IEEE Open Access Journal of Power and Energy

Received 28 February 2024; revised 24 April 2024 and 13 June 2024; accepted 2 August 2024.
Date of publication 7 August 2024; date of current version 15 August 2024.

Digital Object Identifier 10.1109/OAJPE.2024.3439856

BESS-Set: A Dataset for Cybersecurity Monitoring in a Battery Energy Storage System

GIOVANNI BATTISTA GAGGERO[1] (Member, IEEE), ALESSANDRO ARMELLIN[1] (Graduate Student Member, IEEE), GIULIO FERRO[2] (Member, IEEE), MICHELA ROBBA[2] (Member, IEEE), PAOLA GIRDINIO[1], AND MARIO MARCHESE[1] (Senior Member, IEEE)

[1]Department of Electrical, Electronic and Telecommunications Engineering, and Naval Architecture (DITEN), University of Genoa, 16145 Genoa, Italy
[2]Department of Informatics, Bioengineering, Robotics and Systems Engineering, University of Genoa, 16145 Genoa, Italy
CORRESPONDING AUTHOR: G. B. GAGGERO (giovanni.gaggero@unige.it)

This work was supported in part by the Project Security and Rights in the Cyberspace (SERICS) under Ministero dell'Università e della Ricerca (MUR) National Recovery and Resilience Plan funded by European Union—NextGenerationEU under Grant PE00000014.

ABSTRACT Smart grids are nowadays featured by distributed energy resources, both renewables, traditional sources and storage systems. Generally, these components are characterized by different control technologies that interact with the generators through smart inverters. This exposes them to a variety of cyber threats. In this context, there is a need to develop datasets of attacks on these systems to evaluate the risks and allow researchers to develop proper monitoring algorithms. This paper addresses this need by presenting BESS-Set, an open-source dataset for cybersecurity analysis of a Battery Energy Storage System (BESS).

INDEX TERMS Dataset, cybersecurity, anomaly detection, smart grid, storage, distributed energy resources.

I. INTRODUCTION

IN THE rapidly evolving landscape of distributed energy resources (DERs) [1], Battery Energy Storage Systems (BESS) play a pivotal role in improving grid stability, energy efficiency, and overall reliability. As these systems become integral components of modern energy infrastructures, ensuring the robust cybersecurity of such assets becomes paramount. The relentless integration of digital technologies into energy systems has enabled unprecedented opportunities for efficiency gains but has also exposed these systems to emerging cybersecurity threats [2]. Cyberattacks targeting BESS jeopardize the reliability of energy storage and pose a significant risk to the stability of the broader power grid. Reference [3] presents a cyber attack scenario targeting DERS, in which the power output of the DER is manipulated to cause sustained oscillations or even system instability. Reference [4] also evaluates the impact of controlling a large number of DERs, but focusing on storage systems. Reference [5] show how it can violate voltage boundaries through cyberattacks on DERs on the CIGRE medium voltage benchmark grid. Reference [6] consider the case of electric vehicle charging for assessing the cyber attack's impact on that infrastructure.Reference [7] presents a review of the impacts of cyber attacks on the smart distribution grid. Also [8] propose a review of the state of the art regarding Cyber-Attacks in Power Systems, both from the impact perspective and detection and mitigation strategies. A growing body of literature highlights how attacks toward DERS can threaten the safety of the whole power system. The work proposed in [9] analyzes adversarial capabilities and objectives in attacking DER assets, showing how protocol and device-level vulnerabilities can result in cyberattacks impacting power system operations; authors also discuss mitigation strategies and future directions of DER cybersecurity research.

To fortify defenses against such threats, there is a critical need for data sets that facilitate developing and validating advanced cybersecurity monitoring and fault detection algorithms specific to BESS [10]. In response to this need, we present BESS-Set [11], a publicly accessible dataset

tailored for monitoring and fault detection in a BESS. Our dataset is composed of measures extracted by a BESS, serving as a representative example of the diverse challenges encountered in the realm of DERs. This compilation encompasses a broad spectrum of operational scenarios, capturing fluctuations in energy demand, varying environmental conditions, and potential anomalies indicative of cyber threats or system faults. By providing a public repository of these measures, our aim is to foster collaborative research and innovation in developing robust and resilient cybersecurity solutions tailored to the unique characteristics of BESS. We also made the Simulink model that we used to collect the dataset public. To the best of our knowledge, this is the first work that specifically provides a dataset for a BESS that considers the physical measures.

The paper is structured as follows. Section II-A introduces physics-based anomaly detection algorithms and analyzes related work regarding public cybersecurity datasets. Section III presents in detail the use case, including the system's architecture and the attacks carried out. Section IV presents the dataset in all its parts. Section V discusses some possible dataset usage. Finally, in Section VI, conclusions are drawn.

II. BACKGROUND

A. PHYSICS BASED ANOMALY DETECTION

Anomaly detection plays an important role in various fields, including cybersecurity, by identifying patterns in data that do not conform to expected behavior. These atypical patterns often signal critical incidents like security breaches, fraudulent transactions, or mechanical failures. Traditional approaches to anomaly detection for cybersecurity take data related to network traffic and/or logs generated by applications running on the nodes of the network as input only. Physics-based anomaly detection introduces a novel paradigm by leveraging domain-specific knowledge from physics to enhance the detection process. This approach is grounded in the understanding that many systems operate according to fundamental physical laws, especially in engineering and natural sciences. Incorporating these laws into the anomaly detection framework makes it possible to model system behaviors more accurately and identify deviations that signify anomalies. Physics-based models can offer several advantages over traditional approaches for cybersecurity monitoring and can operate together to obtain better visibility of the process. A literature review on physics-based anomaly detection is presented in [12]; the paper analyzes the works from different domains that usually do not interact, such as control theory, information security, and power systems, identifying the relationships between these fields and facilitating interactions among researchers of different disciplines. The paper also highlights the growing literature on the field. Newer approaches heavily rely on deep learning, which can help to face issues such as the growing volume of data and the need for domain-specific knowledge [13] Physics-based techniques are already employed in several scenarios in power systems. Reference [14] proposes a watchdog algorithm that involves continuous monitoring for irregularities in the execution times of relay algorithms and their related performance metrics. Reference [15] proposes an autoencoder-based anomaly detection algorithm for anomaly detection of a Battery Energy Storage System connected to the grid. This field of research is expanding thanks to the advancements in neural network techniques. A promising technique is the implementation of physics constraints between inputs in the optimization functions of a neural network; this technique is also called ''Physics-informed neural network [16]. For these reasons, it is reasonable to foresee a spread of the implementation of physics-based anomaly detection techniques for security monitoring of ICS [17]. In this context, the proposed BESS-Set could be a useful tool for cybersecurity research.

