doi: 10.46793/EEE23-4.01S

Originalni naučni rad

UDK 004.451.52.056.5:621.316

Cyber Physical Security of Distributed Energy Resources

Sajber fizička bezbednost distribuiranih energetskih resursa

Luka Strezoski[*,], Zorana Babic[*], Dejan Milojicic[***]**

[*] Faculty of Technical Sciences, University of Novi Sad, Serbia

[**] DerMag Consulting International, Novi Sad, Serbia

[***] Hewlett Packard Labs, Milpitas, California, USA

Abstract - Huge amounts of data are coming from the electrical grid, through smart meters, smart inverters, and Supervisory Control and Data Acquisition (SCADA) protocols. This makes emerging power systems, and especially distribution grids, heavily dependent on real-time data from the field, as well as on the IT infrastructure for observation and control of field devices. As a consequence, emerging electrical systems are becoming fully digitized, cyber-physical systems with all the accompanying advantages and challenges. Such a power system is called a "Smart Grid". As all cyber-physical systems, Smart Grids are heavily dependent on Information and Communication Technology (ICT) infrastructure. Therefore, they are highly vulnerable to attacks that can compromise uninterrupted data flow, such as denial of service attacks and interruptions due to natural disasters, cataclysmic events, or wars, as well as due to malicious cyber-attacks.

In this paper, we summarize the state-of-the-art in the cyber-physical security of distributed energy resources (DERs). We explore pain points to which monitoring and control of DERs in emerging electrical systems are exposed due to malicious cyber-attacks. We continue with analyzing the accompanying consequences to the safety and reliability of emerging Smart Grids. Finally, we present our idea of Digital Twin technology as a tool for assisting distribution system operators and grid engineers, to detect, attenuate, and prevent malicious cyber-attacks in DERs.

Index Terms - Distributed energy resources, DERMS, Cyber security, False data injection, Microgrids

Rezime - Velike količine podataka pristižu iz električne mreže putem pametnih brojila, pametnih invertera i protokola za nadzor i akviziciju podataka (SCADA). To čini novonastale elektroenergetske sisteme, a posebno distributivne mreže, snažno zavisnim od podataka u realnom vremenu sa terena, kao i od IT infrastrukture za posmatranje i kontrolu uređaja na terenu. Kao posledica toga, novonastali elektroenergetski sistemi postaju potpuno digitalizovani, sajber-fizički sistemi sa svim pratećim prednostima i izazovima. Takav elektroenergetski sistem se naziva "Pametna mreža". Kao i svi sajber-fizički sistemi, Pametne mreže su u velikoj meri zavisne od infrastrukture informacionih i komunikacionih tehnologija (ICT). Stoga su izuzetno ranjive na napade koji mogu ugroziti neprekidan protok podataka, kao što su napadi odbijanja usluge i prekidi zbog prirodnih katastrofa, kataklizmičkih događaja ili ratova, kao i zbog zlonamernih sajber-napada.

U ovom radu sažimamo najnovija dostignuća u sajber-fizičkoj bezbednosti distribuiranih energetskih resursa (DER). Istražujemo kritične tačke na koje su osetljivi nadzor i kontrola DER-ova u novonastalim elektroenergetskim sistemima usled zlonamernih sajber-napada. Nastavljamo sa analizom pratećih posledica po sigurnost i pouzdanost novonastalih Pametnih mreža. Na kraju predstavljamo našu ideju tehnologije Digitalnog Blizanca kao alata koji može pomoći operatorima distributivnog sistema i inženjerima mreže u otkrivanju, ublažavanju i sprečavanju zlonamernih sajber-napada u DER-ovima..

Ključne reči - Distribuirani energetski resursi, DERMS, sajber bezbednost, injektiranje lažnih podataka, mikromreže

I INTRODUCTION

For over a century, electrical power systems were designed and operated in a traditional way: electrical energy was produced in bulk, by large fossil-fueled power plants, transmitted through a high-voltage network to distribution substations, and finally, distributed to end consumers through a passive distribution grid [1]. Thus, it was a one-way energy flow, with highly predictive conditions across the entire power system, able to be modeled with simple mathematical models, and with almost no need for any actions from operators in real-time. However, in the last two decades, we are witnessing a massive paradigm shift, mainly caused by the following three reasons:

1. Integration of huge amounts of renewable generation in an effort to decarbonize the electrical energy sector,
2. Decentralization of electrical energy production and introduction of distributed energy resources (DERs), such as solar photovoltaics (PVs), wind turbines, energy storages (ES), electric vehicles (EVs), etc., and
3. Digitization of control centers and automation of control and management processes, through the introduction of Energy Management Systems (EMS), Advanced Distribution Management Systems (ADMS), and Distributed Energy Resources Management Systems (DERMS) [2, 3].

These three points, especially decentralization and digitization parts, are transforming traditional power systems into highly complex, fully digitized systems. The role of grid operators is

required to evolve from (almost) passive observers to actively engaged participants, that must be alert and ready to react and actively manage highly dynamic grid conditions in real time.

This paradigm shift is also accompanied by huge amounts of data, coming from the grid to control centers through smart meters, smart inverters (by which most of DERs are connected to the grid), and Supervisory Control and Data Acquisition (SCADA) protocols. Therefore, emerging power systems, and especially distribution grids, are heavily dependent on real time data from the field, as well as on the IT infrastructure for observation and control of field devices, thus becoming fully digitized, cyber-physical systems with all the accompanying advantages and challenges. Such a power system is called a "Smart Grid" [4].

As all cyber-physical systems, Smart Grids are heavily dependent on Information and Communication Technology (ICT) infrastructure. Therefore, they are highly vulnerable to attacks that can compromise uninterrupted data flow, such as denial of service attacks and interruptions due to natural disasters, cataclysmic events, or wars, as well as due to malicious cyber-attacks.

Figure 1, at a high-level, summarizes potential avenues of cyber-attacks in a very complex Smart Grid ecosystem.

