Strengthening Cybersecurity for Industrial Control Systems: Innovations in Protecting PLC-Based Infrastructure

Peng-Hao Huang, *Member, IEEE*, Hasan Ibrahim, *Member, IEEE*, Jaewon Kim, *Member, IEEE*, Prasad Enjeti, *Fellow, IEEE* P. R. Kumar, *Fellow, IEEE* J. V. Rajendran, *Member, IEEE*
Department of Electrical & Computer Engineering, Texas A&M University, College Station, TX - 77845
Email: alexamiiah79@tamu.edu

***Abstract*— In this paper, we propose two new approaches aimed at enhancing the security of industrial control systems (ICS) that utilize programmable logic controllers (PLCs) for the control of critical processes. The first approach involves the addition of a unique digital watermark to the PWM control that adjusts the motor speed to control the critical process. This enables efficient detection and identification of any unauthorized modifications to the sensor signals responsible for controlling the plant. The second approach focuses on monitoring the input current (i.e power) drawn by the PLC during the execution of critical process control tasks. Malicious intrusions to change the PLC parameters and/or unauthorized firmware updates can be rapidly detected. Both approaches demonstrate a substantial improvement in the security of ICS, effectively safeguarding against potential cyber-attacks. Experimental results from a laboratory scale water tank level controlled via PLC showcases rapid intrusion detection capabilities.**

***Keywords*— ASD, CPS (cyber physical system), watermarking, PLC**

I. Introduction

Cybersecurity plays a crucial role in safeguarding industrial control systems (ICS) and ensuring the uninterrupted operation of nations critical infrastructures. With the increasing integration of industrial internet of technologies (IIoT) into industrial processes, the reliance on interconnected systems has grown tremendously [1], making industrial environments more vulnerable to cyber threats. As a result, the importance of robust cybersecurity measures in industrial control systems cannot be overstated. Critical industrial control systems such as programmable logic controllers (PLCs), motor/pump drives are responsible for managing and controlling various essential operations, including power generation, water treatment, manufacturing processes, transportation systems, and more. Any disruption or compromise to these systems can have far-reaching consequences, leading to significant economic losses, environmental damage, and even potential threats to public safety [2]. Attackers can exploit vulnerabilities to gain unauthorized access, manipulate PLCs' sensor data, change control parameters, and perform unauthorized firmware updates to disrupt operations, or even cause physical damage [6].

In this short paper we present two new approaches. Fig. 1 shows both defense mechanisms for the industrial control system and the PLC. To address these security vulnerabilities and mitigate the risks associated with cyber-attacks, various security measures have been proposed, including encryption, authentication, intrusion detection, and watermarking. In this paper, we focus on the use of watermarking as a means of enhancing ICS cybersecurity to guard against sensor data manipulation and the use of PLC sidechannel to monitor its power consumption by monitoring its input current signature. It is shown that the PLC input current signature depicts several patterns that correspond with various control functions. Unauthorized manipulation of PLC control parameters can be detected by monitoring the current (sidechannel). The effectiveness of this approach is demonstrated through experimental evaluation on laboratory prototype ICS.

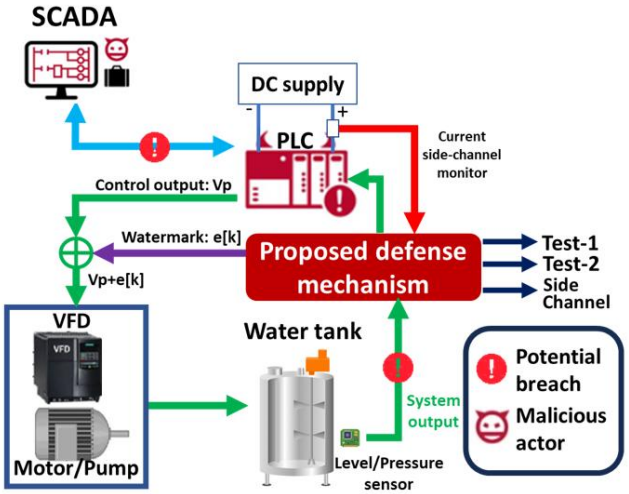

Fig. 1 Industrial control systems (ICS) with the proposed defense mechanism to protect PLC-based infrastructure.

