IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 16 June 2023, accepted 10 July 2023, date of publication 20 July 2023, date of current version 2 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3297145

RESEARCH ARTICLE

Designing an Intrusion Detection for an Adjustable Speed Drive System Controlling a Critical Process

FARIS H. ALOTAIBI, (Graduate Student Member, IEEE), HASAN IBRAHIM, (Graduate Student Member, IEEE), JAEWON KIM, (Graduate Student Member, IEEE), P. R. KUMAR, (Life Fellow, IEEE), AND PRASAD ENJETI, (Life Fellow, IEEE)

Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843, USA

Corresponding author: Faris H. Alotaibi (alotaibi@tamu.edu)

This article is the updated version of [1] and include additional cyber attack scenarios and hardware experimental results among other changes.

ABSTRACT In this article, we address the cyber-security problem of industrial control systems (ICSs) when their sensor measurements may be compromised due to an attacker who has intercepted those measurements via a network. We introduce a general-purpose method "Dynamic Watermarking (DW)" to detect potential cyber-intrusions on speed sensor measurements within industrial control systems, which deploy an adjustable speed drive (ASD) to control a critical process. The DW method is injecting a random private low-amplitude signal with a zero mean Gaussian distribution, "watermark", into one of the input phase voltages powering the ASD system. The watermark signal propagates through the system including pulse width modulation (PWM) power conversion stage and motor, then ultimately appears in the speed sensor measurements. By deploying two statistical DW tests with two proper thresholds, the system can detect potential cyber-intrusions or unobservable cyber-attacks such as replay attacks and false data injection attacks (FDIA). The DW method tested on a laboratory-scale ASD system experimentally to protect the system against cyber-intrusions. This system, powered by a commercial PWM drive operating at 208 V, 3-phase, and 3.7 kW, served as our experimental platform.

INDEX TERMS Cyber-physical systems (CPSs), industrial control systems (ICSs), cyber-attacks, dynamic watermarking, adjustable speed drive (ASD), malicious sensors.

I. INTRODUCTION

Information and communication technologies have paved the path to the fourth industrial revolution in the industrial sector, known as Industry 4.0 [2]. Industry 4.0 represents the integration of advanced technologies via a network. This network connectivity significantly widens intrusion points that inject false data into the system such as false data injection attacks (FDIA), resulting in system disruption and/or damage [3], [4]. Moreover, cyber-intrusions are becoming more sophisticated and diverse and then, intruders have developed ways to camouflage their activities [5]. Attackers are now able to access industrial control systems (ICSs) remotely, allowing them to manipulate sensor data causing critical damage on large-scale systems [3], [6], [7]. One example of such intrusion was the Oldsmar Water Treatment Plant incident in 2021 where the unauthorized individual gained access to the system to increase the levels of sodium hydroxide in the water supply to potentially dangerous levels [8]. Another incident is the ransomware attack that disrupted operations at Semikron, a semiconductor manufacturer, significantly impacting production processes [9].

Adjustable speed drives (ASDs) are essential to the industrial sector. They control many critical industrial processes that are vital to national security, environmental safety, and even human safety. A number of ICSs including

The associate editor coordinating the review of this manuscript and approving it for publication was Mouloud Denai.

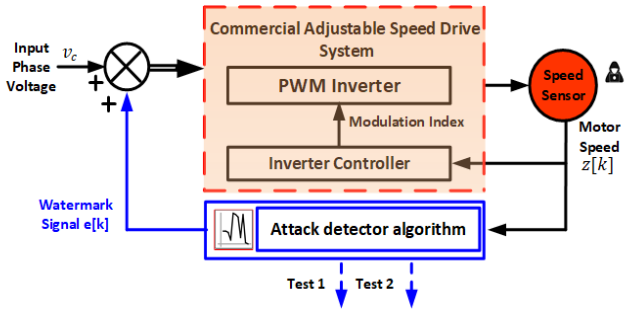

FIGURE 1. Block diagram of the proposed cyber-intrusion detection scheme.

ASDs consist of hardware devices and software that manage necessary control tasks. These ICSs depend on measurements reported from their sensors. However, such systems are vulnerable to cyber-intrusions. Several cyber-intrusions have been documented on critical industrial applications such as Stuxnet [10], [11], showing the vulnerability of such systems against sophisticated cyber-intrusions. In the Stuxnet attack, upon analysis by industry experts, it is believed that the speed sensor data was manipulated, resulting in ASDs controlling centrifuges to increase their speed causing them to self-destruct in time. Fig.1 shows the block diagram closed-loop control of an ASD powering a critical process. If the speed sensor is reporting lower speed, which is manipulated by an attacker (FDIA), the controller will increase the ASD's speed resulting in damaging the system. Therefore, designing a robust method for detecting potential cyber-intrusions is the main topic of this article.

A. RELATED WORKS

Several methods to secure ICSs against cyber-intrusions have been proposed [12], [13], [14], [15], [16], [17], [18], [19], [20]. Masood et al. [12] proposed employing blockchain technologies based fault-tolerant control (FTC) in Industry 4.0. However, a significant drawback of this approach is its limited scalability and potential delays in detecting and responding to cyber-attacks. In [13], a hybrid testbed to generate real-time data-sets for critical infrastructure is utilized for the validation of real-time attack detection algorithms. The approach is essentially a comparison tool between the data obtained via simulation and the plant data collected in real-time. However, this method fails in detecting stealth and unobservable attack. Machine learning (ML) and other data driven techniques based intrusion detection methods have been proposed for applications of ICSs in [14], [15], [16], [17], [18], [19], and [20]. Despite the effectiveness of these methods in detecting cyber attacks, they require large amounts of data to train to be effective, which may be difficult to obtain in ICSs where data is often scarce or difficult to access due to security and privacy concerns. Additionally, these detection methods may classify the manipulated signal as normal.

Multiple approaches to detect replay attacks in ICSs have been proposed in [21], [22], [23], [24], and [25], Guo et al. [21] proposed an output coding scheme where the control input is coded into the measurement output transmitted in the feedback channel. However, this approach faces limitations when applied to commercial industrial control systems due to the inaccessibility of control inputs. Consequently, the proposed method may not be practically viable for real-world applications, hindering its applicability and effectiveness in commercial settings. In the context of intrusion detection in wireless networks, the utilization of watermarking signals for encrypting and decrypting transmitted data has been proposed in [22] and [23]. However, it is important to note that implementing such schemes may necessitate additional computational resources and introduce overhead in terms of communication bandwidth. Ferrari et al. [24] proposed an intrusion detection to add watermark signal into the sensor outputs with a bank of filters. The approach may be compromised if the attacker can substitute the real data before watermarking signal addition. Bessa et al. [25] presents a control framework that uses a dual-rate control approach which presents certain advantages. However, its practical feasibility for commercial industrial applications is limited since it requires access to the control input for injecting the watermark signal.

