2024 IEEE 20th International Conference on Automation Science and Engineering (CASE)
August 28 - September 1, 2024. Bari, Italy

IIOT Cyberattacks in Industrial Field Control Systems: PID Attack and Hardware Trojan Effects

Alessandro Massaro, Nicola Epicoco*, Giuseppe Loseto, Carmelo Ardito

Abstract— **This work analyzes hardware manumissions and attacks in the controller field of industrial Operational Technology (OT) networks. Specifically, the paper models and simulates the analog Trojan effects changing the signals at the output of electronic devices or sensors used for Industrial Internet of Things (IIOT) data transmission. The study enhances the analog Trojan capacitor and resistance effects of a humidity sensor, and the Proportional–Integral–Derivative (PID) controller behavior due to possible attacks. Parametric analyses are performed to study how the change of the electrical parameters influences the deteriorated output signal about a correct reading. The proposed methodology is suitable to design testbed plans simulating electronic cyberattack responses useful to distinguish through the signal analysis possible manumitted devices for sensing and actuation operations.**

I. Introduction

Industry 4.0 concerns with automation, cloud computing, Industrial Internet of Things (IIoT), and machine learning to streamline many processes across every major industry [1], as well as for low automated business companies [2], [3]. Due to the interconnection of machinery and devices, which exchange huge amounts of even sensitive data [4]-[5], cybersecurity represents a challenging issue for all companies committing to Industry 4.0 paradigm [6]. The National Institute of Standards and Technology (NIST) provides some guidelines for the segmentation of industrial networks to enforce cybersecurity [7]. A possible basic way is to separate the Information Technology (IT) network from the Operational Technology (OT) one, as for the Purdue Enterprise Reference Architecture (PERA) model reported in Fig. 1, by the following levels:

- Level 0 (process): defines the physical processes of the industrial production (machinery processes controlled by intelligent decision-making engines in the Industry 5.0 scenarios [6]);
- Level 1 (controller field): it includes the management of sensing and actuation operations of the Programmable Logic Controller (PLC) and the Remote Terminal Unit (RTU) fluxes;
- Level 2 (local control): its main function is to control the Local Area Network (LAN) devices such as Human Machine Interfaces (HMIs), Distributed Control Systems (DCSs), and Supervisory Control and Data Acquisition (SCADA) systems [8];
- Level 3 (Processing LAN): it manages the production data flux and the middleware;
- Level 3.5 (DeMilitarized Zone (DMZ)): it is the interface layer between the IT network and the OT one;
- Level 4 (Enterprise): it manages all the industrial activities with the external network.

The topic discussed in this paper is related to Level 1, analyzing possible attack effects on hardware components such as sensors and controllers.

A possible way to attack hardware components is by means of hardware Trojan (HT). HT is a malicious modification on physical devices typically due to an intentional circuit coupling introducing an analog trigger attack with an added passive electronic component such as a capacitor or resistance. Concerning for example a physical modification of a humidity or temperature sensor, a hardware attack may be the sabotage of an electrode of the sensor. Possible HT attacks are modelled on the right side of Fig. 1, where a capacitor (Trojan capacitor C_T) or an electrical resistance (Trojan resistance R_T) [9],[10] are connected to the IIOT system as payload circuits disturbing or falsifying the data transmission between sensors or electronic circuits and Message Queuing Telemetry Transport (MQTT) [8] broker interfaces (host microcontroller). Therefore, the C_T or R_T Trojans could cause an abnormal change of electrical variables, thus falsifying the output signal. Other hardware attacks are due to the intentional modification of environmental conditions [11]: the change of the manufacturing environment creates noises such as electromagnetic interferences, as well as temperature or humidity variations. The impact of environmental noise in the manufacturing production lines generates, intentionally and unintentionally, packet losses in data transmission. Another possible hardware attack targets the Proportional–Integral–Derivative (PID) gain values of a controller [12] with the goal to force the data-driven regulation by altering the PID gain values of the controller.

In the proposed paper the effects of analog Trojans elements on a humidity sensor and the alteration of gain of a PID controller due to an attack are simulated.

II. Related Work and Motivation

The landscape of cybersecurity in Industrial Internet of Things scenarios has garnered increasing attention in the last years due to the critical role played by Industrial Field Control Systems (IFCS) in modern industrial processes. Previous research has extensively explored the development and implementation of cybersecurity frameworks tailored to IIoT environments. In the relevant literature, several works (see, e.g., [13], [14]) have contributed comprehensive models for securing industrial systems, highlighting the importance of threat detection, incident response, and system resilience.

* Corresponding author.
All authors are with the Department of Engineering of the LUM University "Giuseppe Degennaro". Email addresses (following the author order): {massaro; epicoco; loseto; ardito}@lum.it.

