Real-world Cyber Security Demonstration for Networked Electric Drives

He Yang, *Student Member, IEEE,* Bowen Yang, *Member, IEEE,* Stephen Coshatt, *Student Member, IEEE,* Qi Li, *Member, IEEE,* Kun Hu, *Member, IEEE,* Bryan Cooper Hammond, *Student Member, IEEE,* Jin Ye, *Senior Member, IEEE,* Ramviyas Parasuraman, *Senior Member, IEEE,* Wenzhan Song, *Senior Member, IEEE*

***Abstract*—In this paper, we present the design and implementation of a cyber-physical security testbed for networked electric drive systems, aimed at conducting real-world security demonstrations. To our knowledge, this is one of the first security testbeds for networked electric drives, seamlessly integrating the domains of power electronics and computer science, and cybersecurity. By doing so, the testbed offers a comprehensive platform to explore and understand the intricate and often complex interactions between cyber and physical systems. The core of our testbed consists of four electric machine drives, meticulously configured to emulate small-scale but realistic information technology (IT) and operational technology (OT) networks. This setup both provides a controlled environment for simulating a wide array of cyber attacks, and mirrors potential real-world attack scenarios with a high degree of fidelity. The testbed serves as an invaluable resource for the study of cyber-physical security, offering a practical and dynamic platform for testing and validating cybersecurity measures in the context of networked electric drive systems. As a concrete example of the testbed's capabilities, we have developed and implemented a Python-based script designed to execute step-stone attacks over a wireless local area network (WLAN). This script leverages a sequence of target IP addresses, simulating a real-world attack vector that could be exploited by adversaries. To counteract such threats, we demonstrate the efficacy of our developed cyber-attack detection algorithms, which are integral to our testbed's security framework. Furthermore, the testbed incorporates a real-time visualization system using InfluxDB and Grafana, providing a dynamic and interactive representation of networked electric drives and their associated security monitoring mechanisms. This visualization component not only enhances the testbed's usability but also offers insightful, real-time data for researchers and practitioners, thereby facilitating a deeper understanding of cyber-physical security dynamics in networked electric drive systems.**

***Index Terms*—electric machine drives, cyber security, impact analysis, and cyber-physical systems.**

I. Introduction

The IEEE Power Electronics Society (PELS) has established Technical Committee 10 on Design Methodologies, tasked with the development of hardware and software tools for power electronics design, with a particular focus on ensuring the data communication and cyber-physical security of power electronics systems. In recent years, there has been a growing focus on the safety of modern motor drives and power electronic systems at various levels due to the increasing use of digital controls[1], [2], [3], [4]. Moreover, the economic implications of control systems under cyber attacks are investigated in some recent research [5] along with an increasing number of studies focusing on fault diagnosis and cyber attack detection from an algorithmic perspective[6], [7], [8].

In particular, the number of digitally controlled motor drives is growing dramatically with the rapid development of electric vehicles, wind power generation, and smart manufacturing systems. The rapid development of the Internet of Things (IoT) is also updating motor systems into motor-network systems, which puts new demands on both the cyber and physical security of the devices involved. Some studies on cyber-physical security delve into potential network attacks that connected vehicles and autonomous driving systems may face [9], [10]. Notable examples include the Stuxnet attacks in 2010 [11], the Jeep Cherokee Hack in 2015 [12], the Ukrainian power grid attack in 2015 [13], and the Tesla T BONE attacks in 2020 [14].

Testing faults, attacks, and defenses on a live system pose many issues such as the potential to damage systems, harm to people, and loss of access to services they provide [15]. Simulated data and attacks often generate data that are very clean and are not representative of real-world systems. On the other hand, creating realistic faults and attacks in an isolated system can be challenging and may not fully capture the complexities of real-world scenarios. It is thus necessary to develop cyber-physical testbeds that integrate both simulation and real-world experiments, in which a variety of attacks and faults could be created and generated, and detection and defenses could be tested.

While there are cyber-physical systems (CPS) testbeds in many different applications [16], [17], there remains a

Manuscript received 10 Oct 2024; revised 20 Dec 2024 and 11 Feb 2025; accepted 7 Mar 2025. Date of publication XX XXXX 2025. This research was partially supported by the U. S. National Science Foundation TI-PFI #2414706, DMS- AMPS #2318809, ECCS-EPCN #2102032 and NSF-SATC #2019311. (Corresponding author: Jin Ye.)

He Yang, Jin Ye and Bryan Cooper Hammond are with the Intelligent Power Electronics and Electric Machine Laboratory, University of Georgia, Athens, GA 30602 USA (e-mail: hy39566@uga.edu; jin.ye@uga.edu; bryan.hammond@uga.edu).

Bowen Yang is with the Power Systems Engineering Center, National Renewable Energy Laboratory, Golden, CO 80401 USA(e-mail: Bowen.Yang@nrel.gov).

Stephen Coshatt and Wenzhan Song are with the Center for Cyber-Physical Systems, University of Georgia, Athens, GA 30602 USA (e-mail: stephen.coshatt@uga.edu; wsong@uga.edu).

Qi Li is with Eaton, Cleveland, OH 44122, USA (qi.li@uga.edu).

Kun Hu is with Sino-German College of Intelligent Manufacturing, Shenzhen Technology University, Shenzhen, Guangdong 518118 China (e-mail: hukun@sztu.edu.cn).

Ramviyas Parasuraman is with the Heterogeneous Robotics (HeRo) Research Lab, the School of Computing, University of Georgia, Athens, GA 30602 USA. USA (ramviyas@uga.edu).

significant gap in the availability of cyber-physical testbeds specifically designed for networked electric drive systems. Networked electric drives rely on real-time feedback with stringent timing constraints, making them highly vulnerable to cyberattacks that disrupt control loops, leading to physical damage or operational failure. Unlike generic CPS systems, these drives exhibit strong cross-domain couplings between electrical, mechanical, and communication systems, where attacks on communication protocols can propagate and disrupt physical performance. Additionally, their precision and sensitivity in critical applications demand a level of simulation detail beyond that of conventional CPS testbeds. Finally, networked electric drives span diverse configurations, from single-drive systems to complex multi-drive setups, requiring scalable and adaptable solutions to address both individual and systemic vulnerabilities. These factors underscore the need for a dedicated testbed tailored to the unique challenges of networked electric drives. Most existing testbeds either focus on other domains or rely heavily on synthetic data, which may neglect the high-fidelity models required for accurate representation of power electronics. Additionally, with the continuous development of computer science, it becomes increasingly important to regularly update experimental designs and test algorithms to align with the evolving and expanding scale of cyber threats and security challenges faced by various cyberphysical systems. This includes addressing the emerging vulnerabilities introduced by the integration of Internet of Things (IoT) devices and the shift towards more interconnected and automated systems.

