Volume 9, Issue 7, July – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL664

Artificial Intelligence Based Embedded Security Solution Model for PID Controller

Bitrus Haruna[1]; Mathew Ehikhamenle[2]
Centre for Information and Telecommunication Engineering
University of Port Harcourt Choba, Rivers State, Nigeria

Abstract:- This study investigated the impact of artificial intelligent based embedded security solution model for PID controller. Recent studies have revealed that the conventional mitigation techniques like zoning, demilitarization, firewalls, company's policies to mention but a few are no longer enough to match the sophisticated intelligence being deployed by attackers hence the urgent need for the adoption of artificial intelligent based embedded security solution model. Furthermore, conventional IT security solutions cannot be deployed directly in process controllers given the real time availability requirement of industrial control systems. This has limited the security solutions to firewalls, network segmentation and some laid down policies which the control system operators are not expected to violate. This study will ultimately help deliver algorithms that will be implemented in industrial field device controllers making them resilient to cyber-attacks whose consequences have far reaching implications. With regards to the methodology of the work, four sets of data were collected from the test bed. The first data, Data_1, shown in appendix D is the plant's response to the existing PID algorithm. This was done by taking the temperatures of the plant at interval of 3 seconds after loading the controller with the existing (insecure) PID algorithm shown in appendix A. A total of 100 samples were taken. From the methodology employed, it was discovered that it is seen that the existing PID algorithm was able to achieve the control objective of maintaining the temperature of the process plant within the temperature range of 38 ° C and 43 ° C with 40 ° C as the optimal or ideal performance. From table I in appendix I, the mean steady state error (MSSE) of the existing PID algorithm considering the 27th to 101th temperature data is 0.062631579 which is approximately 0.06. It means the accuracy of the existing PID algorithm is $((40 - 0.06)/40) * 100 = 99.85\ \%$. This showed that the existing PID control algorithm's performance is acceptable under normal condition since the minimum control accuracy required to achieve the control objective in the considered process plant is $(40 - (3\text{-}2)/2)/40) * 100 = 98.75\ \%$.

Keywords: *Artificial Intelligence, Security Solution Model, PID Controller.*

I. INTRODUCTION

In general, we are living in the era of digital warfare (Kim, Countdown to Zero Day, 2021). According to the American National Standard Institute and the International Society of Automation (ANSI/ISA), it has moved up from the internet domain, which is level 5, to the enterprise domain, level 4, and finally to the Process Control Domain, which is levels 0, 1, and 2 (ISA, ANSI/ISA-TR99.00.01-2021 Security Technologies for Industrial Automation and Control Systems, 2021). According to Kotenko & Ulanov's Packet Level Simulation of Cooperative Distributed Defense against Internet Attacks (2018), it appears that conventional mitigation methods like zoning, demilitarization, firewalls, and company policies, to name just a few, are no longer sufficient to match the sophisticated intelligence being deployed by attackers.

In light of these prevalent threats, it is necessary to investigate the control system loop, the fundamental component of a control system, in order to identify any security gaps and offer appropriate solutions to those gaps. The developed solution can also be used in the pharmaceutical, automotive, and robotics industries, among other automation-related fields.

II. PROBLEM STATEMENT

A distributed control system's process controller is similar to a football goalkeeper. Despite the fact that it is the last "man" to be defeated when it comes to attacking industrial processes, it lacks any form of security other than security by obscurity, which cannot be completely relied upon given the open network architecture of contemporary distributed control systems. Tragically, the customary IT security arrangements can't be sent straightforwardly in process regulators given the continuous accessibility necessity of modern control frameworks. As a result, security measures have been restricted to firewalls, network segmentation, and a few predetermined policies that control system administrators are not expected to violate (Shell group of Companies, 2021). Field controllers, which have a recovery time objective (RTO) of zero, can be argued to be more important than other components of a distributed control system, so it has become important to develop enhanced and appropriate security solutions for them. This study sought to critically examine the impact of an embedded security solution model for PID controller based on artificial intelligence on the foregoing.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL664

III. SIGNIFICANCE OF THE STUDY

➢ *The Significance of this Study cannot be Over-Emphasized. These Include but not Limited to:*

- It will help deliver algorithms that will be implemented in industrial field device controllers making them resilient to cyber-attacks whose consequences have far reaching implications.
- This study is also important based on the fact that without field device controllers, industries would lack required efficiency in their business operations. Consequently, it can be said that the device controllers do not only control field devices, but also control economy.

