Received: 8 June 2025 | Revised: 11 June 2025 | Accepted: 18 June 2025 | Vol. 1 | Issue 1 | June 2025
e-ISSN: 3105-2169

International Journal of Mechatronics, Robotics, and Artificial Intelligence
Original article

Towards Smart Manufacturing: Implementing PI Control on PLCs in IIoT-Driven Industrial Automation

Huda S. Jaafer*[1], Ali A. Abed[2]
[1]Computer Engineering Department, University of Basrah, Basrah, Iraq
[2] Mechatronics Engineering Department, University of Basrah, Basrah, Iraq

Correspondence
*Huda Sabah Jaafer
Computer Engineering Department, University of Basrah
Email: pgs.huda.sabah@uobasrah.edu.iq

Abstract
The rapid development of the Internet of Things (IoT) has drawn significant attention from both industry and academia, driven by the integration of cloud computing, big data analytics, machine learning, and cyber-physical systems in manufacturing. Programmable Logic Controllers (PLCs), long central to industrial control systems, have evolved from basic feedback control devices to advanced components capable of networking and data exchange through IoT technologies. The Industrial Internet of Things (IIoT) refers to intelligent automation systems that continuously monitor critical parameters and respond to changes in real time. The integration of IoT with PLCs is transforming industrial automation by enabling remote real-time monitoring, data-driven decision-making, and predictive maintenance through advanced analytics. IIoT technologies enhance manufacturing performance and offer strategic value across sectors. Understanding their impact involves examining current research, including technology assessments and application-based case studies. This study provides an overview of PLC systems evolving into IIoT frameworks, with a focus on implementing proportional-integral (PI) control using the Siemens S7-300. Designed for precise and consistent temperature regulation, this approach enhances process efficiency and product quality, making it highly suitable for industrial and manufacturing environments.

Keywords
Internet of Things, Industry 4.0, IIoT, PLC S7-300, PI controller, Industrial automation.

I. INTRODUCTION

The physical world is evolving into a digital environment, and everything is becoming increasingly interconnected. The proliferation of smart devices and technology has enabled humans to stay connected at all times and from any location. The IoT is a clever technology with many uses in health, the environment, monitoring transportation systems, and other business sectors. The IoT is a network composed of sensors, hardware, software, storage sharing, and internet access that allow these objects to gather, record, manage, and exchange data [1]. Through existing network infrastructure, the IoT enables remote sensing and control of objects, improving efficiency and accuracy while creating opportunities for more direct integration of the physical world into computer-based systems [2]. In recent decades, extensive research has been conducted on real-world IoT operations. According to the description, this technology manages physical objects connected to data via the Internet without requiring human-machine intervention and human-human interactions. This concept is well recognized as the "embedded Internet." However, Kevin Ashton introduced the term "Internet of Things" (IoT) in 1999. The conception of the IoT began to gain traction in the summer of 2010. In 2011, Gartner, a newly emerging research institution, included it in its list of the "Internet of Things." The following year, the largest Internet conference in Europe was called LeWeb. The IoT garnered significant attention in January 2014 when Google announced the acquisition of Nest for $3.2 billion. The Industrial Internet of Things (IIoT) has primarily focused on the economic sector, whereas IIoT serves the industrial sector. Through IIoT technology, data collection, processing, and exchange across connected devices can be achieved. This approach has enhanced effectiveness and reliability. Industrial processes can be monitored and controlled using various techniques, including PLC, supervisory control and data acquisition (SCADA), wireless sensor networks (WSN), and the Internet of Things. PLCs are utilized in multiple industrial automation processes to reduce production costs while improving quality and reliability. IoT currently represents the most practical method for monitoring industrial processes. It combines communication and embedded technologies that enable industrial equipment to connect to the Internet and be monitored via wireless

sensor networks or that allow industrial applications to be managed and monitored through laptops and mobile devices. This technology provides real-time feedback in manufacturing, energy operations, oil, and gas. Smart manufacturing leverages IIoT and advanced control strategies to optimize industrial automation. Implementing PI (Proportional-Integral) control on PLCs within IIoT-driven environments is a key step toward achieving flexible, efficient, and intelligent production systems. Classic PI and PID controllers remain widely used due to their simplicity and robustness. Enhanced versions, such as piecewise affine PI controllers, can be implemented on PLCs to handle system constraints more effectively, resulting in improved performance metrics like reduced settling time and better error management compared to traditional tuning methods. PLCs can be combined with low-cost embedded platforms (e.g., Arduino, Raspberry Pi) and open-source IIoT software to create flexible, distributed control systems. These setups support remote monitoring, fault detection, and human-machine interfaces, demonstrating reliable operation in real-world scenarios.

II. Evolution Revolution of The Internet of Things

There have been enormous advancements in technology, society, and business practices in the twenty-first century. With the wave of global 5G and Industry 4.0, IoT technology is widely utilized across various industries. Alongside the digital transformation of businesses, which continually raises the bar for IoT information and communication software and hardware, Industry 4.0 has elevated smart manufacturing. The Internet of Things is among the emerging technologies that attract interest from many scholars [8]. Most industries have transitioned toward automation and reduced human involvement as a result of the fourth industrial revolution, also known as Industry 4.0. By connecting different devices and using sensors for automation, the developing IoT provides a diverse platform for numerous technologies [9]. It establishes a framework for scaling the use of various smart devices. Once the IoT is implemented, devices can connect without human intervention. Moreover, IoT-based solutions see broad adoption across many industries because they operate independently of human involvement. The essence of IoT transcends merely integrating the latest gadgets into an increasingly interconnected society. Technologies like artificial intelligence, cloud computing, and low-cost sensors emerge as needed and will also play a role in future industrial technologies alongside big data. This new technological layer, known as the IIoT, transforms key industries, including manufacturing, energy consumption, mining, and transportation, thereby significantly impacting the economy as a whole [10]. Dick Marley's invention of one of the greatest manufacturing advancements in history in 1968 marked the onset of the IIoT. The PLC, conceived by Marley and his associates, is foundational for industrial robotics and assembly line automation [11]. Today, smart devices equipped with IoT capabilities include laptops and mobile phones. Single-board computers (SBCs), input/output components, and networking devices with IoT capabilities are rapidly employed in industrial processes. IIoT and Industry 4.0 are adopted in various business procedures, transforming the next generation of industry. The integration of Industry 4.0 and IIoT leads to increased productivity, enhanced quality, reduced overhead, and improved security [10]. One definition of the IIoT describes it as a revolution fundamentally altering the industrial landscape. Intelligent automation has given rise to the technologies and capabilities now integral to the Industrial Internet of Things. The most significant benefit of IIoT is that, while utilizing current IIoT technology, end users and machine builders can gain insights into their existing investments in people and technology. Those overseeing site operations experience a mix of hope and confusion as the industrial Internet of Things evolves. Much of this genre examines how technological advancements influence the automated platforms currently in use. From an industrial IoT perspective, networked smart assets form a larger system that comprises a smart manufacturing company [12]. The IIoT represents a revolutionary change, especially in manufacturing. This concept is appealing to most industries and enhances operational efficiency in the manufacturing cycle by integrating technology and smart automation capabilities with continuous monitoring of smart object recognition processes. This significantly reduces disruption when working in hazardous production environments. IIoT capabilities encompass warehouses, warehousing, assembly lines, manufacturing processes, product finishing, and other management input and output activities. The foundation of the IIoT trend is IoT, which ensures efficient operations in various fields such as industry, society, and business sectors [13].