B. MOTIVATION AND CONTRIBUTION

In this article, a method to reliably detect cyber-intrusions on sensor signals of an industrial control system employing an adjustable speed drive (ASD) system controlling a critical process is discussed. The proposed system comprises the implementation of a private, random signal with a zero mean average, referred to as "watermarking signal $e[k]$", which is added to the input phase voltage v_c of the DC-AC commercial inverter powering the motor [26]. This watermark is shown to create a unique signature (time-varying) that propagates through the system and appears in sensor signals that control the motor such as current, speed, torque, etc. Two statistical tests of variance are performed on sensor measurements to identify anomalies or compromises in the sensor measurements in the face of sophisticated cyber-attacks such as false data injection attacks (FDIA), stealth / unobservable attacks crafted to bypass traditional bad data detection mechanisms proposed by previous researchers. The proposed approach (intrusion detection for ASD system) has the following advantages:

- The watermark signal introduced into one of the input phase voltages (described in Fig. 2) is small in magnitude and does not show any discernible alteration in the system's performance.
- The proposed detection system does not alter the commercial hardware employed in the industrial control system by introducing the watermark signal into the input phase voltage powering the system.
- The proposed Dynamic Watermarking (DW) approach is shown to be a general-purpose method to detect

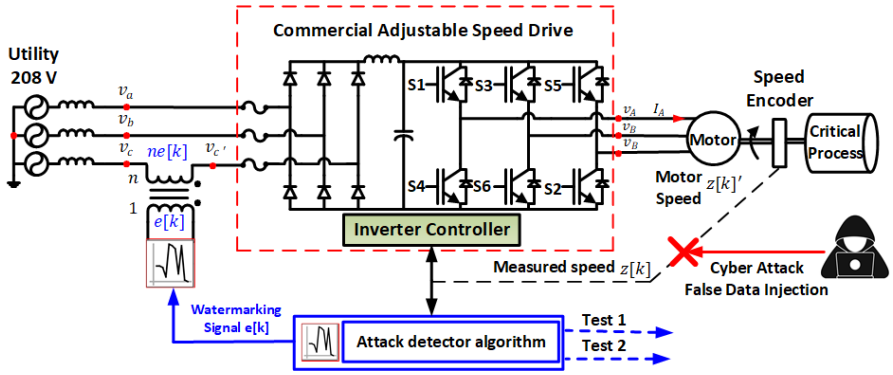

FIGURE 2. Detailed implementation of the proposed intrusion detection system for DC-AC inverter-controlled adjustable speed drive system controlling a critical process. [26].

unobservable FDIA such as record and replay on the motor speed sensor measurements.

- The proposed approach works outside of the closed-loop control system (described in Fig. 2) by employing established data-driven system identification methods [27], [29].
- The approach has been effectively implemented on a low-cost DSP-TI28379D, yielding robust performance as demonstrated by the obtained experimental results.

The remainder of this work is organized as follows: Section II details the various components and processes of the proposed detection mechanism on an adjustable speed drive system controlling a critical process, Section III shows the experimental results and discussions, and Section IV provides an overview of the conclusions drawn from this research, along with the knowledge acquired, and suggests potential areas for future research regarding cyber intrusion detection within the framework of ICSs.

II. PROPOSED INTRUSION DETECTION SYSTEM

Fig. 1 shows the overview of the proposed detection scheme and Fig. 2 shows the implementation of the detection scheme on a commercial ASD system. The proposed defense mechanism is injecting a watermark signal $e[k]$ into the input phase voltage v_c as shown in Fig. 2. A digital signal processor (DSP) is generating the watermarking signal $e[k]$ and a series-connected transformer to inject the $e[k]$ signal into the v_c. Then, this signal will propagate through the PWM power conversion stage and motor, and it will be appeared in the speed sensor measurements of the ASD system. The attack detector also receives the output speed measurements transmitted to the DC-AC commercial inverter controller. As shown in Fig. 2, the motor speed sensor measurements can potentially be altered/modified via possible cyber-intrusions. To identify the integrity of the motor speed sensor signal, the DSP performs two statistical *DW* tests. The background theory, algorithm robustness, and proofs of the *DW* method for detecting cyber-intrusions are explained in [32]. If one or both of the *DW* tests show high value, it can be concluded that the speed sensor measurements have been manipulated [32].

A. ASD AS A SINGLE INPUT SINGLE OUTPUT SYSTEM (SISO)

The ASD system shown in Fig. 2, can be considered as a single input single output (SISO) system. The relationship between the input (one of the phase voltages of the commercial ASD system) and output (motor speed) can be written as:

$$z[k+1] = Az[k] + Bv_c[k] + w[k+1] \tag{1}$$

where $z[k]$ is the motor speed measurements, $v_c[k]$ is one of the input phase voltages, and $w[k+1]$ is the system noise.

Then, the watermarking signal $e[k]$ is injected into the $v_c[k]$; thus, the equation 1 can be written as follows:

$$z[k+1] = Az[k] + B(v_c[k] + e[k]) + w[k+1] \tag{2}$$

Now (2) can be rewritten in two equations as follows:

$$z[k+1] - [Az[k] + B(v_c[k] + e[k])] = w[k+1] \tag{3}$$

or

$$z[k+1] - [Az[k] + Bv_c[k]] = Be[k] + w[k+1] \tag{4}$$

In (3), the left-hand side is equivalent to the system noise. In (4), the left-hand side is equivalent to the system noise with the addition of watermark signal $e[k]$. The next step is to validate the speed sensor measurements utilizing two *DW* variance tests that will compare the actual measurements against the SISO model with and without the watermarking signal $e[k]$ [32].