IV. METHODOLOGY

This work employed a top-down and bottom-up design approach in combination. The mathematical models of the secured PID algorithm, or SPIDA, an artificial intelligence algorithm security solution for industrial process control, were initially developed using a top-down approach. The software codes and flowcharts for putting the secured PID algorithm into action were also created using the same method. The product codes were created utilizing inserted c language with Arduino uno as the objective gadget. Granular perspective was then used to plan and execute a model intensity control framework which was utilized to approve the got PID calculation.

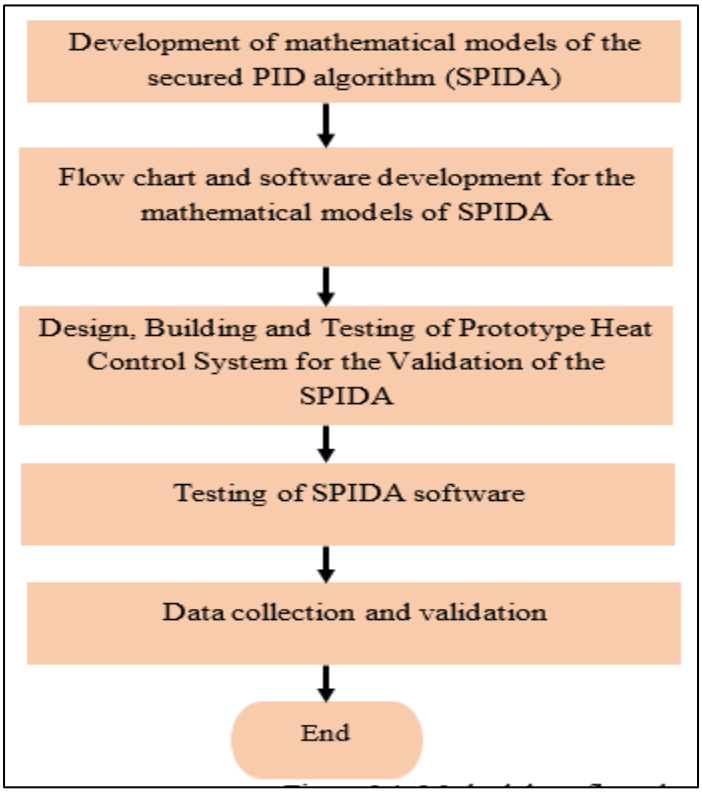

Fig 1: Methodology Flow Chart

Figure 1 above is the sequence of the approach adopted to realize the aim of this work.

V. RESULTS AND DISCUSSIONS

The plant's response to the existing PID algorithm under normal circumstances is depicted in figure 2, while the plant's response to the secured PID algorithm is depicted in figure 3. Under normal conditions, the responses of the process plant to the secured and existing PID algorithms are compared in Figure 4.

The process plant's response to the existing PID algorithm under threat or attack is depicted in Figure 5, while the process plant's response to the secured PID algorithm is depicted in Figure 6 under the same threat or attack conditions.

The plant's response to the existing and secured algorithms under the same threat conditions is compared in Figure 7.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL664