III. Transforming IoT into IIoT

The transition of the IoT from the commercial to the industrial sphere has a significant impact on the continuity and efficiency of global industry. However, because the Industrial Internet of Things provides a platform for global interconnection via the Internet Protocol (IP), it elevates industries or machines to new heights. Regardless of the type of equipment in circulation, one device can communicate with another using the same architecture and protocols, thanks to the IP. IP has a significant impact on both the connectivity of physical devices and network infrastructure. The IIoT integrates big data, machine learning, PLCs, and supervisory control and data acquisition (SCADA) systems. Additionally, it adds self-diagnostic and debugging capabilities to automation technologies. However, process control industries use physical devices (such as flow, level, vibration, temperature, pressure, and many others), and these devices are often used solely as data collection tools. However, new applications are already being developed to exchange, analyze, and correct this data. In addition to being final, scalability is a clear differentiator between the IIoT and the IoT. An industrial or business-oriented network can aid in data collection, scheduling, analysis, interoperability, decision-making, workflow integration, and communication. For business purposes, thousands of new sensors and non-IoT devices, such as controllers, robots, machines, and other

utility applications, are being connected to the Industrial Internet of Things network [15].

IV. Conceptual Architecture of IoT

Each organization has its device clusters with constrained interfaces. Considering the difficulties, there isn't a single answer that addresses every issue. The foundation of the IIOT architecture is the collaboration of multiple elements or tiers. The architecture that this paper proposes, If the goals of the IIoT integration are to be achieved, these components must exist, as shown in Fig. 1. These elements are [10][14]:

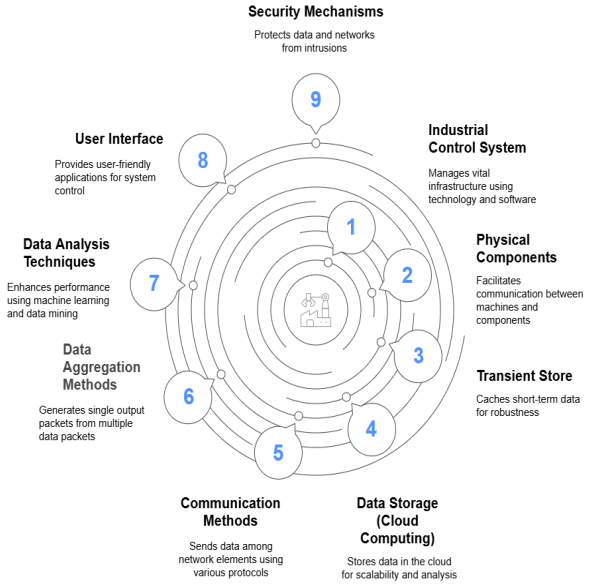

Fig. 1. Conceptual architecture of IIoT

• **Industrial control system:** It is a general term for the use of technology and software in tandem to manage vital infrastructure. Distributed control systems (DCS), PLC, control servers, SCADA systems, remote terminal units (RTU), intelligent electronic devices (IED), human-machine interfaces (HMI), host of other industry-specific systems are typically used in their construction [16][11], as shown in Fig. 2.

• **Physical components:** Elements of the industrial framework that include sensors, actuators, and gateways to facilitate communication between machines and components. The heater, temperature sensor, pump, and water tank are used. These components work together in an integrated system, with the sensor measuring the water temperature and communication between these components via control signals from a PLC to achieve the desired temperature.

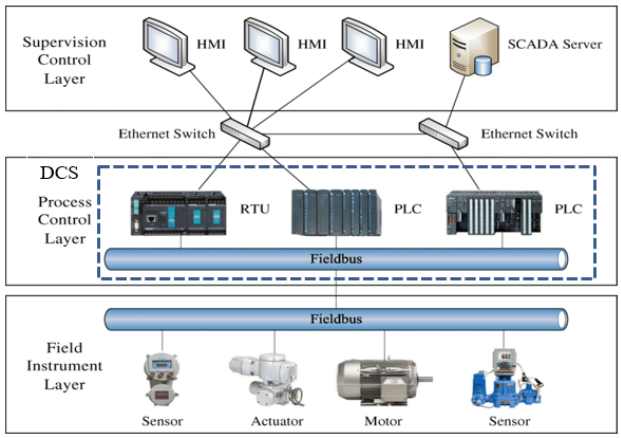

Fig. 2. Industrial control system

• **Transient store:** Is a component of the main architecture that caches or caches short-term data before further processing or transmission. Ensure robustness during operation and system failure, including network failure. It ensures that data is temporarily stored while being transferred from the sensors to the control interface. Node-RED is used to facilitate this storage and ensures that the data is ready to be sent to a database for further use.

• **Data storage (Cloud Computing):** Analytics is becoming more prevalent in industries worldwide. The cloud is a platform that includes powerful software and hardware. Recently, several cloud layers have been proposed, such as fog computing. In addition to the cloud, some manufacturing networks may maintain data in their own data centers or servers, depending on their policies and plans. IIoT now keeps data in the cloud. The most important characteristic of cloud storage is scalability. Data saved in the cloud can be instantly evaluated or interpreted using artificial intelligence or data mining to improve access time.

• **Communication methods:** IIoT relies largely on many communication protocols to send data among network elements, such as 6LowPAN. Communication methods in the IIoT must meet a variety of requirements, which may vary by sector. These requirements include high bandwidth, low power consumption, and reliable connectivity. For example, high-bandwidth PC-to-cloud connectivity is most important, while M2M (machine-to-machine) communication requires a highly reliable connection. M2M communication methods are as shown in Fig. 3.

• **Data aggregation methods:** This is a process that obtains several data packets using standard protocols and generates a single output packet. Given the massive volume of data generated by physical devices, data aggregation is a critical element of the IIoT. Clustering may provide a coherent explanation for such data by reducing existing complexity. Currently, four primary data sets differ by industry: centralized, in-network, tree-based, and clustered methodologies.