B. SYSTEM ID MODEL

The equation for the system model can be represented by (1) with the input phase voltage v_c and the output motor speed $z[k]$ as shown in Fig. 2. To analyze the system, matrices A and B as shown in (1) need to be calculated at specified an operating point. However, due to the nonlinearity of the ASD system, the system model is unknown. Therefore, identifying the values of A and B in (1) is a crucial task. Several system identification methods are described in [27], [28], and [29], we used the least squares method with (auto-regressive model with exogenous inputs) ARX format to determine parameters

in matrices A and B for our system [28]. The general form of the prediction model is expressed as follows:

$$\begin{aligned} &f(x[k-n:k], u[k-m:k], A_n, B_m) \\ &= \alpha_0 x[k] + \alpha_1 x[k-1] + \cdots + \alpha_n x[k-n] \\ &\quad + \beta_0 u[k] + \beta_1 u[k-1] + \cdots + \beta_m u[k-m] \end{aligned} \tag{5}$$

where x is the output speed $z[k]$, u is the input phase voltage v_c, $A_n = [\alpha_0 \ \alpha_1 \ \ldots \alpha_n]^T$, and $B_m = [\beta_0 \ \beta_1 \ \ldots \beta_m]^T$ represent the parameters associated with the inputs and outputs of our system, respectively.

Initially, the dimensions of the output m and input n are unidentified and need to be properly determined based on the data collected previously. For our system, the optimal dimension for the A and B matrices was determined to be four delays. Therefore, the prediction model for our specific system can be expressed as follows:

$$\begin{aligned} z_{system-ID}[k+1] = {} & a_1 z[k] + a_2 z[k-1] + a_3 z[k-2] \\ & + a_4 z[k-3] + b_1 v_c[k] + b_2 v_c[k-1] \\ & + b_3 v_c[k-2] + b_4 v_c[k-3] \end{aligned} \tag{6}$$

where:

$$A = [a_1 \ a_2 \ a_3 \ a_4] \tag{7}$$

$$B = [b_1 \ b_2 \ b_3 \ b_4] \tag{8}$$

Once A and B matrices are computed, the system identification algorithm can predict the output signal $z[k+1]$ according to (5). Fig. 6 shows how the system ID tracks the motor speed sensor measurements experimentally to validate the system ID approach.

C. PROPOSED INTRUSION DETECTION ALGORITHM

Sections II-A and II-B provide a comprehensive examination of the principles behind dynamic watermarking signals and their injection into the input phase voltage v_c that powers the inverter. The proposed intrusion detection scheme of an ASD system controlling a critical process is presented in Fig. 2. The feedback control system adjusts the motor speed based on the motor speed sensor signal output and the reference speed signal. In industrial environments, the motor speed, which is measured by a sensor, is commonly collected through a programmable logic controller (PLC) and transmitted to the system controller via an industrial intranet. As detailed earlier, such systems are susceptible to cyber intrusions, which can manipulate the actual motor speed signal to disrupt the system.

Test 1: The proposed intrusion detection scheme evaluates and compares the actual motor speed signal with the system ID model via Test 1 and Test 2 as detailed in this section. The variance of Test 1, represented by (9), compares the actual motor speed signal, $z[k+1]$, obtained via a sensor with the motor's speed obtained through system identification method ($z_{system-ID}$) as discussed in Section II-B. The equation can be rewritten for our specific plant as follows:

$$\lim_{K\to\infty} \frac{1}{K} \sum_{k=0}^{K-1} \Big(z[k+1] - (z_{system-ID}[k+1] + e[k]) \Big)^2 = \sigma_\omega^2 \tag{9}$$

The output from the system identification continuously depicts the expected output of a healthy system and serves as a reference for comparison with the actual system's measurement obtained from the sensor data. The algorithm evaluates both speed signals, $z[k+1]$ and $z_{system-ID}[k+1]$, for the presence of the watermarking signal $e[k]$ to determine if the system has been manipulated or not. During normal operation, Test 1 (9) output will produce the variance of the system noise, σ_w^2, which is nearly zero. However, in the case of an intrusion, where the speed sensor measurement, $z[k+1]$, is manipulated with false data, Test 1 (variance) will produce a higher value, indicating a possible intrusion on the system.

Test 2: Equation (10) details variance Test 2, which serves to assess the system's security status by comparing the actual motor speed signal data to the system identification model as described in Section II-B. The equation can be rewritten for our specific plant as follows:

$$\lim_{K\to\infty} \frac{1}{K} \sum_{k=0}^{K-1} \Big(z[k+1] - z_{system-ID}[k+1] \Big)^2 = B^2\sigma_e^2 + \sigma_\omega^2 \tag{10}$$

Unlike Test 1, the watermarking signal, ($e[k]$), is not included in the output of the system identification block. This redundancy in the intrusion detection system ensures a more robust approach [32]. In normal operating conditions, the result of Test 2 will reflect the system's noise variance, σ_w^2, and the variance of the watermarking signal, σ_e^2 which is nearly zero. However, in the event of an intrusion where the sensor data, $z[k+1]$, is altered, the output of Test 2 will be greater than expected, indicating a potential intrusion on the system.

III. EXPERIMENTAL RESULTS AND DISCUSSION

In this section two attack scenarios that were implemented on a 208V, 3-phase 3.7 kW adjustable speed drive system operating in closed-loop speed control (Table 1) and Fig. 3 [33] are discussed. These malicious intrusions include speed amplitude manipulation and replay attack. Further, Fig. 4 shows; the motor speed at 1200 rpm (Ch 1), PWM output voltage v_{AB} (Ch 2), and motor current I_A in steady state (Ch 3). The proposed detection system has been implemented on a low-cost DSP (TI28379D).

As discussed in section I, the watermarking signal used in the system is extremely small and does not impact the operation of the inverter or motor. Fig. 5 provides additional evidence of the minimal impact of the watermarking signal by showcasing the watermark signal $e[k]$ (Ch 1), which is 2.5V (equivalent to 2% of the phase voltage v_c). The figure demonstrates two scenarios: one without the watermarking

TABLE 1. Experimental PWM ASD inverter and induction motor setup [33].