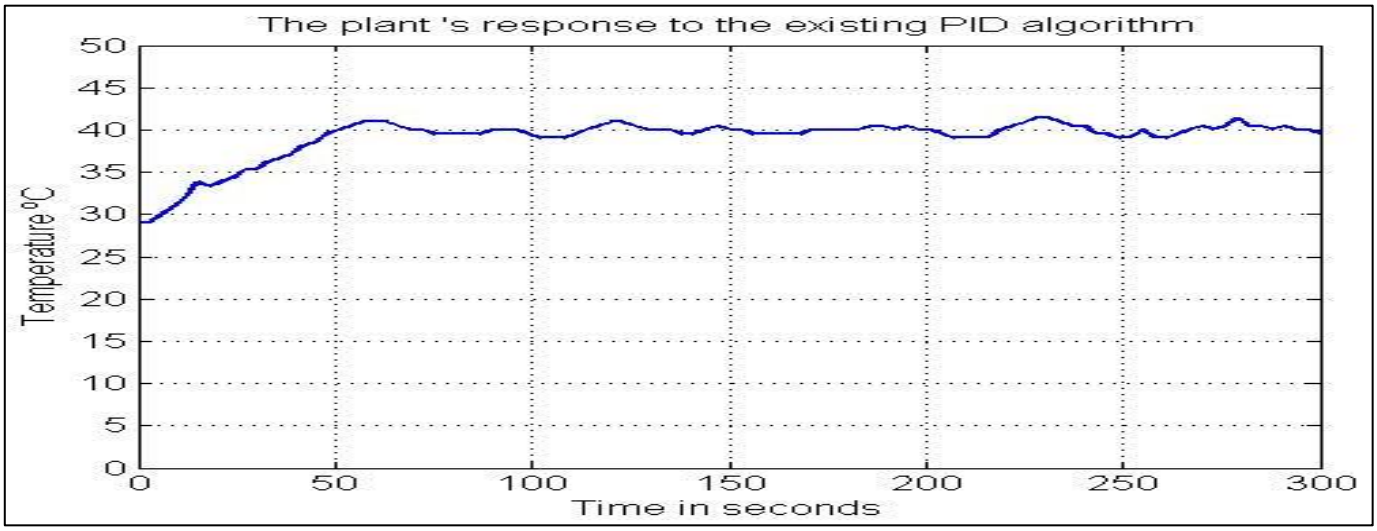

Fig 2: Plant's Response to the Existing PID Algorithm Under Normal Condition

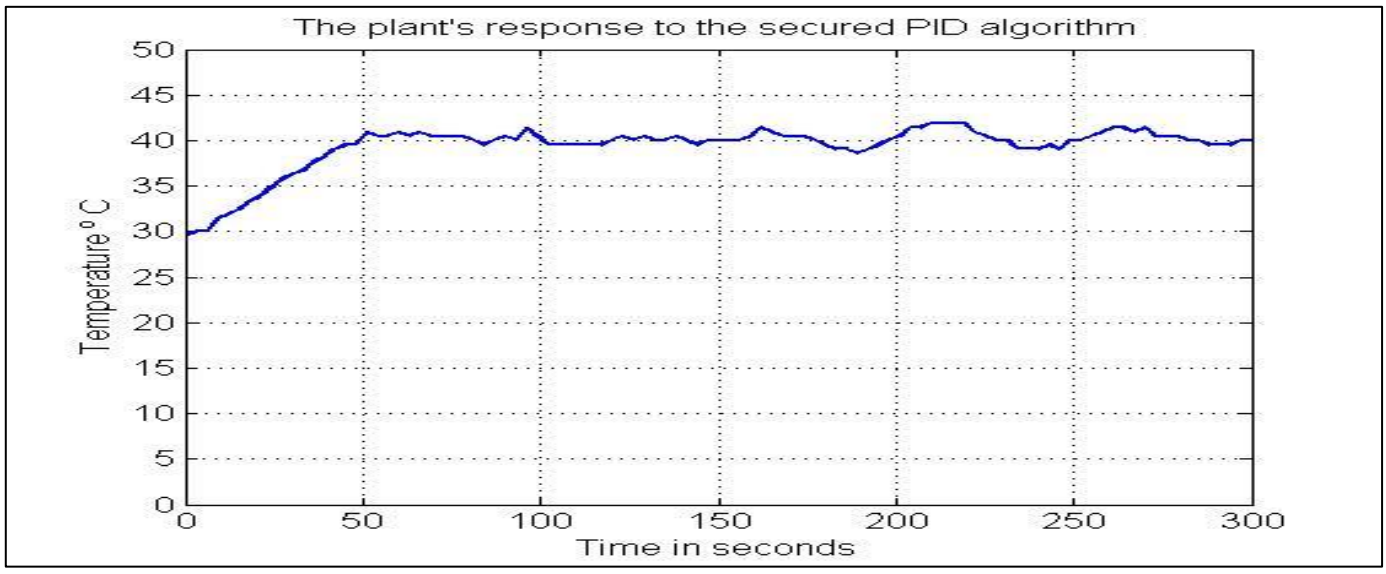

Fig 3: Plant's Response to the