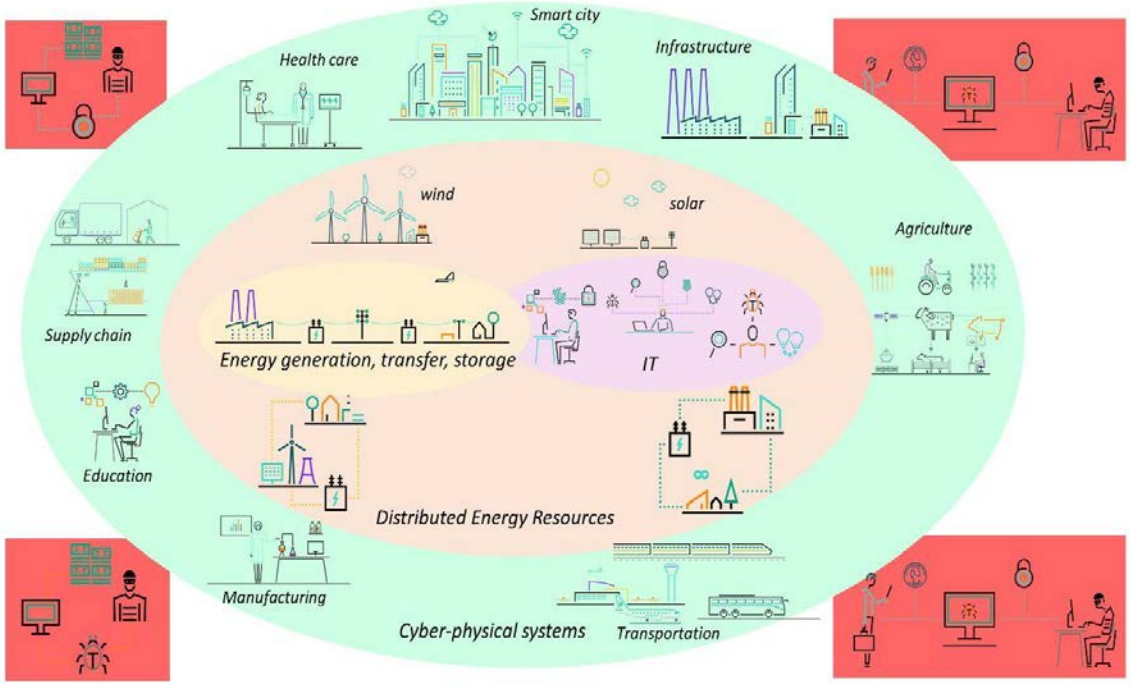

Figure 1. High Level Overview of Potential Cyber Attacks

Dangers from cyber-attacks on Smart Grids are even more attenuated by the fact that the electrical energy sector is one of the, if not the most critical sector for the existence and well-being of humanity. Cyber-attacks may cause extreme damages, such as blackouts of entire cities, and even countries, as recently witnessed in the 2015 Ukraine Blackout [5], false tripping by protective devices, and even cascade tripping of multiple devices, leaving catastrophic damages to the equipment as well as to the uninterrupted power supply to end customers, which would further cause high monetary penalties to be paid by electric utilities.

All of this could have been avoided if the utility personnel had been equipped with proper tools that would timely detect and deter the attacks. Thus, it is of critical importance to apply all the available knowledge and lessons learned from other sectors with longer experience in the cyber-physical world, to develop proper tools that will provide safety and reliability to the uninterrupted operation of emerging Smart Grids.

Therefore, the motivation of this research is to explore what has been accomplished so far in the field of cyber-physical security of DERs, to detect the main shortcomings of the available tools, and to consequently offer our viewpoint of how these shortcomings could be overcome.

The main goals of this paper are to:

1. Summarize the state-of-the-art in cyber-physical security of DERs;
2. Systematically list main vulnerability points to which DERs are exposed due to various types of cyber-attacks and their consequences on the reliability of Smart Grids; and
3. Propose a new avenue of research in applying a Digital Twin technology in developing tools for real-time detection, attenuation, and prevention of cyber-attacks in DERs.

After the Introduction, the rest of the paper is organized as follows. In Section II we briefly explain various DER technologies and types, as well as different communication channels through which utility control centers communicate with

DERs. We also identify the main points of attacks to which these communication channels are exposed. In Section III, we summarize the state-of-the-art in cyber-physical security of DERs, where we classify different types of cyber-attacks by the identified vulnerability points, as well as their consequences to the reliability of Smart Grids. In Section IV, we present our idea of applying a Digital Twin technology as a tool for distribution system operators (DSOs) and grid engineers, to detect, attenuate, and prevent malicious cyber-attacks in DERs. The paper is concluded in Section V.

II DER Types and Communication Infrastructure

A term DER can relate to various types of devices. First, every type of distributed generation (DG), such as solar panels, wind turbines, small hydro power plants, and combined heat and power (CHP) units, when connected to the distribution grid, are DERs. Further, different types of energy storage systems, such as batteries or flywheels, when connected to the distribution grid, are also DERs. Moreover, from a distribution system operator's (DSO's) perspective, electrical vehicles (EVs) and EV charging stations are DERs as well. In addition, increasing number of scholars, researchers, and industry experts consider demand response (DR) and Energy Efficiency (EE) programs as DERs [2]. Thus, as various novel and very different types of resources, with a completely different nature are considered DERs, they impose new challenges to which DSOs are not accustomed [2, 3].

Besides their widely different nature, DERs can also be divided to front-of-the-meter (FTM) and behind-the-meter (BTM) assets, which further dictates communication channels between a utility's control center and DERs. FTM DERs are mostly larger devices, ranging from several hundred kilowatts up to several megawatts, and in most cases are wired by SCADA systems. On the other hand, BTM DERs are small-scale devices (rooftop solar PVs, household batteries, EV chargers, etc.), which are not wired by SCADA and with which, in most cases, utilities communicate through 3rd party DER Aggregators using various internet protocols [2]. High level communication between a utility control center and various DER types, with identified points of possible cyber-attacks, are depicted in Fig. 2.