Parameter	Magnitude
Commercial Inverter Power	3.7 KW
Switching Frequency	4 KHz
Line Frequency	60 Hz
Input Voltage v_{ab}	208 V
Rated Motor Speed	1770 R.P.M
Number of Motor Poles	4

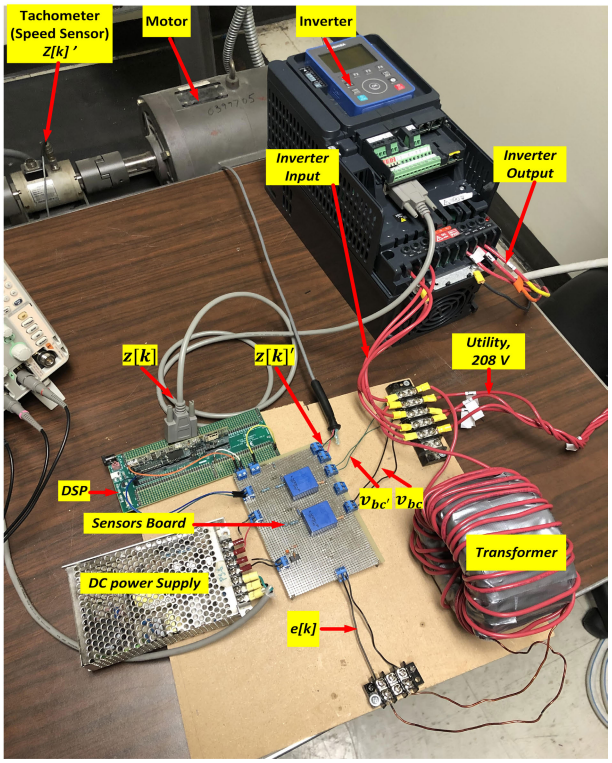

FIGURE 3. Experimental implementation of the proposed intrusion detection scheme on a 3 phase, 208V, 3.7kW PWM ASD inverter motor drive system (schematic shown in Fig. 2).

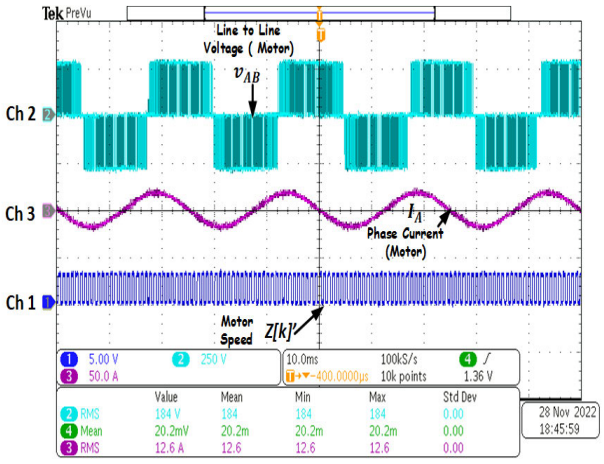

FIGURE 4. Experimental results of the ASD system (Fig. 2) with superimposed watermarking signal $e[k]$ into the phase input voltage v_c, (Ch 1) Motor Speed (tachometer signal), $z[k]'$, (Ch 2) Line to Line voltage of the motor, v_{AB}, (Ch 3) Phase current of the motor, I_A. The oscilloscope scale: (time: sec/div is 10m),(Ch 1: volt/div is 5), (Ch 2: volt/div is 250), and (Ch 3: A/div is 50).

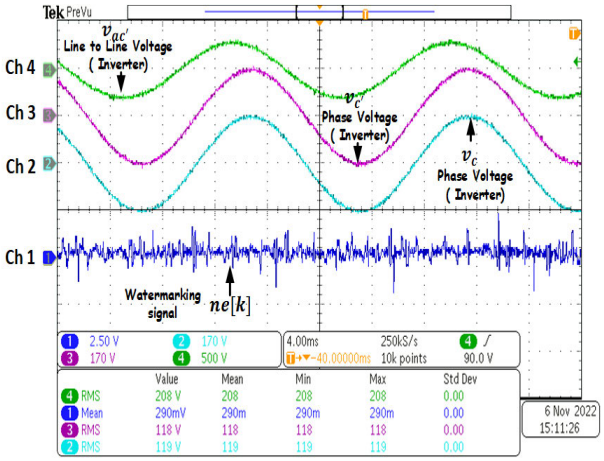

FIGURE 5. Experimental results of the ASD system (Fig. 2) with superimposed watermarking signal $e[k]$ into the input phase voltage v_c, (Ch 1) watermarking signal, $ne[k]$ (note: n is the turns ratio = 5), (Ch 2) Phase voltage without watermarking signal, v_c, (Ch 3) Phase voltage with superimposed watermarking signal, v_c', (Ch 4) Line to Line voltage with superimposed watermarking signal, $v_{ac'}$. The oscilloscope scale: (time: sec/div is 4 ms),(Ch 1: volt/div is 2.5), (Ch 2: volt/div is 170), (Ch 3: volt/div is 170), and (Ch 4: volt/div is 500).

signal (Ch 2) and another with the watermarking signal (Ch 3). It can be observed that there are no discernible visual differences between the two cases, indicating the negligible effects of adding the watermarking signals to the sensors. Furthermore, the figure also displays the line-to-line voltage $v_{ac'}$ (Ch 4) applied to the inverter terminals with the addition of the watermarking signal.

A. SYSTEM ID VALIDATION

In this section, Fig. 6 shows the validation of the system identification (system ID) through experimental results. The comparison between the system ID and the actual motor speed sensor data demonstrates the system ID's high accuracy in accurately tracking the measured motor speed.

B. EVALUATION OF VARIOUS TYPES OF CYBER ATTACKS ON ASD MOTOR DRIVE SYSTEM (Fig. 2)

In this section, the experiment results on PWM ASD inverter motor drive setup (Table 1 and Fig. 3) are discussed. Fig. 3 shows the hardware setup of the experiment. As shown in Fig. 2 and Fig. 3, $z[k]'$ represents the motor speed signal which is processed via a DSP and $z[k]$ represents the manipulated (attacked) signal generated by the DSP. The DSP is used to perform (simulate) several attack scenarios such as FDIA on the motor via altering motor speed $z[k]$ and feeding it back to the controller as a manipulated signal. Fig. 7 shows the normal operation of the system where (Ch 1) is the motor speed $z[k]'$, (Ch 2) is the speed signal generated by the DSP $z[k]$, and (Ch 4) and (Ch 3) represent variance tests 1 and 2, respectively. It is noted that for normal operation (no attack) the mean values of the variance for Test 1 and Test 2 are 407mV and 382 mV, respectively. These values will serve

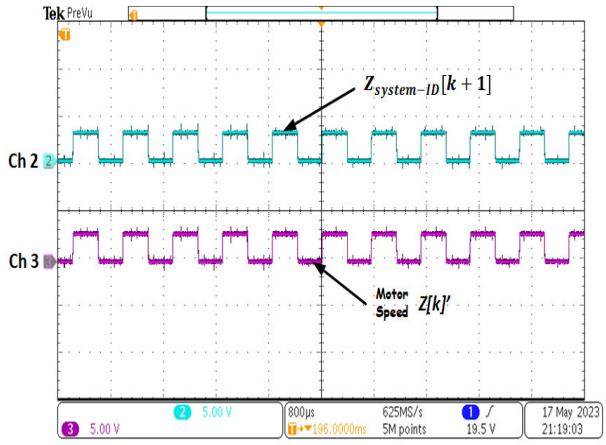

FIGURE 6. Experimental results of the ASD system (Fig. 2) demonstrating the system ID validation (Discussed in Section II-B.) (Ch 3) actual motor speed signal, $z[k]'$, (Ch 4) The predicted motor speed signal, $z_{system-ID}[k+1]$. The oscilloscope scale: (time: sec/div is 800 μs),(Ch 3: volt/div is 5), and (Ch 4: volt/div is 5).