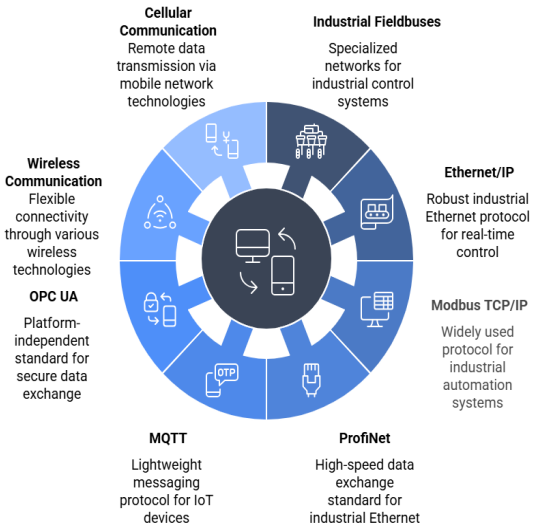

Fig. 3. M2M communication methods

• **Data analysis techniques:** It's critical to continuously enhance the IIoT or manufacturing network's performance. Most data analysis approaches and big data technologies include machine learning algorithms, data mining techniques, and statistical procedures that can be used to do this. These technologies provide the Industrial Internet of Things with features including enhanced support, lower resource consumption, automated help, quality of service, and failure detection. Data analysis techniques are usually developed for data kept in the cloud since the cloud offers a multitude of tools that automate the cycle of data gathering and analysis.

• **User interface:** A system control interface is often found in the application layer, and the IIoT may allow user-friendly applications at both the information and protocol levels. Interfaces for various devices and applications should be compatible. The introduction of IIoT user interfaces improves industrial networks by allowing the system to be controlled remotely. These programs give personnel visibility into real-time field operations and assist them in managing equipment, interacting with other systems, and processing data. Notification, notifications, and visualization assist them in making informed and calculated choices [11] [17].

• **Security mechanisms:** Privacy and security are two of the most important factors when constructing any pipeline manufacturing system from start to finish. These aspects, which include data authorization, encryption, authentication, firewalls, and many others, are typically implemented using specialized ways. Other technologies, including security and privacy aspects, such as machine learning and blockchain technology, are used in some production systems.

V. IIOT RELATE TO INDUSTRY 4.0

The digital revolution digitizes the physical world and connects everything. Humanity can now communicate constantly and anywhere, at any time, thanks to the explosion of smart devices and technologies. The industrial Internet of Things, or Industry 4.0, is a subset of the IoT market made possible by the IoT movement. The fourth Industrial Revolution is known as Industry 4.0, or I 4. 0, and it places a strong emphasis on connection, automation, autonomy, machine learning, and real-time data [16]. The German government's attempt to develop Industry 4.0 in 2010 has resulted in the country becoming the most competitive industrial nation, if not the world leader, in manufacturing equipment. It is possible to merge Industry 4.0, smart sensors, and the Internet of Things. Industry 4.0 integrates the ever-evolving technological landscape with conventional production and industrial techniques. To provide a productive and exciting future with efficient performance, this includes the widespread use of machine-to-machine interactions and the IoT, which benefits both manufacturers and consumers by increasing automation, improving communication, enhancing monitoring, and enabling self-diagnosis along with new levels of analysis. Every facet of the industrial sector relies on security. We utilized an intelligent system to identify and address the main challenges presented by Industry 4.0. A sensor is an electronic device that detects a physical quantity and transforms it into an electrical value. It can sense pressure, temperature, humidity, and other characteristics. Sensor data can be gathered, processed, and displayed on a computer screen for human consumption. Nowadays, sensors are frequently used in industry, security, and site monitoring [17]. Industry 4.0 is rooted in comprehensive ICT, which drives supply chain and production development, resulting in automation and digitalization [18]. Industry 4.0 will radically change how goods and services are produced, operated, and maintained through networked machines, people, and components. Industrial production systems are expected to operate 25% more efficiently and 30% faster as a result of Industry 4.0 [19]. The interests and requirements of these businesses have propelled the development of IoT into a new technological era known as IIoT. Industrial Automation & IIoT

Nowadays, everything must be digitized. Previously, we could only monitor conditions through the use of cameras. To eliminate manual overhead, we have installed the IoT in the industry to monitor and notify the responsible person to take relevant measures, but this will only partially meet our requirements. This process can be delayed at times, causing damage to both property and people [20]. The design and implementation of industrial automation networks will change in the future due to the IIoT. The Industrial Automation Network's productivity will increase because of IIoT. While classifying cybersecurity techniques, it's critical to take into account the significance of newly available data at the end device due to the large number of currently classified coupled end devices. By identifying early warning indications of danger and preventing them from getting worse, the IIoT can prevent downtime for industrial systems. Industrial system operators can monitor equipment accurately and in almost real-time by installing IoT sensors. Sensors offer a comprehensive report and/or details regarding the security, functionality, and state of the device. Anticipating system malfunctions can help one avoid falling [21].

VI. CYBERSECURITY AND DATA ANALYTICS IN IIOT

These mechanisms may include data authorization, encryption, authentication, firewalls, etc. Certain production systems make use of additional technologies, such as blockchain. Using a range of strategies to protect computers, software, networks, and data from intrusions or unwanted access is known as cybersecurity. It can also be defined as safeguarding an organization's cyberspace from threats to its internal and external security. The International Telecommunications Union (ITU) classifies it as: "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and users' assets.". Therefore, a system that employs IIoT should satisfy at least one security mechanism for its data and networks [22]. Therefore, a system that employs IIoT should also check the security of the aforementioned method or technology. In today's economy, data analysis is extremely essential since it boosts productivity and operational effectiveness. Three categories apply to big data: analysis, security, and storage. Within IIoT, data analytics are categorized based on their intended use, including real-time, offline, memory-level, business intelligence, and large analytics. The information is utilized for other purposes, like processing audio, video, picture, and sensor data [10]. Data analytics can be categorized into four parts:

- Inspecting-During the data inspection process, a corrupted or erroneous record is recognized in the database and sent for further processing.
- Cleansing -In the data cleansing process, faulty data can be updated, erased, or replaced. It is carried out via data-wrangling tools using scripts. The resulting data then goes through the transformation procedure.
- Transforming -Data transformation involves converting data from one format to another. It then moved to modeling.
- Modelling data -The data modeling method includes applying specific formal techniques to build an information system's data model [10].

.