II. Proposed Active Defense Mechanism

Fig. 1 shows a block diagram of our proposed active defense mechanism to guard against cyber intrusions in ICS. The PLC is tasked/programmed with closed loop control functions (such as PI/PID) to adjust the variable frequency drive (VFD) speed to adjust the flow rate to control the water tank level (Fig. 2). A pressure sensor in the water tank-1 translates the water level via a sensor signal that is then fed back to the PLC. During normal operation, the closed loop system functions appropriately by adjusting the VFD motor/pump to regulate the water tank level-1 (Fig 2). The defense mechanism consists of adding a unique small magnitude digital watermarking signal (a random variable with a gaussian distribution and zero mean average) to the control signal to adjust the VFD speed [4]. The watermark signal then propagates through the VFD/Motor/Pump and its signature is reflected on the water tank level sensed by the pressure sensor. Two variance tests (shown in eq (2) and eq (3) are then conducted continuously to realize a defensive mechanism by observing the signals' presence and validate its signature by comparing it to the system model. A high value in the variance computed in Test-1 and Test-2 is shown to indicate the presence

of false date in the water tank level information (i.e., the pressure sensor data has been manipulated – see Fig. 1)

II.1 Water tank level control equations:

The water tank level control system shown in Fig. 2 can be modeled by a first order differential equation shown below [5]:

$$\dot{L_1}[k+1] = \frac{1}{A_{t1}}\{(V_p[k]\cdot K_p) - (A_{o1}\cdot\sqrt{L_1[k]\cdot 2g}\,)\} \quad (1)$$

Where L_1 is the water level in Tank 1, A_{t1} is Tank 1 area, V_p is the controller output voltage that controls the motor speed which is proportional to the flow rate, K_p is the driver gain, A_{o1} is Tank 1 drain area, and g is the gravity. This equation serves as a means to determine and calculate the water tank level $L_1[k]$ given V_p.

II.2 Dynamic watermarking [4]:

Per dynamic watermarking theory detailed in [4], a small magnitude random varying signal termed as watermark $e[k]$ is added to the control input (see Fig. 1). Two variance tests, Test 1 and Test 2 are conducted to computer variance to determine potential cyber intrusions (attacks) to manipulate sensor data with false data injection.

Test-1: In eq (1), $z[k+1]$ is the water level in Tank 1 acquired from the physical sensor. And $\dot{L_1}[k+1]$is the water level in Tank 1 computed from the mathematical model with the watermark signal added. Test-1 is the variance of the difference between the sensor output and the value obtained by the model and is given by,

$$\lim_{K\to\infty}\frac{1}{K}\sum_{k=0}^{K-1}\left(z[k+1] - \int\left[\frac{1}{A_{t1}}\{((V_p[k]+e[k])\cdot K_p) - (A_{o1}\cdot\sqrt{L_1[k]\cdot 2g}\,)\}\right]\right)^2 = \sigma_\omega^2 \quad (2)$$

The variance in eq (2) is computed repeatedly with window size K as sampling interval. During normal operation, since both the measurement and model results are the same, outputs from Test-1 variance will only yield system noise variance denoted σ_ω^2. However, when the sensor data is compromised, the variance output from eq (2) will be high indicating an anomaly.

Test-2: Like Test 1, Test 2 compares the water tank level sensor signal $z[k+1]$ with the value obtained from the mathematical model. However, in this test the watermark is not added to the mathematical model. As a result, the test will yield the variances of the system noise and the watermark denoted σ_ω^2 *and* σ_e^2 respectively. During normal operation, variance of Test-2 will also yield a small value. When the sensor data is compromised Test-2 will also show high value indicating a cyber intrusion. Ref [4] has detailed explanation and proofs as to why two tests are required to fully assure the integrity of the sensor signal. Ref [7,8] experimentally tested the dynamic watermarking methodology on a prototypical chemical process control system.

$$\lim_{K\to\infty}\frac{1}{K}\sum_{k=0}^{K-1}\left(z[k+1] - \int\left[\frac{1}{A_{t1}}\{(V_p[k]\cdot K_p) - (A_{o1}\cdot\sqrt{L_1[k]\cdot 2g}\,)\}\right]\right)^2 = \sigma_\omega^2 + \beta^2\sigma_e^2 \quad (3)$$

III. Experimental Results/Verification

To evaluate the effectiveness of the proposed approaches, experiments were conducted on laboratory prototype hardware of a closed loop water tank system with an Allen-Bradley Micro820™ PLC controlled pump drive (see Fig. 2). The PLC is programmed to operate as a proportional-integral (PI) controller to regulate the water tank level by adjusting the motor speed. A hardware in the loop (HIL) setup is used to implement the proposed defense mechanism (see Fig. 1), to generate the watermark *e[k]*, provide the system model equations and perform Test-1, Test-2. In an actual system, the HIL box can be replaced by a dedicated digital signal processor (DSP) or an embedded controller. As discussed, the watermark signal *e[k]* generated by the defense mechanism block is added to the control signal (see Fig. 1) that controls the VFD/Motor/Pump speed that in turn adjusts the water tank level. In the scenario the water level sensor data is manipulated with false data and/or the PLC be compromised due to upstream SCADA interfaced to the IIoT network, the manipulated water level sensor data can potentially cause the tanks to overflow. Fig. 2 (b) shows such an attack scenario in which both Test-1 and Test-2 indicate high value indicating system compromise.