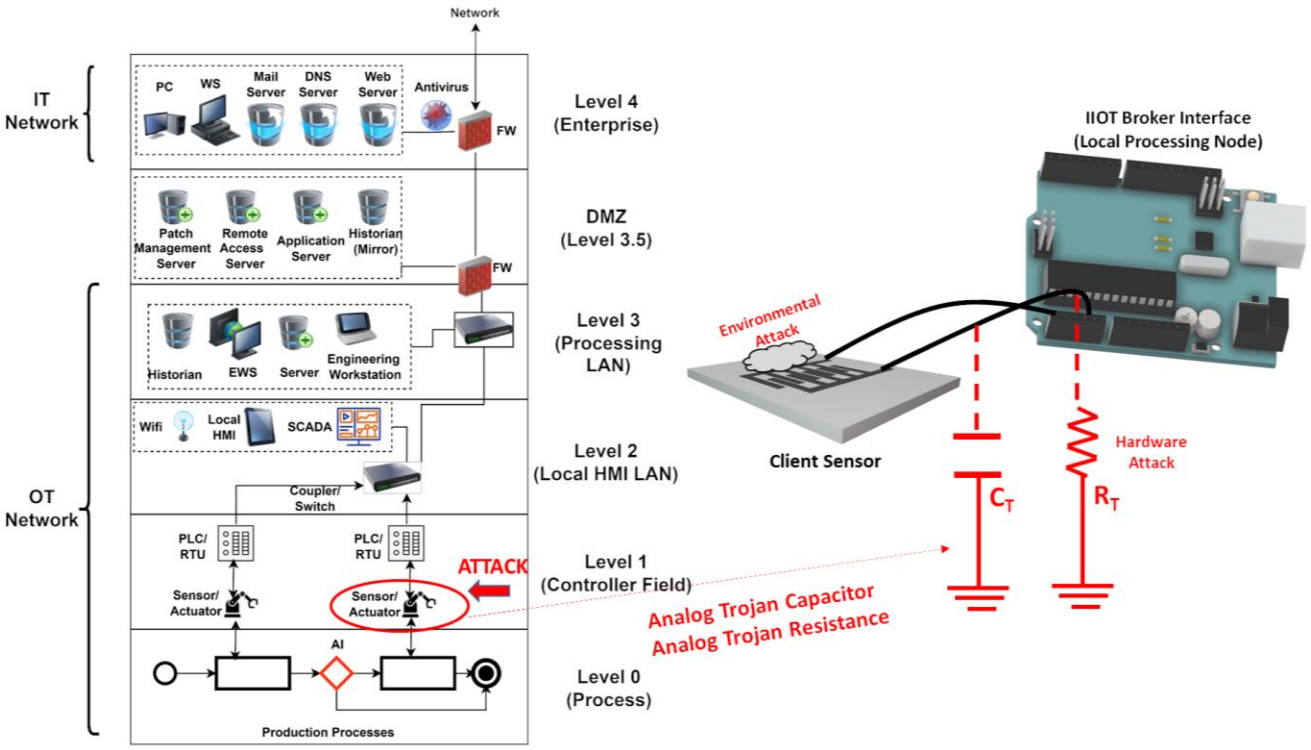

Figure 1. (Left) Purdue Enterprise Reference Architecture (PERA) model, and (right) hardware attacks, which concern level 1 of the OT network.

Investigations into the vulnerabilities of IFCS have also shed light on potential points of exploitation in IIOT emphasizing the need for robust security measures in the face of evolving attack vectors [15]. Moreover, the integration of cyber-physical systems in industrial scenarios has brought forth new challenges and attack surfaces. As discussed in [16], several attack and defense strategies have been proposed to address the interconnected nature of cyber-physical systems. These works lay the groundwork for understanding the broader context of threats involving both cyber and physical aspects, setting the stage for a more focused examination of hardware-specific vulnerabilities.

In particular, the existing literature presents a multifaceted view of the challenges associated with detecting Hardware Trojans in IIOT scenarios. HTs operate at the physical level, introducing unauthorized alterations embedded within the hardware components of electronic devices, with the intent to compromise their functionality, integrity, or security. An accurate taxonomy of HT threats has been presented in [17]. The paper provides a structured understanding of the diverse forms HTs can take, focusing on the attacker's methods, capabilities, and challenges when the attacker designs and implements a hardware trojan.

Different cutting-edge detection techniques for HTs have been proposed in recent practical implementations based on anomaly detection methods [18], side-channel analysis [19], and machine learning models [20]. In sophisticated scenarios, attackers might deploy both hardware trojans and PID attacks in a coordinated manner. PID attacks represent a specific manipulation of Proportional-Integral-Derivative control systems emerged as a further significant concern in industrial security. A detailed analysis of the vulnerabilities associated with PID controllers has been reported in [20] along with a novel scheme for the detection of industrial process control attacks affecting the normal operations of PLCs. The paper demonstrates how malicious actors can compromise control loops to tamper with industrial processes and identifies potential system weaknesses and susceptibilities to cyber threats.

