Designing an Intrusion Proof Adjustable Speed Drive System Controlling a Critical Process

1st Faris Alotaibi
Texas A&M University
College Station, U.S.A
alotaibi@tamu.edu

2nd Hasan Ibrahim
Texas A&M University
College Station, U.S.A
hasanibrahim@tamu.edu

3rd Jaewon Kim
Texas A&M University
College Station, U.S.A
jwkim8804@tamu.edu

4th Prasad Enjeti
Texas A&M University
College Station, U.S.A
enjeti@tamu.edu

***Abstract*—In this paper, an intrusion proof adjustable speed drive system controlling a critical process in an industrial control system is detailed. In such a system, should the motor speed sensor signal data be compromised and/or altered via a cyber-attack, the system can potentially be unregulated, over speed and/or malfunction thereby disrupting the critical process. The proposed active detection scheme detailed in this paper introduces a private (secret) random signal termed as "watermark" into the inverter control signal that determines the PWM gating signals of the DC-AC inverter powering the motor. The watermarking signal introduced into the PWM modulation for the DC-AC inverter is shown to propagates its unique signature, which appears in all sensors signals at the inverter output such as voltage/current/speed used to control the motor. Now employing the measured data (from sensors), two statistical variance tests are conducted to identify anomalies if any in the presence of the watermarking signal. It is shown when an intrusion occurs to manipulate the sensor data to disturb and/or destabilize the process, the proposed tests immediately display a high value indicating a compromise in sensor data. It is shown that the proposed system is capable of immediate detection of a sophisticated attacks such as record/reply attack in which the actual speed sensor is disconnected and a prerecorded speed signal from the past of the same magnitude is played back to the controller. Several types of cyber-attacks such as speed reduction/increase including vibration have been tested. Extensive simulation results verify the proposed concepts. Experimental results will be discussed in the conference presentation.**

***Index Terms*—Cybersecurity, dynamic watermarking, malicious sensors, cyber-physical system, industrial control system ICS, induction motor.**

I. Introduction

Industry 4.0 refers to a new phase in the Industrial Revolution that focuses heavily on inter-connectivity, automation, machine learning, and real-time data. Industry 4.0, which encompasses industrial internet of things (IIoT) and smart manufacturing, marries physical production and operations with smart digital technology, machine learning, and big data to create a more holistic and better connected ecosystem for many industries. IIoT systems allow simplification of product lines and ease of installation and commissioning, such flexibility introduces the potential for misuse. Industrial control systems (ICS) are increasingly tied to the IIoT to enable remote monitoring and control, creating new vulnerabilities. Malicious actors may now remotely access hardware, change settings, or reprogram devices to cause real physical damage on an unlimited scale [1], [4]. Adjustable speed drive systems (ASDs) are widely used to control many critical industrial processes. ASDs are used in numerous industrial applications that are vital to national security, environmental safety, and even human safety. ASDs generally become more vulnerable once connected to an IIoT ecosystem. Critical industrial applications have already demonstrated their vulnerability to cyber-attacks such as Stuxnet [2], [3], in which a group of ASDs controlling centrifuges (in a nuclear facility) were attacked to increase their speed that introduced unacceptable wobble and caused them to self-destruct. Since the safety limits of ASDs were programmed in software, some industry experts believe that Stuxnet attack spoofed the speed sensor signal data, allowing the centrifuges to operate beyond safety limits [2], [3].

It is well known that employing IIoT enables Industry 4.0 with remote tuning and parameter updates of ASD systems. Such features save significant time in controlling industrial processes. Such a connected environment also makes ASDs more vulnerable due to additional entry points for external attacks. Consequently, safe use of ASDs within an overall IIoT ecosystem requires a robust, validated cyber security solution that can be adapted to the latest technological advancements and is a subject matter of this paper.