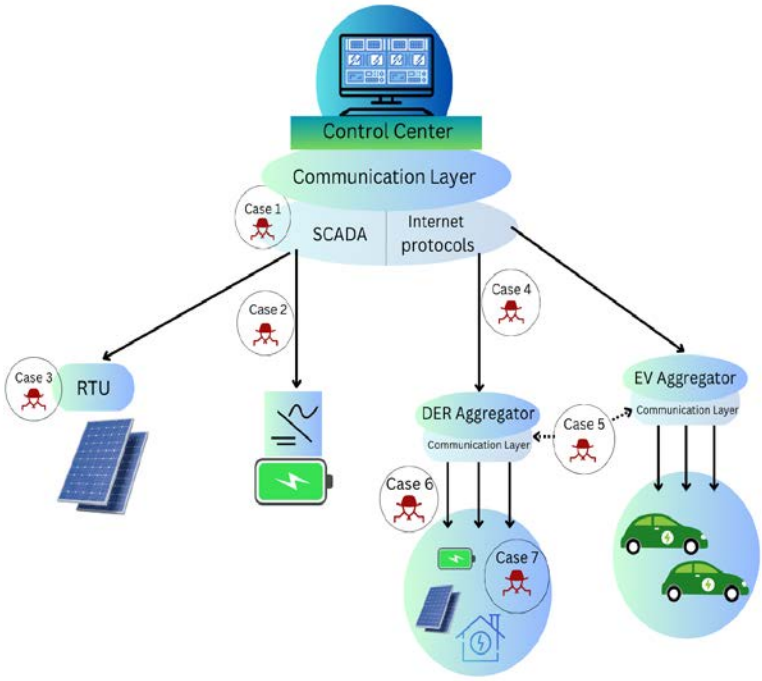

Figure 2. High Level Communication Between a Utility and DERs with Identified Points of Cyber-Attacks

As can be seen from Fig. 2, due to a very complex communication system between the utility control center and various DERs, multiple potential vulnerabilities to malicious cyber-attacks are identified. We classify them as follows:

- Case 1: Attackers gain access to the entire SCADA system or other communication systems inside the utility's control center,
- Case 2: Attackers interrupt communication network between SCADA and a FTM DER,
- Case 3: Attackers gain access to a FTM DER's remote terminal unit (RTU) or smart inverter,
- Case 4: Attackers interrupt communication network between a utility and a DER Aggregator,
- Case 5: Attackers gain access to a DER Aggregator's communication system,
- Case 6: Attackers interrupt communication network between a DER Aggregator and a BTM DER's smart inverter,
- Case 7: Attackers gain access to a BTM DER's local energy management system.

Following the identified cases of cyber-attacks on DERs, in the next section we discuss state-of-the-art in cyber-physical security

of DERs, summarizing various types of cyber-attacks, as well as how each of the identified attacks affects the security and reliability of DERs.

III State of the Art in Cyber-Physical Security of DER

A recent report by The US Department of Energy (DOE) [6], provides recommendations to integrate best practices for cybersecurity of Smart Grids, such as multi factor authentication, and encryption to enforce a zero-trust model. The report insists on the importance to implement the existing and standardized protocols for a secure communication with DERs. The authors claim that standardizing and adopting standardized protocols for communicating with DERs is of utmost importance, as the current situation with multiple vendors using a wide range of different protocols is not sustainable, as it is highly vulnerable to cyber-attacks. Besides direct communication with DERs, standardizing the communication protocols between the control center and DER aggregators is of a significant importance for the security and reliability of Smart Grids [2, 6]. The authors conclude that a key to develop and implement a robust cybersecurity communication standard for DERs is the involvement of industry, and leveraging the industrial experience in feasible implementation [6]. Further, it is important to take into consideration the geographical position of DERs when it comes to cybersecurity [7, 8]. Geographical and topological factors can influence the physical resiliency of DERs inside a distribution grid and/or microgrids, so besides the communication infrastructure, at remote locations, special care should be taken to physically securing DERs. J. Qi et al. detected challenges that increase the possibility of an attack, by increasing the number of smart inverters and battery controllers, spreading over many locations at different consumers [9]. These issues are mostly pronounced for BTM DERs that can be spread all over the grid [7-9].

The security in critical infrastructure (SCADA, ADMS, and/or DERMS) is the most critical case of attacks on DERs. For this case, it is important to adopt Intrusion Detection Systems (IDS). The modeling of IDSs becomes difficult with evolving of a critical infrastructure [10]. The IDSs can be divided into two categories: the first one is based on detecting known attacks and it is known as signature-based, while the second one relies on capturing deviation and detecting unknown attacks. The second category is known as anomaly-based. A. Khraisat et al. provide a review of emerging IDSs as well as an overview of datasets that are commonly used for developing the IDSs [10]. S. Ma et al. propose a Programmable Intrusion Detection method that relies on anomaly-based IDS, able to detect only known attacks [11]. J. T. Johnson et al. identify two-level vulnerabilities (device and cyber levels), such as poor firewall configuration and malicious firmware update, supply chain, weak encryption, etc. [12]. They presented an experiment for a hybrid IDS for DERs and concluded that a chance of detecting attacks increases when physical and cyber data are analyzed at the same time.

J. Qi et al. propose an attack-resilience framework for protecting power grid infrastructure from malicious cyber-attacks [13]. It is designed for cyber, physical, and utility layers, focusing on grid's reliability and stability. They provide a comprehensive summary of DER system architecture and divide it into four domains: DER devices and controllers (our Cases 3, 6, and 7, from the previous Section), distribution utility communication and control (Cases 1, 2, and 4), third parties (Case 5), and transmission operations (not in scope of this paper). The authors detect actors, interactions, and vulnerable points in every domain with an overview of frameworks and potential attacks, and conclude that the attacks on transmission and distribution communication infrastructure is the most critical (Case 1), followed by attacks on large-scale DERs (Cases 2 and 4). R. S. de Carvalho et al. summarize the most common types of attacks on DER communication infrastructure, which are: Man-in-the-middle, Replay, Eavesdropping, Spoofing, Denial of Service (DoS), and Brute force credentials [14]. The most commonly used protocols for communication with DERs, which are mostly vulnerable to these attacks are Modbus, DPN3, and SEP2. The authors conclude that Modbus and DNP3 are susceptible to all of the identified attacks, while the SEP2 is resilient to all of the attacks except the DoS and brute force credentials, as it implements cryptography. They conclude that the most dangerous class of attacks, which are also the hardest to detect, are all the attacks that implement False Data Injection Attack (FDIA) logic [14].