Despite there are various mitigation approaches for PID attacks, several limitations and constraints persist. Industrial processes are often highly complex, involving interconnected systems with intricate dependencies and usually distributed across large IoT networks. Moreover, determining what constitutes an anomaly requires a deep understanding of the normal operating conditions, and distinguishing between expected variations and potential attacks can introduce latency due to the volume of involved data [21].

This work underscores the importance of safeguarding industrial processes against cyber threats. Understanding mitigation strategies and applying robust defense procedures is crucial for developing resilient PID control systems that can withstand and recover from potential security breaches.

III. Hardware Attacks Simulation

In this section, two hardware attacks of a HR202 humidity sensor and of a PID controller are simulated by means of the LTSpice tool, a SPICE-based analog electronic circuit simulator open-source software [22]. For both the simulations, we consider the transient time-domain analysis.

A. Analog Capacitor and Analog Resistance Models

The HR202 is a humidity-sensitive resistor made from organic macromolecule materials, having a wide range of applications, such as, for instance, meteorology, storage facility humidity control, textile industry, hospitals, building management, and other applications which require an ambient humidity monitoring [23]. The circuital model of the HR2002

sensor implemented for a detection system is sketched in Fig. 2, where the analog Trojan attack of Fig. 1 is also modelled in red, by adding the Trojan capacitor C_T and the Trojan resistance R_T, which influence the output of the humidity detection system. In order to distinguish the single effects of R_T and C_T, two different simulations are performed by adding, in turn, only R_T and only C_T. Complex hardware attacks could include both the C_T and the R_T effects.

The HR202 is a resistive humidity sensor measuring the Relative Humidity (RH) as a change of the electrical impedance of a hygroscopic material: its resistance changes inversely with humidity. For each measured resistance (R_1 of the model in Fig. 2) a RH value corresponds.

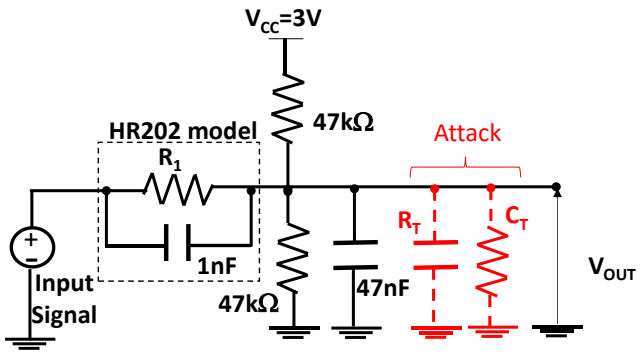

Figure 2. HR202 humidity sensor model and Analog Trojan capacitor/resistance effects influencing the output voltage. R1 is the detected resistance indicating a specific relative humidity (RH).

Figure 3 shows how the output voltage changes with the R_1 variation due to a change of RH. The time-domain analysis is performed by considering a pulsed voltage of amplitude 3 Volts as input signal.

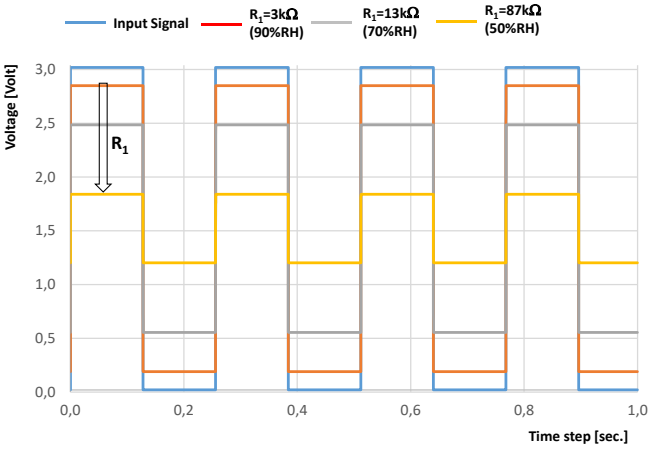

Figure 3. LTSpice simulation: HR202 humidity sensor simulated response reading voltage signal corresponding to a relative humidity value (measured at 25 °C). The input signal is a pulsed voltage having an amplitude of 3 Volts.

In Table I the electrical resistances R_1 of the HR202 sensor are listed together with the corresponding relative humidity measurements RH.

Figure 4 highlights the effects of the first performed simulation, that is, when only the resistance R_T=50 kΩ is added: with respect to the outputs of the no-attack case a decrease of the output voltage V_{out} is observed. For R_1 values higher than 5 MΩ the V_{out} amplitude will further decrease.

Other simulations prove that the decrease effect is inversely proportional with the R_T value. This trend is clearly illustrated in Fig. 5, obtained by considering three different R_T values (R_T=1 kΩ, R_T=5 kΩ, and R_T=50 kΩ).