B. RELATED WORKS

Publicly available datasets are a very useful tool to promote research and allow non-experts of the specific field, such as machine learning engineers, to apply their methodologies and algorithms. In [18] the authors propose a methodology to generate reliable anomaly detection datasets in ICS, and then use the proposed method to generate a dataset of electric traction substations used in the railway industry, while [19] proposes a survey on the testbed and datasets of industrial control systems for security research; the survey focuses on datasets of industrial control systems traffic and their specific protocols but does not analyze the datasets related to the physical behavior of the processes. However, most of the data sets focus only on network traffic, not providing tools to develop physics-based anomaly detection algorithms. Reference [20] presents a dataset to support researchers in developing algorithms for Intrusion Detection Systems (IDS) based on artificial intelligence and machine learning techniques for the detection of attacks against Water Distribution; data are acquired from a hardware-in-the-loop Water Distribution Testbed developed by the authors. Generating a data set is very useful in promoting an integrated approach to developing monitoring algorithms. Finally, [21] analyzes typical distribution level substations and several of their critical electrical protection operation scenarios and simulates several cyber-attack scenarios; then, it presents the dataset with multiple traces that correspond to these scenarios to support cybersecurity research.

III. SIMULATION ENVIRONMENT

A. BATTERY ENERGY STORAGE SYSTEM

Battery storage systems encompass a variety of electric, electronic, and communication components. For our analysis, we focus on a typical scenario involving a storage system linked to a microgrid under the supervision of a SCADA system. From an electrical perspective, the system includes:

- Modules of cells (one or more), each equipped with its Battery Management System (BMS). The BMS

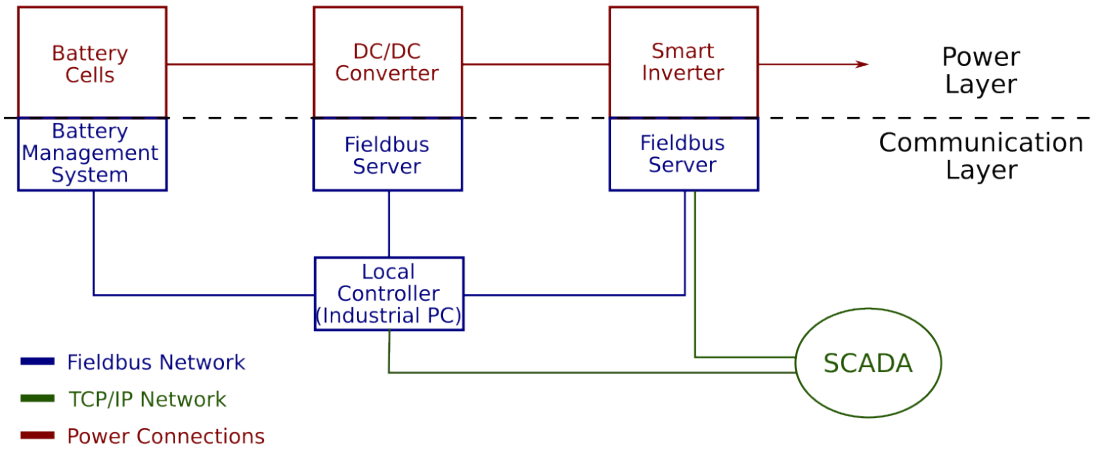


FIGURE 1. **Network architecture of the BESS.**

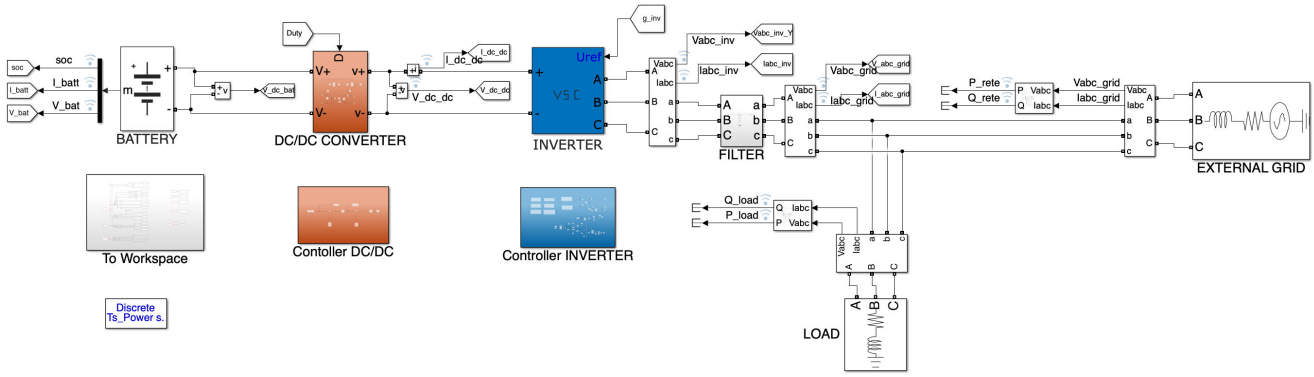


FIGURE 2. **Simulink model of the BESS.**

maintains safe voltage, current, temperature, and other physical parameters within the specified range.

- DC/DC converter: an electronic device that adapts the cell voltages to a level suitable for the Active Front End (AFE).
- Active Front End: an electronic converter that transforms direct current into three-phase alternating current (AC), facilitating bidirectional power flow.

The BMS, serving as an electronic system overseeing a rechargeable battery, performs key functions such as safeguarding the battery from unsafe operating conditions, monitoring its state, calculating secondary data, reporting information, controlling its environment, and authenticating and/or balancing it. Communication between the BMS and a higher-level controller occurs through various solutions, including serial communication protocols such as CANBus and Modbus and specific protocols and gateways in series [15].