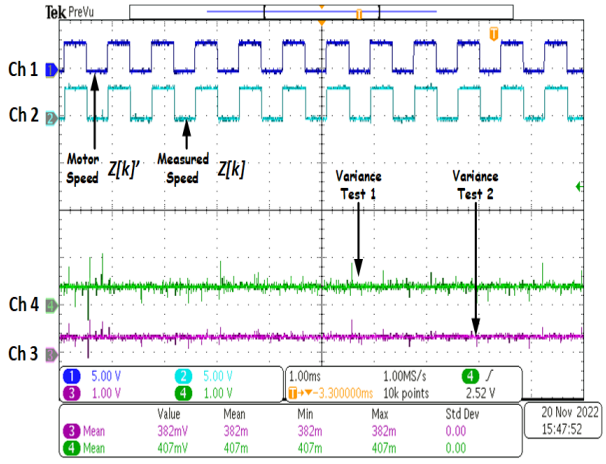

FIGURE 7. Experimental results show the normal operation of the ASD, (Ch 1) actual motor speed signal, $z[k]'$, (Ch 2) feedback motor speed signal, $z[k]$, (Ch 3) mean variance of test 2, and (Ch 4) mean variance of test 1. The oscilloscope scale: (time: sec/div is 1 ms),(Ch 1: volt/div is 5), (Ch 2: volt/div is 5), (Ch 3: volt/div is 1), and (Ch 4: volt/div is 1).

as a comparison baseline to identify cyber-intrusions on the system when they occur.

1) MOTOR SPEED INCREASE ATTACK

In this attack scenario, the assumption is that an attacker gains control of the incoming motor speed measurements, $z[k]'$, which is equal to 1200 rpm in normal operation and then, the attacker is able to modify the signal by decreasing it to 1100 rpm (false data injection). The system controller now reacts to regulate the speed by increasing the speed above 1200 rpm to 1345 rpm. Fig. 8 details this scenario of speed measurement manipulation. It is shown in Fig. 8 that both variance tests signals show a sudden increase, indicating that the motor speed signal has been manipulated. Fig. 9 shows the continued steady-state operation of the motor drive system at the increased speed level of 1345 rpm. The steady-state values of Test 1 and Test 2 are observed to be 2.45 and

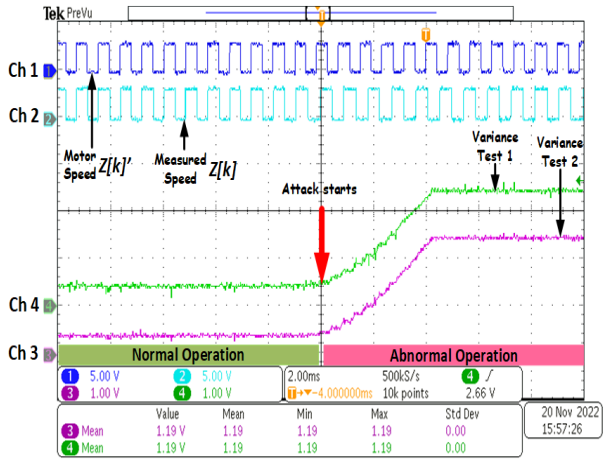

FIGURE 8. Experimental results show motor speed false data injection that reports lower speed, this results in motor speed to increase, (Ch 1) actual motor speed,$z[k]'$, (Ch 2) manipulated motor speed signal (reduced by 8.3%),$z[k]$, (Ch 3) mean-variance of test 2, and (Ch 4) mean-variance of test 1. The oscilloscope scale: (time: sec/div is 2 ms),(Ch 1: volt/div is 5), (Ch 2: volt/div is 5), (Ch 3: volt/div is 1), and (Ch 4: volt/div is 1). Notice the rapid increase in Test 1 and Test 2 variance indicating intrusion detection.

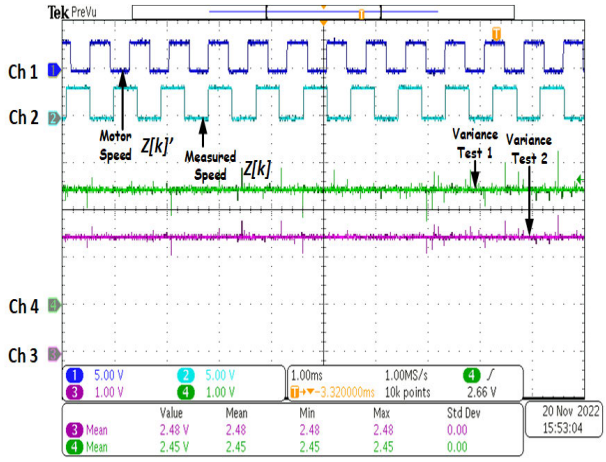

FIGURE 9. Experimental results show the mean variance values of test 1&2 when the attack happens to show an attack. The mean variances of test 1&2 jumps from 407 mV & 382 mV to 2.45 & 2.48 respectively, which is passed the threshold value of 1, (Ch 1) motor speed, $z[k]'$, (Ch 2) feedback motor speed, $z[k]$, (Ch 3) mean variance of test 2, (Ch 4) mean variance of test 1. The oscilloscope scale: (time: sec/div is 1 ms),(Ch 1: volt/div is 5), (Ch 2: volt/div is 5), (Ch 3: volt/div is 1), and (Ch 4: volt/div is 1).

2.48, respectively. Comparing this to Fig. 7, both Test 1 and Test 2 show a six-fold increase, clearly indicating speed manipulation and successful detection within milliseconds after the attack begins.

