strict rules
	Manipulation	Timestamp, IP/Port/MAC, Original Commands	Reject manipulated commands and take the original commands
	Injection	Timestamp, IP/Port/MAC, Injected Commands	Reject injected commands
	Drop	Timestamp, IP/Port/MAC, Dropped Commands	Take the dropped commands
	Stop	Timestamp, IP/Port/MAC	Apply normal rules

Table 1 summarises examples of IDS alerts and RC actions. The IDS will alert an attack to relevant RCs. If possible, original data will be provided and RCs can determine whether to adopt the original data or not. By exchanging information between RCs and IDSs, the IDSs can keep track of the RCs’ evaluation of the droop laws and alert suspicious setpoints at an early stage. These interactions can be defined as rules depending on systems. The connection between the global centre and RCs enables reaction to attacks in the distribution grid to maintain voltage stability.

5 Testbed and Experiments

The testbed used to develop and validate the presented approach consists of a coupled simulation of a power distribution and communication grid infrastructure, linked to laboratory and field equipment [20]. This comprises three systems, shown in Fig. 4: a distribution grid simulation, a physical PV inverter, and a communication network.

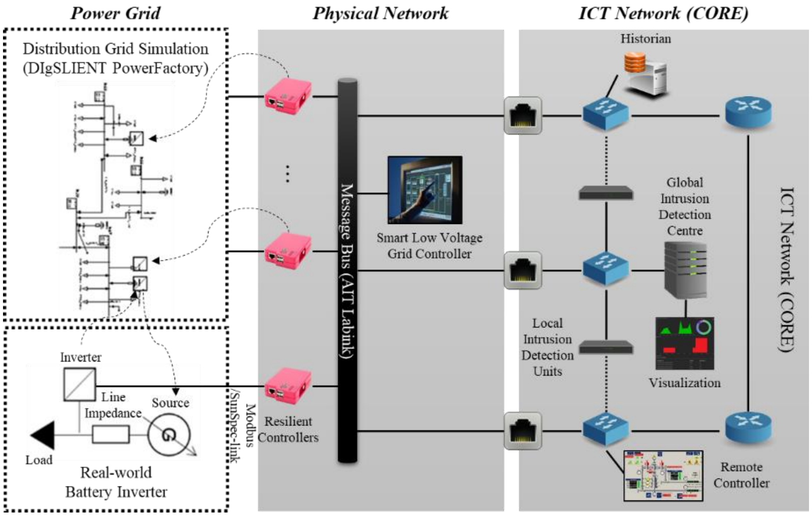

Fig. 4. Communication and power network setup used in the experiment.

DIgSILENT PowerFactory is used to simulate a rural distribution grid consisting of one medium to low voltage transformer, 13 households and 4 PV inverter systems. The PV systems are connected to the Smart Low Voltage Grid Controller (SLVGC) [21], which measures the remote voltage levels and creates reactive power setpoints in the form of *Q*(*U*) characteristics for the PV inverters. The distribution grid is simulated with typical household loads and typical PV generation of a sunny spring weekday. To assess the IDS and RC, a real battery inverter is integrated to the coupled simulation. The resulting Power-Hardware-in-the-Loop (PHIL) setup uses a three phase Spitzenberger & Spies power amplifier (G in Fig. 4), representing the grid connection point, controlled by voltage values from one of the simulated nodes. Two impedances (line impedance 240 mΩ, 480 µH and load impedance 70.5 Ω) connect the 2.5 kVA battery inverter to the power amplifier. This PHIL set-up is driven by the real-time PowerFactory simulation and also integrates the inverter into the communication system by its SunSpec communication interface. CORE and AIT Lablink are used to emulate the ICT network and the communication between power grid simulator and the real-world inverter. Under normal operation, the inverters feed (surplus) PV power to the distribution grid. In case the voltage at the feeding point rises over a certain point as specified in the droop law, reactive power is consumed to counteract the voltage rise. This experiment represents a distribution grid use-case with low load and strong PV generation. Like real low voltage distribution grids, the testbed is dimensioned so the default droop law voltages do not rise more than 3% over a nominal value of 230V.