Similar communication protocols are applicable to power electronic converters for intra-communication and interaction with a Process Control System (PCS), typically implemented by an industrial PC. The industrial PC interfaces between the SCADA system and local controllers. PCSs are equipped with a local Human Machine Interface (HMI) that facilitates interaction with monitoring and control functions. The overall scheme that comprehends electronic components, electrical connections, and communication channels is shown in Figure 1

A simulation model for storage systems has been developed, featuring different arrays of cells, a DC-DC boost converter, and an active front-end inverter, each equipped with its dedicated controller. The parameters of the BESS are the following: $V_{AC} = 230V$, (Voltage, single phase) $S = 60\ kVA$ (Power Capacity), $V_{DC} = 750V$ (Voltage DC), $f = 50Hz$ (frequency). The AFE is connected to the main grid with a three-phase connection. The model is electromagnetic in nature. The control strategy is structured with a straightforward feedback loop for the DC-DC converter, ensuring constant voltage at the DC link. A conventional control approach for the inverter is also applied, employing Park transformation. The entire system is implemented using MATLAB/Simulink software, leveraging the Simscape library [22]. Figure 2 illustrates the comprehensive Simulink schematic depicting the entire system.

TABLE 1. Features of the dataset.

Feature	Symbol	Description
X_1	SOC_t	battery state of charge estimated by the BMS
X_2	V_{cells}	voltage measured at the terminals
X_3	I_{cells}	current emitted by cells array
X_4	V_dc	average voltage in the DC link
X_5	V_a	voltage of phase a (AC side)
X_6	V_b	voltage of phase b (AC side)
X_7	V_c	voltage of phase c (AC side)
X_8	I_a	current of phase a
X_9	I_b	current of phase b
X_{10}	I_c	current of phase c
X_{11}	f_a	frequency of phase a
X_{12}	f_b	frequency of phase b
X_{13}	f_c	frequency of phase c
X_{14}	THD_a	total harmonic distortion of voltage on phase a
X_{15}	THD_b	total harmonic distortion of voltage on phase b
X_{16}	THD_c	total harmonic distortion of voltage on phase c
X_{17}	P	active power emitted by the inverter
X_{18}	$Pset$	last active power setpoint sent by the SCADA controller
X_{19}	Q	reactive power emitted by the inverter
X_{20}	$Qset$	last reactive power setpoint sent by the SCADA controller

We extract a series of measures, which are typical measures that the inverter exchanges with a SCADA system. The measures are detailed in Table 1

B. DETAILS OF THE ATTACKS

Several attacks can be carried out toward DERs. Reference [9] analyzes cyberattacks targeting DER assets on both the device and communication levels. We took as reference a simplified version of the taxonomy of attacks towards smart inverters in the smart grid provided by [23]. In particular, we distinguish three main categories of attacks:

- Bad Data Injection: in a bad data injection, the attacker can modify the commands that a controller sends to the inverter. Usually, the commands that can be sent to a smart inverter are related to the power setpoints (Active and reactive power setpoints, power factor, etc.). For example, the attack can be implemented through a Man-in-the-Middle attack on the communication network. Several commonly-used protocols (such as Modbus, IEC 61850 etc) do not present any authentication mechanism; therefore, the attack is even simpler and sufficient to inject a packet into the communication network.
- False Data Injection: in a false data injection, the attacker is able to modify the measures that the inverter sends to the main controller. In this case, any measure can be tampered through a Man-in-the-Middle attack, or simple packet injection, exploiting the vulnerabilities of communication protocols. The aim is to induce the central controller, for example a SCADA system, to make wrong decisions and, therefore, send wrong commands.
- Firmware Modification: in this case, the attacker can modify the internal functioning of the inverter, potentially controlling all the parameters of the power converter. The attack could be implemented by having physical access to the machine or remotely exploiting the vulnerabilities of other web services that the inverter may expose. In this case, the consequences may be much more severe: the attacker may modify different parameters of the power converter, for example, to modify the generated waveform, to cause problems to the local distribution grid.

This classification can be used regardless of the actual communication technology. For example, [24] shows the implementation of the Man-in-the-middle attack on an IEC 61850-base network, which is a commonly used standard for microgrids and for the control of DERs in general.

In our dataset, all the attacks have been carried out on the previously described simulation environment. In particular: the Bad Data Injection attack has been simulated through the modification of the setpoint parameters at the terminals of the inverter; the False Data Injection attack has been simulated through the artificial modification of the data saved from the model; the firmware modification attack has simulated through the modification of the code for the control of power converters.

IV. DATASET DESCRIPTION

The dataset is composed of 9 different parts, as shown in Table 2. The Table provides the names of the files in the publicly available repository, the dimensions of the dataset, and a brief description. The following subsection details all the datasets. In all the datasets, each line corresponds to an instant of system functioning under a 1-second sampling time. The training dataset does not contain any label, while the last column of the other datasets is the label (0 for normal behavior, 1 for anomaly).

As detailed in the next subsections, the attacks affect primarily the BESS or the grid at a local level (such as in voltage levels or power quality). Usually, a single generator cannot influence the distribution grid at a broader level,

TABLE 2. Resume of .csv dataset files.

File name	Dimension	Description
training.csv	30000x20	Normal behaviour (8 hour)
BDI_P_overlimit.csv	900x21	Bad Data Injection: P Exceeds Limits
BDI_Q_overlimit.csv	785x21	Bad Data Injection: Q Exceeds Limits
BDI_P_oscollation.csv	90x21	Bad Data Injection: P Oscillation
BDI_Q_oscollation.csv	90x21	Bad Data Injection: P Oscillation
FDI_P.csv	320x21	False Data Injection: P Tampering
FDI_SOC.csv	2360x21	FDI + BDI: SOC Tampering
FIRMWARE_THD_modification.csv	180x21	Firmware Modifications: Harmonics Tampering
FIRMWARE_Voltage_modification.csv	180x21	Firmware Modifications: V Battery Tampering