The FDIA, when combined with Replay attack, is extremely hard to detect as the operator in the control room is fed by the logically expected data, but recorded from some of the previous days or, for example, the same day from the previous week. Thus, if not timely detected, it can easily mislead the operator's awareness of the grid conditions. The consequences of this kind of an attack, especially directly to the control room (Case 1), can be disastrous, as it can lead to cascade tripping of protection equipment and consequently to blackouts of huge portions of an electrical grid [14]. G. Liang et al. provide a state-of-the-art summary of FDIA attacks on Smart Grids. The authors categorize research of FDIAs as theoretical, defensive, and application research. Like in [14], the authors conclude that FDIAs can have a disastrous impact on the Smart Grid, by disrupting the entire grid, potentially causing blackouts of huge amounts of customers.

Most of the papers in the available literature that deal with FDIAs start with the assumption that attackers know everything about the system. However, M. A. Rahman et al. present a realistic FDIA case, where attackers do not have all the information regarding the values of all the grid elements [16]. They further compare the influence on the grid, depending on the level of information about the grid elements that the attackers have. The authors conclude that an attack can be successful with the large impact on the grid reliability, if the attacker has the knowledge of admittance values for just a several lines. Thus, a comprehensive tool for detecting and attenuating attacks in real time is critically needed [17]. In the following, we summarize the existing tools for detecting and/or preventing cyber-attacks on DER infrastructure, categorizing these tools per the seven cases of cyber-attacks, identified in the previous section.

IIIA Existing Solutions to Cyber-Attacks on DER Infrastructure

M. Ganjkhani et al. propose an algorithm for detecting FDIAs that is based on a data centric paradigm [18]. This paradigm analyzes FDIAs focusing on data in physical and cyber layers with the goal of integrating these two layers. The proposed

algorithm is based on the margin setting for mitigating FDIAs. The algorithm deals with detecting FDIAs that occur in a direct communication with DERs, regardless of their sizes (Cases 2, 6, and 7). The authors discuss that the consequences of attackers interrupting the communication between the control center and large-scale DER (Case 2) can be serious, whereas Cases 6 and 7 are of a milder nature. Y. Huang et al. propose a real-time algorithm for detecting FDIAs in a direct communication with DERs [19]. The proposed algorithm has an advantage over the classical detection test as it can handle unknown parameters and process multiple measurements simultaneously, thus detecting multiple simultaneous attacks. These algorithms do not deal with attackers gaining access to the communication infrastructure inside the control room (Case 1).

Y. Li et al. provide an overview of different types of attacks on a device level [20]. The authors analyze attacks on a communication between the control center and a smart inverter on large-scale DERs (Case 2). Two types of attack are detected: 1) measurement-based attacks with a goal to change measurements and influence decisions that are made in the control center, and 2) command-based attacks that have a goal to block commands from the control center to the inverter. The authors conclude that both types of attacks, when successfully performed on large-scale DERs, can have serious consequences as the operator can be misled by false data, or a DER can be shut down without an actual need, leaving large portions of the grid (fed by a compromised DER) without power.

A. Majumdar et al. propose a centralized volt-var optimization (VVO), that considers a possibility of malicious attacks on DER monitoring and control processes [21]. The proposed VVO algorithm considers attacks on various levels of the distribution system, such as gaining access to SCADA (Case 1), interrupting communication between the control center and large-scale DERs (Case 2), and gaining access to a DER's RTU (Case 3). The authors propose two solutions for mitigating compromised data in VVO, the first being based on local voltage regulation controller set-points, and the other employing historical data and forecast information. The authors show that the proposed solutions successfully detect compromised data in VVO applications, improving the accuracy of voltage optimization in DERs.

N. Duan et al. analyze the impact of cybersecurity attacks on DERMS (Case 1) [22]. Two types of scenarios are presented. The first type sets malicious configuration on the DERMS that results in all the DERs being shut down. The second type is an embedded malicious code that disconnects DERs and disables them from receiving additional instruction serially and concurrently. Both of these types have two scenarios considering if an inverter is implemented with a delay or not. The authors conclude that these kinds of attacks (when attackers gain access to an entire DER management platform) are the most severe to the reliability of the Smart Grid, while regarding the two cases that they have analyzed, a larger impact on the system is when a delay on inverters is not implemented. The authors propose a co-simulation platform for analyzing the impact of cyber-attacks on DERMS, but do not propose a solution for detecting and attenuating attacks.

In [23-25], the authors use a hardware-in-the-loop (HIL) technology, as a platform to analyze consequences of potential cyber-attacks on DERs. J. Choi et al. propose a HIL testbed for testing cyber-attacks on power electronic devices [23]. Simulated attacks are based on exploiting vulnerabilities in the system including insecure network protocols and firmware updates. The testbed consists of a real-time system simulator with multiple solar inverters, using real-life communication protocols and cloud servers, simulating attacks between a DER Aggregator and the control center (Case 4). Two types of cyber-attacks are tested: an FDIA attack by modifying communication and a Packer Drop DoS attack. The FDIA attack is the most dangerous and if a compromised DER Aggregator consists of a large amount of small-scale DERs, a successful attack can have serious consequences to the reliability of the grid. J. Zhang et al. propose a HIL testbed that is built to simulate the harmonics of power electronic converters for cyber-physical security of inverter-based PV farms [24]. The authors observe three types of attacks on PV inverters: FDIA, Replay attack, and Delay attack. The authors consider that attackers gain access to inverter's controllers (Cases 3 and 7). Based on multiple performed simulations, the authors conclude that FDIA and Replay attacks, on large-scale DER (Case 3) may cause a blackout of a large DER, leaving multiple customers without power. J. Han et al. introduce a real-time simulation and HIL testing platform that is specifically designed for prototyping, demonstrating, and testing digital twins of DERs [25]. The authors show that the HIL can be successfully used as a real-time digital twin for DERs, providing accurate responses, indistinguishable from real DERs in the field.