Furthermore, Fig. 3 shows the experimental results of PLC sidechannel observations. The input current drawn by the Allen-Bradley Micro820™ PLC during various stages of its function (Fig. 3) is shown to have many features such as unique frequency variation and sudden changes in values from low to high. Fig 3 (a) shows current drawn during normal PI control operation, Fig. 3(b) shows the current variation during unauthorized manipulation of the PI controller constants/damping factor and Fig 3(c) shows an input current pattern during an unauthorized program download. By conducting a thorough examination of the frequency spectrum of the input current and its distinctive attributes during normal system operation, it becomes feasible to detect any malicious activities aimed at altering system parameters. This can be achieved by deploying pattern recognition and machine learning algorithms, which facilitate the identification of such anomalous behaviors.

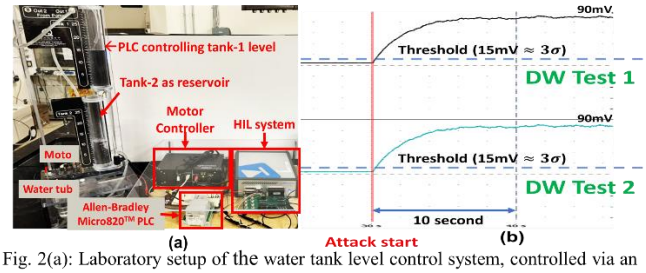

Fig. 2(a): Laboratory setup of the water tank level control system, controlled via an Allen-Bradley Micro820™ PLC. Fig. 2(b): Variance of Test-1 and Test-2 output before and after attack.

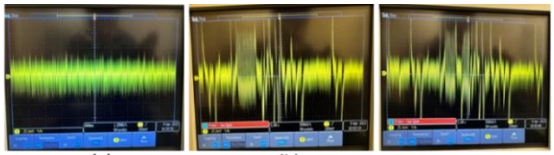

Fig. 3 PLC Side-channel, input current drawn during various stages of its functions, (a) normal PI control operation, (b) unauthorized parameter update, (c) unauthorized program download

Conclusion

In this paper, two new approaches to strengthen ICS with PLCs have been presented. Experimental results have shown that by watermarking the control signal feeding to the plant allows the detection of unauthorized sensor data manipulation. Furthermore, monitoring the sidechannel of PLC instantaneous current has enabled the identification of unauthorized actions via network. By employing proposed mechanisms, robustness of an ICS would be significantly improved.

ACKNOLODGEMENT

This material is based upon work partially supported by the US Army Contracting Command under W911NF-22-1-0151, US Office of Naval Research under N00014-21-1-2385; U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technologies Office Award Number DE-EE0009031. The views expressed herein, and conclusions contained in this document are those of the authors and should not be interpreted as representing the views or official policies, either expressed or implied, of the U.S. ONR, ARO, Department of Energy, or the United States Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

REFERENCES

[1] M. Wiboonrat, "Cybersecurity in Industrial Control Systems: An integration of information technology and operational technology," IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society, Brussels, Belgium, 2022, pp. 1-6, doi: 10.1109/IECON49645.2022.9968468.

[2] Wang Z, Zhang Y, Chen Y, Liu H, Wang B, Wang C. A Survey on Programmable Logic Controller Vulnerabilities, Attacks, Detections, and Forensics. Processes. 2023; 11(3): 918. https://doi.org/10.3390/pr11030918

[3] Y. Liu, L. Wei, Z. Zhou, K. Zhang, W. Xu, and Q. Xu. On code execution tracking via power side-channel. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 1019– 1031. ACM, 2016.

[4] B. Satchidanandan and P. R. Kumar, "Dynamic Watermarking: Active Defense of Networked Cyber–Physical Systems," in Proceedings of the IEEE, vol. 105, no. 2, pp. 219-240, Feb. 2017, doi: 10.1109/JPROC.2016.2575064.

[5] Doff-Sotta, Martin & Cannon, Mark. (2022). Difference of convex functions in robust tube MPC. 10.13140/RG.2.2.32656.69126.

[6] S. McLaughlin et al., "The Cybersecurity Landscape in Industrial Control Systems," in Proceedings of the IEEE, vol. 104, no. 5, pp. 1039-1057, May 2016, doi: 10.1109/JPROC.2015.2512235.

[7] Kim, Jaewon, Woo-Hyun Ko, and P. R. Kumar. "Cyber-security with dynamic watermarking for process control systems." 2019 AIChE Annual Meeting. AIChE, 2019.

[8] Kim, Jaewon, and P. R. Kumar. "Security of Control Systems with Erroneous Observations." IFAC-PapersOnLine 53.2 (2020): 2225-2230.