To address the emerging need for a cyber-physical security study of electric drive systems, we have built a testbed for networked electric drive systems to address cyber-physical security needs, merging power/control engineering with computer science for the first time to explore cyber-physical interactions. This initiative represents one of the first security testbeds specifically designed for networked electric drives that bridge the gap between these two critical fields. The setup includes four electric machine drives, simulating IT and OT networks for cyberattack analysis. This comprehensive configuration is crucial for the generation and study of various types of cyber attacks, providing a realistic and practical platform for cybersecurity research.

As an illustration of real-world cyber security scenarios, we developed a Python script for WLAN step-stone attacks and implemented cyber attack detection algorithms. This script allows for the execution of step-stone attacks by leveraging a series of input IP addresses of the target, simulating a common attack vector in wireless networks. To counter such attacks, we have integrated our cyber-attack detection algorithms into the testbed, enabling the evaluation of defense mechanisms in a controlled environment.

Additionally, with InfluxDB, we offer real-time visualization of electric drives and their security, making this a holistic security research tool for electric drive systems. The incorporation of real-time data visualization using InfluxDB not only enhances the testbed's usability but also provides a dynamic and interactive representation of networked electric drives and their associated security monitoring systems.

II. Design of Real-World Security Testbeds

A. System Architecture Overview

Fig. 1 shows the real connection and structure of the developed security testbed.

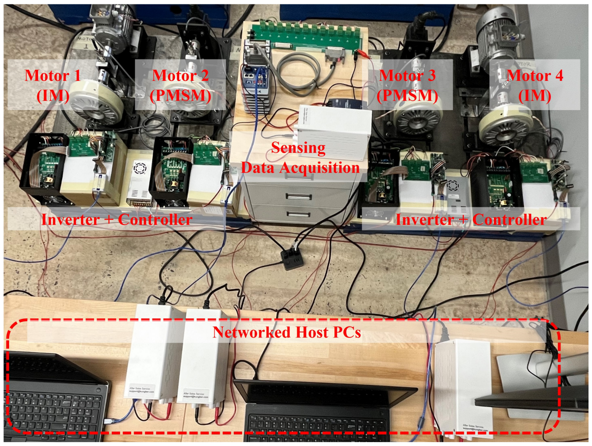


Fig. 1. Cyber-physical security testbed for networked electric drives.

This cyber-physical security testbed includes four electric machine drives sharing the same DC power supply. Four digital control units control the four electric machine drive units, respectively. Furthermore, each control unit has a host PC connected through lab networks, emulating the operating networks in real-world applications. The NI cDAQ-9132, with similar configurations to the Hardware-In-the-Loop (HIL) simulation security testbed, also forms the isolated monitoring system.

Figure. 2 shows the topology structure of this cyber-physical security testbed. The top half of the structure includes the physical layer and control layer, which represents the four motors, inverter, controller, sensors and networked host PCs. The bottom half represents cyber layer which contains WiFi Router, InfluxDb server and cyber attack source.

With shown the real and topology structure, this security testbed aims not only to emulate a real-world operating environment and generate authentic data sets across various scenarios but also to verify the results from the Hardware-In-the-Loop (HIL) simulation security testbed. Additionally, it is designed to test and demonstrate the developed cyber-attack detection and diagnosis algorithms in a real-world setting, providing a practical platform for evaluating the effectiveness of these algorithms. Furthermore, the testbed showcases the integrated visualization and monitoring systems, highlighting their capabilities in real-time data representation and security monitoring.

B. Software and Network Design

The testbed simulates small information technology (IT) and operational technology (OT) networks using a combination of commercial, open-source, and custom software. Key commercial components include Texas Instruments (TI) Code Composer Studio (CSS) and Debug Server Scripting

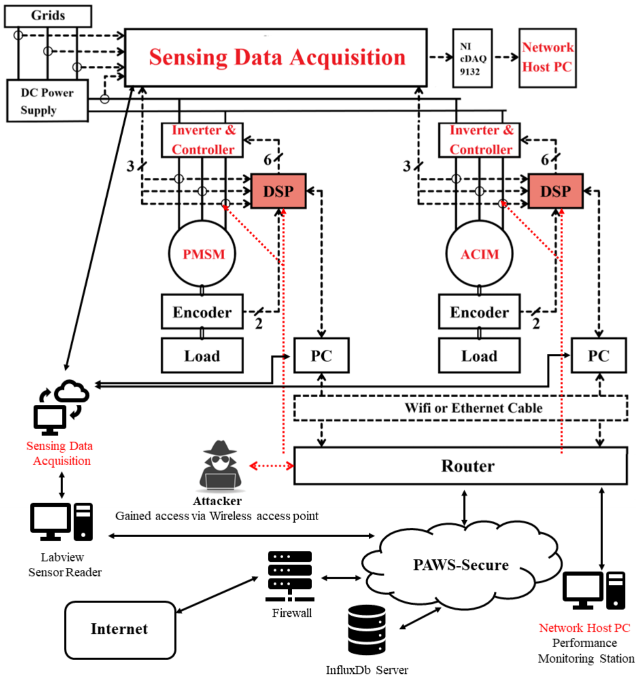


Fig. 2. Diagram of cyber-physical security testbed for networked electric drives.

(DSS). Open-source components include CollectD, Eclipse Paho MQTT, InfluxDb, TI's TestServer, and Tshark.

The commercial software is primarily used for the development, debugging, and deployment of custom software onto motor control units. Modifications to TI's TestServer, an open-source software tool, provide a backdoor to gain enhanced control over the system. Since TestServer is part of the Code Composer Studio suite, its use within the OT network is less conspicuous.

CollectD is used to gather system data from Pi4 devices that emulate IT network stations, representing user workstations. Eclipse Paho MQTT, which complies with the MQTT 3.1.1 ISO standard (ISO/IEC 20922), is used as a publish/subscribe messaging service to transmit commands from compromised IT workstations to the TestServer on the OT network. InfluxDb, an open-source time-series database and visualization tool, records system data, facilitating fault and attack diagnostics through custom dashboards.

The network setup features a small IT network connected to an OT network. The IT network consists of Pi4 devices acting as user workstations connected via WiFi. A router is used to segment the IT network from the OT network. The OT network includes four Windows workstations, each connected to motors through DSP controllers. Sensors attached to the motors monitor three-phase current, while a PCC sensor oversees all four motors. Data from the sensors is streamed directly to InfluxDb for further analysis.