N. Zivkovic et al. assume that attackers gain access to SCADA (Case 1) or an RTU (Case 3), or interrupt communication between SCADA and RTU (Case 2) [26]. The authors propose an algorithm to detect an FDIA attack, based on Kalman filter. The proposed algorithm relies on forecast results and the authors show that it is capable to detect false positives and to identify FDIA inside the control center. The proposed algorithm is meant to be used in a conjunction with the state estimation application, as a pre-step to filter bad data from malicious sources. However, [26] deals with transmission networks and the energy management system (EMS) inside the transmission system operator's control center. As the communication infrastructure and communication protocols used for transmission networks are different than the ones used in distribution grids for communication with DERs, the proposed algorithm may not be applicable for DERs.

IIIB Classification of Different Types of Cyber-Attacks on DERs

Based on a presented literature review, in Table 1 we classify the identified seven cases of cyber-attacks on DERs, per the severity and consequences on the reliability of Smart Grids.

As can be seen from Table 1, the most critical case is Case 1, followed immediately by Cases 2 and 4. The severity of Cases 3 and 5 depend on the size and energy supplied by a single large-scale DER and/or a group of smaller DERs being compromised. Finally, Cases 6 and 7 are mild, as their consequences are limited to a single customer on a low voltage grid.

Consequences of successfully performed attacks marked by Cases 1, 2, and 4 can be disastrous to the reliability of the entire Smart Grid, and thus a significant effort needs to be employed to develop proper tools for detecting and attenuating these attacks.

However, as can be seen from the literature review in this section, most of the authors so far focused on developing methodologies for detecting and/or blocking a single type of an attack, or on developing platforms for offline analysis of the consequences that potential cyber-attacks have on the reliability of DERs. There is a very limited set of proposed tools that would enable DSOs and grid engineers to detect, attenuate, and prevent any kind of a cyber-attack, for the most severe points of attack (Cases 1, 2, and 4 above), in real-time. Therefore, we are proposing a new avenue of research, in which we use a Digital Twin technology to develop a real-time tool for DSOs and grid engineers, that would help them to detect, attenuate, and prevent critical cyber-attacks that cause severe consequences to the Smart Grid's reliability. Our ideas are set forth in Section IV.

Table 1. Severity and Consequences of Various Cyber-Attacks on DERs

Severity	Cases	Consequences
Highly severe	1	Operator completely losses awareness of the conditions in the grid; Highly likely to cause maloperation of the control and protection equipment; Highly possible to cause blackouts of an entire distribution grid or of large parts of the grid by causing unwanted tripping of main protective devices.
Severe	2, 4	Likely to cause tripping of a group of DERs; Likely to cause a blackout of a large part of the grid supplied by compromised large DERs and/or group of smaller DERs; May cause undesired topology changes and transferring a compromised group of DERs to neighboring substations without an actual need; May cause overloads, voltage problems, and/or reverse power flows on neighboring substations.
Medium	3, 5	Likely to cause tripping of one large DER or a group of smaller DERs; Likely to cause a blackout of a smaller part of the grid supplied by a compromised DER; May cause undesired topology changes and transferring a compromised DER to neighboring feeders without an actual need; May cause overloads, voltage problems, and/or reverse power flows on neighboring feeders.
Mild	6, 7	Likely to cause loss of communication with a single BTM DER; Likely to cause loss of awareness of a small part of low voltage grid; May cause a blackout of a single low voltage customer.

IV Digital Twins for Cyber-Physical Security of DER

To develop a comprehensive solution for DSOs and grid engineers in the utility control centers to detect, attenuate, and prevent the most critical cyber-attacks on DERs (Cases 1, 2, and 4), we are proposing a novel tool based on a Digital Twin technology. Digital Twin is a commonly used tool in domains such as the IT [27], automotive [28], aerospace [29], and manufacturing [30], as well as in Power System industry, such as for testing new devices [31] and setting and coordination of the protective devices [32]. However, as per our knowledge, Digital Twin technology has not been thoroughly used for cyber-physical security of DERs. We see a significant opportunity in leveraging communication and IT infrastructure, as well as hardware-in-the-loop (HIL) technology. Thus, we are developing a comprehensive Digital Twin aimed for DSOs and grid engineers, for detecting, attenuating, and preventing cyber-attacks in DERs.

IVA Our Solution

Our solution is based on replicating the actual field with physical DER devices, into a Digital Twin environment using the HIL advancements. Further, we propose to connect the developed DT to actual DERs in the field, through industrial internet protocols for collecting real-time measurements. Furthermore, we are developing a State Estimation application that estimates the state in the field in real-time based on collected measurements, and provides a faithful replica of DER conditions in the field. Finally, our DT will be directly connected with the utility control center, which will consequently be able to provide means for DSOs and grid engineers to automatically compare the grid state as shown in their grid management software solutions, such as ADMS or DERMS, with the developed DT. Thus, if the data exchange between the utility control center and the field becomes compromised, or if attackers gain access to the entire SCADA system in the utility's control center, attacks will be detected through a discrepancy between the actual state as replicated by the DT and the false state of the grid conditions, calculated based on the compromised data in the control center. A high-level depiction of this idea is presented in Fig. 3.

To develop the proposed DT, we have used hardware-in-the-loop setup, depicted in Fig. 4. This setup consists of the HIL device marked with ① and the HIL software marked with ②. The HIL has its own library, with highly accurate models of all types of DERs on both levels (electrical part and signal processing part), marked with ③ in Fig. 4. Signal processing part of DERs' models from the HIL setup's software library can provide exactly the same response with the response obtained from real controller which can be connected to the HIL [32]. Thus, this HIL environment serves as a basis for our DT.

Further, we have developed a small 11-bus testbed microgrid in the HIL, that consists of different DER types and loads, as depicted in Fig. 5.

The testbed is currently being tested and thus far, it has provided satisfactory results, regarding the ability to accurately calculate conditions inside the microgrid, for different levels of load and DER production.