Secured PID Algorithm Under Normal Condition

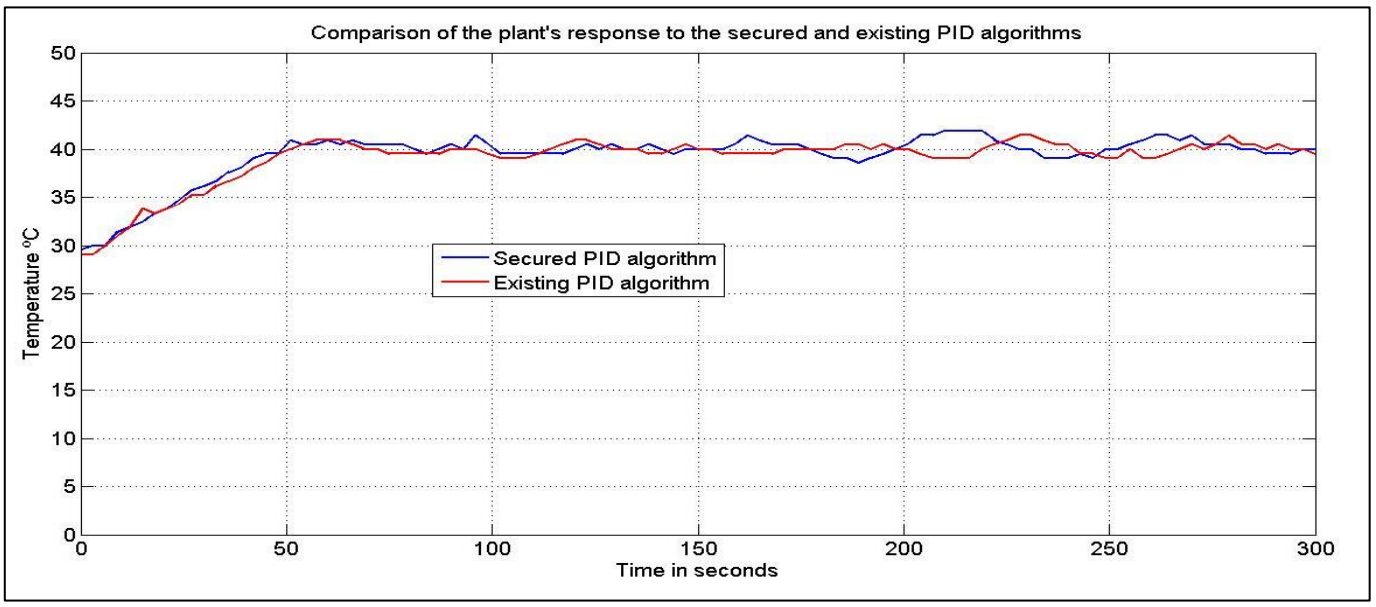

Fig 4: Response of the Process Plant to the Secured and the Existing PID Algorithms Under Normal Condition