C. Hardware and Controller Design

While Hardware-in-the-Loop (HIL) simulation security testbeds offer a low-cost, risk-free, and effective tool for analyzing system behavior, real-world hardware experiment security testbeds are still desirable for the following reasons:

1) They can verify the authenticity of simulated environmental factors in HIL simulations.
2) They can assess the impact of additional factors not considered in HIL simulations.

However, despite their advantages, HIL testbeds have several limitations when it comes to cybersecurity testing, particularly for networked electric drive systems. HIL platforms are primarily designed for real-time hardware testing and focus on ensuring communication accuracy and system performance rather than addressing sophisticated cybersecurity threats.[18] They often rely on synthetic data and predefined configurations, which limit their ability to simulate complex, multi-layer network attacks or analyze the nuanced behavior of real-world systems under such threats.[19], [20] Furthermore, their flexibility and customization capabilities are constrained, making it challenging to adapt them for evolving security challenges.

This section introduces a developed real-world hardware security testbed designed for intelligent electric drive systems. The following table compares the key differences between HIL testbeds, the previous testbed proposed by our laboratory[21], and the newly proposed testbed, highlighting the unique advantages of our approach:

TABLE I
TESTBED COMPARISON

Aspect	HIL Testbeds	Previous Testbed[21]	Proposed Testbed
Focus	Real-time cyber-security testing	Lab-scale cyber-security testing	Real-world cyber-security testing
Network	Simulated Scenarios	Lab-scale Scenarios	Real Scenarios
Flexibility	Limited	Basic	High
Attack Simulation	Basic capabilities	Network and control layer	Complex,multi-layer scenarios
Customize	Predefined configurations	Basic customizable	Highly customizable
Model Fidelity	Low	Medium	High
Data Fidelity	Emulated data	Lab-scale experimental data	Real-world data

The hardware testbed includes two induction machines (IMs) and two permanent magnet synchronous machines (PMSMs), with all electric drive units using a Texas Instruments (TI) C2000 TMS320F28335 microcontroller as the digital control unit. The TMS320F28335 is a high-performance microcontroller based on the C28x core, optimized for high-speed real-time control tasks, such as motor control, power electronics, and digital power conversion. It operates at up to 150 MHz and includes a range of peripheral interfaces, such as multiple serial communication ports, analog-to-digital converters, and pulse-width modulation (PWM) outputs.

Key features of the TMS320F28335 include advanced control algorithms like proportional-integral-derivative (PID) controllers and vector control algorithms, which are ideal for high-speed control applications. Additionally, it offers hardware acceleration for fast Fourier transforms (FFTs) and other signal processing algorithms, enhancing the implementation of advanced control techniques. Designed to operate in harsh industrial environments, it is resistant to electromagnetic interference (EMI) and electrostatic discharge (ESD), and includes features such as a memory protection unit and a watchdog timer for system reliability and safety. Furthermore, it supports efficient software development through TI's Code Composer Studio IDE and the TMS320x2833x reference manual.

All four electric drives in this testbed utilize a field-oriented control (FOC) strategy for precise speed and torque control. FOC is a widely used method for controlling both IMs and PMSMs, where the currents in the stator windings are manipulated to create a rotating magnetic field that aligns with the rotor field, providing high levels of control over machine performance. In the case of induction machines, FOC requires transforming stator currents from a stationary reference frame (ABC) to a rotor reference frame (d-q) based on the rotor flux angle. For permanent magnet synchronous machines, FOC is simplified due to the presence of permanent magnets, which provide a known rotor field.

In both machine types, the control system uses proportional-integral (PI) controllers to adjust stator current phase and magnitude, ensuring optimal rotor flux alignment and machine efficiency. The PI controllers generate current and voltage commands, which are processed by PWM converters to achieve the desired stator current. FOC offers precise control over machine torque and speed, even under varying loads and conditions, and is essential in applications such as electric vehicles and industrial automation.

Tables II list the key parameters for the PMSMs and IMs used in this testbed, while Fig. 3 illustrates the FOC control diagram. The control system allows smooth operation and can optimize energy consumption by maximizing machine efficiency.

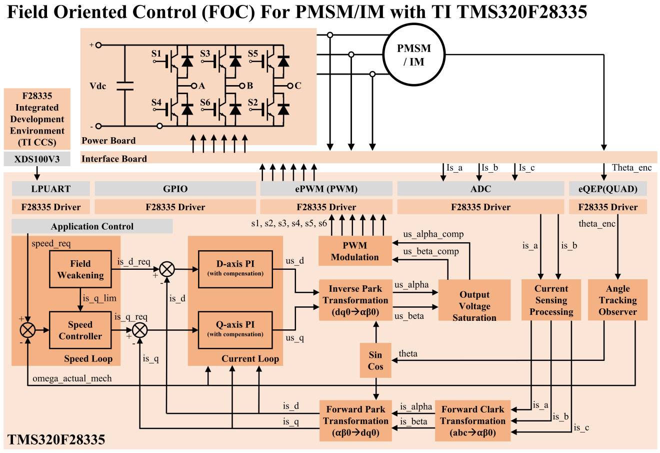


Fig. 3. Controller diagram for field-oriented control (FOC) for PMSM and IM.

In summary, although HIL simulations offer valuable insights in a safe and cost-effective manner, real-world hardware testbeds, like the one described here, are crucial for verifying the accuracy of simulations and assessing additional factors that may influence system behavior. The hardware testbed provides a robust platform for studying the security and performance of intelligent electric drive systems under real-world conditions.

TABLE II
SPECIFICATIONS OF THE PMSMS AND IMS IN THE DEVELOPED HARDWARE EXPERIMENT SECURITY TESTBED.

PMSM			
Rated Power	1.5 kW	Stator Resistance	0.4050 Ω
Rated Current	8.2 A	Stator Inductance	0.0024 H
DC Bus Voltage	200 V	Magnet Flux Linkage	0.0599 Wb
Rated Frequency	250 Hz	Number of Pole Pairs	5
Control Frequency	10 kHz	Motor Inertia	3.10e-4 kgm^2
IM			
Rated Power	1.5 kW	Stator Resistance	1.85 Ω
Rated Current	3.4 A	Stator Inductance	0.1084 mH
DC Bus Voltage	200 V	Rotor Resistance	1.98 Ω
Rated Frequency	150 Hz	Rotor Inductance	0.1116 H
Control Frequency	10 kHz	Number of Pole Pairs	3

D. Monitoring System Design

The isolated monitoring system is similar to the one in the HIL simulation security testbed, which is discussed in previous sections. The difference in the hardware experiment security testbed is that it has an extra sensor integration board, as shown in Fig. 1. This sensor integration board integrates the signals from remote current sensors at each motor, DC bus, and PCC. This integration board then uses a DB37 connection to route these signals to the NI cDAQ-9132 chassis. This setup allows the cDAQ to select desired signals with high flexibility. The visualization dashboard of the monitoring system, shown in Fig 4, created with InfluxDB cloud service, displays the system's status, showing if it's operating normally or experiencing a real-time attack. Data is first gathered by the cDAQ-9132, processed using algorithms to determine features and detection outcomes, and then sent to the InfluxDB cloud, where the dashboard periodically visualizes the results.