5.1 Voltage Oscillation Attack

Experiments showed that a voltage oscillation attack can be triggered by an intruder by changing setpoints of the *Q*(*U*) characteristic sent from the SLVGC. The *Q*(*U*) curve of an inverter (Fig. 5 A) describes its voltage support behaviour. It tells the inverter the deviation of the phase angle between voltage and current – in this case proportional to the current node voltage. Depending on the impedance of the PV's connection point, the voltage can be influenced by changing this phase angle and the reactive power.

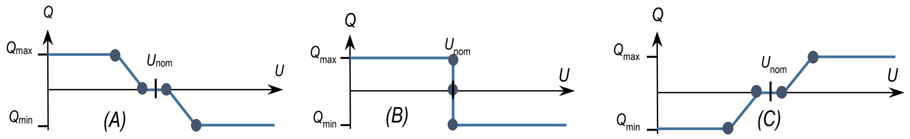

Fig. 5. Typical (A) and attacked *Q*(*U*) characteristics (B, C). The high gain in (B) causes oscillations, the inverted curve (C) results in amplification of voltage variations.

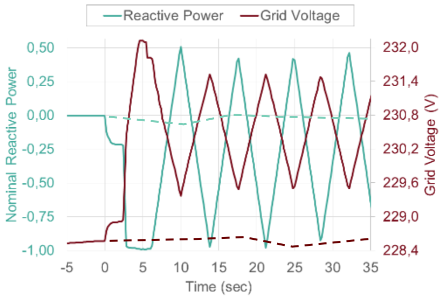

Fig. 6. Laboratory measured effects of the oscillating attack to the PHIL-connected inverter.

An attacker could aim to increase the characteristic gain of the inverter (B in Fig. 5), to cause local oscillation of the inverter around voltage V_0. To achieve this in the testbed, an MITM attack is executed with a custom written code that can intercept and modify

IEC 61850 messages to modify the gain settings. The effects of the reactive power oscillation and the grid voltage oscillation are depicted in Fig. 6. By implementing a RC locally at each PV, the oscillation attack can be prevented. Before applying the received $Q(U)$ droop law, it will be checked with Rule 1 and 2 of the RC (see Section 4.1). In case of the oscillation attack, the gain of the droop law approaches infinity and therefore it will trigger Rule 2, which checks the stability of the new droop law. When the Rule 2 is triggered the new droop law is rejected and the PV stays with its current droop law. Hence, the attack is automatically mitigated and no oscillations will occur (see dotted lines in Fig. 6). As the stability of a new droop law is judged based on local knowledge, less extreme gain settings which still result in oscillations can also be detected.

5.2 Over-Voltage Attack

The second attack scenario is caused by an MITM attacker who modifies the setpoints of the $Q(U)$ characteristic transmitted by the SLVGC controller. The attacked curve is depicted as (C) in Fig. 5. By inverting the reactive power curve in the inverters, a knowledgeable attacker could force any attacked inverters to revert their reactive power flow. This naturally leads to an omission of the voltage support and a further increase of an already high voltage. With knowledge of this system behaviour, an attacker could provoke such a situation in times of high PV infeed and thus lead the local voltage levels to exceed the voltage limits (e.g. EN 50160). This would cause the inverters to disconnect from the grid immediately. Fig. 7 shows the measured effects of this attack in the laboratory PHIL experiment. At time 0 – when the attack happens – the already high grid voltage rises even further because of the inverse reactive power characteristic. The physical inverter as well as the simulated inverters are attacked and contribute to the voltage rise with a time shift of around two seconds due to interface delays. It can also be seen how the observed physical inverter reduces its reactive power support as the voltage rises. After reaching a level of 253V, the physical inverter disconnects (or rather ramps down) after 1.2 seconds for safety reasons. This results in a sudden drop in voltage, which afterwards increases again due to the other attacked inverters.