Fig.1 shows an example DC-AC inverter-controlled induction motor ASD system powering a critical process. In such a system, should the motor speed sensor data collected and transmitted via IIoT (PLC) to the motor controller be compromised/spoofed via a cyber-attack and/or an intrusion, the system can potentially over speed and/or malfunction and damage the process. In this paper a robust active intrusion detection system is proposed. The proposed system consists of a private (secret) random signal (of zero mean average) termed as "watermark" is added to the inverter control signal (modulation index m_a) , see Fig.1 that determines the PWM switching duty cycle via the gating signals of the DC-AC inverter powering the motor. The watermarking signal introduced into the PWM modulation is shown to propagates its unique signature, which appears in all sensors signals such as voltage/current/speed used to control the critical process. Now employing the measured data (from sensors), two statistical variance tests are conducted to identify anomalies if any in the presence of the watermarking signal. It is shown when an intrusion were to occur to manipulate the sensor data to disturb and/or destabilize the process, the proposed tests immediately

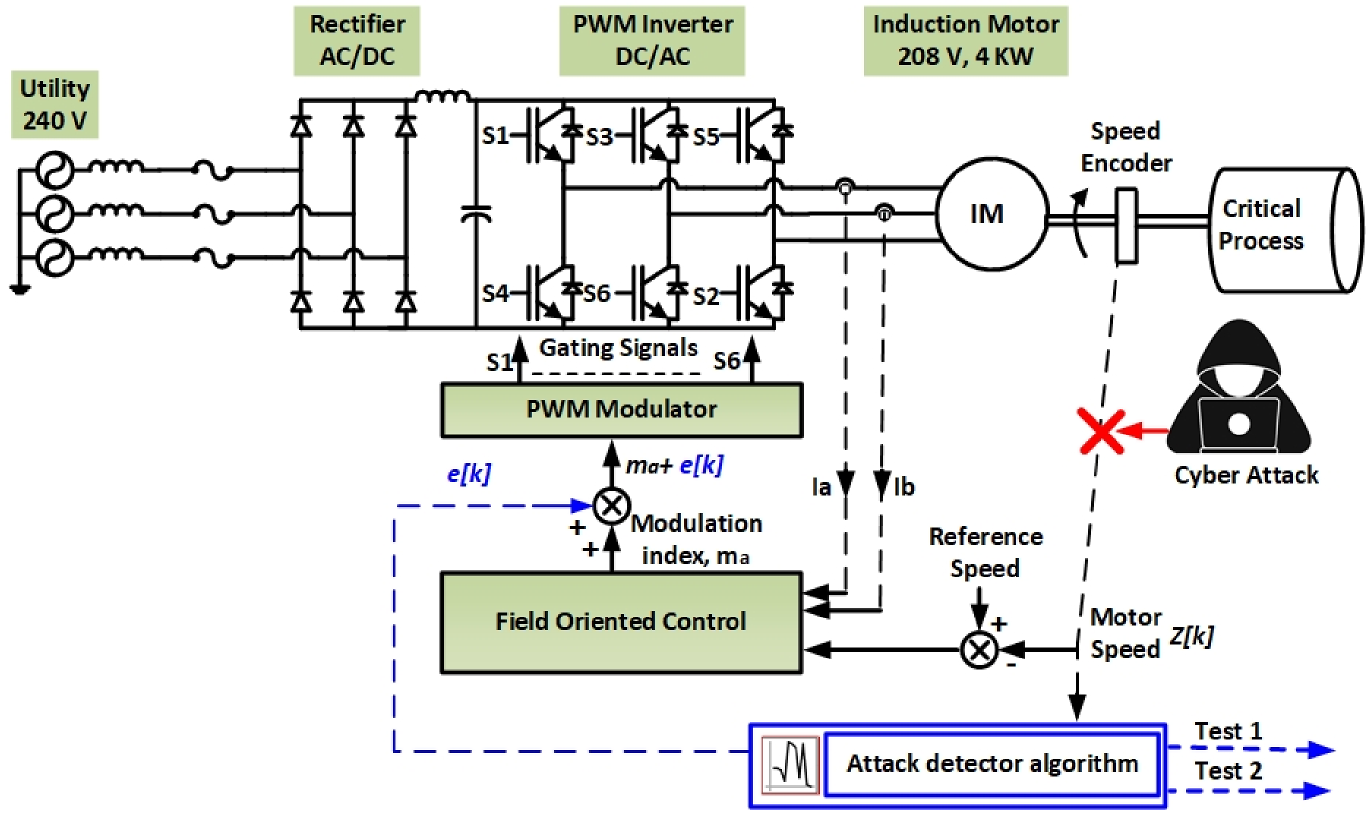

Fig. 1. Proposed intrusion detection system for DC-AC inverter-controlled induction motor drive powering a critical process.