TABLE I. ELECTRICAL RESISTANCES OF THE HR202 SENSOR CORRESPONDING TO RELATIVE UMIDITY (RH) VALUES.

RH[a][%]	R_1[a] [Ω]	RH[a][%]	R_1[a] [Ω]
20%	5.0 MΩ	**60%**	31 kΩ
25%	2.6 MΩ	**65%**	19.5 kΩ
30%	1.3 MΩ	**70%**	13 kΩ
35%	630 kΩ	**75%**	8.4 kΩ
40%	310 kΩ	**80%**	5.7 kΩ
45%	160 kΩ	**85%**	4.0 kΩ
50%	87 kΩ	**90%**	2.8 kΩ
55%	49 kΩ		

a. Values at 25 ° C.

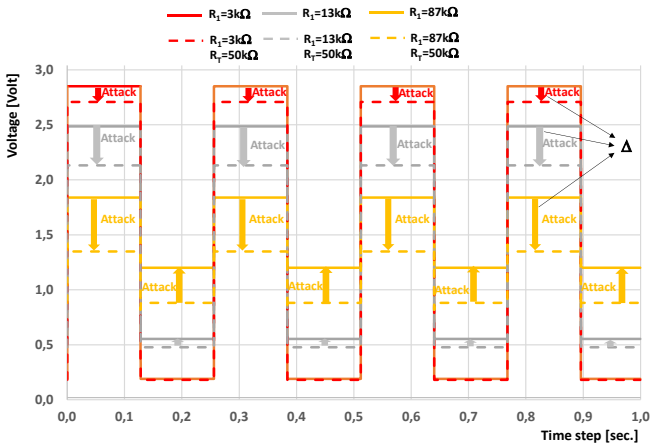

Figure 4. LTSpice simulation: HR202 humidity sensor response simulating an analog Trojan attack introducing a Trojan resistance R_T = 50 kΩ which decreases the voltage amplitude at the output of the sensor circuit. The no-attack cases follow a no direct proportionality with R_1 values. The dashed lines refer to the attack cases.

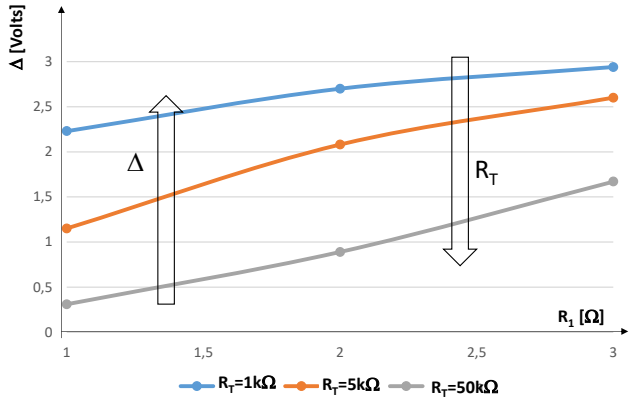

Figure 5. LTSpice simulation: HR202 humidity sensor Δ trend simulating an analog Trojan attack introducing Trojan resistances of R_T = 1 kΩ, R_T = 5 kΩ, R_T = 50 kΩ. The parameter Δ is graphically indicated in Fig. 4.