The over-voltage attack has two critical consequences: it results in high grid voltages and a sudden loss of PV power. If many units are attacked, this can even have a strong impact on frequency stability. Depending on individual controller implementations of the PV units, it would also be possible to provoke large-scale active power oscillations. Using the interactions described in Table 1 (MITM “Manipulation”) the IDS detects the manipulated data in the network and provides alerts to the RC at the real-world inverter (Fig. 4, bottom right). Upon receipt of alert information, the RC will use stricter rules. In this experiment that means it will no longer accept new commands received through the network as long as the MITM attack is active. Here, the combination and interaction of IDS and RC preserves the grid operability and performance even though the attack was successful due to vulnerabilities in the cyber domain. Fig. 7 shows two different runs of the scenario. The solid lines show the previously described instabilities that occur when the attack is allowed to succeed. The dotted lines show continued normal operation, whereby the RC determines that it will ignore newly received setpoints based on alert information from the IDS.

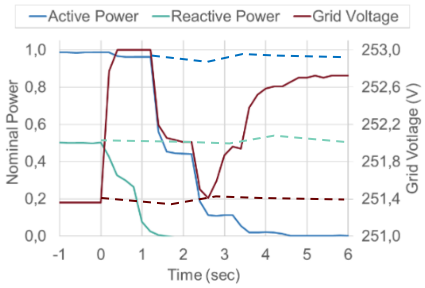

Fig. 7. Laboratory measured effects of the MITM attack to the PHIL-connected inverter. The attack happens at time 0.

6 Conclusion

Many new services are expected to emerge as the digitalization of energy infrastructure continues. It is essential that new services can be integrated without risking the resilient operation of the power system due to cyber vulnerabilities. As a result, there is a significant challenge to understand how cyber vulnerabilities might be used to compromise resilience, and to develop solutions to ensure stable operation when integrated IT systems are attacked. In this work, an intrusion resilience mechanism has been proposed towards enabling an automated response to cyber-attacks against a realistic distribution grid use-case. The use-case focuses on maintaining voltage stability in a distribution system that uses local control loops for remote configuration and monitoring to support local voltage control. The presented approach has been developed in a testbed comprising a distribution grid simulation, a communications network, and physical power system equipment. As shown in Section V, the testbed is highly realistic and combines IP-based real-world communication configurations with a mixed real-world and simulated power distribution setup. Contributions are made beyond studies such as [3] which focus on understanding the potential physical implications of advanced targeted attacks, without investigating mitigation. Contributions are also made compared to IRS solutions such as [13], aimed only at classic IT infrastructure. Finally, a practical solution is realized beyond the comprehensive, yet theoretical, investigations in cyber response and resilience technologies for smart grids presented by [14] and [15].

References

1. H. Lei, C. Singh, and A. Sprintson, “Reliability modeling and analysis of IEC 61850 based substation protection systems,” IEEE Trans. on Smart Grid, vol. 5, no. 5, Sep. 2014.
2. T. Athay, R. Podmore, and S. Virmani, “A practical method for the direct analysis of transient stability,” IEEE Trans. Power Apparatus and Systems, vol. PAS-98, no. 2, Mar. 1979.
3. A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, “Cyber-physical security testbeds: architecture, application, and evaluation for smart grid,” IEEE Trans. Smart Grid, vol. 4, no. 2, pp. 847–855, Jun. 2013.