display a high value indicating a compromise in sensor data. The proposed approach has the following advantages:

- A small magnitude private (secret) random signal (small magnitude with zero mean and time varying) termed as “watermark” introduced into the inverter control signal (modulation) does not result in any noticeable change in system behavior.
- The watermarking signal introduced into the PWM modulation propagates through the switching inverter and appears in all the measured sensor data such as voltage/current/speed etc. The presence of the watermark signature can be detected via two statistical variance tests. The tests are shown to indicate a high value at the instant any of the sensor date is manipulated externally.
- The proposed approach is shown to detect sophisticated attacks / intrusions such as when the attacker upon gaining access, records the data, then disconnects the sensor and replays the prerecorded signal to the controller. Since the prerecorded signals do not have the same random signature of the current watermark signal, the two variance tests are shown to indicate a high value at the instant such an intrusion were to occur. The approach is shown to also detect various other types of attacks such as changes in magnitude, phase shift, additional noise added etc. to the sensor signals.
- As an additional side benefit, the proposed system can now detect sensor malfunction, i.e. should a sensor controlling the critical process malfunction and/or report a an high enough error due to poor calibration etc, the two tests indicate high value. This warrants a thorough incident postmortem to determine the failure of the sensor and/or a cyber attack. Continuous condition monitoring of all the sensors in the critical process is therefore an additional benefit of the proposed method.

II. Proposed Intrusion Detection System for Adjustable Speed Drive Systems.

This section details various components of the proposed intrusion detection system on an ASD system controlling a critical process.

A. Dynamic Watermarking

As detailed in the earlier section and as shown in Fig. 1, a private (secret) random signal (of zero mean average) termed as “watermark” $e[k]$ is added to the inverter control signal (modulation index m_a) that determines the PWM switching duty cycle via the gating signals of the DC-AC inverter powering the motor. The attack detector box in Fig. 1 consists of a digital signal processor (DSP) that generates the watermark signal e[k] is then added to the modulation index m_a generated by the closed loop motor control system. Further, the attack detector box (see Fig. 1) also receives the output speed signal delivered to the motor controller. The DSP in the attack detector box now performs two tests to determine the integrity of the motor speed signal. The next sections detail the algorithm employed to detect the cyber attacks on the speed sensor signal. The background theory and robustness and proofs of the DW approach are detailed in references [5] . The authors previous work [6], a detection scheme for a single phase grid tied inverter with DW approach was analyzed and experimentally tested.

B. ASD as a Single input Single Output Systems (SISO)

For the purposes of the attack detector algorithm with DW approach, the ASD speed control system shown in Fig. 1 can be treated as a single input single output (SISO) system. The relationship between the inverter modulation index m_a and motor speed can be written as follows:

$$x[k+1] = Ax[k] + Bu[k] + w[k+1] \tag{1}$$

where, $x[k+1]$ and $x[k]$ is the motor speed (output state variable), $u[k]$ is the input i.e. modulation index m_a, A, B are system constants and $w[k+1]$ is the system's noise. Next, we add the watermarking signal $e[k]$ to the control input $u[k]$ in Eqn (1) (see Fig.1). As a result Eqn (1) is modified as follows:

$$x[k+1] = Ax[k] + Bu[k] + Be[k] + w[k+1] \tag{2}$$

Now Eqn (2) can be rearranged in two ways as follows:

$$x[k+1] - Ax[k] - Bu[k] - Be[k] = w[k+1] \tag{3}$$

or

$$x[k+1] - Ax[k] - Bu[k] = Be[k] + w[k+1] \tag{4}$$

The left hand side of Eqn (3) is system noise. However, the left hand side of Eqn (4) is system noise $w[k+1]$ + $Be[k]$. The next step is to introduce two variance tests to check the integrity of speed sensor measurements against the SISO model with and without the watermark $e[k]$ [5]. The two variance tests can be written as follows:

$$\lim_{K\to\infty} \frac{1}{K} \sum_{k=0}^{K-1} \Big(z[k+1]-Az[k]-Bu[k]-Be[k]\Big)^2 = \sigma_\omega^2 \tag{5}$$