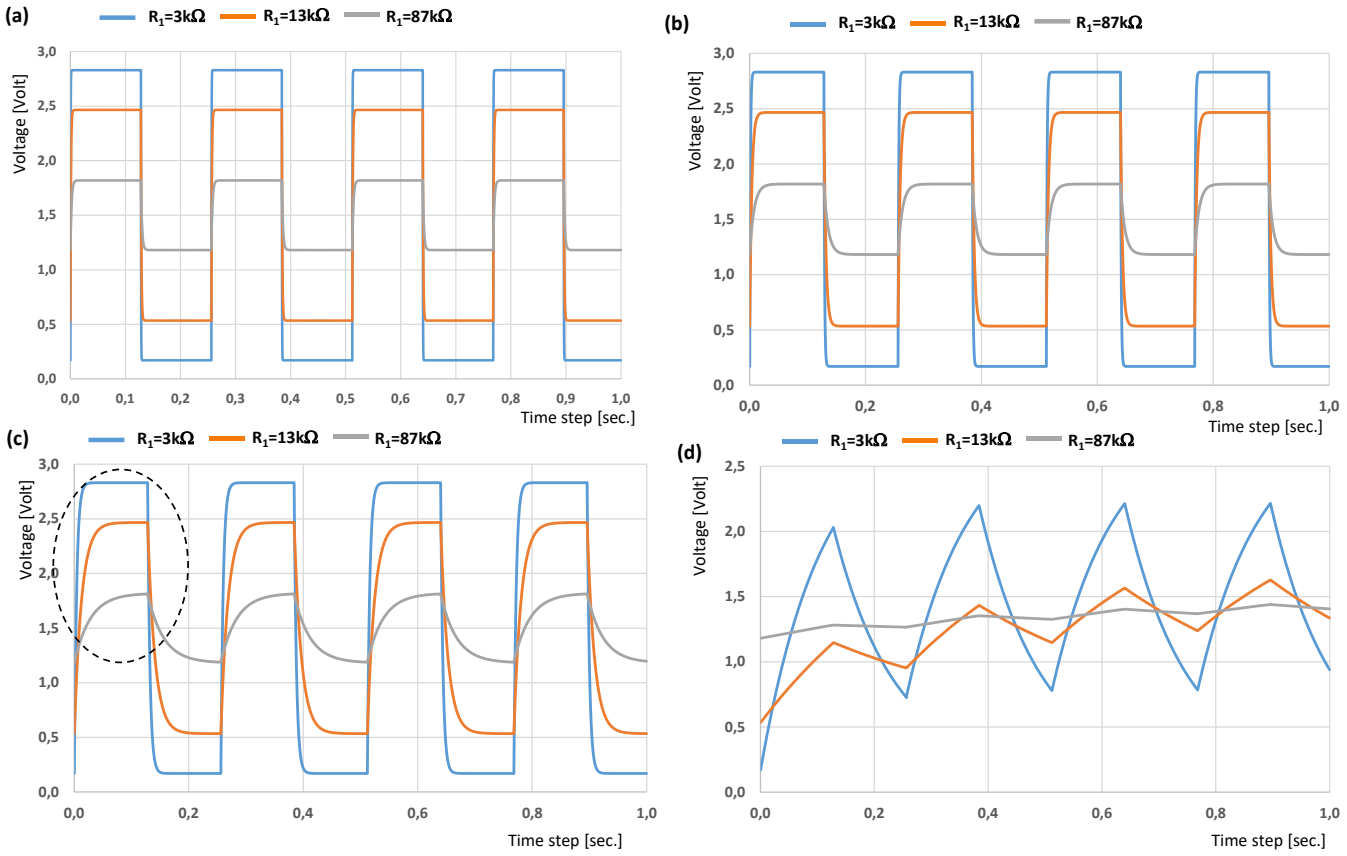

Figure 6. LTSpice simulation: HR202 humidity sensor repsonses under attacks introducing a Trojan capacitor C_T: (a) $C_T = 0.1$ µF; (b) $C_T = 0.4$ µF; (c) $C_T = 1.5$ µF; (d) $C_T = 40$ µF.

The second simulation analyzes the effect of the only C_T as a deterioration of the V_{out} signal (see Fig. 6), where the deterioration degree is directly proportional to the C_T value. More in detail, four C_T values are considered (i.e., $C_T = 0.1$ µF, $C_T = 0.4$ µF, $C_T = 1.5$ µF, and $C_T = 40$ µF).

The V_{out} profile of Fig. 6c (see the dashed region) is zoomed in Fig. 7 to better show how the deterioration mainly impacts the first part of the signal generating a wrong reading of the voltage.

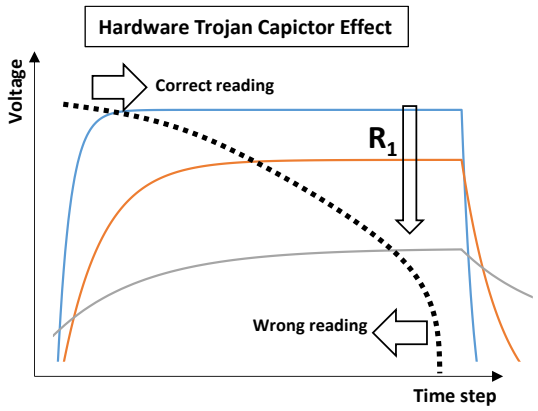

Figure 7. HR202 humidity sensor simulated response for an analog Trojan Attack introducing the Trojan resistance R_T which decreases the voltage amplitude at the output of the sensor circuit.

In Fig. 8 both the Trojan effects for particular values of R_T and C_T are illustrated. It is to be noticed that for low values of C_T (that is, C_T =40 µF, showing in Fig. 6 a stronger signal deterioration) both the effect of the signal amplitude decrease and of the profile deterioration can be observed.

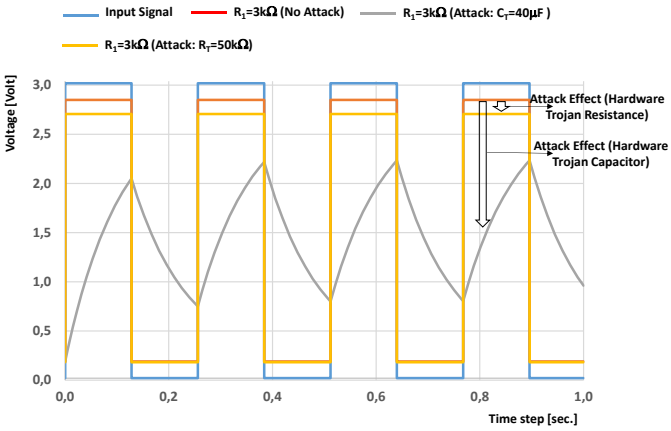

Figure 8. LTSpice simulation: HR202 humidity sensor simulated responses comparing an analog Trojan Resistance attack with an analog capacitor attack (behavior of the output voltage signal). By considering both the R_T and C_T effects the voltage signal will be further deteriored, making more difficult to distinguish the single effect.