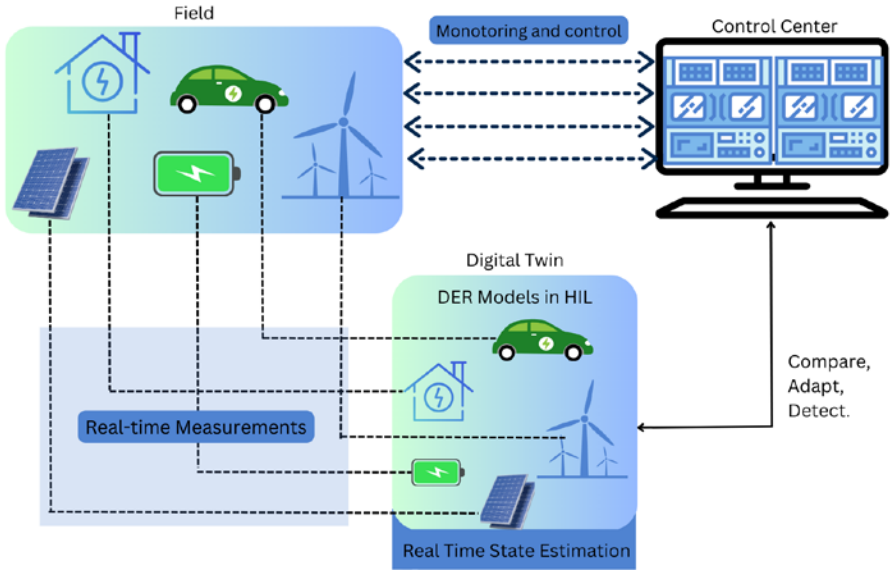

Figure 3. High Level Architecture of the Proposed Digital Twin for Cyber-Physical DER

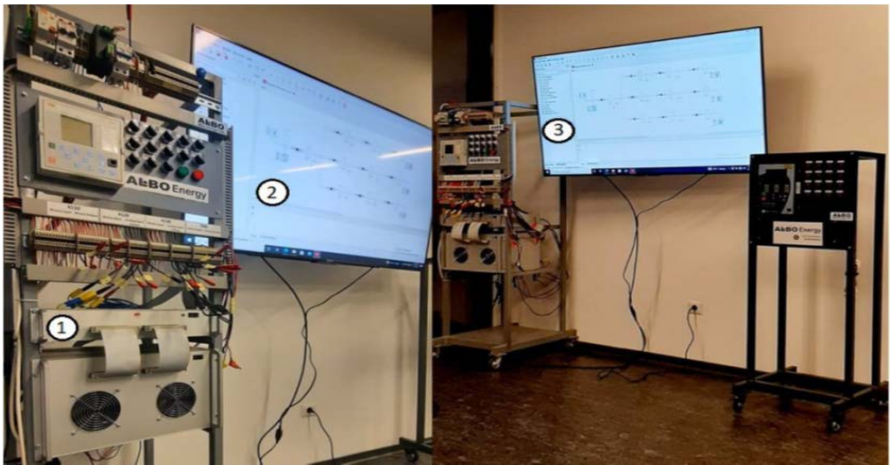

Figure 4. The HIL Setup for the Proposed DT

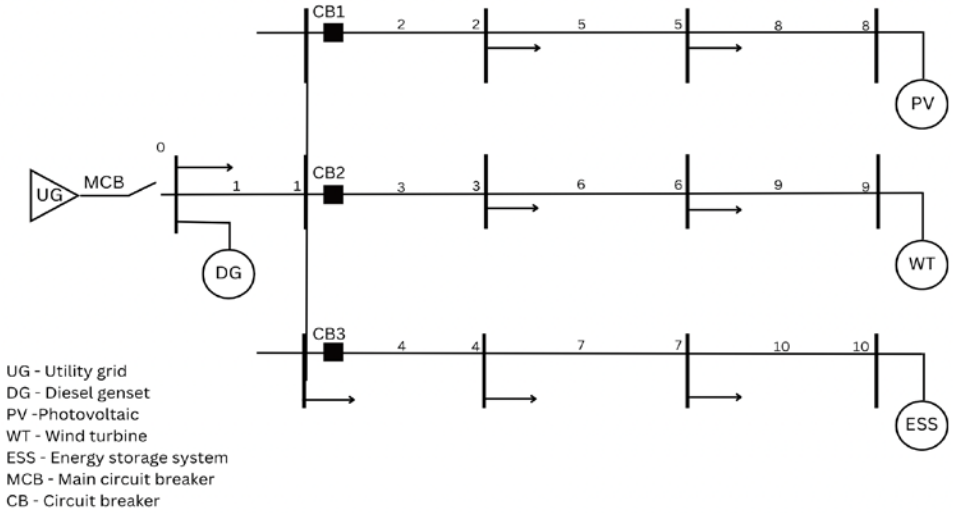

Figure 5. Microgrid Testbed

IVB Future Work

The next phases of this research will be oriented towards the following five directions:

1. Developing highly accurate models for all DER types and technologies, and connecting actual physical controllers to these models, in order to completely emulate DER behavior in our Digital Twin environment.
2. Developing a real-time State Estimation application, able to accurately estimate the conditions in the Smart Grid, based on a limited set of data coming from the field. Note that this is a challenging task, as the available set of measurement in distribution grids is much less than in traditional transmission networks, and novel algorithms are required [33].
3. Applying the State Estimation application on the Digital Twin in the HIL.
4. Connecting a developed Digital Twin to the field devices as well as to a DER Management software in the utility control center, as in Fig. 3.
5. Applying various cases of cyber-attacks on DERs and testing a developed Digital Twin for its ability to detect, attenuate and prevent malicious attacks.

In addition, we will evolve the degrees of Digital Twin evolution as follows [27]:

- Separate entities, serving as a replica of the grid state,
- Integrated with the physical instance, sharing some parts of the state,
- Coordinated with the physical instance, where some actions could be executed on either instance,
- Distributed system comprised of many instances of DERs and DT.

There are also different degrees of how tightly closed loops between digital and physical twins are, they could be synchronized upon events, or with different time periods. Depending on the time scale of the coupleness, there are different degrees of timeliness of the actions that could be undertaken.