and

$$\lim_{K\to\infty} \frac{1}{K} \sum_{k=0}^{K-1} \Big(z[k+1]-Az[k]-Bu[k]\Big)^2 = B^2\sigma_e^2 + \sigma_\omega^2 \tag{6}$$

where $z[k+1]$ and $z[k]$ are the speed sensor signal data received by the motor controller at $[k+1]$ and $[k]$ respectively. In the event of a cyber attack the actual speed signal $x[k+1]$ and $x[k]$ has been assumed to be modified by the attacker to $z[k+1]$ and $z[k]$, hence the new notation. The A and B are system constants to be obtained from system identification (explained in the next section), input $u[k] = m_a$ and $e[k]$ is the watermark signal.

C. System ID Model

As discussed in the previous section, Eqn (1) details the SISO system equation between the input $u[k] = m_a$ modulation index and output $x[k]$ and $x[k+1]$ the output speed at $[k]$ and $[k+1]$ respectively, constants A and B need to be extracted from the model at the given operating point. In most cases, the exact system model of actual system is not known due of the non-linearity and complexity of the actual system. Hence, proper identification method for the system constants A and B in Eqn (1) is an important task. We can deploy several well known data-driven method to identify these parameters [7]. Popular among these is the least square method. Relevant equations for the least square method are detailed in Appendix A.

D. Cyber Threat Detection: Variance Test 1 and Test 2

As discussed in the previous section Eqn (5) and Eqn (6) detail two statistical variance Test 1 and Test 2 respectively. Fig.2 illustrates how the two variance tests are computed by the attack detector shown in Fig. 1. As shown in Fig.2, the motor speed sensor output $z[k+1]$ along with the watermark signal $e[k]$ is used as inputs to the system ID computational block (see Appendix A). Similarly the motor speed sensor output $z[k+1]$ is processed via the system ID block (see Fig.2). The two outputs from the system ID block when combined with the system constants A and B results in the two outputs $Ax[k]+Bu[k]+Be[k]$ and $Ax[k]+Bu[k]$ respectively. These two outputs are then used Eqn (5) and Eqn (6) to compute variance Test 1 and Test 2 respectively. It should be noted in Test 1 , the watermarking signal $e[k]$ is added to the sensor's signal that is fed into the system ID algorithm block, we can see that $e[k]$ is reflected in the output of the system ID box. Whereas in Test 2, the control signal is pure and thus the $e[k]$ won't be reflected in the output of Test 2 system ID block output. This is done as fail/safe measure to ensure the successful detection of any intrusion [6].

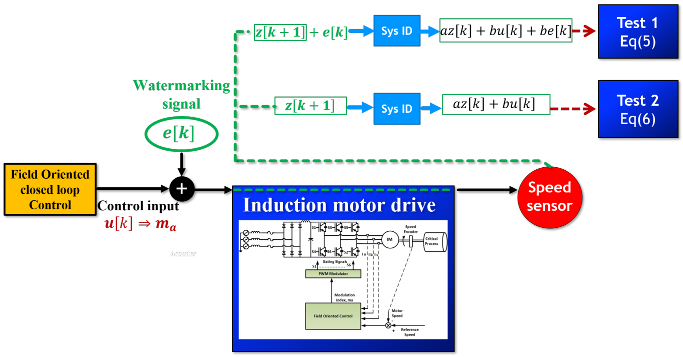

Fig. 2. Block diagram showing the mechanism for computing cyber threat detection variance Test 1 & 2 detailed in Eqn (5) and (6).

E. Proposed detection algorithm operation to detect cyber intrusion to alter the speed

Sections A to D have detailed the principles of dynamic watermarking signal and its injection into the modulation index

m_a controlling the inverter. Fig.1 shows the block diagram of a an example adjustable speed drive system controlling critical process. The feedback control system adjusts the speed of the motor via field-oriented control based on the speed sensor output and the reference speed. In an industrial setting the DC-AC inverter and the motor controlling the process are separated by a physical distance. Motor speed measured via a sensor is typically collected via a PLC and communicated to the motor speed control system via industrial intranet. Such a system is vulnerable to cyber intrusions and the motor speed sensor data can be manipulated to destabilize the system.