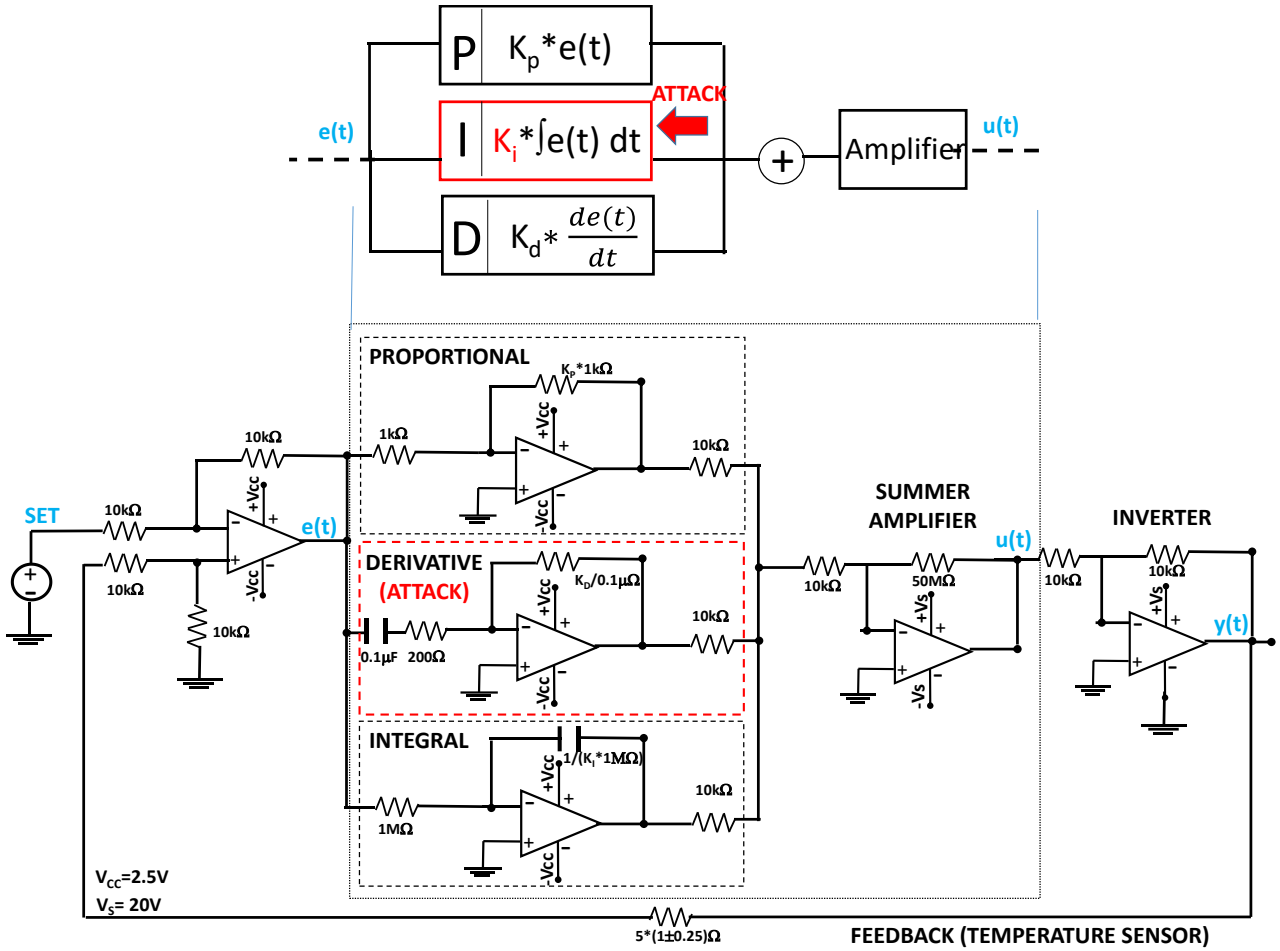

Figure 9. Electronic layout of the simulated PID controller with an attack influncing the only derivative circuit.