VII. VARIOUS CASE STUDIES

Integrating the IoT with PLCs offers numerous benefits, significantly improving industrial processes and operational efficiency. One of the most significant benefits is real-time data collection and analysis. IoT devices can collect large amounts of data from various sensors and machines, then feed this data into PLCs for rapid processing. This capability enables more precise control of production processes, improving output and reducing downtime [23]. Adaptability also ensures businesses maintain their flexibility in a competitive market. Integrating the IoT with PLCs also enhances energy efficiency. Smart sensors can track energy consumption in real time and adjust processes to save energy without compromising efficiency. This reduces operating expenses while meeting increasingly stringent requirements for sustainable practices by both authorities and customers. Finally, enhanced remote monitoring features enable managers to monitor multiple production sites from a single central location or even while on the move using a mobile phone. This remote access facilitates faster decision-making and problem-solving, streamlining overall operations [24].

The combination of the IoT and PLCs has become a revolutionary force in the dynamic manufacturing industry. A good example is the story of a medium-sized auto parts company that used smart manufacturing to improve operational efficiency and reduce downtime. The company turned to IoT-enabled PLCs as a solution to its problems of frequent production delays and inconsistent quality control [4]. By integrating IoT sensors across its production line, the company was able to obtain real-time data on machine performance, environmental conditions, and product quality. These sensors provided the advanced PLC with vital data that it could process immediately. The results were impressive. Instead of reactive repairs, the PLC used machine learning algorithms to anticipate potential equipment failures before they occurred [5].

With a 30% reduction in unscheduled downtime, our predictive maintenance solution achieved significant cost savings. Additionally, this integration enabled improved quality control procedures. Any deviations from quality requirements could be detected immediately through real-time data analytics. A PLC ensured consistent product quality by automatically adjusting machine parameters or halting production lines when anomalies were detected. This deployment also encouraged increased traceability and transparency throughout the supply chain [6]. PLCs and IoT generate accurate logs used to accurately record each component's journey from raw material to finished product. IoT and PLCs have also revolutionized energy management solutions across many industries in an era where energy efficiency is paramount. A noteworthy case study focuses on a large-scale manufacturing facility aiming to reduce operational expenses and optimize its energy usage. The facility used IoT sensors installed throughout its buildings to track real-time energy consumption data [7]. A centralized PLC system was connected to these sensors, coordinating data collection and control procedures. IoT devices installed on machinery, lighting systems, HVAC units, and other energy-intensive equipment provided inputs to the PLC, which served as the central nervous system. The integrated system could detect inefficiencies and patterns in energy usage by employing machine learning algorithms and advanced analytics. For example, the system was able to identify equipment consuming large amounts of energy during off-peak hours or HVAC systems operating unnecessarily in vacant spaces. [8] Based on this information, the PLC could automatically adjust operations, allowing it to reduce or shut down equipment as needed without human intervention. The results were astonishing. In the first year of operation, the manufacturing facility reduced its overall energy consumption by 20%. Additionally, thanks to lower electricity costs and reduced wear and tear on machines resulting from streamlined operating schedules, significant cost savings have been achieved [9]. By reducing

unnecessary energy use, this seamless integration of the IoT with PLCs has improved operational efficiency and contributed significantly to sustainable practices.

A leading automotive component manufacturer integrated IoT technology with its existing PLCs to create a predictive maintenance framework. This case study examines how the integration of these technologies impacts their operational and maintenance efficiency. The facility ran on a reactive maintenance schedule before integration, servicing equipment only after it broke down [1].

This frequently resulted in unplanned malfunctions and expensive fixes. The plant obtained real-time insights into operating variables like temperature, vibration, and pressure by integrating IoT sensors into vital machinery components, including motors, conveyors, and hydraulic systems. These Internet of Things sensors regularly supplied data to PLCs, which were equipped with algorithms that could analyze trends and spot anomalies before equipment broke down. The PLCs then used an industrial network protocol, like Ethernet/IP or Modbus TCP/IP, to relay this data back to a central monitoring system [2].

Their strategy changed from being reactive to being proactive with the advent of predictive maintenance. If the system noticed anomalies that suggested possible problems, for example, elevated vibration levels indicating bearing wear, it issued notifications for preventive maintenance or replacement of parts before catastrophic breakdowns transpired. Consequently, the manufacturer witnessed a noteworthy decrease of more than 30% in unscheduled downtime, an extension of machinery lifespan by prompt interventions, and substantial cost savings on repairs and lost production time [3].

VIII. IoT Communication Protocols for PLC Systems

Within the domain of IoT-integrated PLC systems, communication protocols are essential for enabling smooth data interchange and interoperability. Strong communication frameworks that can handle real-time data processing, remote monitoring, and control applications are required as PLCs and IoT technologies converge [25].

MQTT (Message Queuing Telemetry Transport) is a well-known protocol that is intended for lightweight communication in restricted settings. Because of it publish-subscribe architecture, which facilitates effective communication between PLCs and IoT devices, it is especially well-suited for scenarios with constrained bandwidth or sporadic connectivity. Constrained Application Protocol, or CoAP, provides a RESTful method for IoT connections, allowing PLC systems to communicate with web services with minimal overhead.

Furthermore, OPC UA, or Open Platform Communications Unified Architecture, has become a vital industrial automation protocol. It offers a platform-neutral, secure architecture that supports intricate data structures and makes it easier for various systems to communicate with one another. This is particularly crucial in settings where the equipment from different manufacturers needs to function together harmoniously.

Integrating these protocols into PLC systems enhances their overall capabilities, enabling improved decision-making, predictive maintenance, and real-time analytics. Optimizing PLC performance and achieving operational efficiency will critically depend on understanding and applying suitable communication protocols as industries continue to embrace digital transformation through IoT technology [26].

IX. Temperature Case Study: PI Controller Implementation in Siemens PLC

In many industrial and experimental settings, temperature control is essential and must be precisely regulated to maintain the required conditions. Therefore, the adopted control algorithm must satisfy the precise required conditions and operations. For this reason, PI (Proportional – Integral) control algorithm is frequently utilized because of its ease of use and efficiency in preserving constant temperature conditions, in addition to its industry-wide applications. Using the PI control algorithm, the water temperature in the tank is controlled. PI controller programming is a standard practice for Siemens PLC controllers in sophisticated and expert systems. The PI controller controls its plant by measuring the "error" signal e(t), which is the difference between the process value (PV) (output) and the set point (SP) in each loop with a transfer function in eq.1, as shown in Fig. 4.

$$T(s) = \frac{Gc(s)\cdot Gp(s)}{1+Gc(s)\cdot Gp(s)\cdot H(s)} \quad (1)$$

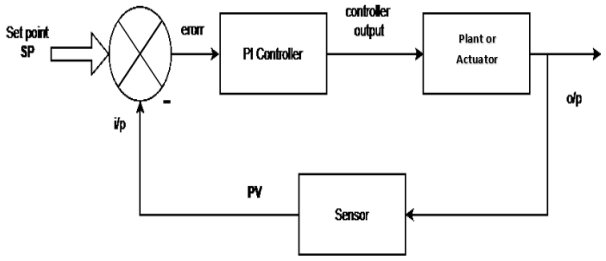

Fig. 4. The closed-loop control system

The P-term considers the error and attempts to account for PV's (process value) distance from SP (set point). As PV gets closer to SP, the error gets smaller but still cannot be caught; this suggests that the control system always has a steady state error (SSE) that is an offset from SP. The following mathematical equation represents the P-term's (controller's) output:

$$p_{term} = k_p \, . \, e\,(t) \quad (2)$$

k_p: is the gain factor, *e(t)* is the error signal.