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL664

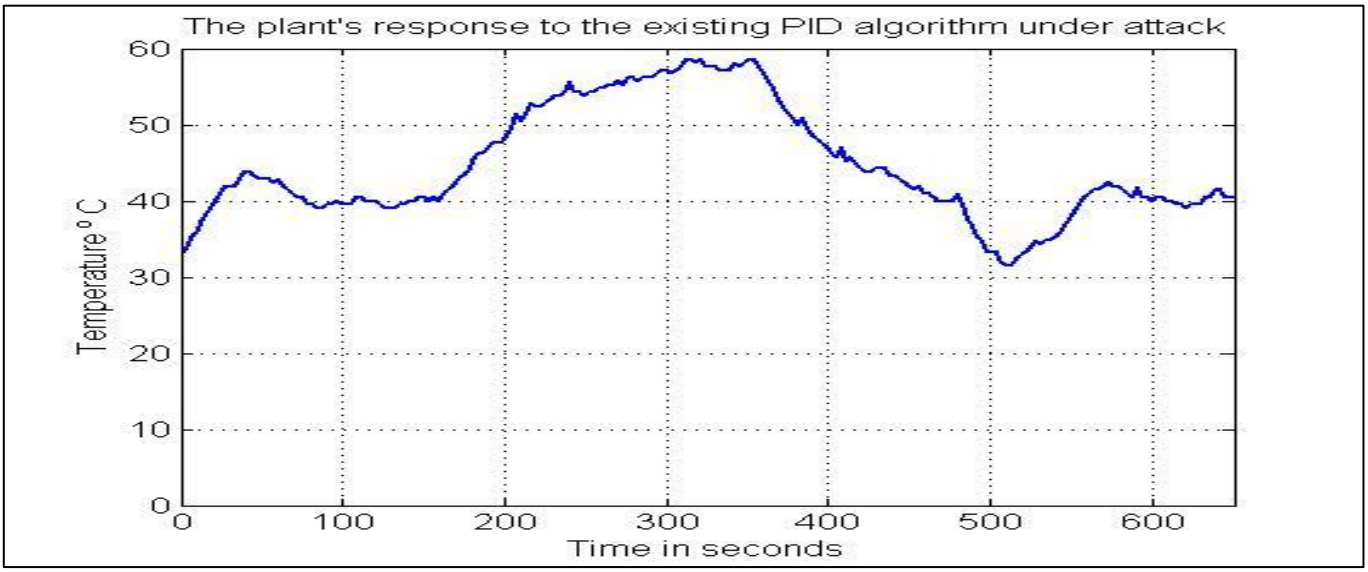

Fig 5: Response of the Process Plant with the Existing PID Algorithm Under Threat Conditions

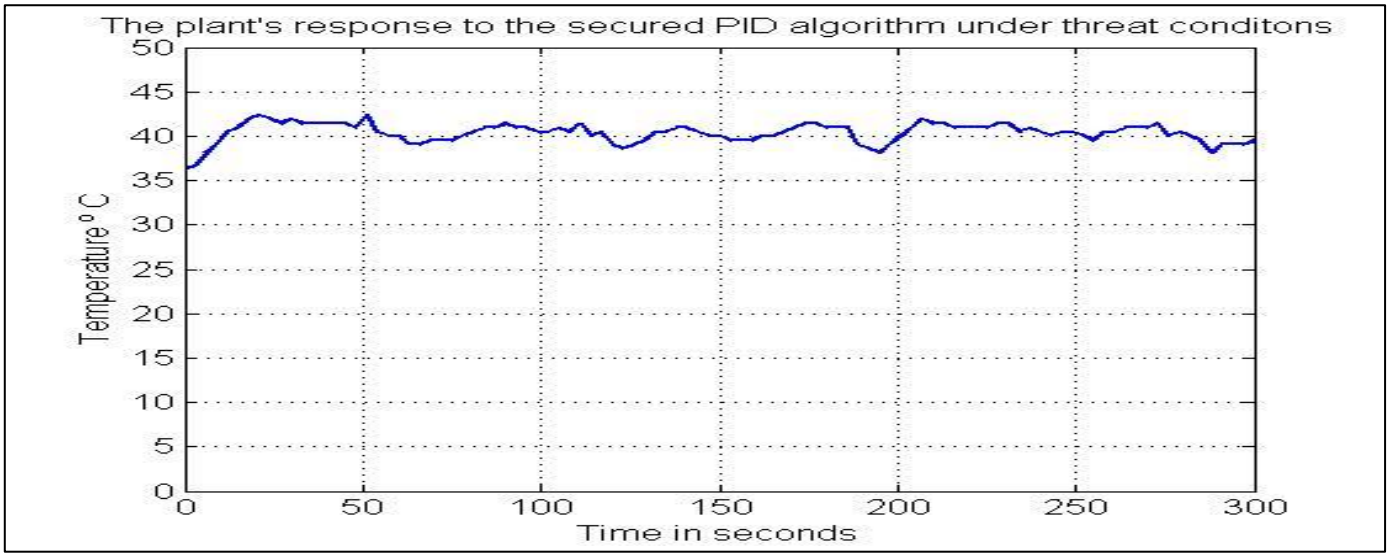

Fig 6: Response of the Process Plant with the Secured PID Algorithm Under Threat Conditions