Moreover, there are many techniques from IT that could be applied to DT in support of DERs. Applying AI techniques at the edge (DER) to reduce the amount of the state brought from PT to DT and at the DT for anomaly detection, is another direction of our future research.

In addition, some other IT techniques could be applied, such as root of trust at the DER and end-to-end supply chain management to make sure that all DERs and prevent compromises by deploying modified DERs.

Finally zones of trust could be introduced to delineate most critical equipment from those deployed at the very edge that may not be trusted at all.

V Conclusion

In this paper, we summarized the state-of-the-art in the cyber-physical security of DERs. We identified the main points of cyber-attacks on DERs, and based on the available literature sorted different cyber-attacks per their severity on the reliability of Smart Grids. We have concluded that direct attacks on the communication infrastructure inside a utility's control center (Case 1) is the most severe attack, followed immediately by attacks on the communication channels between a utility and FTM DERs and/or DER Aggregators (Cases 2 and 4). Regarding types of cyber-attacks, FDIAs combined with Replay attacks are the most dangerous, as these attacks may completely mislead the operator, causing unnecessary tripping of protective equipment and blackouts to large portions of the grid. Finally, we presented our idea of Digital Twin technology as a tool for distribution system operators and grid engineers, to detect, attenuate, and prevent malicious cyber-attacks, in real-time. The future directions of this research will be oriented towards actually developing the proposed Digital Twin, connecting it to DERs in the field, and to the DER management software inside a utility's control center, and implementing various types of attacks, to test and validate the applicability of the proposed tool.

Literatura/References

[1] Stevenson, W., Grainger, J. *Power System Analysis*. McGraw-Hill Education, 1994.

[2] Strezoski, L. Distributed energy resource management systems— DERMS : State of the art and how to move forward, WIREs Energy and Environment, Vol. 12, No. 1, e460, 2023. https://doi.org/10.1002/wene.460

[3] Strezoski, L., Padullaparti, H., Ding, F., Baggu, M. Integration of Utility Distributed Energy Resource Management System and Aggregators for Evolving Distribution System Operators, Journal of Modern Power Systems and Clean Energy, Vol. 10, No. 2, pp. 277-285, 2022, https://doi.org/10.35833/MPCE.2021.000667

[4] Li, Y., Yan, J. Cybersecurity of Smart Inverters in the Smart Grid: A Survey, IEEE Transactions on Power Electronics, Vol. 38, No. 2, pp. 2364-2383, 2023. https://doi.org/10.1109/TPEL.2022.3206239

[5] Liang, G., Weller, S. R., Zhao, J., Luo, F., Dong, Z. Y. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks, IEEE Transactions on Power Systems, Vol. 32, No. 4, pp. 3317-3318, 2017. https://doi.org/10.1109/TPWRS.2016.2631891

[6] Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid . https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf [pristupljeno 15.05.2023]

[7] Gan, H., Zhang, J., Wang, J., Hou, D., Jiang, Y., Gao, D.W. Cyber Physical Grid-Interactive Distributed Energy Resources Control for VPP Dispatch and Regulation, in Proc. *IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, Espoo, Finland, pp. 1-5, 18-21 October 2021. https://doi.org/10.1109/ISGTEurope52324.2021.9640131

[8] Sarker, P. S., Venkataramanan, V., Cardenas, D. S., Srivastava, A., Hahn, A., Miller, B. Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5, in Proc. *2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, Sydney, NSW, Australia, pp. 1-6, 21st April 2020. https://doi.org/10.1109/MSCPES49613.2020.9133689

[9] Qi, J., Hahn, A., Xiaonan, L., Jianhui, W., Chen-Ching, L. Cybersecurity for Distributed Energy Resources and Smart Inverters, IET Cyber-Physical Systems: Theory & Applications, Vol. 1, No. 1, pp. 28-39, 2016. https://doi.org/10.1049/iet-cps.2016.0018

[10] Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J. Survey of intrusion detection systems: techniques, datasets and challenges, Cybersecurity, Vol. 2, No. 1, 2019. https://doi.org/10.1186/s42400-019-0038-7

[11] Ma, S., Li,Y., Du, L., Wu, J., Zhou, Y., Zhang, Y., Xu, T. Programmable intrusion detection for distributed energy resources in cyber–physical networked microgrids, Applied Energy, Vol. 306, Part B, 118056, 2022. https://doi.org/10.1016/j.apenergy.2021.118056

[12] Johnson, J. T. *Cybersecurity for DERMS*, United States, 2019. https://www.osti.gov/servlets/purl/1645242

[13] Qi, J., Hahn, A., Lu, X., Wang, J., Liu, C.-C. Cybersecurity for distributed

energy resources and smart inverters, IET Cyber-Physical Systems: Theory & Applications, Vol. 1, No. 1, pp. 28-39, 2016. https://doi.org/10.1049/iet-cps.2016.0018

[14] de Carvalho, R. S., Saleem, D. Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources, in Proc. *2019 Resilience Week (RWS)*, San Antonio, TX, USA, 2019, pp. 226-231, 4-7 November 2019. https://doi.org/10.1109/RWS47064.2019.8972000

[15] Liang, G., Zhao, J., Luo, F., Weller, S. R., Dong, Z.Y. A Review of False Data Injection Attacks Against Modern Power Systems, IEEE Transactions on Smart Grid, Vol. 8, No. 4, pp. 1630-1638, 2017. https://doi.org/10.1109/TSG.2015.2495133

[16] Rahman, M.A., Mohsenian-Rad, H. False data injection attacks with incomplete information against smart power grids, in Proc. *2012 IEEE Global Communications Conference (GLOBECOM)*, Anaheim, CA, USA, pp. 3153-3158, 3-7 December 2012. https://doi.org/10.1109/GLOCOM.2012.6503599

[17] Sundararajan, A., Chavan, A., Saleem, D., Sarwat, A. A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security, Energies, Vol. 11, No. 9, pp. 2360, 2018. https://doi.org/10.3390/en11092360