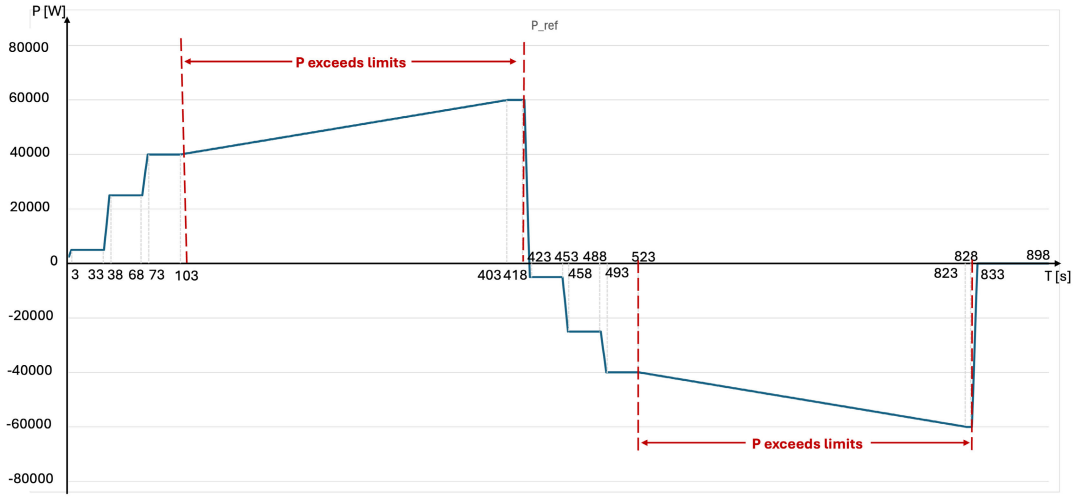


FIGURE 3. Bad data injection - P Exceeds Limits - P Trend.

due to the limited size of generation. Still, as discussed in Section I the control of multiple generators can significantly affect the grid. Therefore, a monitoring algorithm generated through the proposed dataset should be implemented for all the involved generators. Still, in some cases, the manipulation of a single generator can cause severe damage. These cases are mostly related to an islanded operation mode in microgrids, as pointed out in [25]. In these cases, it would be necessary to do a customized simulation, depending on the specific architecture of the microgrid.

A. NORMAL FUNCTIONING

The model simulates a complete cycle of charge and discharge of the battery, that lasts approximately 8 hours. During this time, the battery starts with a SOC of 95%, discharges up to 34%, and charges again to 95%. The active power varies between $+40kW$ and $-40kW$, while the reactive power varies between $+10kvar$ and 0 (it does not emit inductive power). The parameters of the network (voltages over the three phases) and control (voltages of the DC/DC link, of the battery, THD) remain approximately constant.

B. BAD DATA INJECTION - P EXCEEDS LIMITS

In this case, the attacker sends the wrong setpoint of active power to the inverter. In particular, the setpoint exceeds the limits that the model learned during training. In particular, after a period of normal functioning, starting from $+40kW$, the active power goes up following a ramp up to $+60kW$, which is a variation of $+50\%$ in respect to the limit. The same behavior is repeated for negative power: starting from $-40kW$, the active power goes down following a ramp up to $-60kW$, which is a variation of -50%. Figure 3 depicts the overall power trend.

The expected behavior of an anomaly detection algorithm is that the model generalizes the limits of the training dataset but recognizes significant variations concerning the normal performance, that is the behavior of the training dataset.

C. BAD DATA INJECTION - Q EXCEEDS LIMITS

During this attack, the attacker sends the wrong reactive power setpoint to the inverter. In particular, the setpoint exceeds the limits that the model learned during training. In particular, after a period of normal functioning, starting from $+10kW$, the reactive power goes up following a ramp up to $+15kW$, which is a variation of $+50\%$ in respect to the limit. A similar behavior is repeated for negative power: starting from 0, the active power goes down following a ramp up to $-5kW$, which is the same variation in the module of the ramp up. Figure 4 depicts the overall power trend.

FIGURE 4. **Bad Data Injection - Q Exceeds Limits - Q Trend.**

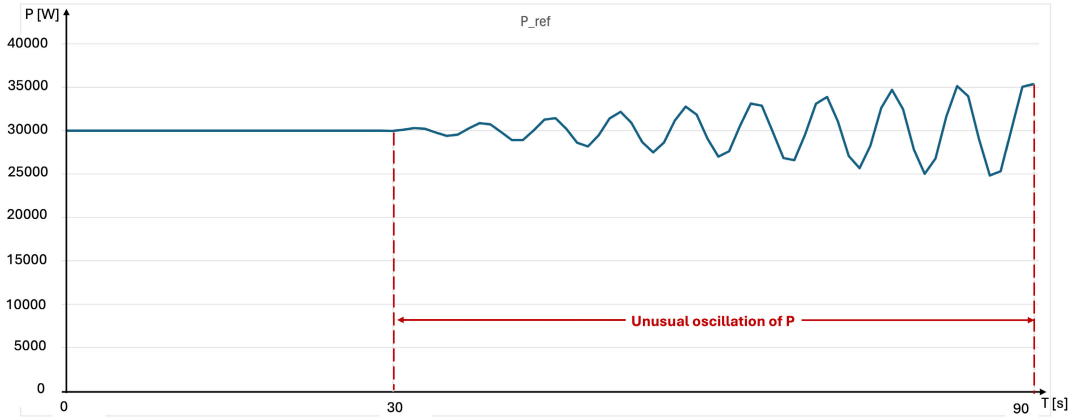


FIGURE 5. **Bad Data Injection - P Oscillations - P Trend.**

The expected actions of an anomaly detection algorithm is that the model generalizes the limits of the training dataset, but recognizes significant variations concerning the normal behavior, that is the behavior of the training dataset.

D. BAD DATA INJECTION - P OSCILLATIONS

This example represents an attacker that sends a wrong setpoint of active power to the inverter. In particular, the setpoint of the power continues to vary, producing an oscillation. This is the effect of partial Man-in-the-Middle attacks on different industrial communication protocols. Usually, the SCADA periodically sends the setpoint to the inverter, but it does not implement any authentication mechanism. If an attacker can send simply fake packets to the inverter, the two setpoints overlap; the physical consequence is that the inverter continues to believe to the last command received, producing an oscillation between the legitimate setpoint and the rogue one. We hypothesize that the rogue setpoint is a ramp, resulting in a sine wave multiplied by a ramp. Figure 5 depicts the overall power trend.

The expected behavior of an anomaly detection algorithm is that, after a few cycles, the algorithm recognizes the wrong trend (the wrong variation over time), that is not present in the training dataset (where the variations of power are simple ramps).