A private signal $e[k]$, smaller than the system's noise, that is truly random and has Gaussian distribution with zero mean is superimposed into the control input, modulation index, of the inverter. The detection scheme compares the measurement readings of motor speed and the system model of an induction motor via Test-1 and Test-2 as detailed in Eqn (5) and Eqn (6) respectively.

Test 1: Eqn (5) represents variance Test 1. The algorithm is comparing the actual system sensor's measurement ($z[k+1]$) with the motor's speed obtained via system ID as shown in fig. 2. This output from the systems ID will depict the healthy system's output continuously providing us a reference to compare the actual system's measurement obtained via the sensor data. The algorithm compares both signals and checks for the traces of the watermarking signal to decide if the system was tampered with. In normal operation i.e healthy state, the Test-1 from Eqn (5) will yield the system's noise variance, σ_w^2 ,since the system ID can't replicate the system noise. In the event of an attack/intrusion i.e. manipulation of speed sensor measurement, will yield a bigger value showing a jump in Test-1 output and signaling a possible attack on the system.

Test 2: Similar to Test-1, the Test-2 detailed in Eqn (6) compares the actual sensor's measurement to that of the system ID to identify any intrusion on the system's sensors. However, the only difference is that the watermarking signal $e[k]$ is not added to the system ID output. The reason for creating this test is to provide a more resilient system of detecting. Under normal operation, the Test-2 will yield the systems noise variance σ_w^2 and the watermarking signal variance σ_e^2. During malicious activity on a sensor, the algorithm will output a bigger value depicting a possible attack on the system's sensors.

III. Simulation Results and Discussion

In this section extensive simulations employing MATLAB/Simulink and conducted on a 3-phase adjustable speed drive system controlled in closed loop with an example field oriented control (see Fig. 1) to regulate the motor speed controlling a critical process. Table 1 detail the ASD system design parameters.

TABLE I
Design parameters for induction motor system

Power	4 KW
Number of Poles	4
Rated Speed	1770 R.P.M
Stator Resistance	1.6 ohm
Rotor Resistance	1 ohm
Stator Inductance	0.08 H
Rotor Inductance	0.08 H
Mutual Inductance	0.8 H
Inertia	0.04 Kg.m2
Friction Factor	0.002187 N.M.S
Frequency	60 Hz
Rated Voltage (line to line)	208 V

A. Effect of digital watermarking signal to the modulation index of the inverter

Fig. 3 shows the simulation results of the proposed ASD system (Fig. 1) regulating the speed in closed loop at 1770 rpm. The watermarking signal $e[k]$ is superimposed into the modulation index, m_a of the inverter at $t = 1$ second. The superimposed random signal value is small in magnitude and is therefore shown to have negligible effect on the motor speed.

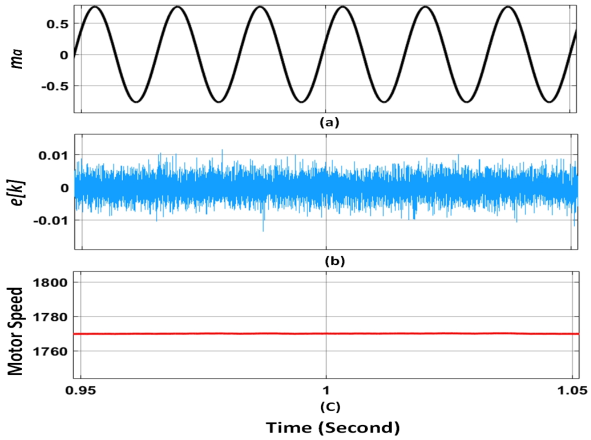

Fig. 3. Simulation results of the ASD system (Fig. 1) with superimposed watermarking signal $e[k]$ into the modulation index at t = 1 s, (a) Modulation signal m_a, (b) Watermarking signal $e[k]$, (c) Motor speed in rpm

B. Evaluation of Various types of Cyber Attacks on ASD motor Speed Signal

In this section a systematic evaluation of various types of cyber attacks on ASD motor speed shown in Fig. 1 is evaluated. The controller of the ASD is achieved by either the PLC or human machine interface (HMI) to maintain the reference speed.