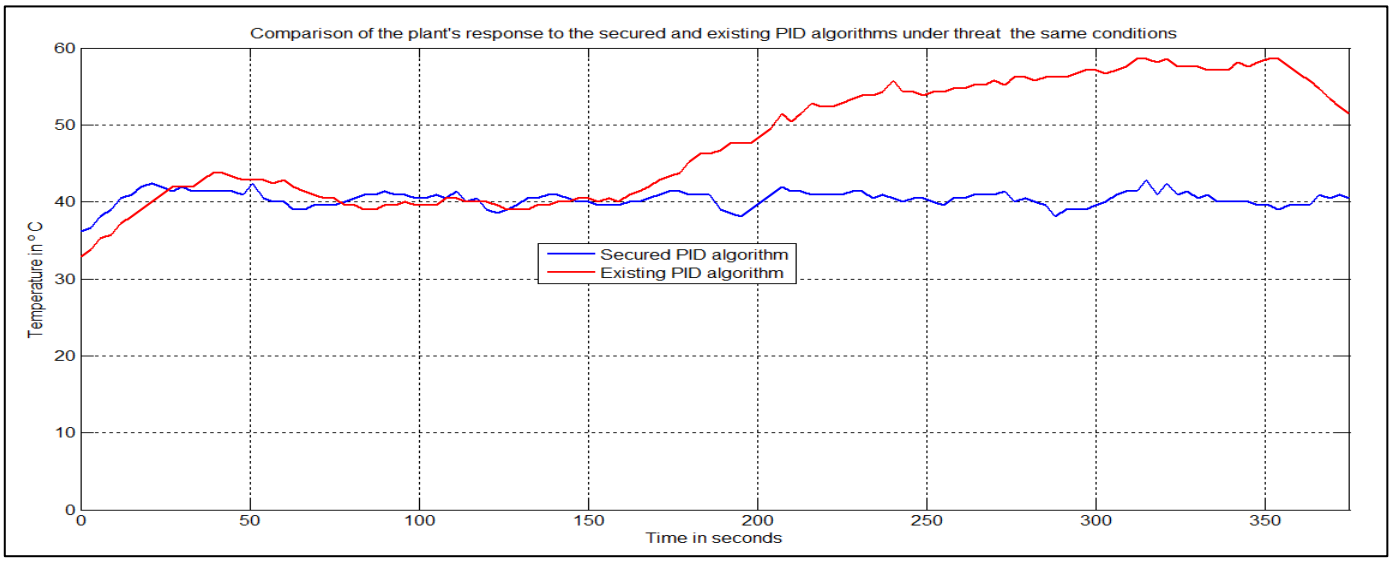

Fig 7: Response of the Process Plant to the Secured and the Existing PID Algorithms Under the Same Threat Conditions

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL664

A. Discussion on the Plant's Response to the Existing PID Algorithm Under Normal Condition

From figure 2, it is seen that the current PID calculation had the option to accomplish the control objective of keeping up with the temperature of the interaction plant inside the temperature scope of 38 º C and 43 º C with 40 º C as the ideal or optimal execution. The current PID algorithm's mean steady state error (MSSE) for the 27th to 101st temperature data is 0.062631579, or approximately 0.06, according to table I in appendix I. This indicates that the current PID algorithm is accurate to ((40 – 0.06)/40)*100, or 99.85 percent. Since the minimum control accuracy required to achieve the control objective in the considered process plant is ((40 – (3-2)/2)/40)*100=98.75 percent, this demonstrated that the performance of the existing PID control algorithm is acceptable under normal conditions.

Figures 3 and 4 show that the secured PID algorithm was also able to achieve the control objective of maintaining the process plant's temperature within the temperature range of 38 o C to 43 o C, with 40 o C representing the optimal or ideal performance

B. Discussion on the Plant's Response to the Secured PID Algorithm

Under Normal Conditions The secured PID algorithm's mean steady state error (MSSE) for the 27th to 101st temperature data is 0.288421, or approximately 0.29, according to table I in appendix I. This indicates that the secured PID algorithm is accurate to ((40 – 0.29)/40)*100, or 99.28 percent. This demonstrated that, despite the fact that the secured PID control algorithm has an effect on the availability and integrity of the process plant, the impact is still within an acceptable range.