2) REPLAY ATTACK

In the replay attack, the attacker has access to the motor speed data $z[k]'$ and is able to record the real speed measurements of the motor. The attacker then disconnects the actual measured speed signal $z[k]'$ and transmits the pre-recorded signal to the motor controller to test the system operation and may decide to further manipulate the speed at a later time. Since the recorded signal is identical to the actual motor speed

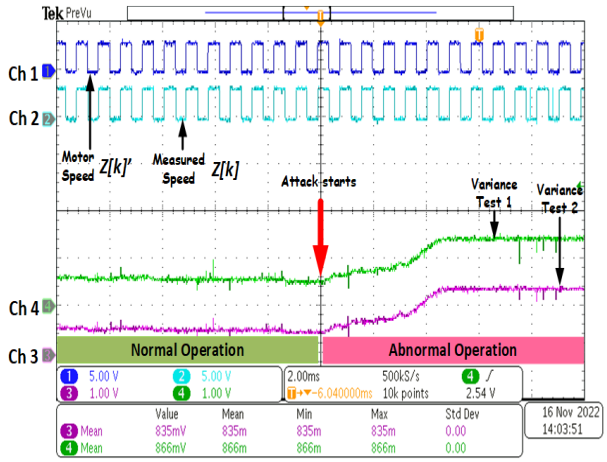

FIGURE 10. Experimental results show motor speed replay attack scenario, (Ch 1) actual motor speed,$z[k]'$, (Ch 2) feedback motor speed signal,$z[k]$, (Ch 3) mean variance of test 2, (Ch 4) mean variance of test 1. It is observed that there is a significant increase in the magnitude of Test 1 and Test 2 when the attack begin. The oscilloscope scale: (time: sec/div is 2 ms),(Ch 1: volt/div is 5), (Ch 2: volt/div is 5), (Ch 3: volt/div is 1), and (Ch 4: volt/div is 1).

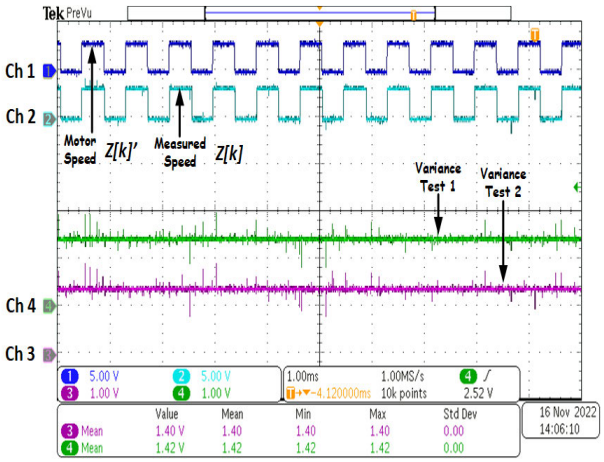

FIGURE 11. Experimental results show the mean variance values of test 1&2 when the attack occurs to show an attack. The mean variances of test 1&2 jumps from 407 mV & 382 mV to 1.42 & 1.40 respectively, which is passed the threshold value of 1, (Ch 1) motor speed, $z[k]'$, (Ch 2) feedback motor speed, $z[k]$, (Ch 3) mean variance of test 2, and (Ch 4) mean variance of test 1. The oscilloscope scale: (time: sec/div is 1 ms),(Ch 1: volt/div is 5), (Ch 2: volt/div is 5), (Ch 3: volt/div is 1), and (Ch 4: volt/div is 1).

signal, it is nearly impossible to detect any manipulation on the actual system's signals using conventional physics-based cyber security methods.

Fig. 10 shows the variance Test 1 (9) and variance Test 2 (10) results of the replay attack on the speed sensor measurements. The attacker recorded the actual speed sensor data at some time in the past, then replays them back to the controller as a current speed sensor measurement at the attack time. It should be noted that the recorded speed signal that feeds back to the controller has an embedded watermark signal from a previous time, which is a different signature since the random nature of the watermark signal $e[k]$. Fig. 10 illustrates that there's a sudden increase in the variance of Test 1 and Test 2, indicating a cyber intrusion on the motor speed sensor measurements. As it is shown in Fig. 11, (Ch 3 and Ch 4) shows the steady state values of both variance tests are observed to be 1.42 and 1.4, respectively after the attack occurs. Comparing this to Fig. 7, both tests show 3.5 times increase. Therefore, the *DW*-based two specific tests with two pre-specified thresholds can detect the replay attack successfully once the attack initiates.

C. EFFECT OF UTILITY VOLTAGE DISTURBANCES ON THE INTRUSION DETECTION MECHANISM

In this section, the resilience of the proposed detection algorithm to distinguish between actual manipulations on the sensors and a natural disturbance on the grid will be demonstrated. Fig. 12 shows natural disturbances on the input utility ac voltage and their effect on the detection algorithm, namely the variance values of Test 1 and Test 2. A 30 % voltage sag on $v_{ac'}$ is triggered, as shown in Fig. 12. This natural change in the grid's voltage shows negligible effect on variance values in Test 1 and Test 2 proving the robustness of the proposed method to not only detect manipulations but also to accurately differentiate between an attack and a natural change in the system.

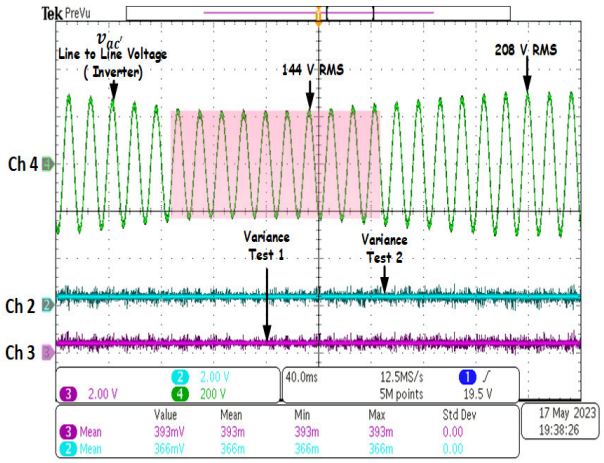

FIGURE 12. Effect of utility voltage disturbance on the intrusion detection. (Ch 4) Input voltage $v_{ac'}$ dropped from 208 V RMS to 144 V RMS (30 % voltage sag). (Ch 3) Mean variance value of Test 1, (Ch 2) Mean variance value of Test 2. The oscilloscope scale: (time: sec/div is 40 ms), (Ch 2: volt/div is 2), (Ch 3: volt/div is 2), and (Ch 4: volt/div is 200). It is observed that Test 1 and Test 2 do not respond during the normal operation of the system.