4. C. W. Ten, J. Hong, and C. C. Liu “Anomaly detection for cybersecurity of the substations,” IEEE Trans. Smart Grid, vol. 2 no. 4, Dec. 2011.
5. C. G. Rieger, D. I. Gertman, and M. A. McQueen, “Resilient control systems: next generation design research,” in Proc. 2nd Conf. Human System Interactions, 2009, pp. 632–636.
6. D. I. Urbina, J. A. Giraldo, A. A. Cardenas, N. O. Tippenhauer, J. Valente. M. Faisal, J. Ruths, R. Candell, H. Sandberg, “Limiting the impact of stealthy attacks on industrial control systems,” in Proc. ACM SIGSAC Conf. Computer and Communications Security, 2016.
7. Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, “Detection of cyber attacks against voltage control in distribution power grids with PVs”, IEEE Trans. Smart Grid, vol. 7, no. 4, pp. 1824-1835, Jul. 2016.
8. A. Teixeira, K. Paridari, H. Sandberg, and K. H. Johansson, “Voltage control for interconnected microgrids under adversarial actions,” in Proc. IEEE 20th Conf. Emerging Technologies & Factory Automation (ETFA), Luxembourg, Sep. 2015.
9. B. Genge, D. A. Rusu, and P. Haller, “A connection pattern-based approach to detect network traffic anomalies in critical infrastructures,” in Proc. the 7th European Workshop on System Security, Apr. 2014.
10. Y. Yang, H. Xu, L. Gao, Y. Yuan, K. McLaughlin, and S. Sezer, “Multidimensional intrusion detection system for IEC 61850-based SCADA networks”, IEEE Trans. Power Delivery, vol. 32, no. 2, pp. 1068–1078, Apr. 2017.
11. M. Caselli, E. Zambon, and F. Kargl, “Sequence-aware intrusion detection in industrial control systems,” in Proc. 1st ACM Workshop on Cyber-Physical System Security, 2015.
12. H. Yoo, and T. Shon, “Novel approach for detecting network anomalies for substation automation based on IEC 61850,” Multimedia Tools and Applications, vol. 74, no. 1, Jan. 2015.
13. Z. Inayat, A. Gani, N. B. Anuar, M. K. Khan, and S. Anwar, “Intrusion response systems: foundations, design, and challenges,” J. Net. and Comp. App., vol. 62, pp. 53–74, Feb. 2016.
14. H. He and J. Yan, “Cyber-physical attacks and defences in the smart grid: a survey,” IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 13–27, Dec. 2016.
15. J. Qi, A. Hahn, X. Lu, J. Wang, C. Liu, “Cybersecurity for distributed energy resources and smart inverters,” IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, 2016.
16. X. Li, C. Zhou, Y. Tian, and Y. Qin, “A dynamic decision-making approach for intrusion response in industrial control systems,” IEEE Trans. Industrial Informatics, vol. 15, no. 5, pp. 2544–2554, May 2019.
17. F. D. Mango, M. Liserre, A. Dell’Aquila, “Overview of anti-islanding algorithms for PV systems. Part II: active methods,” in Proc. 12th Int. Power Electronics and Motion Control Conf., 2006, pp. 1884–1889.
18. F. Andrén, B. Bletterie, S. Kadam, P. Kotsampopoulos, and C. Bucher, “On the stability of local voltage control in distribution networks with a high penetration of inverter-based generation,” IEEE Trans. Industrial Electronics, vol. 62, no. 4, pp. 2519–2529, Aug. 2015.
19. H. K. Khalil, Nonlinear systems. 3rd Edition, Prentice Hall, 2002.
20. G. Lauss, F. Andrén, M. Stifter, R. Bründlinger, T. Strasser, K. Knöbl, and H. Fechner, “Smart grid research infrastructures in Austria: Examples of available laboratories and their possibilities,” in Proc. 13th Int. Conf. Industrial Informatics (INDIN), 2015, pp. 1539–1545.
21. A. Einfalt, A. Lugmaier, F. Kupzog, and H. Brunner, "Control strategies for smart low voltage grids - The project DG DemoNet -Smart LV Grid," in Proc. CIRED Workshop, 2012.