E. BAD DATA INJECTION - Q OSCILLATIONS

Like the active power case, the attacker sends the wrong reactive power setpoint to the inverter. In particular, the setpoint of the power continues to vary, producing oscillations. Similarly to the previous case, this is the effect of partial Man-in-the-Middle attacks on different industrial communication protocols. We make the hypothesis that the rogue setpoint is a ramp; therefore, the result is a sine wave multiplied by a ramp. Figure 6 depicts the overall power trend.

The expected behavior of an anomaly detection algorithm is that, after a few cycles, the algorithm recognizes the wrong trend (the wrong variation over time), that is not present in the training dataset (where the variations of power are simple ramps).

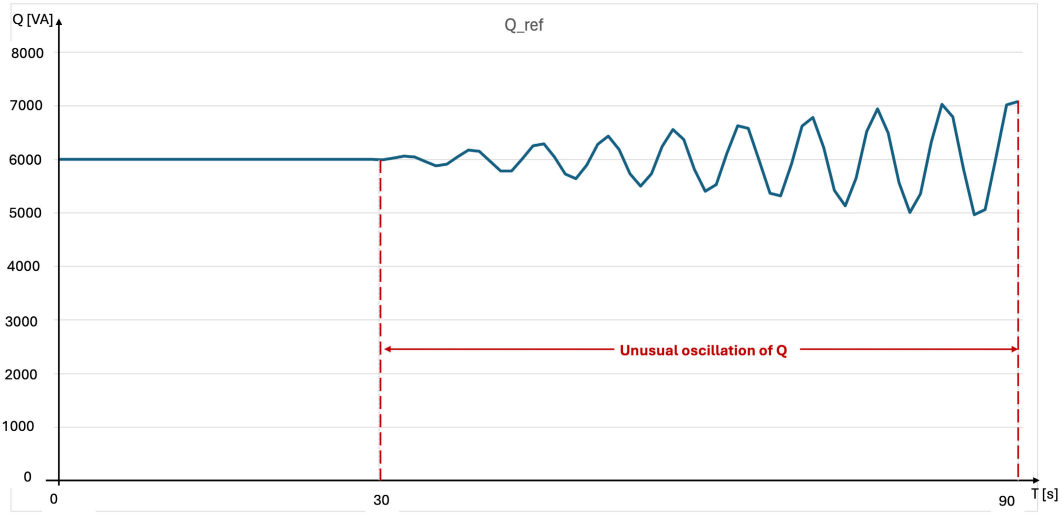


FIGURE 6. **Bad Data Injection - Q Oscillations - Q Trend.**

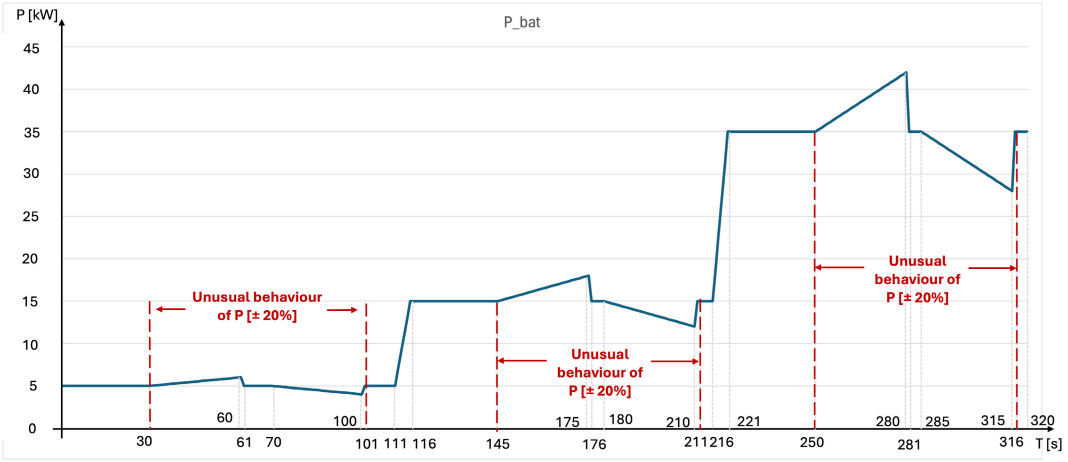


FIGURE 7. **False Data Injection - P Tampering - P trend.**

F. FALSE DATA INJECTION - P TAMPERING

During this attack, the attacker can modify the power injection measure that the inverter sends to the SCADA. This can be achieved through a Man-in-the-Middle Attack. We assume that the attacker can modify only a subset of measures per time; in this case, it modifies only the active power measure. This results in an impossible vector of measures: after the attack, the active power that the SCADA receives is not coherent with the measures of current and voltages (in particular, is not the vector product of voltages and currents). We simulated three orders of magnitude of the attack. In particular, starting from three setpoints ($5kW$, $15kW$ and $25kW$), the power increases and subsequently decreases as a ramp, reaching a value of $\pm 20\%$ of the real value. Figure 7 shows the overall trend of active power.

The expected behavior of an anomaly detection algorithm is that it promptly recognizes the attack since the vector of measures produced by the attack represents a physically impossible functioning.

G. FDI + BDI - SOC TAMPERING

During this attack, the attacker is able to modify the measure of the SOC that the inverter sends to the SCADA. This can be achieved through a Man-in-the-Middle Attack. We conjecture that the attacker can modify only a subset of measures per time; in this case, it modifies only the SOC measure. This results in an impossible vector of measures: in fact, after the attack, the variation over time of the SOC that the SCADA receives is not coherent with the measures of current and voltages (in particular, the SOC does not increase or decrease by the product of power over time, both in the DC and AC parts of the system). In particular, the SOC varies as follows: in the first phase, the SOC decreases more slowly than the real value; then, it increases while the battery discharges.