Motor Speed Increase Attack: In this scenario, the attacker gains control of the motor speed signal data, Fig.4 (a), shows the motor speed sensor data and motor speed is shown to be healthy until 1.6 sec. Starting at 1.6 sec the attacker periodically decreases the value of the measured speed data. The incorrect speed sensor data now reaches the the ASD motor controls and the system responds by increasing

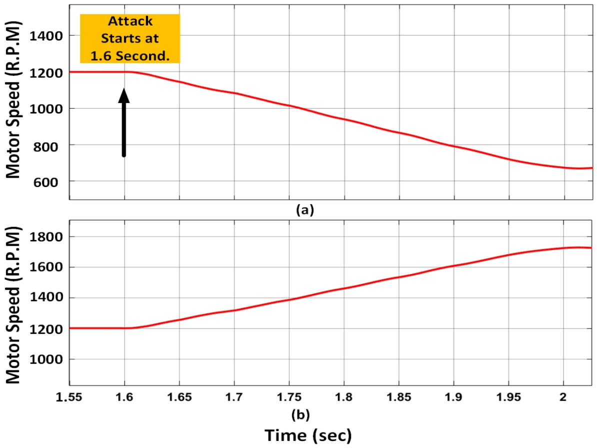

Fig. 4. Motor speed increase attack results: (a) Motor speed sensor signal manipulated (see Fig. 1) starting at t = 1.6 sec. i.e. the attacker progressively decreases the amplitude of the measured speed signal. (b) Actual motor speed. Notice the increase in motor speed due to the ASD speed controller is trying to maintain the motor speed as the motor speed appears to decrease during this attack.

the motor speed. As shown in Fig.4 (b), as the speed sensor data is manipulated slowly to decease its value, the actual motor speed increases from 1200 rpm to 1750 rpm in this example. Such an attack when goes undetected can cause of the motor speed, may cause failure (similar to STUXNET attache [2], [3]). Therefore, detecting any anomalies in the sensor data manipulation is therefore necessary. The next sections demonstrate the superior features of the proposed watermarking approach to detect many such intrusions.

Replay Attack: In the replay attack, it is assumed that the attacker has gained access to the motor speed data signal and is able to record the healthy speed signal for a length of time. After this the attacker disconnects the actual measured speed data and transmits the recorded signal to the ASD motor controller. Since there is no manipulation to increase/decrease the motor speed signal and the recorded speed signal is nearly identical to its previous value, it is nearly impossible to detect this type of attack with AI/ML type methods. Fig.5 shows the results from a replay attack at t = 1.3 sec. Fig.5 (a) shows no change in motor speed as the ASD system controller is unable to detect any changes in the manipulated speed signal. Fig.5 (b) and (c) show the results of proposed Test 1 and Test 2 which computer the variance of the difference in speed sensor data and the values obtained from the system ID model (see Eqn 5 and Eqn. 6). These results clearly show that both Test 1 and Test 2 outputs show high value starting at t = 1.3 sec when the replay attack is initiated. The primary reason for Test 1 and Test 2 to display high value is due to the fact that the recorded signal has a different random signature of the watermark signal and also the system noise does not match the current conditions. These differences are sufficient to indicate high value to conclude that the speed data signal received by the ASD speed controller is NOT authentic. Under such situations the next steps are to raise a flag and possibly initiate a safe shutdown. These measures will be discussed in another paper and is not the subject matter of this current effort.

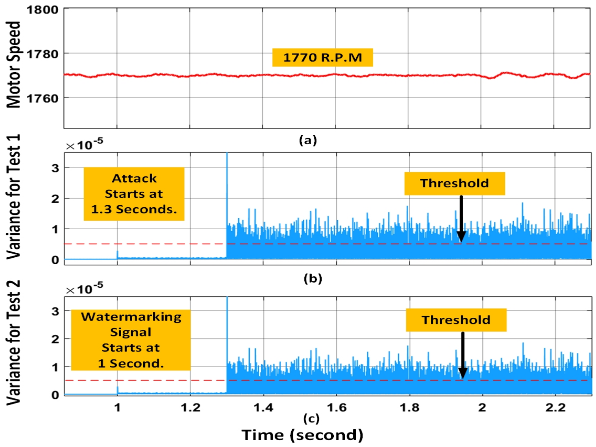

Fig. 5. Replay attack results: (a) Motor speed sensor output - at t = 1.3 sec is disconnected and a pre-recorded signal of the same magnitude is fed to the ASD controller, (b) Variance Test 1 magnitude as a function of time , (c) Variance Test 2 magnitude as a function of time. Notice a big jump in Test 1 and 2 magnitude at t = 1.3 sec when the attack begins.