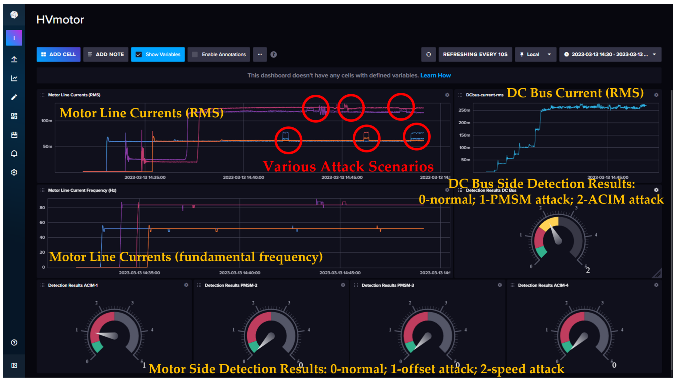

This dashboard doesn't have any cells with defined variables. Learn How

Fig. 4. Screenshot of the real-time visualization dashboard when ACIM-1 is under attack 8 in III.

In conclusion, our testbed design is inherently extensible and versatile, offering broad applicability across a wide range of communication protocols, infrastructural variations, and device types. Using TCP / IP stacks as the foundation, the platform seamlessly incorporates higher level standards, such as IEC 61850, IEC 61400-25, ISO / IEC 15118 and OCPP, through targeted adaptations of the network layer. These adaptations, in turn, directly influence the motor control layer and ultimately shape the behavior of the physical system.

Central to the testbed is the high-performance TI C2000 TI28335 MCU/DSP, which provides ample flexibility and connectivity options to interface with induction motors, permanent magnet synchronous motors, and other load devices. This versatility extends to power input configurations, enabling operations under both industrial and residential power supplies, as well as single-phase and three-phase power conditions. At the converter stage, the testbed accommodates variable frequency drives, inverters, and rectifiers capable of transforming diverse input energy specifications into the appropriate levels required by the load. Consequently, a wide array of DC and AC devices can be tested—including automotive motors, household appliances, charging stations, and energy storage batteries—under conditions that closely mimic real-world operation.

Moreover, the platform not only matches but surpasses the capabilities of traditional hardware-in-the-loop (HIL) simulations by generating stable inputs that accurately reproduce real-world scenarios. It can also introduce adjustable noise and attack vectors to explore conditions often too complex or risky to replicate in purely simulated environments. This unique combination of realism and controllability supports comprehensive experimentation across multiple research and practical domains. Although MQTT is currently used due to its suitability in low-resource and unstable network environments, it can be readily substituted with more specialized protocols when communication or reliability demands shift.

III. Experimental Results of Real-world Security Demonstrations

Fig. 5 shows the detailed flowchart for the monitoring algorithms implemented in the demo prototype. The entire testbed's systems are integrated through the operational information flow shown in this diagram, operating and testing according to predefined cyber-attack scenarios.

A. Cyber-attack Design

Realizing cyber-attacks in real-world hardware security testbeds is always challenging due to the trade-off between the fidelity and controllability of the attack scenarios. An ideal attack scenario should be one of the real-world attacks from historical studies. However, cyber-attacks are highly unpredictable, and the impacts on the physical systems are even more challenging to manage. Therefore, the developed hardware experiment security testbed adopts fully controllable false data injection attack (FDI) scenarios. The emulated attacks are pre-defined and embedded in the TMS320F28335 MCUs with some triggers. These triggers are backdoors for various FDI attacks. Therefore, the attack policies could be fully controllable, and the impacts on physical systems could be manageable. The hacker then could trigger one of the pre-defined backdoors, and the impacts could be analyzed through the acquired data sets from the cDAQ systems.

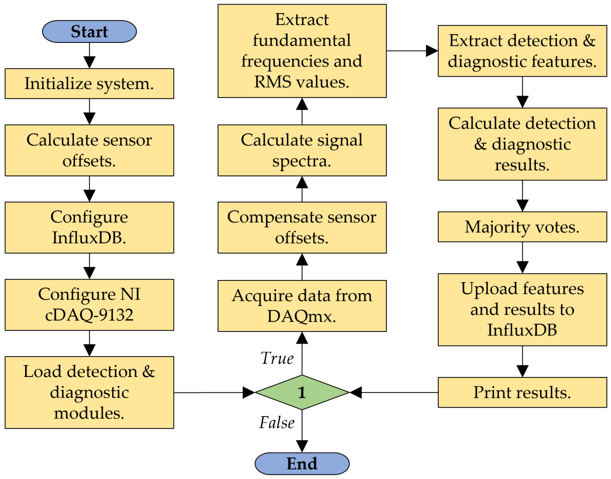

Start
Initialize system.
Calculate sensor offsets.
Configure InfluxDB.
Configure NI cDAQ-9132
Load detection & diagnostic modules.
1
True
False
End
Acquire data from DAQmx.
Compensate sensor offsets.
Calculate signal spectra.
Extract fundamental frequencies and RMS values.
Extract detection & diagnostic features.
Calculate detection & diagnostic results.
Majority votes.
Upload features and results to InfluxDB
Print results.

Fig. 5. Flowchart of the demo prototype condition monitoring system software.

For our proposed step-stone attack, we developed a Python script that launches a chain attack in the WLAN based on the input series of IP addresses of the target. The complete workflow is as follows:

1) The attacker gained access to the IT network via an unsecured wireless access point shown in Fig. 1
2) The attacker launches a port scan to locate other workstations on the network
3) brute force password cracking attack based on the target victim IP address, which is arbitrarily selected from the scan
4) once the password is cracked, the attacker logs in and loads and runs a script that sends JSON-RPC commands to the NXP Lite server to execute motor commands. This allows the attacker to speed up, slow down, stop, restart, and disconnect the motor
5) The compromised Pi then launches this attack on another Pi
6) Repeat the above procedures

B. Attacks Case Studies and Descriptions

This section presents experimental results from two major categories: one involving various false data injection attacks (FDIAs) targeting the Permanent Magnet Synchronous Motor (PMSM) electric drive units, and the other focusing on Alternating Current Induction Motors (ACIM). These two motors were chosen because of their widespread use and representativeness as controlled and attacked objects of physical systems. These distinct test cases are detailed in Table III.