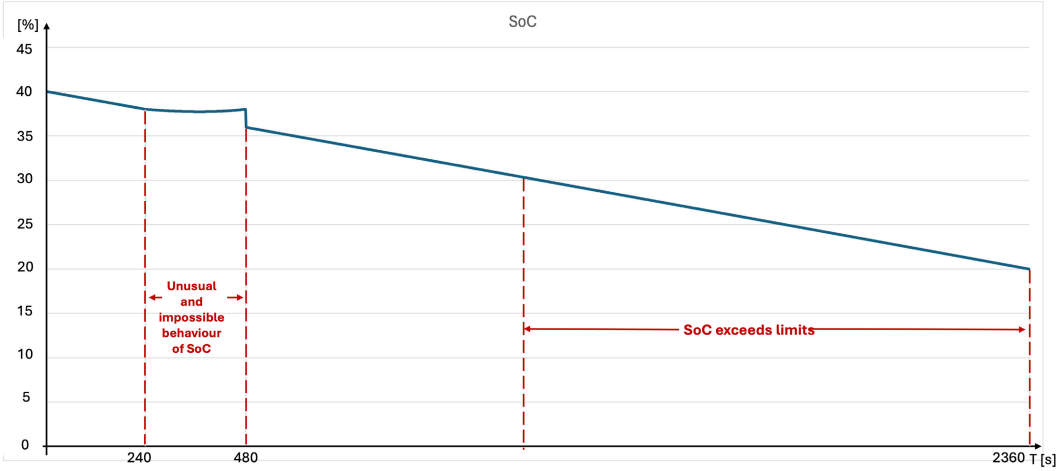


FIGURE 8. **FDI + BDI - SOC Tampering - SOC Trand.**

From a numeric point of view, there is an increasing distance between the real value and the integral of the power over time. In the second phase, following a ramp, the SOC exceeds the training dataset's limits. We expect that the inverter has a safety function that prevents the battery from operating outside the safe limits of charging of the cells. Therefore, it is impossible that the system is operating, for example, at 20% of the SOC, while the limit has been established during training at around 35%. In this case, from a numeric point of view, the error resides in exceeding the usual limits.

The expected behavior of an anomaly detection algorithm is that it promptly recognizes the attack, since the vector of measures produced by the attack represents a physically impossible functioning over time.

H. FIRMWARE MODIFICATIONS - HARMONICS TAMPERING

During this attack, the attacker can modify the internal functioning of the inverter; in particular, the attack can modify the waveform produced by the inverter. We make the hypothesis of injecting an additional harmonic to the sine waveform. The magnitude of the harmonic increases by five steps. Since the first step, the THD has exceeded the power quality limits defined by the IEEE 519-2022 Standard. This choice is to produce an attack that can be distinguished by noise and would effectively impact the grid. Then, the value further increases, as detailed in Figure 9.

The expected behavior of an anomaly detection algorithm is that it promptly recognizes the attack, since some measures significantly vary, in particular the THD of the voltage in all three phases.

I. FIRMWARE MODIFICATIONS - V BATTERY TAMPERING

During this attack, the attacker can modify the internal functioning of the inverter; in particular, the attack can modify the control of the DC/DC converter. This can be particularly dangerous, since it may result in dangerous working conditions of the cells, that can damage them. The magnitude of the variation increases by five steps, as shown in Figure 10.

The expected behavior of an anomaly detection algorithm is that it promptly recognizes the attack, since some measures significantly vary, in particular, the Voltage of the Battery and the Voltage of the DC/DC link.

V. USAGE OF THE DATASET

The dataset showed the effects on the electrical measures of a cyberattack targeting a battery storage system connected to the grid. Therefore, it can be used for multiple purposes:

- Evaluate the risk associated with cyberattacks: the model and the dataset can be used during a risk assessment phase to quantify the effects of a cyberattack. While different works have taken into account the vulnerabilities associated with smart inverters, it is usually hard to quantify the risk. The dataset can be used to quantify the effects of a potential attack: for each attack described in Section III-B the dataset provides the trend of each critical measure of the system. Moreover, it is possible to customize the simulation through the direct use of the model, that has been published together with the dataset.
- Developing proper electrical protections: the possibility of using electrical protection functions as an incident response tool will be an innovative field of research. Power system engineers may decide to implement different protection functions on the relay to guarantee the system's safety under cyberattacks properly. The dataset quantitatively provides the effects of cyberattacks, allowing engineers to set the protections appropriately.
- Developing physics-based anomaly detection algorithms: the main purpose of the dataset is to develop algorithms able to identify all the possible attacks that can be done on a BESS. Physics-based anomaly detection is a promising field of research, as discussed