It is seen from figures 6 and 7 that the got PID calculation (SPIDA) had the option to accomplish the control objective even within the sight of the mimicked danger specialists. Taking into account temperature data from the 27th to the 126th, the MSSE of SPIDA was determined to be 0.372475248, or approximately 0.37, according to table J2 in appendix J. ((40 – 0.37)/40)*100 = 99.08 percent accuracy. Still, this is perfectly acceptable! Figure 5 makes it abundantly clear that the current PID algorithm (EPIDA) was unable to accomplish its control goal. Based on the 27th to 126th temperature data in appendix J's table J1, the MSSE of EPIDA is 9.50029703. ((40 – 9.5)/40)*100=76.25 % is the accuracy. In the process plant under consideration, the minimum control accuracy required to achieve the control objective is currently 98.75 percent. The EPIDA is not suitable for remote applications where threat agents may have access to process control parameters because 76.25 percent is less than 98.75 percent. The fact that the finished product does not meet standard requirements will have a practical effect on the acid gas removal procedure from natural gas. The company (SNEPCo) will face sanctions as a direct result. In addition to making customers unhappy, this will give competitors an advantage in business.

C. Contribution of this Article to the Body of Knowledge

The following are the contributions that this work made to the existing body of knowledge:

- It created and incorporated proactive security into the widely used back-end control algorithm used in the automation industry, positioning the sector for cloud-based automation without posing a threat from within or outside the organization.
- The cycle plant worked to approve the got PID calculation can be taken on in colleges and polytechnics for effective educating and learning of PID control standards particularly in the creating and immature nations of the existence where the investigation of control designing is a greater amount of numerical speculations than reasonable. Students will be better prepared for successful careers in the automation industry as a result of this.

REFERENCES

[1]. bdel-geliel, M., Qaud, F., & Ashour, H. (2020). Realization of adaptable PID controller within an industrial automated system. *IEEE 11th international conference on control & automation* (pp. 965-970). Taichung: IEEE.

[2]. Anthony, K. (2018). *Fundamental of PID control.* PDH Center.

[3]. Eric, D. K. (2011). *Industrial network security: securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems.* USA: Elsevier publisher.

[4]. Fairchild, S. (2017, August 29). *Datasheet catalog.* Retrieved August 29, 2017, from Datasheetcatalog: http://www.datasheetcatalog.com/datasheets_pdf/4/N/3/5/4N35.shtml

[5]. Fawzi, H., Tabuada, P., & Diggavi, S. (2012). Security for control systems under sensor and actuator attacks. *IEEE international conference on Decision and Contro* (pp. 3412 – 3417). Maui HI : IEEE.

[6]. Gupta, D., Mohapatra, P., & Chuah, C. (2008). Efficient monitoring in wireless mesh networks: overheads and accuracy trade-offs. *IEEE 5th international conference on Mobile Ad Hoc and Sensor systems* (pp. 13-23). Atlanta: IEEE hjkml. (2017). gghhl. *ghjk* (p. 67). bbb: bb

[7]. Hong, R. (2011). Research and application of TCP/IP protocol in embedded system. *IEEE 3rd international conference on communication software and networks* (pp. 584-587). Xi'an: IEEE.

[8]. Hongji, W., & Zhenqiu, H. (2011). PID parameter optimization of pressure and phear testing controller based on CLPSO algorithm. *International conference on computer-aided design, manufacturing, modelling and simulation* (pp. 105-109). Switzerland: Trans Tech Publications.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL664

[9]. ICS-CERT. (2019, December 12). *ICS-CERT*. Retrieved September 24, 2015, from https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT#need: https://d36spl5w3z9i0o.cloudfront.net/dcd/scormapi_v60/launcher.html?host=ics-cert-training.inl.gov&id_user=22129&id_reference=203&scorm_version=1.3&id_resource=24203&id_item=111&idscorm_organization=111&id_package=111&id_course=17&launch_type=popup&auth_ ICS-CERT. (2021, June 30). *ICS-CERT*.

[10]. Ikhlef, A., Kihel, M., Boukhezzar, B., Mansouri, N., & Hobar, F. (2015). Remote PID control of tank level system. *International Conference on Interactive Collaborative Learning* (pp. 20-24). Italy: IEEE.