The higher value of p_{term} may cause PV to become equal to SP, but this may cause instability in the system and overshoots or oscillations. Therefore, the I_{term} is are required in addition to the p_{term} to obtain the PI controller. The I-term takes into account the error history, accumulating the error from the start to a particular point. The following formula can be used to express the I term:

$$I_{term} = \int_0^T k_i \, . e\,(t)dt \qquad (3)$$

k_i : is the integral gain, and T is the total time of the controller's operation. The overall controller output will be:

$$u=k_p \, . e\,(t) + \int_0^T k_i \, . e\,(t)dt \qquad (4)$$

The PI controller is designed to improve transient and steady-state responses. Practically speaking, the PI controller's performance may exhibit a response with small overshoots as shown in Fig. 5. This overshoot could be minimized with parameter tuning. To implement PI control in a TIA portal using the S7-314 PLC, the process begins by structuring the control logic using function blocks (FB) or Organization blocks (OB). The CONT-S, as shown in Fig. 6, function blocks are used to link input variables, such as the PV and SP, ensuring accurate control execution. The control parameters Kp and Ki are adjusted based on the system response, with appropriate scaling applied to improve accuracy. The system is simulated and tested using a PLC simulator to monitor performance characteristics, such as overshoot and stability, allowing for dynamic adjustments to improve efficiency. After validation, the software is deployed to the S7-314 PLC and monitored in real-time through trend graphs and data analysis tools within the TIA portal. Continuous improvements ensure optimal performance and stability of the control system in an industrial environment. To perform FB CONT_S controller tuning in a TIA portal, a systematic approach is required to optimize the PI parameters to ensure stable and efficient control performance. The tuning process begins by defining control objectives, ensuring that the PV adheres precisely to the SP with minimal steady-state error and optimal response time. Using manual tuning, the Kp is adjusted first to optimize system response, followed by the Ki to eliminate residual errors over time.

When creating and fine-tuning the PI controller of all the PID controller types, the PI controller is algorithm is straightforward, practically implementable, and easy to comprehend. Eq. (5) illustrates the relationship between the error and the PI controller's output, as well as the P and I parameters:

$$u(t)=k_c \, . e\,(t)+\frac{k_c}{T_i}\int_0^t e(t)dt \qquad (5)$$

Where: u(t) “Time domain output of the PI controller”, e(t) (e = SP - PV) and the error indicator, Ti is the integral time (tunable), and kc is the controller gain (tunable).

A. Hardware Task

Fig. 6 shows the complete parts of the implemented water heating system, which consists of:

1) Water tank with capacity (60 liters) accompanied by its analog thermometer with temperature range (0-100 °C).
2) PLC s7-300; 16 digital inputs; 8 analog inputs; DO 16*REL AC 120/230 V digital outputs.
3) Since the heater's high current can harm the plc, the AC heater is linked to a connector that is controlled by the plc (0 VDC fully closed and 230 VDC fully open.
4) Analog temperature sensor PT100 with temperature range (0-100 °C). When the heating process starts; The analog sensor measures the hot water temperature and sends it to the analog input of the PLC (dotted red line), which will process it and send the result to the heater driven by a connector via the digital expansion output module (dotted red line) to determine if the PV=SP to on/off heater
5) Two floats for high /low-level water that are connected to a digital input that works as a switch to control the water pump approach to compute the values of kc and Ti. The trend view of Fig. 7 illustrates this process, which involves setting the controller to manual mode, doing the test, and then performing calculations [4]. the following tuned parameter selections in our PI controller design: Ti = 300ms and Kp = 0.7.