[18] Ganjkhani, M., Fallah, S.N., Badakhshan, S., Shamshirband, S., Chau, K. A Novel Detection Algorithm to Identify False Data Injection Attacks on Power System State Estimation, Energies, Vol. 12, No. 11, pp. 2209, 2019. https://doi.org/10.3390/en12112209

[19] Huang, Y.,Tang, J., Cheng, Y., Li, H., Campbell, K.A., Han, Z. Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis, IEEE Systems Journal, Vol. 10, No. 2, pp. 532-543, 2016. https://doi.org/10.1109/JSYST.2014.2323266

[20] Li, Y., Yan, J. Cybersecurity of Smart Inverters in the Smart Grid: A Survey, IEEE Transactions on Power Electronics, Vol. 38, No. 2, pp. 2364-2383, 2023. https://doi.org/10.1109/TPEL.2022.3206239

[21] Majumdar, A., Agalgaonkar, Y.P., Pal, B.C., Gottschalg, R. Centralized Volt–Var Optimization Strategy Considering Malicious Attack on Distributed Energy Resources Control, IEEE Transactions on Sustainable Energy, Vol. 9, No. 1, pp. 148-156, 2018. https://doi.org/10.1109/TSTE.2017.2706965

[22] Duan, N., Yee, N., Salazar, B., Joo, J. -Y., Stewart, E., Cortez, E. Cybersecurity Analysis of Distribution Grid Operation with Distributed Energy Resources via Co-Simulation, in Proc. *2020 IEEE Power & Energy Society General Meeting (PESGM)*, Montreal, QC, Canada, pp. 1-5, 2-06 August 2020. https://doi.org/10.1109/PESGM41954.2020.9281757

[23] Choi, J., Narayanasamy, D., Ahn, B., Ahmad, S., Zeng, J., Kim, T. A Real-Time Hardware-in-the-Loop (HIL) Cybersecurity Testbed for Power Electronics Devices and Systems in Cyber-Physical Environments, in Proc. *2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, Chicago, IL, USA, pp. 1-5, 28 June -1 July 2021. https://doi.org/10.1109/PEDG51384.2021.9494202

[24] Zhang, J., Guo, L., Ye, J. Hardware-in-the-Loop Testbed for Cyber-Physical Security of Photovoltaic Farms, in Proc. *2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, Chicago, IL, USA, pp. 1-7, 28 June - 01 July 2021. https://doi.org/10.1109/PEDG51384.2021.9494258

[25] Han, J., Hong, Q., Feng, Z., Syed, M., Burt, G., Booth, C. Design and Implementation of a Real-Time Hardware-in-the-Loop Platform for Prototyping and Testing Digital Twins of Distributed Energy Resources, Energies, Vol. 15, No. 18, pp. 6629, 2022. https://doi.org/10.3390/en15186629

[26] Živković, N., Sarić A.T., Detection of false data injection attacks using unscented Kalman filter, Journal of Modern Power Systems and Clean Energy, Vol. 6, No. 5, pp. 847-859, 2018. https://doi.org/10.1007/s40565-018-0413-5

[27] Faraboschi, P., Frachtenberg, E., Laplante, P., Milojicic, D., Saracco, R. Digital Transformation: Lights and Shadows, Computer, Vol. 56, No. 4, pp. 123-130, 2023. https://doi.org/10.1109/MC.2023.3241726

[28] Damjanovic-Behrendt, V. A Digital Twin-based Privacy Enhancement Mechanism for the Automotive Industry, in Proc. *2018 International Conference on Intelligent Systems (IS)*, Funchal, Portugal, pp. 272-279, 25-27 September 2018. https://doi.org/10.1109/IS.2018.8710526

[29] Li, L., Aslam, S., Wileman, A., Perinpanayagam, S. Digital Twin in Aerospace Industry: A Gentle Introduction, IEEE Access, Vol. 10, pp. 9543-9562, 2022. https://doi.org/10.1109/ACCESS.2021.3136458

[30] Wang, Y., Kang, X., Chen, Z. A Survey of Digital Twin Techniques in Smart Manufacturing and Management of Energy Applications, Green Energy and Intelligent Transportation, Vol. 1, No. 2, 100014, 2022. https://doi.org/10.1016/j.geits.2022.100014

[31] Dufour, C., Soghomonian, Z., Li, W. Hardware-in-the-Loop Testing of Modern On-Board Power Systems Using Digital Twins, in Proc. *2018 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM)*, Amalfi, Italy, pp. 118-123, 20-22 June 2018. https://doi.org/10.1109/SPEEDAM.2018.8445302

[32] Strezoski, L., Simic, N. Quantifying the Impact of Inverter-Based Distributed Energy Resource Modeling on Calculated Fault Current Flow in Microgrids, International Journal of Electrical Energy & Power Systems, Vol. 151, 109161, 2023. https://doi.org/10.1016/j.ijepes.2023.109161

[33] Švenda, G., Strezoski, V., Kanjuh, S. Real-life distribution state estimation integrated in the distribution management system, International Transactions on Electrical Energy Systems, Vol 27, No 5, e2296, 2016. https://doi.org/10.1002/etep.2296

[34] Bresniker, K., Gavrilovska, A., Holt, J., Milojicic, D., Tran, T. Grand challenge: applying artificial intelligence and machine learning to cybersecurity, Computer, Vol. 52, No. 12, pp. 45-52, 2019. https://doi.org/10.1109/MC.2019.2942584

[35] Milojicic, D. The edge-to-cloud continuum, Computer, Vol. 53, No. 11, pp. 16-25, 2020. https://doi.org/10.1109/MC.2020.3007297

Autori/Authors

Luka Strezoski, PhD, associate professor, Faculty of Technical Sciences, University of Novi Sad, lukastrezoski@uns.ac.rs, ORCID 0000-0003-0109-4320

Zorana Babic, MS, assistant, Faculty of Technical Sciences, University of Novi Sad, zbabic@uns.ac.rs, ORCID 0000-0002-6453-3231

Dejan Miloicic, PhD, Distinguished Technologist, Hewlett Packard Labs, Palo Alto, CA, dejan.milojicic@hpe.com, ORCID 0000-0001-9830-8588