[11]. NIST. (2021, January 30). *National Institute of Standards and Technology*. Retrieved 2 3, 2015, from www.csrc.nist.gov: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[12]. Okeke, P. N., & Ndupu, B. L. (1983). *Ordinary level physics.* New Jersey: Prentice Hall Press.

[13]. Peng, Z. (2010). *Advanced Industrial Control Technology*. Amsterdam: Elsevier.

[14]. Peter, L. (2013, April 23). *TechTarget*. Retrieved September 25, 2015, from http://searchsecurity.techtarget.com: http://searchsecurity.techtarget.com/resources/Hacker-Tools-and-Techniques-Underground-Sites-and-Hacking-Groups

[15]. Philips. (2021, August 29). *Datasheet Catalog.* Retrieved August 29, 2017, from DataSheetcatalog: http://www.datasheetcatalog.com/datasheets_pdf/B/T/1/3/BT139.shtml

[16]. Reddy, Y. J. (2015). *Industrial process automation systems: design and implementation.* Amsterdan: Elsevier.

[17]. Schneidar, E. (2013, July 23). *The Engineering Toolbox*. Retrieved October 23, 2015, from www.engineeringtoolbox.com: http://www.engineeringtoolbox.com/air-properties-d_156.html

[18]. Schneider, E. (2021, September 25). *PID Control made easy*. Retrieved August 28, 2017, from Eurotherm: http://www.eurotherm.com/pid-control-made-easy

[19]. Shahrukh, A., & Sandip, G. (2014). *Microcontroller implementation of digital pid* . Rourkela: National Institute of Technology.

[20]. Shell Global Solutions, I. (2015). *DESIGN AND ENGINEERING PRACTICE.* Netherlands: Shell Group of Companies.

[21]. Shell group of Companies. (2021, May 12). *DEP-00.00.05.05-GEN.* Retrieved February 03, 2015, from www.scribd.com: Shell group of Companies, “Design Engineering Practice Specification: prowww.scribd.com/archive/plans?doc=238070612&escape=false&

[22]. Silva, V., Carvalho, V., Vasconcelos, R., & Soares, F. (2016). *Remote PID Control of a DC Motor.* International Journal of Online Engineering.

[23]. Smith, D. J., & Kenneth, G. S. (2011). *Safety Critical Systems Handbook: a straightforward guide to functional Safety, IEC 61508 and related standards.* USA: Elsevier pulishers.

[24]. Stan, Ż. (2013). *An Introduction to Proportional-Integral-Derivative (PID) Controllers.* Lafayette: Purdue University.

[25]. Stuart, M. (2000). *Operational aspects of oil and gas well testing.* USA: Elsevier publisher.

[26]. Texas, I. (2015, June 4). *DatasheetCatalog.com*. Retrieved November 10, 2015, from LM35 Precision Centigrade Temperature Sensors: http://www.datasheetcatalog.com/datasheets_pdf/L/M/3/5/LM35.shtml

[27]. Timberlake. (2015). *Chemistry: An Introduction to General, Organic, and Biological Chemistry.* Los Angeles: Pearson .

[28]. Torres, G. (2014, November 13). *Hardwaresecrets*. Retrieved March 25, 2015, from www.hardwaresecrets.com: www.hardwaresecrets.com/article/433

[29]. Vicomsoft. (2014, September 12). *Vicomsoft Leraning Centre*. Retrieved April 4, 2015, from www.vicomsoft.com: www.vicomsoft.com/learning-center/firewalls/ Weli, W. (2014). *Bonga South West Instrument Operation Summary.* Lagos: SNEPCo.

[30]. Wikipedia. (2015, January 3). *Wikipedia encyclopedia*. Retrieved February 12, 2015, from http://en.wikipedia.org: http://en.wikipedia.org/wiki/Systems_analysis

[31]. WWittrisch, C., & Chole, H. (2012). *Progressing cavity pumps: oil well production artificial lift.* Energies Nouvelles.

[32]. Yadong, L., Wenqiang, C., Danlan, L., & Ru, i. Z. (2011). Research based on OSI model. *IEEE international conference on communication software and Networks* (pp. 554-557). Xi'an: IEEE.