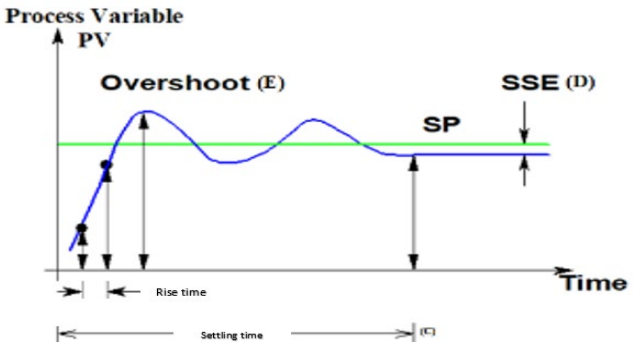

Fig. 5. Typical response of the PI controller

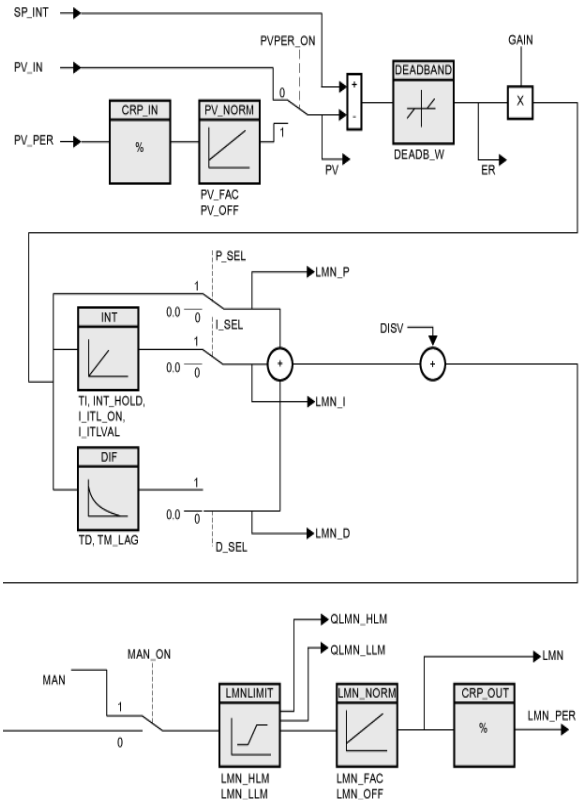

Fig. 6. The **CONT_S** block function design

Fig. 6. Hardware setup

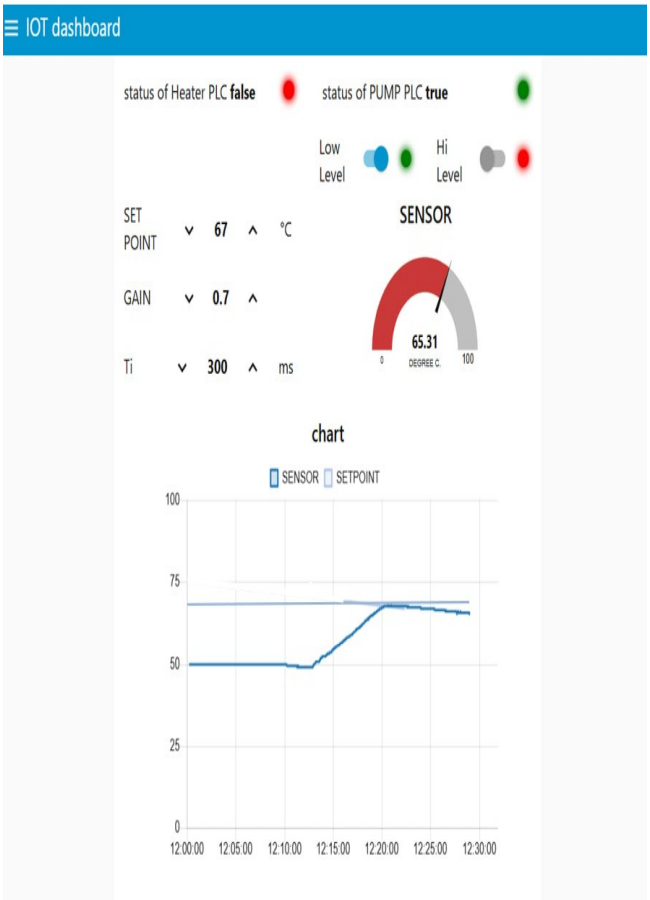

Fig. 7. HMI for the output PI controller

B. Scaling Signals

Analog input scaling: In this case, as shown in Fig. 8 the processing of the analog signal and the Fig. 9, the relation between the input temperature and the output mA of the sensor, because of the linear nature of the relationship, a change in temperature of 1°C causes a change in current of 0.16 (mA/°C).

The connection between the standard values and the analog input values. that the gain is (0.16) and the offset is (0). The following outcomes are obtained when calculating multiple input temperature values, as shown in Table I.

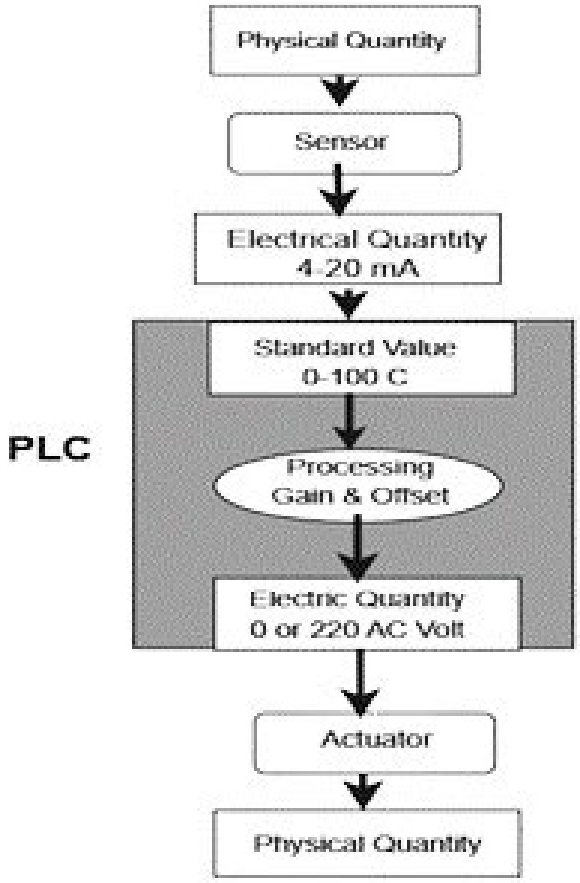

Fig. 8. Processing analog quantities by PLC

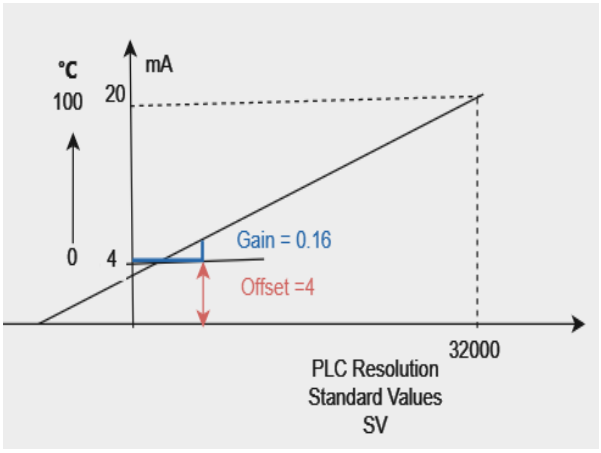

Fig. 9. Relationship between input analog values and standard values

Digital output scaling: As seen in Fig. 10, a digital module is utilized as the output, and the motor changed the PLC's digital output values from (0-1) to (0-120/230 ACV). Using the pi function, the output is two values, UP/DOWN, where these two values were used to control the operation of the breaker responsible for operating the heater.

TABLE I.
THE INPUT PARAMETERS

Temperature (°C)	Current (mA)	PV
0	4	0
30	8.8	8400
40	10.4	11100
50	12	14000
70	15.2	19400
80	16.8	22500
90	18.4	25000
100	20	32000

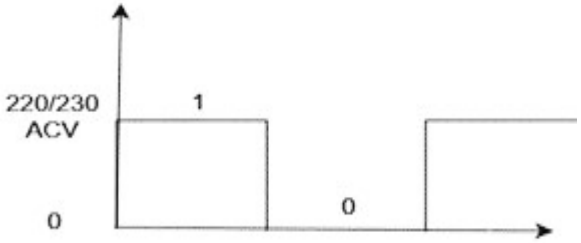

Fig. 10. PLC digital output

Program description: Figs. 11 and 12 display the control system's whole FBD program. It is made up of an analog input that receives the hot water temperature in milliamperes from the PT100 sensor. The hot water temperature is then sent to the PI controller, which decides what to do and sends the decision along with two signals that are sent to the actuator to control the on and off.

Results: The designed HMI shown in Fig. 7 provides the operator with information about the actual SV and PV, the output value, and the operation history. It is a method by which SV values can be changed over the Internet, and the changes can be monitored remotely using different methods and protocols used in the IIoT. This section explains how each PI controller parameter behaves. The black line indicates the SP (set point) value of the system's water temperature, which is adjusted by the operator using the controller. it explains how the system responded when the PI controller is used, as shown in Fig. 13. Using the specific PI function block in Tia portal as shown in Fig. 11 to call the controller and the output produced two signals using it in the main program to control the actuator (heater) as described in Fig. 12 in network 2. In network 1, the ladder diagram of controlling the pump is given.