IV. CONCLUSION

In this article, a general-purpose detection method "Dynamic Watermarking" against potential cyber intrusions on speed sensor measurements on an adjustable speed drive (ASD), has been discussed. Experimental test results of the Dynamic Watermarking (DW) method on a lab-scale 208 V, 3-phase, 3.7 kW induction motor drive system have been shown to detect speed sensor signal manipulations and replay attacks within 0.4 ms. Furthermore, the effect of input voltage disturbances has been evaluated. The proposed detection system

has been implemented on a low-cost DSP (TI28379D). The additional cost of the additional hardware is low to provide a robust defense against cyber-attacks in critical processes. We are applying the Dynamic Watermarking (DW) method on multiple ASDs connected system to identify the attack locations.

REFERENCES

[1] F. Alotaibi, H. Ibrahim, J. Kim, and P. Enjeti, "Designing an intrusion proof adjustable speed drive system controlling a critical process," in *Proc. IEEE 13th Int. Symp. Power Electron. Distrib. Gener. Syst. (PEDG)*, Kiel, Germany, Jun. 2022, pp. 1–7, doi: 10.1109/PEDG54999.2022.9923160.

[2] O. Elijah, P. A. Ling, S. K. A. Rahim, T. K. Geok, A. Arsad, E. A. Kadir, M. Abdurrahman, R. Junin, A. Agi, and M. Y. Abdulfatah, "A survey on industry 4.0 for the oil and gas industry: Upstream sector," *IEEE Access*, vol. 9, pp. 144438–144468, 2021, doi: 10.1109/ACCESS.2021.3121302.

[3] J. Weiss and J. Weiss, *Protecting Industrial Control Systems From Electronic Threats*. New York, NY, USA: Momentum Press, 2010.

[4] J. Weiss, R. Stephens, and N. Miller, "Control system cyber incidents are real—And current prevention and mitigation strategies are not working," *Computer*, vol. 55, no. 1, pp. 128–137, Jan. 2022, doi: 10.1109/MC.2021.3124359.

[5] M. Wan, J. Li, Y. Liu, J. Zhao, and J. Wang, "Characteristic insights on industrial cyber security and popular defense mechanisms," *China Commun.*, vol. 18, no. 1, pp. 130–150, Jan. 2021, doi: 10.23919/JCC.2021.01.012.

[6] C. Lohninger, B. Voglauer, K. Matheis-Weiss, and M. Kozek, "Efficient modelling and control design for suppression of pressure oscillations in an industrial condensation process," in *Proc. 22nd Int. Conf. Syst. Theory, Control Comput. (ICSTCC)*, Sinaia, Romania, Oct. 2018, pp. 31–38, doi: 10.1109/ICSTCC.2018.8540686.

[7] R. Hunter and J. Weiss, "Cybersecurity and data centers," in *Data Center Handbook: Plan, Design, Build, and Operations of a Smart Data Center*. Hoboken, NJ, USA: Wiley, 2021, pp. 349–358, doi: 10.1002/9781119597537.ch20.

[8] C. Vasquez. (Apr. 10, 2023). Did someone really hack into the Oldsmar, Florida, water treatment plant? New details suggest maybe not. CyberScoop. [Online]. Available: https://cyberscoop.com/water-oldsmar-incident-cyberattack/

[9] S. Gatlan. (Aug. 2, 2022). Semiconductor manufacturer Semikron hit by LV ransomware attack. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/semiconductor-manufacturer-semikron-hit-by-lv-ransomware-attack/

[10] K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, NY, USA: Crown Publishing Group, 2014.

[11] D. Kushner, "The real story of stuxnet," *IEEE Spectr.*, vol. 50, no. 3, pp. 48–53, Mar. 2013, doi: 10.1109/MSPEC.2013.6471059.

[12] A. B. Masood, A. Hasan, V. Vassiliou, and M. Lestas, "Control over blockchain for data-driven fault tolerant control in industry 4.0," in *Proc. 20th Medit. Commun. Comput. Netw. Conf. (MedComNet)*, Paphos, Cyprus, Jun. 2022, pp. 131–139, doi: 10.1109/MedComNet55087.2022.9810433.

[13] M. Noorizadeh, M. Shakerpour, N. Meskin, D. Unal, and K. Khorasani, "A cyber-security methodology for a cyber-physical industrial control system testbed," *IEEE Access*, vol. 9, pp. 16239–16253, 2021, doi: 10.1109/ACCESS.2021.3053135.

[14] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 3, pp. 377–391, Mar. 2022, doi: 10.1109/JAS.2021.1004261.

[15] M. Kravchik and A. Shabtai, "Efficient cyber attack detection in industrial control systems using lightweight neural networks and PCA," *IEEE Trans. Depend. Sec. Comput.*, vol. 19, no. 4, pp. 2179–2197, Jul. 2022, doi: 10.1109/TDSC.2021.3050101.

[16] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021, doi: 10.1109/TII.2020.3023430.

[17] M. R. G. Raman and A. P. Mathur, "A hybrid physics-based data-driven framework for anomaly detection in industrial control systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 9, pp. 6003–6014, Sep. 2022, doi: 10.1109/TSMC.2021.3131662.

[18] K. H. Kim, B. I. Kwak, M. L. Han, and H. K. Kim, "Intrusion detection and identification using tree-based machine learning algorithms on DCS network in the oil refinery," *IEEE Trans. Power Syst.*, vol. 37, no. 6, pp. 4673–4682, Nov. 2022, doi: 10.1109/TPWRS.2022.3150084.

[19] E. A. Boateng, J. W. Bruce, and D. A. Talbert, "Anomaly detection for a water treatment system based on one-class neural network," *IEEE Access*, vol. 10, pp. 115179–115191, 2022, doi: 10.1109/ACCESS.2022.3218624.

[20] W. Hao, T. Yang, and Q. Yang, "Hybrid statistical-machine learning for real-time anomaly detection in industrial cyber–physical systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 20, no. 1, pp. 32–46, Jan. 2023, doi: 10.1109/TASE.2021.3073396.

[21] H. Guo, Z.-H. Pang, J. Sun, and J. Li, "An output-coding-based detection scheme against replay attacks in cyber-physical systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 10, pp. 3306–3310, Oct. 2021, doi: 10.1109/TCSII.2021.3063835.

[22] J. Huang, D. W. C. Ho, F. Li, W. Yang, and Y. Tang, "Secure remote state estimation against linear man-in-the-middle attacks using watermarking," *Automatica*, vol. 121, Nov. 2020, Art. no. 109182, doi: 10.1016/j.automatica.2020.109182.

[23] D. Wang, J. Huang, Y. Tang, and F. Li, "A watermarking strategy against linear deception attacks on remote state estimation under K–L divergence," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 3273–3281, May 2021, doi: 10.1109/TII.2020.3009874.