False data injection attacks targeting closed-loop control systems are a type of cyber-attack that aims to manipulate the output of a control system by injecting malicious data into its input. This type of attack is particularly dangerous because it can cause the system to behave in unexpected and potentially damaging ways. In a closed-loop control system, the output of the system is fed back into the input, where it is used to adjust the control action. An attacker can exploit this feedback loop to inject false data that modifies the output of the system in a way that is detrimental to the control objectives.

TABLE III
DETAILS OF CYBER-ATTACK SCENARIOS FOR DEMO PROTOTYPE.

Case No.	Target System	Target Variables
0	Motor Side	Normal Running Condition
1	PMSM	ADC offset-phase A current feedback
2	PMSM	ADC offset-phase B current feedback
3	PMSM	ADC offset-phase C current feedback
4	PMSM	ADC offset-phase A&B current feedback
5	PMSM	ADC offset-phase A&C current feedback
6	PMSM	ADC offset-phase B&C current feedback
7	PMSM	Speed reference
8	IM	ADC offset-phase A current feedback
9	IM	ADC offset-phase B current feedback
10	IM	ADC offset-phase C current feedback
11	IM	ADC offset-phase A&B current feedback
12	IM	ADC offset-phase A&C current feedback
13	IM	ADC offset-phase B&C current feedback
14	IM	Speed reference

One common approach for FDIAs in closed-loop control systems is to manipulate the sensor measurements that are used as feedback signals. For example, an attacker can inject false measurements that cause the control system to make incorrect decisions, such as increasing the output of a system beyond its safe limits. In some cases, the attacker may also modify the control commands that are sent to the actuators, which can cause the system to behave in unexpected ways. These attacks can be challenging to detect because the injected data may appear to be valid sensor readings, making it difficult for the control system to distinguish between normal and malicious inputs.

False data injection attacks (FDIAs) targeting closed-loop control systems are becoming an increasing concern in many critical infrastructure systems, including power grids, water distribution systems, and transportation networks. These systems heavily rely on closed-loop control to maintain their safe and reliable operation, making them prime targets for attackers aiming to disrupt their function. Given the harmful and representative nature of FDIAs, this testbed has chosen FDIAs as the testing method for subsequent experiments. Through related testing, it is hoped that advanced machine learning algorithms can be utilized to better identify and block malicious attacks in real-time, mitigating potential issues before any damage occurs to the system. In this testbed, a False Data Injection Attack (FDIA) is strategically introduced at the network layer, compromising the integrity of the control layer by introducing biases into sensor readings and controller decisions. This cascading compromise manifests as physical-level disturbances in the motor system, including unbalanced three-phase currents, distorted magnetic fields, and irregular torque outputs. Unlike methods that rely solely on algorithmic simulations, this testbed integrates physical domain knowledge with cyber-physical interactions, enabling the collection of high-fidelity data that reflects real-world scenarios. By correlating these anomalies with network interactions, the testbed provides a robust foundation for detecting and mitigating cyberattacks through advanced control mechanisms and machine learning approaches. In contrast, our testbed leverages high-accuracy simulations and hardware-in-the-loop (HIL) platforms to produce data that is both precise and interpretable, aligning closely with real-world operational conditions. This enables a comprehensive analysis of system vulnerabilities, especially under multi-layered attack scenarios that span network, control, and physical layers. These scenarios, captured by devices such as the NI cDAQ-9132, facilitate the direct observation of physical responses to injected attacks, enhancing the understanding and mitigation of potential risks.

As illustrated in the flowchart presented in Figure 5, five distinct classification models (Random Forests (RF), Multivariate Logistic Regression (LG), Support Vector Machines (SVM), K Nearest Neighbor (KNN), Convolutional Neural Networks (CNN)) have been evaluated. A sampling frequency of 2 kHz is utilized, with each monitoring window gathering 500 data points. The primary features extracted for detection and diagnostic purposes consist of the signal magnitude within the frequency domain. The testing process, as outlined by the scenarios in Table III, comprises two levels for all monitors: individual monitoring of permanent magnet synchronous machine (PMSM) three-phase line currents, individual monitoring of induction machine (ACIM) three-phase line currents, and system monitoring of DC bus line current. For individual monitors, the first level aims to differentiate between normal conditions, ADC offset attacks (cases 1-6 and 8-13), and speed reference attacks (cases 7 and 14). The second level seeks to distinguish each attack scenario for both PMSM (cases 1-7) and ACIM (cases 8-14) monitors. Subsequently, in the case of the DC bus system monitor, the first level involves identifying normal conditions, PMSM attacks (cases 1-7), and ACIM attacks (cases 8-14). The second level focuses on differentiating ADC offset attacks in PMSM (cases 1-6), speed reference attacks in PMSM (case 7), ADC offset attacks in ACIM (cases 8-13), and speed reference attacks in ACIM (case 14).

Furthermore, an additional third level of complexity is introduced for the system monitor. This level distinguishes all 14 cases and normal conditions solely based on the current DC bus line. The following pages show the detailed results and some sample raw waveforms from different scenarios.

IV. Testbed Results and Data Analysis

A. Test Results

Fig. 6 illustrates the variation of DC bus current over time during motor operation under no load, normal load, and various FDIA scenarios. We observe that under both no-load and normal-load conditions, the harmonic patterns on the DC bus are similar. Meanwhile, when FDIA attacks the A-phase of PMSM and ACIM motors, the erroneous harmonic components exhibit similar patterns. Similarly, when FDIA targets the speed reference of both motors, the erroneous harmonics remain consistent, indicating a regular pattern in FDIA-induced errors.

Additionally, both low and high-frequency harmonics on the DC bus reveal imbalances in the three-phase motor currents and torque, demonstrating FDIA's capability to physically

This article has been accepted for publication in IEEE Journal of Emerging and Selected Topics in Power Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2025.3550830

disrupt motor control systems, posing significant threats to operational and personal safety.

Fig. 7 shows the target PMSM three-phase line currents and DC bus line current of a sample FDIA targeting the phase A ADC offset variable. The bias injected is 0.1, which represents around 1A bias in the machine feedback. These scenarios include four target onboard control-related resources. Three are the ADC offset variables for three-phase current feedbacks, respectively. The rest is the rotating speed reference variables. For ADC offsets, the attack falsely injects 0.05 bias into their original values. For speed references, the attack falsely injects a periodic disturbance to the original values. Such a disturbance has a magnitude of ± 0.01 p.u. and a period of 0.1s.