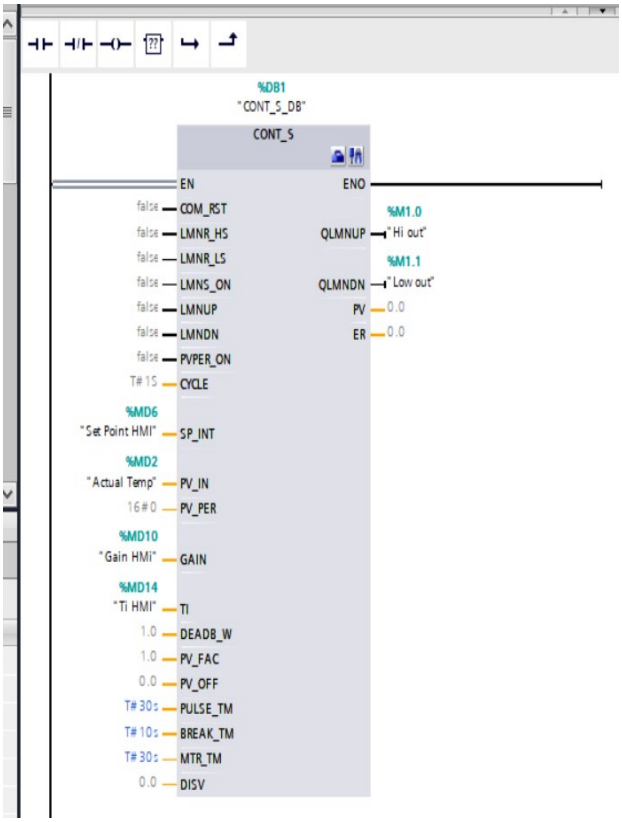

Fig. 11. CONT_S PI function block setting

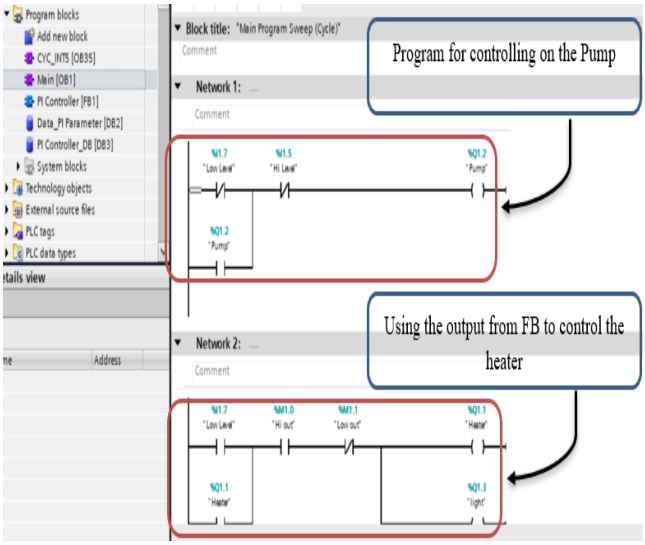

Fig. 12. Signals produced by the PI controller

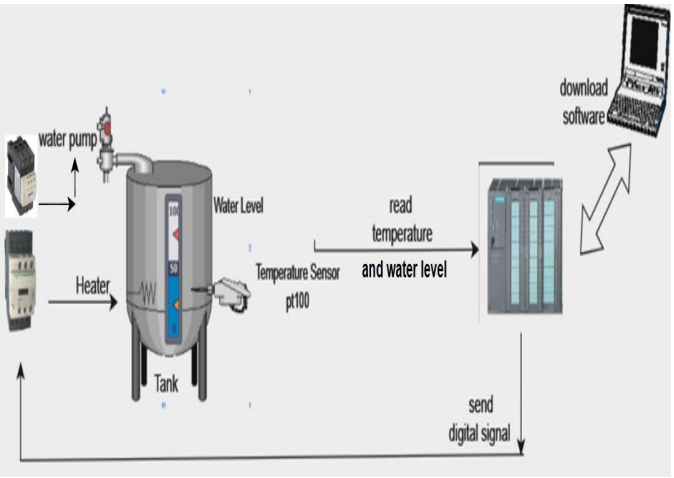

Fig. 13. The overall control system setup

X. CONCLUSION

Today, most people consider Industry 4.0 to represent a radical shift in society. There is tremendous potential for a wide range of commercial and industrial applications with the IoT and the IIoT. Many lessons have been learned from the integration of IoT with PLCs, highlighting the potential for increased productivity, better data analytics, and improved operational control across a variety of industries. IoT devices are increasingly becoming attractive targets for cyber threats as they become more prevalent in industrial environments. Regular upgrades and comprehensive security practices can help mitigate these risks. Another notable realization is the need for interoperability standards. Different PLCs and IoT devices often come from different vendors and use multiple communication protocols. Standardized protocols make it easier to exchange data and work together, reducing integration complexity and improving system reliability. Scalability has also become an important factor. Successful case studies show that scalable solutions are essential to support future expansions without the need for major overhauls. In the future, the combination of IoT-PLC systems and AI is likely to redefine industry standards. AI-powered predictive maintenance can anticipate equipment failures before they occur, reducing downtime and simplifying maintenance plans. Furthermore, edge computing will be essential for processing data locally on PLCs or adjacent servers, which will help reduce latency issues associated with cloud-based analytics. In conclusion, this study looks at automating a basic system with PLC methods through an easy-to-use program that makes use of the special qualities of the tuned PI controller to regulate the hot water temperature. By using the PI controller techniques included in the PLC system, this solution lessens the amount of work that must be done by humans to regulate the water temperature in this system. The only obstacle to commercializing this technology, which the authors want to perform, is the high cost of the PLC system.

In Future Work, developments can focus on enhancing the PI control system by integrating adaptive and intelligent algorithms such as fuzzy logic or model predictive control (MPC) to improve performance in highly nonlinear or time-varying environments. Additionally, implementing machine learning techniques could enable dynamic tuning of PI parameters based on real-time process feedback, enhancing system robustness and reducing manual intervention.

CONFLICT OF INTEREST

One of the authors, Prof. Dr. Ali Ahmed Abed, is the Editor-in-Chief of the *International Journal of Mechatronics, Robotics, and Artificial Intelligence (IJMRAI)*. To ensure transparency and avoid any potential conflict of interest, he was not involved in the editorial processing or peer review of this manuscript. The review process was handled independently by other qualified editors. The authors declare no other conflicts of interest related to this work.