Low Frequency Attack:

In this scenario, the motor speed sensor data is manipulated with a low frequency (20 Hz) signal. As a result the motor speed starts to oscillate at the operating point of 1700 rpm. Such low frequency speed oscillation can potentially disrupt the critical process. Should the low frequency speed oscillation is nearer the mechanical resonance excessive damage can result. Fig.6 shows the simulation results. At t = 1.4 sec low frequency speed oscillations is initiated by the attacker by manipulating the speed signal. It is clear from Fig.6 (b) and (c), Test 1 and Test 2 signals exhibit a high value indicating the detection of the attack and manipulation.

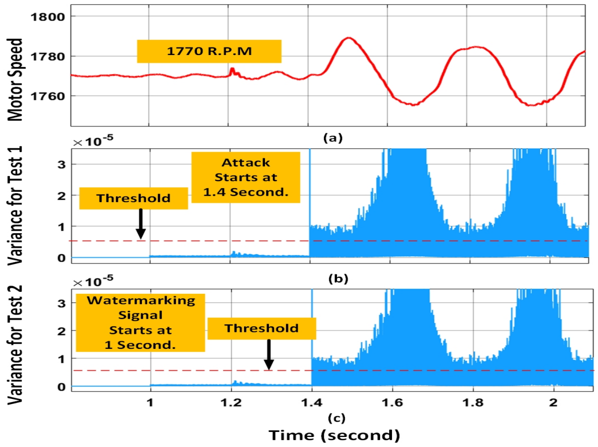

Fig. 6. Low frequency (20 Hz) attack at t = 1.4 sec, (a) Speed sensor value is manipulated at t = 1.4 ses to have an amplitude change of 20Hz, (b) Variance Test 1 magnitude as a function of time, (c) Variance Test 2 magnitude as a function of time

Effect of supply voltage disturbances on speed:

Fig.7 shows the effect of input ac voltage disturbance and its effect on speed. At t = 1.2 sec, the motor speed is altered due to sudden changes in input ac supply. The speed controller is shown to regulate the speed back to its base value of 1770 rpm. Fig.7 (b) and (c) show the Test 1 and Test 2 outputs before and after the speed disturbance. It is clear that during routine speed disturbances both Test 1 and Test 2 outputs do not increase beyond a certain value and hence do not trigger an alarm. The proposed system is robust to indicate high Test 1 and Test 2 values under attacks as demonstrated in previous section.

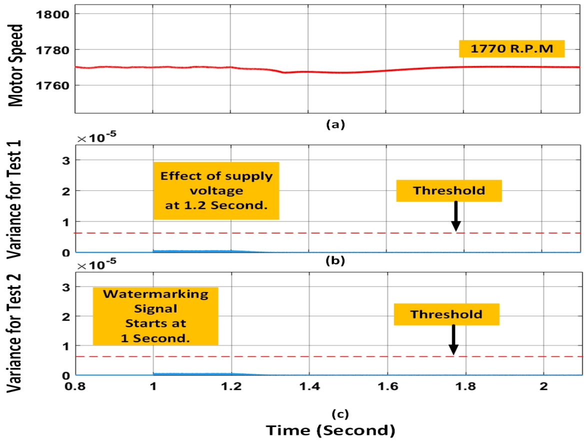

Fig. 7. Effect of supply voltage disturbance on motor speed, (a) Motor speed variation at t = 1.2 sec due a change in the input supply voltage, (b) Variance Test 1 magnitude as a function of time, (c) Variance Test 2 magnitude as a function of time. Notice Test 1 and Test 2 do not respond to normal operation

IV. Conclusion

In this paper, the analysis and design of a robust cyber attack intrusion detection system on an adjustable speed drive system controlling a critical process has been explored. The proposed approach of adding a watermark to the motor PWM modulating signals has been shown to be a powerful tool to guard against intrusions/attacks on motor speed sensor measurements. The approach can be extended to others sensors in the ASD system controlling a critical process. The proposed method is shown to be capable of detecting sophisticated attacks such as record/reply attack in which the speed sensor data is disconnected and pre-recorded signal is played back to the ASD system controller. Both Test 1 and Test 2 have been shown to detect a cyber attack almost instantaneous. An additional side benefit, the proposed system is that it can detect sensor malfunction and contribute to the system reliability. Extensive simulation results show the feasibility of the proposed scheme. Experimental results will be presented at the conference.