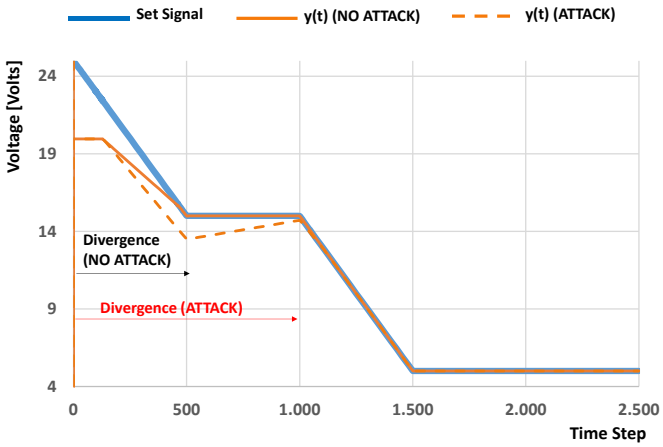

Figure 10. LTSpice simulation: comparison of the PID output response *y(t)* in case of attack (change of the derivative gain constant K_d) and no attack.

B. PID Controller Attack simulation

A PID controller can read a sensor, computing the actuator output by calculating proportional, integral, and derivative responses and summing these three components to compute the final output.

It is a feedback system widely used in industrial control systems and for other applications requiring continuous modulation of the control action: a PID controller continuously calculates an error value *e(t)* as the difference between a desired set point (Set) and a process variable (controlled variable *y*(*t*)) measured by sensors, and applies a correction based on the proportional, integral, and derivative terms (P, I, and D respectively).

The output signal *u(t)* to the PID is then given by:

$$u(t) = K_p e(t) + K_i \int_0^t e(t)dt + K_d \frac{de(t)}{dt} \quad (1)$$

The K_p parameter provides a control action proportional to the error: the bigger the error at the controller input the greater the regulator control action. The derivative parameter K_d improves the closed loop stability over time. As limitation the derivative could amplify signals with harmonic content at high frequencies, and could lead to instability, thus compromising the control quality (an important parameter for possible attacks). Finally, *Ki* ensures that the controlled variable assumes the set-point value at steady state regime. PI controllers allow to achieve higher precision without worsening the stability of the system. Another important aspect impacting on the signal processing is the industrial noise disturbing amplification. In this field, recent works are considering the use of Artificial Neural Networks (ANN) to correct noisy signal in operational amplifier systems [24].

A good PID control is characterized by a faster convergence of the output signal *y*(*t*) to the regulation one (i.e., the set point). An example of a PID electronic circuit used to tune a machine controlling the production temperature is

illustrated in Fig. 9. The circuit layout of Fig. 9 is simulated by the LTSpice tool [22]. The circuit is designed by means of operational amplifiers (*UniversalOPAmp2* component) characterized by the following characteristics: Gain BandWidth (GBW) = 10 MHz, open-loop gain = 1E6, slew rate = 1E7 V/s, Rail = 0, Rin = 500 MΩ.

A possible way to analyze the extent of hardware attacks is to simulate the behavior of a PID system when the gain constant changes, thus consecutively varying the controlled variable *y(t)*. The input (set point signal) is a Piecewise Linear Functions (PWL) type voltage signal.

Figure 10 compares the case of an attacked PID (that is, a change of the only gain constant K_d [11] due to a modification of the resistances of the derivative block in Fig. 9) with the same PID behavior without attacks. The latter system (that is characterized by the gain constants K_p = 20, K_d = 350, K_i = 0.001E-3) ensures a faster convergence of the output signal *y(t)* to the regulation signal (Set) if compared with the attacked PID system (where K_p = 20, K_d = 1500, K_i = 0.001E-3) which conversely exhibits a higher divergence (see Fig. 10).

IV. Conclusion

The proposed paper presents a theoretical methodology to estimate the effects of hardware attacks happening in the controller field level of the Operational Technology (OT) network.

Results highlight that the effect of the analog Trojan resistance is in the decrease of the output voltage; besides the introduction of an analog Trojan capacitor could decrease the output amplitude by simultaneously deteriorating the signal profile. Furthermore, the study shows the attack effect in PID controlled systems as a convergence time extension regarding the effectiveness of the regulation.

The proposed methodology is suitable to analyze the response sensitivity of the electrical variables of circuits under hardware attacks as environmental attack or intentional circuit modification. The analyzed simulation models can be integrated in more complex electronic systems for digital twin IIOT parametric testbed models. Finally, future work directions include: (i) development of a comprehensive prototype including real sensors and actuators to evaluate the proposed mitigation approaches in a reference IoT environment; (ii) integration of tiny machine learning algorithms for edge-based anomaly detection and behavioral analysis. The main limitations of the proposed work lie in the classification of all noisy signals which may be due either to forms of attacks or to circuit defects.

Acknowledgment

The proposed work has been developed within the framework of the project: "*xTech NextHub: Competence Center for Innovative Solutions Development*" (Bando regionale della Puglia per gli aiuti in esenzione n. 17 del 30/09/2014 -BURP n. 139 suppl. del 06/10/2014 e s.m.i. - TITOLO II CAPO 2 DEL REGOLAMENTO GENERALE "Avviso per la presentazione dei progetti promossi da Grandi Imprese ai sensi dell'articolo 17 del Regolamento").