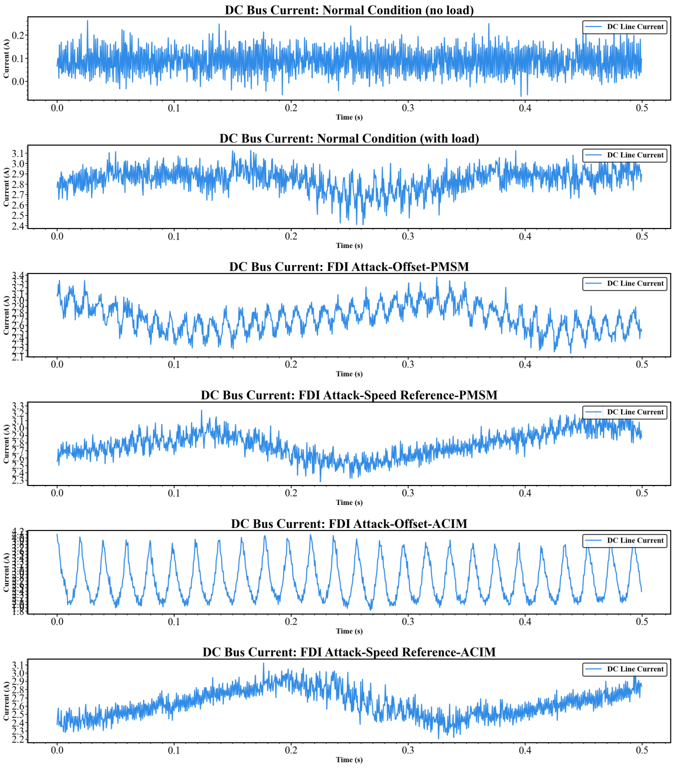
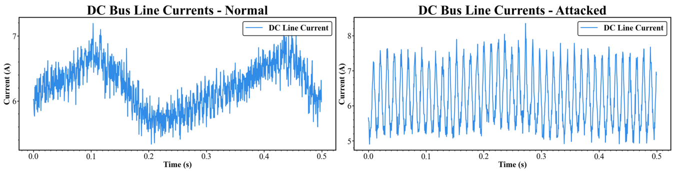


Fig. 6. DC Bus line currents of a sample FDIA targeting the single motor phase A ADC offset variable. The bias injected is 0.1, which represents around 1A bias in the machine feedback.(1) Normal Condition without load, (2) Case 0, (3) Case 1, (4) Case 7, (5) Case 8, (6) Case 14.

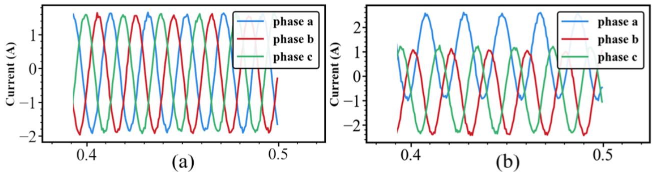
Figure 7 provides a comprehensive visualization, showcasing a detailed comparison of current values within the DC bus when subjected to both the presence and absence of FDI attacks. When not under attack, the DC bus current is naturally fluctuating with the motor load. Meanwhile, when an attack occurs, an intuitive and noticeable change in the type of harmonics in the DC bus is found in the figure.

Notably, the depicted data reveals a discernible pattern in the current output, akin to the patterns observed in injected attacks. This observed regularity in the current output not only serves as an interesting insight but also establishes a foundation for contrasting and pinpointing potential attacks specifically at the network layer. This expanded description offers a more in-depth analysis of the findings presented in Figure 7, shedding light on the nuanced observations related to FDI attacks and their impact on the DC bus current values.



(a) (b)

Fig. 7. DC Bus line currents of a sample FDIA targeting two PMSMs' phase A ADCoffset variable. The bias injected is 0.1, which represents around 1A bias in the machine feedback.(a) Case 0, (b) Case 1.



(a) (b)

Fig. 8. Three Phase currents of a sample FDIA targeting the single motor phase C ADC offset variable. The bias injected is 0.1, which represents around 1A bias in the machine feedback. (a) Case 0, (b) Case 3

Figure 8 illustrates various raw waveforms obtained from experiments conducted on the PMSM. The results indicate that when one of the ABC three phases is subjected to an FDI attack, the currents in the other two phases exhibit noticeable fluctuations and deviations. Similarly, when two out of the three phases experience FDI attacks, the third-phase current still demonstrates significant fluctuations and deviations. Moreover, when all three phases (ABC) are subjected to FDI attacks simultaneously, a considerable decrease in the amplitude of the three-phase currents is observed. The distinctive waveforms associated with different attack scenarios not only allow for differentiation from the normal operating state of the motor system but also exhibit unique error features under various attack conditions.

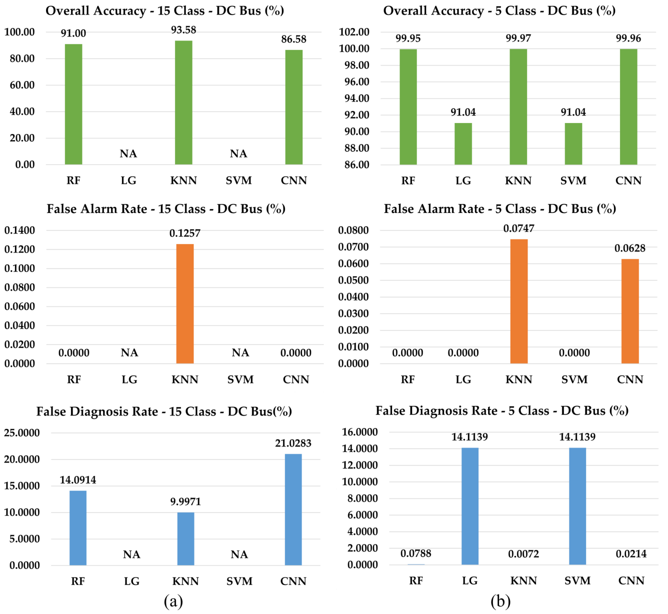
In other words, the experimental setup successfully detects network attacks on the motor and can distinguish between different fault types without further data processing, such as confusion matrices.

B. Data Analysis and Comparison

In Figure 9, we compare the fault diagnosis accuracy of five algorithms—Randow Forest(RF), K-Nearest Neighbors(KNN), Convolutional Neural Network(CNN), Logistic Regression(LG), and Support Vector Machine(SVM)—using two different datasets. All algorithms use data collected from the DC bus, with case 0 serving as the baseline for normal operation, while the other cases are labeled with different fault scenarios.

The first dataset in Figure 9 (a) includes all defined cases, while the second dataset represents a scenario of insufficient training data, containing only case 0 as normal samples. The other dataset in Figure 9 (b) includes case 0,1,7,8 and 14. Cases 1 and 7 representing different types of FDIA attacks on the PMSM. These attacks disrupt the three-phase current balance by injecting currents into each phase and alter the motor's normal operation by injecting speed reference errors, affecting overall current, operating temperature, and key indicators like equipment aging. The same applies to cases 8 and 14.