Appendix A

This appendix details the necessary equations to determine the system ID model between the modulation index (m_a) and the motor speed ($z[k+1]$) of the SISO system (see section II B and C). System constants (A) and (B) in Eqn (1) need to be computed at an operating point. In most cases, the exact system model of actual system is not known due of the non-linearity and complexity of the actual system. Hence, proper identification method for the system constants (A) and (B) in Eqn (1) is an important task. We can deploy several well known data-driven method to identify these parameters [1] Popular among these is the least square method. Relevant equations for the least square method are as follows:

In a general system, the SISO system, has the following form:

$$x[k+1] = Ax[k] + Bu[k] \tag{A.1}$$

To calculate the A and B matrices of a system, several delays of the system's input and output signals are considered as follows:

$$x[k+1] = a_1x[k] + a_2x[k-1] + a_3x[k-2] + a_4x[k-2]+$$

$$b_1u[k] + b_2u[k-1] + b_3u[k-2] + b_4u[k-3] \tag{A.2}$$

where:

$$A = [a_1 a_2 a_3 a_4] \tag{A.3}$$

$$B = [b_1 b_2 b_3 b_4] \tag{A.4}$$

Once A and B matrices are identified, the system ID algorithm can generate a replication of the healthy output signal of the system when a healthy input signal, $u[k]$, and healthy output signal, $x[k]$, are provided.

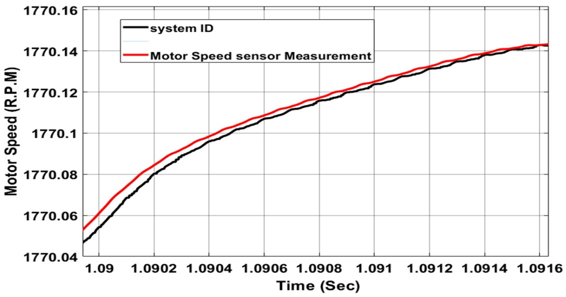

Fig. A.1. Tracking of system ID output to the actual speed measurement

System ID is an algorithm that uses the healthy data from inputs and outputs data of a system to construct a model at various operating points. This output from the systems ID will depict the healthy system's output continuously providing us a reference to compare the actual system's measurement obtained via the sensor data. Fig (A.1) shows the tracking of the actual system ID to the speed sensor measurement, validating the approach of the system ID.

REFERENCES

[1] J. Weiss, “Protecting Industrial Control Systems from Electronic Threats”, Momentum Press, 2010, ISBN: 978-1-60650-197-9

[2] Zetter, Kim. Countdown to Zero Day: STUXNET and the Launch of the World’s First Digital Weapon. Crown Publishers, 2016, ISBN: 978-0-7704-3617-9

[3] D. Kushner, ”The real story of STUXNET,” in IEEE Spectrum, vol. 50, no. 3, pp. 48-53, March 2013, doi: 10.1109/MSPEC.2013.6471059.

[4] M. G. Angle, S. Madnick, J. L. Kirtley and S. Khan, ”Identifying and Anticipating Cyberattacks That Could Cause Physical Damage to Industrial Control Systems,” in IEEE Power and Energy Technology Systems Journal, vol. 6, no. 4, pp. 172-182, Dec. 2019, doi: 10.1109/JPETS.2019.2923970.

[5] B. Satchidanandan and P. R. Kumar, “Dynamic watermarking: Active defense of networked cyber-physical systems,” Proceedings of the IEEE, Vol. 105, Issue 2, Feb. 2017, pp. 219-240

[6] H. Ibrahim et al., ”An Active Detection Scheme for Sensor Spoofing in Grid-tied PV Systems,” 2021 IEEE Energy Conversion Congress and Exposition (ECCE), 2021, pp. 1433-1439, doi: 10.1109/ECCE47101.2021.9595733.

[7] Schoukens, Johan. ”Mastering System Identification in 100 Exercises”, Wiley, ISBN:9780470936986, 2012