References

[1] M. Ragnoli et al., "A condition and fault prevention monitoring system for industrial Computer Numerical Control machinery", IEEE Access, vol. 12, pp. 20919-20930, 2024.

[2] M. Dotoli et al. "A Timed Petri Nets model for intermodal freight transport terminals", IFAC Proc. Vol., vol. 47 (2), pp. 176-181, 2014.

[3] G. Cavone et al., "Hybrid Petri Nets to re-design low-automated production processes: the case study of a Sardinian bakery", IFAC-PapersOnLine, vol. 51 (7), pp. 265-270, 2018.

[4] M. Dotoli et al., "A Nash equilibrium simulation model for the competitiveness evaluation of the auction based day ahead electricity market", Comput. Ind., vol. 65 (4), pp. 774-785, 2014.

[5] M. Dotoli and N. Epicoco, "Integrated network design of agile resource-efficient Supply Chains under uncertainty", IEEE Trans. Syst. Man. Cybern., vol. 50 (11), pp. 4530-4544, 2020.

[6] M. Lezzi, M. Lazoi, A. Corallo, "Cybersecurity for Industry 4.0 in the current literature: A reference framework", Comput. Ind., vol. 103, pp. 97-110, 2018.

[7] NIST Special Publication, NIST SP 800-82r3, "Guide to Operational Technology (OT) security", 2023.

[8] A. Massaro, *Electronic in advanced research industry: From Industry 4.0 to Industry 5.0 advances.* Wiley/IEEE Press, 2022. ISBN: 9781119716877.

[9] N.M.R. Monjur et al., "Hardware security in sensor and its networks," Front. Sens., vol. 3, pp. 1-12, 2022.

[10] M. R. Monjur, S. Sunkavilli, Q. Yu, "ADobf: Obfuscated detection method against analog trojans on I2C master-slave interface", 2020 IEEE 63rd Int. Midwest Symposium on Circuits and Systems, Springfield, MA, USA, 2020, pp. 1064-1067.

[11] M. Monjur, J. Calzadillas, Q. Yu. "Hardware security risks and threat analyses in advanced manufacturing industry", ACM Trans. Des. Automat. El. Sys., vol. 28 (5), art. 83, 2023.

[12] T. Phillips, H. Mehrpouyan, J. Gardner, S. Reese, "A covert system identification attack on constant setpoint control systems", 7th Int. Symposium on Computing and Networking Workshops, Nagasaki, Japan, 2019, pp. 367-373.

[13] M. Serror et al., "Challenges and opportunities in securing the Industrial Internet of Things", IEEE Trans. Ind. Inform., vol. 17 (5), pp. 2985-2996, 2021.

[14] D. Bhamare et al., "Cybersecurity for industrial control systems: A survey", Comput. Secur., vol. 89, art. 101677, 2020.

[15] T. Alladi, V. Chamola, S. Zeadally, "Industrial control systems: Cyberattack trends and countermeasures", Comput. Commun., vol. 155, pp. 1-8, 2020.

[16] W. Duo, M. Zhou, A. Abusorrah, "A survey of cyber attacks on Cyber Physical Systems: Recent advances and challenges", IEEE/CAA Journal of Automatica Sinica, vol. 9 (5), pp. 784-800, 2022.

[17] M. Xue et al., "Ten years of hardware trojans: A survey from the attacker's perspective", IET Comput. Digit. Tech., vol. 14, pp. 231-246, 2020.

[18] S. Guo et al., "Securing IoT space via hardware trojan detection", IEEE Internet Things J., vol. 7 (11), pp. 11115-11122, 2020.

[19] C. He et al., "A side-channel hardware trojan detection method based on fuzzy C-Means clustering and fusion distance algorithms", IEEE Internet Things J., vol. 11 (8), pp. 13927-13937, 2024.

[20] R. Yasaei, L. Chen, S. -Y. Yu and M. A. A. Faruque, "Hardware trojan detection using Graph Neural Networks", IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst., 2022.

[21] J. Liu et al., "ShadowPLCs: A novel scheme for remote detection of industrial process control attacks", IEEE Trans. Depend. Secure Comput., vol. 19 (3), pp. 2054-2069, 2022.

[22] www.analog.com/en/resources/design-tools-and-calculators/ltspice-simulator.html.

[23] R. Carli et al., "Model Predictive Control for thermal comfort optimization in building energy management systems", 2019 IEEE Int. Conf. Systems, Man and Cybernetics, Bari, Italy, 2019, pp. 2608-2613.

[24] A. Massaro, "ANNs predicting noisy signals in electronic circuits: A model predicting the signal trend in amplification systems", AI, vol. 5 (2), pp. 533-549, 2024.