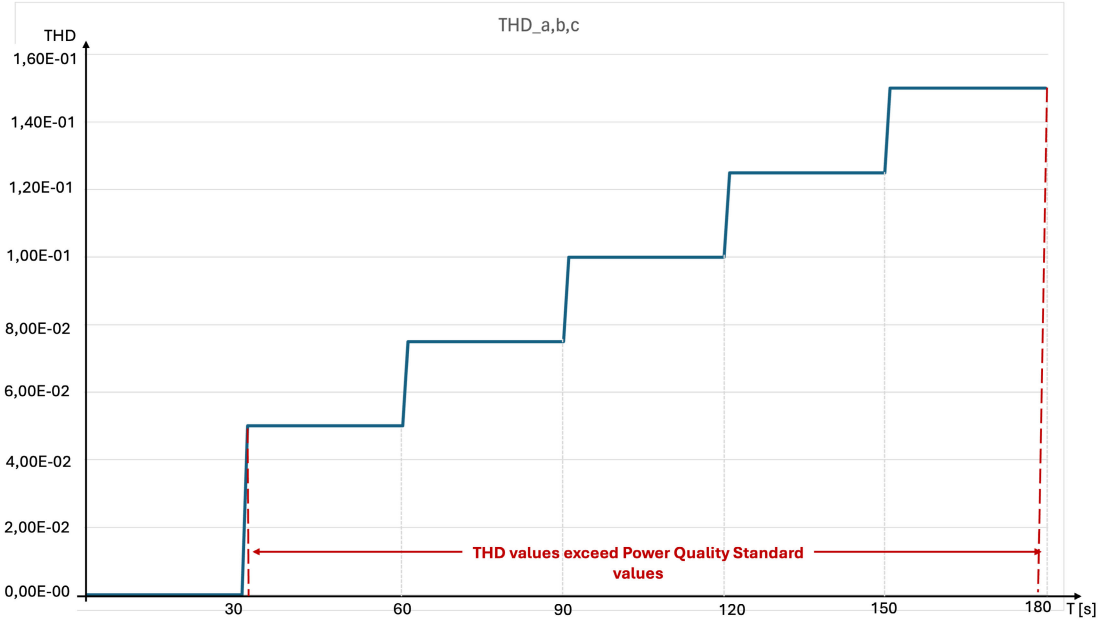


FIGURE 9. **Firmware Modifications - Harmonics Tampering - THD Trend.**

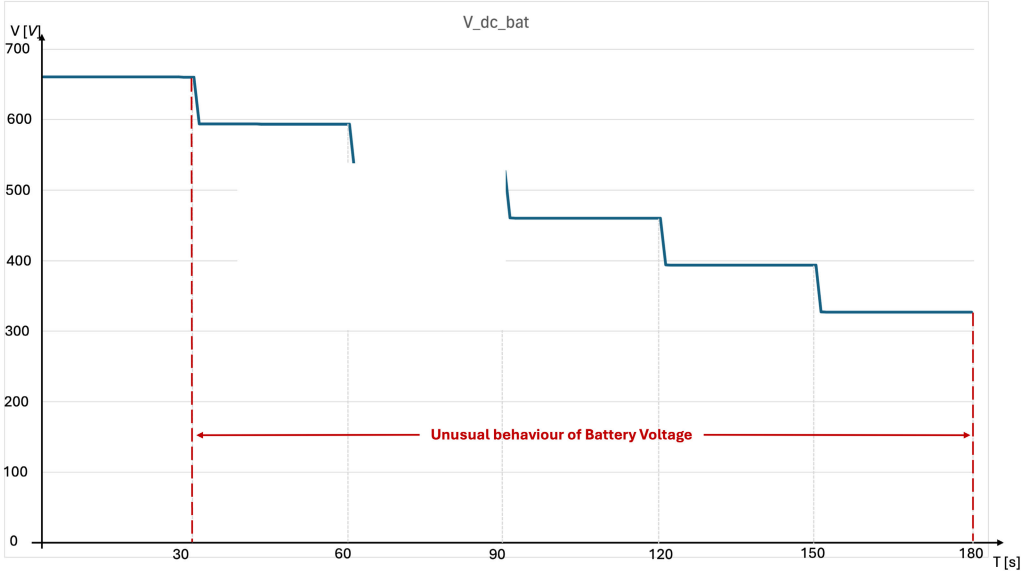


FIGURE 10. **Firmware Modifications - V Battery Tampering - V Battery Trend.**

in Section II-A. The dataset allows machine learning experts to work on a new use case: in particular, providing labeled datasets allows testing monitoring algorithms for machine learning researchers who do not have a power system background. The development of datasets for monitoring industrial control systems is particularly important to exploit the interdisciplinary competencies of researchers.

The set of features described in Table 1 has been chosen after an analysis of manuals of the commercial inverters' communication modules, and comprehends all the most common exchanged measures and commands. Therefore, BESS-Set allows testing algorithms before their actual implementation on the field for a wide range of commercial inverters; in case a product produces a smaller set of measures, it is possible to remove the unused features from the dataset and use the remaining.

VI. CONCLUSION

This paper presented BESS-Set, an open-source dataset of a BESS under cyberattack. The dataset and the Simulink model are publicly available for the scientific community [11]. The

aim is to help the scientific community produce results in the field of cybersecurity of DERs; in particular, the dataset can be used to develop physics-based anomaly detection algorithms, representing a promising field of research for enhancing the security of the Smart Grid.

REFERENCES

[1] Z. Zheng, M. Shafique, X. Luo, and S. Wang, "A systematic review towards integrative energy management of smart grids and urban energy systems," *Renew. Sustain. Energy Rev.*, vol. 189, Jan. 2024, Art. no. 114023.

[2] G. B. Gaggero, D. Piserà, P. Girdinio, F. Silvestro, and M. Marchese, "Novel cybersecurity issues in smart energy communities," in *Proc. 1st Int. Conf. Adv. Innov. Smart Cities (ICAISC)*, Jan. 2023, pp. 1–6.

[3] R. Bhattarai, S. J. Hossain, J. Qi, J. Wang, and S. Kamalasadan, "Sustained system oscillation by malicious cyber attacks on distributed energy resources," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2018, pp. 1–5.

[4] M. Tuttle, M. Poshtan, T. Taufik, and J. Callenes, "Impact of cyber-attacks on power grids with distributed energy storage systems," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2019, pp. 1–6.

[5] P. Linnartz, A. Winkens, and S. Simon, "A method for assessing the impact of cyber attacks manipulating distributed energy resources on stable power system operation," in *Proc. IEEE PES Innov. Smart Grid Technol. Eur. (ISGT Europe)*, Oct. 2021, pp. 01–05.

[6] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Comput. Secur.*, vol. 112, Jan. 2022, Art. no. 102511.

[7] T. O. Olowu, S. Dharmasena, A. Hernandez, and A. Sarwat, "Impact analysis of cyber attacks on smart grid: A review and case study," in *New Research Directions in Solar Energy Technologies*. Singapore: Springer, 2021, pp. 31–51.

[8] N. Tatipatri and S. L. Arun, "A comprehensive review on cyber-attacks in power systems: Impact analysis, detection, and cyber security," *IEEE Access*, vol. 12, pp. 18147–18167, 2024.

[9] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *IEEE Syst. J.*, vol. 17, no. 4, pp. 6695–6709, Dec. 2023.

[10] J. Dai, W. Chen, and X. Zhou, "Fuzzy high order differentiator observer based resilient control for distributed battery energy storage systems against unbounded FDI attacks," *IET Control Theory Appl.*, Jan. 2024, doi: 10.1049/cth2.12622. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/cth2.12622

[11] *BESS-Set*. Accessed: Feb. 26, 2024. [Online]. Available: https://ieee-dataport.org/documents/bess-set

[12] J. Giraldo et al., "A survey of physics-based attack detection in cyber-physical systems," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–36, Jul. 2019.

[13] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, "Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities," *ACM Comput. Surv.*, vol. 54, no. 5, pp. 1–36, Jun. 2022.

[14] H. Tarazi, S. Sutton, J. Olinjyk, B. Bond, and J. Rrushi, "A watchdog model for physics-based anomaly detection in digital substations," *Int. J. Crit. Infrastruct. Protection*, vol. 44, Mar. 2024, Art. no. 100660.