As shown in the first row of Figure 9, RF, KNN, and CNN exhibit a reasonable decline in prediction accuracy as the complexity of the cases increases. In contrast, the increased nonlinearity due to more cases makes it impossible for LG and SVM to train and analyze the data effectively. Both datasets demonstrate that KNN achieves the highest accuracy. The second row of Figure 9 shows that the false alarm rate for all algorithms is close to 0%, indicating that all methods reliably avoid such errors. However, relying solely on KNN for analyzing this type of experimental data may lead to significant economic losses in practical applications. As illustrated in the third row of Figure 9, when the number of cases is low, the false diagnosis rates for nonlinear algorithms remain low. However, the high false diagnosis rates of LG and SVM suggest that they struggle to handle nonlinearity even in low-complexity scenarios. KNN also slightly outperforms RF and CNN in high-complexity cases.



(a) (b)

Fig. 9. FDIAs Classification Detection Accuracy comparison in five algorithms. All data training and comparisons are based on the benchmark data collected from the DC bus. (a)Case 0-14. (b)Case 0,1,7,8,14

As shown in Figure 10, since there is no training data for the 15-case scenario for LG and SVM, we examine their performance in simpler cases.

It is evident that both algorithms fail to identify the same two cases, specifically the speed reference FDIA. This demonstrates their poor handling of nonlinearity, as well as the significant nonlinearity, or harmonic distortion, introduced by the FDIA attacks on the DC bus. This greatly impacts the power quality of the motor control system. Based on the performance of confusion matrix, linear regression and machine learning algorithms based on similar principles are not well-suited for fault diagnosis data analysis.

As shown in Figure 11, RF, CNN, and KNN are well-suited for handling highly nonlinear data. In Figure 11 (b), with only five cases, the distinction between normal samples and various FDIA cases is clear, allowing these three algorithms to nearly fully identify each fault. In the confusion matrix for the 15-case dataset, RF achieves high accuracy when processing FDIA for PMSM, but its accuracy for ACIM data is less ideal. In comparison, CNN struggles with distinguishing between attacks on different phases of both motors, particularly confusing single-phase and two-phase attacks. KNN, on the other hand, shows stable performance, making almost no errors in identifying PMSM data, though its accuracy slightly declines with ACIM data.

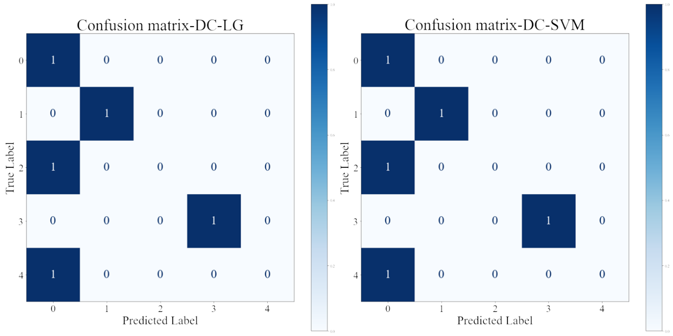


Fig. 10. LG and SVM Confusion Matrix of 5 Case datasets. (Case 0,1,7,8,14)

From these comparisons, the confusion matrix suggests that faults in ACIM are generally more difficult to distinguish than in PMSM. Single-phase and two-phase errors in three-phase motors are particularly challenging to differentiate, while speed reference faults are reliably recognized overall. KNN remains stable in identifying phase-related FDIA in ACIM, making it the most reliable algorithm in this testbed. Our cyber-physical security testbed demonstrates effectiveness in creating, detecting, and addressing such issues, providing practical significance and value for the growing security demands in modern motor control systems and IoT systems.

Overall, the testbed effectively discerned network attacks within the relevant cases. In conclusion, the benefits of the motor network security testbed developed in this paper can be outlined as follows. Initially, it establishes a crucial connection between real-world network vulnerabilities and power electronic control models. This connection enables the physical measurement and exploration of vulnerabilities on the network side, facilitating the identification and development of methods to counteract these network attacks. Secondly, it precisely discerns the impact of various types of attack signals on motor drives. Lastly, to a significant degree, this apparatus contributes to the enhancement and assurance of the security of motor network systems—an emerging and inventive category of power electronic systems, showcasing substantial practical value.

V. Conclusion

This paper establishes a crucial linkage between cybersecurity research in the cyber-physical informed system and conventional motor grid-connected systems. An innovative testbed is presented herein, specifically designed for cybersecurity and control of motor drives. The testbed seamlessly integrates

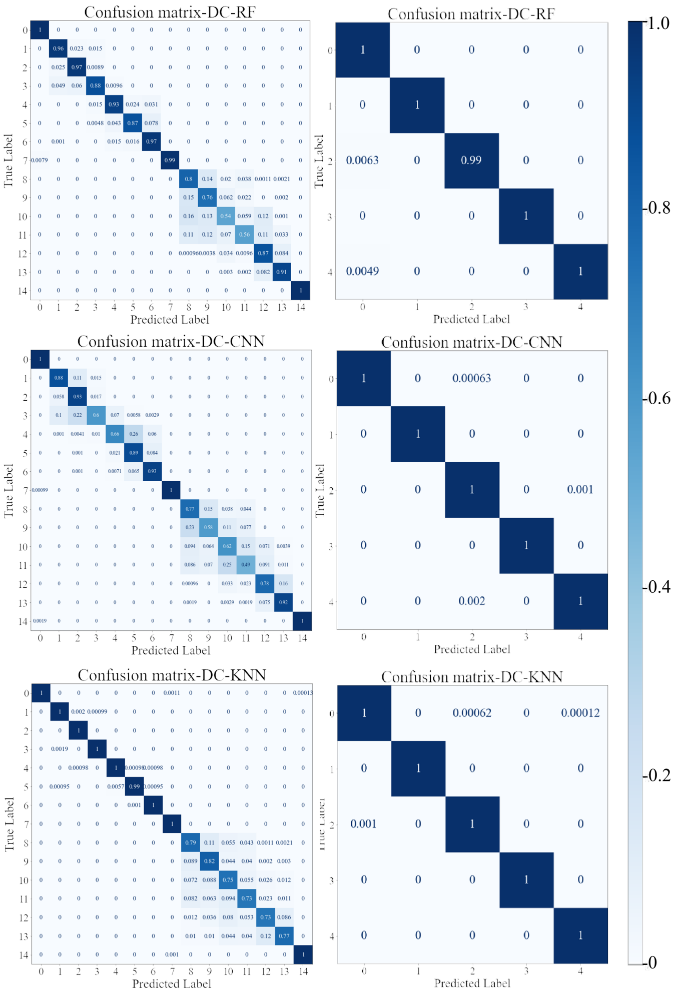


Fig. 11. Two datasets' RF,CNN and KNN Confusion Matrix. All data training and comparisons are based on the benchmark data collected from the DC bus. (a)Case 0-14. (b)Case 0,1,7,8,14