REFERENCES

[1] M. A. Ali, A. H. Miry and T. M. Salman, "IoT Based Water Tank Level Control System Using PLC," *2020 International Conference on Computer Science and Software Engineering (CSASE)*, Duhok, Iraq, pp. 7-12, 2020, doi: 10.1109/CSASE48920.2020.9142067

[2] S. Munirathinam, "Industry 4.0: Industrial Internet of Things (IIoT)," *Advances in Computers*, vol. 117, no. 1, Academic Press Inc., pp. 129–164, https://doi.org/10.1016/bs.adcom.2019.10.010

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet Things J*, vol. 1, no. 1, pp. 22–32, 2014, https://doi.org/10.1109/JIOT.2014.2306328

[4] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Computer Society*, 2014, https://doi.org/10.1109/TII.2014.2300753.

[5] J. D. Lin, A. M. K. Cheng, and G. Gercek, "Partitioning Real-Time Tasks with Replications on Multiprocessor Embedded Systems," *IEEE Embed Syst Lett*, vol. 8, no. 4, pp. 89–92, 2016, https://doi.org/10.1109/LES.2016.2620473

[6] H. Son, N. Kang, B. Gwak and D. Lee, "An adaptive IoT trust estimation scheme combining interaction history and stereotypical reputation," *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, pp. 349-352, 2017, https://doi.org/10.1109/CCNC.2017.7983132

[7] D. Navani, S. Jain, and M. S. Nehra, "The internet of things (IoT): A study of architectural elements," *in 13th International Conference on Signal-Image Technology and Internet-Based Systems*, SITIS 2017, Institute of Electrical and Electronics Engineers Inc., pp. 473–478, 2017, https://doi.org/10.1109/SITIS.2017.83

[8] I. V. Nițulescu and A. Korodi, "Supervisory Control and Data Acquisition Approach in Node-RED: Application and Discussions," *Internet of Things*, vol. 1, no. 1, 2020, doi: 10.3390/iot1010005

[9] T. A. Chen, S. C. Chen, W. Tang, and B. T. Chen, "Internet of Things: Development of Intelligent Programmable IoT Controller for Emerging Industry

Applications," *Sensors*, vol. 22, no. 14, 2022, https://doi.org/10.3390/s22145138

[10] M. Mamoona, S. Habib, A. J., M. Rizwan, G. Srivastava, T. R. Gadekallu, and J. C. Lin, "Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review," *Sensors* 22, no. 6, 2022, https://doi.org/10.3390/s22062087

[11] I. Brass, L. Tanczer, M. Carr, M. Elsden, and J. Blackstock, "Standardising a Moving Target: The Development and Evolution of IoT Security Standards," *in Living in the Internet of Things: Cybersecurity of the IoT* - 2018, Institution of Engineering and Technology, pp. 24, 2024, https://doi.org/10.1049/cp.2018.0024

[12] O. Meyer, G. Rauhoeft, D. Schel, and D. Stock, "Industrial Internet of Things: covering standardization gaps for the next generation of reconfigurable production systems," *in 2018 IEEE 16th International Conference on Industrial Informatics (INDIN), IEEE*, pp.1039–1044, 2018, https://doi.org/10.1109/INDIN.2018.8472048

[13] M. Aqeel, F. Ali, M. W. Iqbal, T. A. Rana, M. Arif, and M. R. Auwul, "A Review of Security and Privacy Concerns in the Internet of Things (IoT)," *Hindawi Limited*, 2022, doi: 10.1155/2022/5724168

[14] M. Alabadi, A. Habbal, and X. Wei, "Industrial Internet of Things: Requirements, Architecture, Challenges, and Future Research Directions,"*Institute of Electrical and Electronics Engineers Inc*.,2022, https://doi.org/10.1109/ACCESS.2022.3185049

[15] A. A. Abed, "Android-based remotely accessed PLC Control Systems" *Al-Qadisiyah Journal for Engineering Sciences*, vol. 9, no. 4, 2016.

[16] A.A. Abed, AbdulAdhem A. Ali, and Nauman Aslam, "Building an HMI and demo application of WSN-based industrial control systems," *in 1st International Conference on Energy, Power and Control (EPC-IQ), Basrah, Iraq: IEEE*, pp. 302–206, 2010.

[17] F. Zhou, H. Qu, H. Liu, H. Liu, and B. Li, "Fingerprinting IIoT Devices Through Machine Learning Techniques," *J Signal Process Syst*, vol. 93, no. 7, pp. 779–794, 2021, https://doi.org/10.1007/s11265-021-01656-0

[18] S. Munirathinam, "Industry 4.0: Industrial Internet of Things (IIOT)," *in Advances in Computers,* vol. 117, no. 1, Academic Press Inc., pp. 129–164, 2020, https://doi.org/10.1016/bs.adcom.2019.10.010

[19] G. R. Kanagachidambaresan, R. Anand, E. Balasubramanian, and V. Mahima Editors, "Internet of Things for Industry 4.0," *in EAI/Springer Innovations in Communication and Computing. Cham: Springer International Publishing*, 2020, https://doi.org/10.1007/978-3-030-32530-5

[20] E. Manavalan and K. Jayakrishna, "A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements," *Comput Ind Eng*, vol. 127, pp. 925–953, 2019, https://doi.org/10.1016/j.cie.2018.11.030

[21] A. Deshpande, G. H. Raisoni, P. Pitale, and S. Sanap, "Industrial Automation using Internet of Things (IoT)," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 5, no. 2, 2016.

[22] A. M. Qazi, S. H. Mahmood, A. Haleem, S. Bahl, M. Javaid, and K. Gopal, "The impact of smart materials, digital twins (DTs) and Internet of things (IoT) in an industry 4.0 integrated automation industry," *Mater Today Proc*, vol. 62, pp. 18–25, 2022, doi: 10.1016/J.MATPR.2022.01.387

[23] N. Z. Jhanjhi, M. Humayun, and S. N. Almuayqil, "Cyber security and privacy issues in industrial internet of things," *Computer Systems Science and Engineering*, vol. 37, no. 3, pp. 361–380, 2021, https://doi.org/10.32604/csse.2021.015206

[24] M. Syafrudin, G. Alfian, N. L. Fitriyani, and J. Rhee, "Performance analysis of IoT-based sensor, big data processing, and machine learning model for real-time monitoring system in automotive manufacturing," *Sensors* (Switzerland), vol. 18, no. 9, 2018, https://doi.org/10.3390/s18092946

[25] E. R. Alphonsus and M. O. Abdullah, "A review on the applications of programmable logic controllers (PLCs)," Jul. 01, 2016, *Elsevier Ltd*. https://doi.org/10.1016/j.rser.2016.01.025

[26] C. Li, Y. Chen, and Y. Shang, "A review of industrial big data for decision making in intelligent manufacturing," 2022, *Elsevier B.V*. https://doi.org/10.1016/j.jestch.2021.06.001