[15] G. B. Gaggero, R. Caviglia, A. Armellin, M. Rossi, P. Girdinio, and M. Marchese, "Detecting cyberattacks on electrical storage systems through neural network based anomaly detection algorithm," *Sensors*, vol. 22, no. 10, p. 3933, May 2022.

[16] M. J. Zideh, P. Chatterjee, and A. K. Srivastava, "Physics-informed machine learning for data anomaly detection, classification, localization, and mitigation: A review, challenges, and path forward," *IEEE Access*, vol. 12, pp. 4597–4617, 2024.

[17] D. I. Urbina et al., "Survey and new directions for physics-based attack detection in control systems," Dept. U.S. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST GCR 16-010, 2016.

[18] Á. L. P. Gómez et al., "On the generation of anomaly detection datasets in industrial control systems," *IEEE Access*, vol. 7, pp. 177460–177473, 2019.

[19] M. Conti, D. Donadel, and F. Turrin, "A survey on industrial control system testbeds and datasets for security research," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2248–2294, 4th Quart., 2021.

[20] L. Faramondi, F. Flammini, S. Guarino, and R. Setola, "A hardware-in-the-loop water distribution testbed dataset for cyber-physical security testing," *IEEE Access*, vol. 9, pp. 122385–122396, 2021.

[21] P. P. Biswas, H. C. Tan, Q. Zhu, Y. Li, D. Mashima, and B. Chen, "A synthesized dataset for cybersecurity study of IEC 61850 based substation," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2019, pp. 1–7.

[22] Mathworks, Natick, MA, USA. (2022). *MATLAB Version: 9.13.0 (R2022B)*. [Online]. Available: https://www.mathworks.com

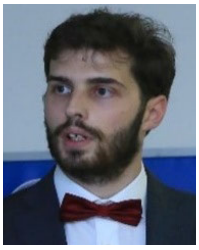
[23] Y. Li and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Trans. Power Electron.*, vol. 38, no. 2, pp. 2364–2383, Feb. 2023.

[24] M. M. Roomi, S. M. S. Hussain, D. Mashima, E.-C. Chang, and T. S. Ustun, "Analysis of false data injection attacks against automated control for parallel generators in IEC 61850-based smart grid systems," *IEEE Syst. J.*, vol. 17, no. 3, pp. 4603–4614, Sep. 2023.

[25] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, "Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems," *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1330–1339, May 2017.

GIOVANNI BATTISTA GAGGERO (Member, IEEE) received the M.Sc. degree in electrical engineering and the Ph.D. degree in electronic and telecommunication engineering from the University of Genoa. He is currently an Assistant Professor with the Satellite Communications and Heterogeneous Networking Laboratory, University of Genoa. He is also the CEO of the spinoff of the University of Genova and AIrFIELD Security srl. His research interests include network security of industrial control systems, microgrids, and smart grids.

ALESSANDRO ARMELLIN (Graduate Student Member, IEEE) received the master's degree in electrical engineering from the University of Genoa, in March 2021. He is currently pursuing the Ph.D. degree with the Satellite Communications and Heterogeneous Networking Laboratory (SCNL), University of Genoa. He collaborates with IREN SpA that is a relevant Italian energy company. His research interests include cybersecurity of industrial control systems, microgrids, and smart grids.



GIULIO FERRO (Member, IEEE) received the B.S. degree in industrial engineering, the M.S. degree in power systems engineering, and the Ph.D. degree in systems engineering from the University of Genoa, Italy, in 2014, 2016, and 2020, respectively. He was a Visiting Student with the AAC Laboratory, MIT, Cambridge, MA, USA. He is currently an Assistant Professor with the University of Genoa. He has co-authored more than 40 publications in international journals, books, invited chapters, and conference proceedings. His research interests include optimization and management of microgrids, distribution networks, and decentralized optimization.

MICHELA ROBBA (Member, IEEE) received the degree in environmental engineering and the Ph.D. degree in electronic and computer engineering from the University of Genoa, Italy, in 2000 and 2004, respectively. She is currently an Associate Professor with the University of Genoa. She has co-authored more than 130 publications in international journals, books, invited chapters, and conference proceedings. Her research interests include the development of methods and models for environmental and energy systems planning, management, and control, through the methodologies of operation research, automation, and systems analysis. She is the President of the Liguria Region Energy Consortium, the Chair of the IFAC TC 6.3 Power and Energy Systems, and a member of the Scientific Committee of the National Cluster on Energy. She is an Associate Editor of IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING and *The International Journal of Robotics Research*.

PAOLA GIRDINIO was a Board Member with ENEL, the Costa Crociere Foundation, Ansaldo STS, Banca Carige, Ansaldo Energia, D'Appolonia (RINA Group), and the University of Genoa. She is currently a Full Professor of electrotechnics with the Faculty of Engineering, University of Genoa, where she was formerly the Dean of the Faculty. She is also the Chair of the Center of Competence for Security and Optimization of Strategic Infrastructure 4.0 (Start 4.0). She is also a member of the Board of Directors of Ansaldo Energia, WSENSE of the Scientific Committee of the Eurispes Security Observatory, and a member of the Technical Committee of the AZIMU Infrastructure Fund. She was selected in the 2018 European Awards Short List BCI. For her commitment to academic and professional spheres, she was included in the role of experts in technological innovation established by Italian Ministry of Economic Development.

MARIO MARCHESE (Senior Member, IEEE) received the Laurea degree (cum laude), in 1992, and the Ph.D. degree in telecommunications from the University of Genoa, in 1997. From 1999 to January 2005, he was with Italian Consortium of Telecommunications (CNIT), where he was the Head of Research. From February 2005 to January 2016, he was an Associate Professor and has been a Full Professor with the University of Genoa, since February 2016, where he has been a Rector's Delegate to Doctoral Studies, since December 2020. He is the author of the book "*Quality of Service over Heterogeneous Networks*" (John Wiley and Sons, Chichester, 2007), and the author/co-author of more than 300 scientific works, including international magazines, international conferences, and book chapters. The most important contribution of his scientific activity is in the field of networking, quality of service over heterogeneous networks, software-defined networking, satellite networks, network security, critical infrastructure security, and intrusion detection systems.

Open Access funding provided by 'Università degli Studi di Genova' within the CRUI CARE Agreement