fault detection, problem analysis, and treatment methods for both cyber-attacks and motor control. The proposed approach pioneers the combination of machine learning with traditional motor control techniques. By amalgamating machine learning from computer science with control methods from power electronics, the experimental system detailed in this paper proficiently identifies anomalies in the grid-connected motor system and provides corresponding control solutions. Diverse problem scenarios are examined to affirm that the developed test bench significantly enhances the physical security and network security of the emerging motor system. This contribution establishes a more dependable and user-friendly testing environment and hardware program. These empirical findings confirm a more dependable and user-friendly testing environment, underscoring the tangible, hands-on advancements brought forth by our framework.

We introduce a novel cyber-physical attack analysis framework that bridges the gap between theoretical attack models and their real-time physical manifestations. By integrating cyber-physical system interactions into our detection methods, we highlight how subtle and long-term threats—such as torque imbalances and mechanical wear—can be detected where traditional cybersecurity frameworks may fail. Our testbed serves as a theoretical model for adaptive, scalable, and comparative testing across diverse motor types, system topologies, and attack vectors. Ultimately, this work lays the foundation for future theoretical advancements in CPS security, guiding the development of more sophisticated algorithms and broader research on CPS integrity and resilience.

References

[1] Q. Li, J. Zhang, J. Zhao, J. Ye, W. Song, and F. Li, "Adaptive hierarchical cyber attack detection and localization in active distribution systems," *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2369–2380, 2022.

[2] B. Yang, J. Ye, S. Coshatt, W. Song, and F. Zahiri, "Data-driven approach for detection of physical faults and cyber attacks in manufacturing motor drives," in *2022 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2022, pp. 1–6.

[3] B. Yang, J. Ye, and L. Guo, "Fast detection for cyber threats in electric vehicle traction motor drives," *IEEE Transactions on Transportation Electrification*, vol. 8, no. 1, pp. 767–777, 2022.

[4] L. Guo, B. Yang, J. Ye, J. M. Velni, and W. Song, "Attack-resilient lateral stability control for four-wheel-driven evs considering changed driver behavior under cyber threats," *IEEE Transactions on Transportation Electrification*, vol. 8, no. 1, pp. 1362–1375, 2022.

[5] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry, "Understanding the physical and economic consequences of attacks on control systems," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 3, pp. 73–83, 2009.

[6] B. Yang, S. Wu, K. Hu, J. Ye, W. Song, P. Ma, J. Shi, and P. Liu, "Enhanced cyber-attack detection in intelligent motor drives: A transfer learning approach with convolutional neural networks," *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, vol. 5, no. 2, pp. 710–719, 2024.

[7] S. Wu, L. Fang, J. Zhang, T. N. Sriram, S. J. Coshatt, F. Zahiri, A. Mantooth, J. Ye, W. Zhong, P. Ma, and W. Song, "Unsupervised anomaly detection and diagnosis in power electronic networks: Informative leverage and multivariate functional clustering approaches," *IEEE Transactions on Smart Grid*, vol. 15, no. 2, pp. 2214–2225, 2024.

[8] L. Guo, J. Zhang, J. Ye, S. J. Coshatt, and W. Song, "Data-driven cyber-attack detection for pv farms via time-frequency domain features," *IEEE Transactions on Smart Grid*, vol. 13, no. 2, pp. 1582–1597, 2022.

[9] R. M. Gerdes, C. Winstead, and K. Heaslip, "Cps: an efficiency-motivated attack against autonomous vehicular transportation," in *Proceedings of the 29th Annual Computer Security Applications Conference*. ACM, 2013, pp. 99–108.

[10] G. K. Rajbahadur, A. J. Malton, A. Walenstein, and A. E. Hassan, "A survey of anomaly detection for connected vehicle cybersecurity and safety," in *2018 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2018, pp. 421–426.

[11] Robert McMillan, "Siemens: Stuxnet worm hit industrial systems," 2010, https://www.computerworld.com/article/2515570/siemens--stuxnet-worm-hit-industrial-systems.html, Last accessed on 2023-6-3.

[12] N. E. Vellinga, "Connected and vulnerable: cybersecurity in vehicles," *International Review of Law, Computers & Technology*, vol. 36, no. 2, pp. 161–180, 2022. [Online]. Available: https://doi.org/10.1080/13600869.2022.2060472

[13] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, 2017, pp. 1–8.

[14] V. K. Kukkala, S. V. Thiruloga, and S. Pasricha, "Roadmap for cybersecurity in autonomous vehicles," *IEEE Consumer Electronics Magazine*, vol. 11, no. 6, pp. 13–23, 2022.

[15] G. Kavallieratos, S. Katsikas, and V. Gkioulos, *Cyber-Attacks Against the Autonomous Ship: Methods and Protocols*, 01 2019, pp. 20–36.

[16] C. M. Ahmed, V. R. Palleti, and A. P. Mathur, "Wadi: a water distribution testbed for research in the design of secure cyber physical systems," in *Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks*, ser. CySWATER '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 25–28. [Online]. Available: https://doi.org/10.1145/3055366.3055375

[17] G. Lu, D. De, and W.-Z. Song, "Smartgridlab: A laboratory-based smart grid testbed," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 143–148.

[18] J. Zhang, L. Guo, and J. Ye, "Hardware-in-the-loop testbed for cyber-physical security of photovoltaic farms," *IEEE International Symposium on Power Electronics for Distributed Generation Systems*, vol. 2021, 7 2021. [Online]. Available: https://www.osti.gov/biblio/2341854

[19] ——, "Cyber-attack detection for photovoltaic farms based on power-electronics-enabled harmonic state space modeling," *IEEE Transactions on Smart Grid*, vol. 13, no. 5, 10 2021. [Online]. Available: https://www.osti.gov/biblio/1980583

[20] J. Zhang, Q. Li, J. Ye, and L. Guo, "Cyber-physical security framework for photovoltaic farms," in *2020 IEEE CyberPELS (CyberPELS)*, 2020, pp. 1–7.

[21] S. J. Coshatt, Q. Li, B. Yang, S. Wu, D. Shrivastava, J. Ye, W. Song, and F. Zahiri, "Design of cyber-physical security testbed for multi-stage manufacturing system," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, 2022, pp. 1978–1983.