[24] R. M. G. Ferrari and A. M. H. Teixeira, "A switching multiplicative watermarking scheme for detection of stealthy cyber-attacks," *IEEE Trans. Autom. Control*, vol. 66, no. 6, pp. 2558–2573, Jun. 2021, doi: 10.1109/TAC.2020.3013850.

[25] I. Bessa, C. Trapiello, V. Puig, and R. M. Palhares, "Dual-rate control framework with safe watermarking against deception attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 12, pp. 7494–7506, Dec. 2022, doi: 10.1109/TSMC.2022.3160791.

[26] P. Enjeti, P. R. Kumar, and L. Xie, "Methods and systems for detecting compromised sensors using dynamic watermarking," U.S. Patent Appl. 63/352 131, Jun. 14, 2022.

[27] J. Schoukens, *Mastering System Identification in 100 Exercises*. Hoboken, NJ, USA: Wiley, 2012.

[28] P. R. Kumar and P. Varaiya, *Stochastic Systems: Estimation, Identification, and Adaptive Control*. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 2015, pp. 189–228.

[29] J. Ding, F. Ding, X. P. Liu, and G. Liu, "Hierarchical least squares identification for linear SISO systems with dual-rate sampled-data," *IEEE Trans. Autom. Control*, vol. 56, no. 11, pp. 2677–2683, Nov. 2011, doi: 10.1109/TAC.2011.2158137.

[30] F. Ding and T. Chen, "Identification of Hammerstein nonlinear ARMAX systems," *Automatica*, vol. 41, no. 9, pp. 1479–1489, Sep. 2005.

[31] L. Ljung, *System Identification: Theory for the User*. Upper Saddle River, NJ, USA: Prentice-Hall, 1986.

[32] B. Satchidanandan and P. R. Kumar, "Dynamic watermarking: Active defense of networked cyber–physical systems," *Proc. IEEE*, vol. 105, no. 2, pp. 219–240, Feb. 2017, doi: 10.1109/JPROC.2016.2575064.

[33] Toshiba International Corporation. *AS3 | Motors Drives*. Accessed: Jul. 1, 2023. [Online]. Available: https://www.toshiba.com/tic/motors-drives/low-voltage-adjustable-speed-drives/lv-industrial-drives/as3/VFAS3-2037P

FARIS H. ALOTAIBI (Graduate Student Member, IEEE) received the B.S. degree in electrical engineering from Umm Al-Qura University, Saudi Arabia, in 2014, and the M.S. degree in electrical engineering from Gannon University, PA, USA, in 2018. He is currently pursuing the Ph.D. degree with Texas A&M University, College Station, TX, USA. His research interests include advanced power electronics converters design and cyber physical systems security.

HASAN IBRAHIM (Graduate Student Member, IEEE) was born in Kuwait, in 1996. He received the B.S. and M.S. degrees in electrical engineering from Texas A&M University, College Station, where he is currently pursuing the Ph.D. degree in electrical engineering with the Power electronics and Power Quality Laboratory. His current research interests include power electronics, power converter design and control, and cyber physical systems security.

JAEWON KIM (Graduate Student Member, IEEE) is currently pursuing the Ph.D. degree in computer engineering with the Department of Electrical and Computer Engineering, Texas A&M University. He is also a small unmanned aircraft systems (sUAS) pilot. His current research interests include cyber-physical systems (CPS), cyber-security for CPS, machine learning, reinforcement learning, system identification, multi-agent unmanned vehicle systems, resilient real-time network architectures for unmanned aerial and ground vehicles, and fog robotics.

P. R. KUMAR (Life Fellow, IEEE) received the B.Tech. degree from IIT Madras, in 1973, and the D.Sc. degree from Washington University in St. Louis, in 1977. He was a Faculty Member of UMBC (1977–1984) and University of Illinois Urbana–Champaign (1985–2011). He is currently with Texas A&M University. His current research interests include machine learning, cybersecurity, power systems, 5G, unmanned air vehicle systems, cyberphysical systems, and wireless networks. He is a member of the World Academy of Sciences, the U.S. National Academy of Engineering, and the Indian National Academy of Engineering. He was awarded a Doctor Honoris Causa by ETH Zürich. He has received the IEEE Alexander Graham Bell Medal, the IEEE Field Award for Control Systems, the Donald P. Eckman Award of the American Automatic Control Council, the Fred W. Ellersick Prize of the IEEE Communications Society, the Outstanding Contribution Award of ACM SIGMOBILE, the Infocom Achievement Award, the SIGMOBILE Test-of-Time Paper Award, and the COMSNETS Outstanding Contribution Award. He is a fellow of ACM. He was Leader of the Guest Chair Professor Group on Wireless Communication and Networking, Tsinghua University, and a D. J. Gandhi Distinguished Visiting Professor with IIT Bombay. He is an Honorary Professor with IIT Hyderabad. He was awarded the Distinguished Alumnus Award from IIT Madras, the Alumni Achievement Award from Washington University in St. Louis, and the Daniel Drucker Eminent Faculty Award from the College of Engineering, University of Illinois.

PRASAD ENJETI (Life Fellow, IEEE) received the B.E. degree in electrical engineering from Osmania University, Hyderabad, India, in 1980, the M.Tech. degree in electrical engineering from the Indian Institute of Technology Kanpur, Kanpur, India, in 1982, and the Ph.D. degree in electrical engineering from Concordia University, Montreal, QC, Canada, in 1988.

He holds the Texas Instruments Jack Kilby Chair of the Electrical and Computer Engineering Department, and he has been a member of Texas A&M University Faculty, since 1988. He is widely acknowledged to be a distinguished teacher, a scholar, and a researcher. To date, he has graduated 35 Ph.D. and 53 M.S. students. 15 of his Ph.D. students currently serve as a faculty in institutions at home and across the world while others have leadership positions in industry. He along with his students has more than 100 journal publications and received numerous best paper awards from the IEEE. His primary research interest includes advancing power electronic converter designs to address complex power management issues. His current research focus has been on innovative power electronic solutions to interface renewable energy sources to electric utility and developing real time digital tools to enhance cybersecurity and condition monitoring of industrial systems.

Dr. Enjeti was a recipient of the IEEE Fellow Award, in 2000, the Texas A&M University Association of Former Students University Level Teaching Award, in 2001, the R. David Middlebrook Technical Achievement Award from the IEEE Power Electronics Society, in 2012, and the IEEE IAS Distinguished Achievement Award, in 2021, among the many honors.