iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49714

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

Developing an IoT Network to Connect and Control Industrial Device over a Wireless Network

P. Loganathan[1], P. B. Swathi[2], S. Rajathi[3], I. Mercy[4], A. Revath[5]
Electronics and Communication Engineering, Excel Enginnering College, Namakkal , India .

Abstract: ***Industrial IoT Networking is the process of connecting industrial devices and systems to a wireless network for the purpose of remote monitoring, control, and automation. This technology allows for more efficient management of industrial processes and systems, and can greatly reduce costs associated with managing and maintaining industrial operations. By using sensors, controllers, and other intelligent devices, industrial IoT networks can provide real-time data,***
enabling businesses to make better decisions and improve their operations. This paper outlines the development process of an industrial IoT network, including the selection of communication protocols, device selection and deployment, connectivity requirements, and security considerations. Finally, the paper discusses the potential applications of industrial IoT networks and the challenges associated with their implementation. This concept proposes an Internet of Things (IoT) network to connect and control industrial devices over a wireless network. The proposed IoT network will use a combination of hardware and software components, including sensors, actuators, gateways, and a cloud-based platform to monitor and control the devices. The proposed network will enable industrial devices to be monitored and controlled remotely, eliminating the need for manual control and allowing for greater flexibility and scalability. Additionally, the proposed network will provide real-time data and analytics to optimize the performance of the connected industrial devices. The proposed network will be secure and reliable, ensuring that all data is protected and accessible only by authorized personnel.
Keywords: 1. power supply , 2. temperature sensor , 3. gas sensor , 4. current sensor , 5. voltage sensor , 6. PIC controller , 7. LCD , 8. IoT , 9. RELAY , 10. LOAD , 11. Industrial , 12. Connectivity , 13. Wireless , 14. Network , 15. Automation , 16. Control , 17.Monitoring , 18. Cybersecurity.

I. INTRODUCTION

Industrial IoT networking is an emerging technology that enables industrial devices to be connected and controlled wirelessly over a network. by leveraging the power of IoT, industrial operators can leverage the advantages of automation, remote monitoring and analytics to increase productivity and reduce costs. The industrial IoT networking technology allows for a secure and reliable connection between devices, ensuring data integrity and secure transmission. The Internet of Things (IoT) is an emerging field with the potential to revolutionize the way factories and other industrial plants are managed. By connecting industrial devices to a wireless network, IoT provides the opportunity to monitor, control, and analyze the performance of machines, systems and processes in real-time. This technology promises to streamline operations, improve safety, enhance efficiency and productivity of industrial plants, and reduce costs. Developing an IoT network to connect and control industrial devices over a wireless network is therefore a highly attractive option for many businesses.

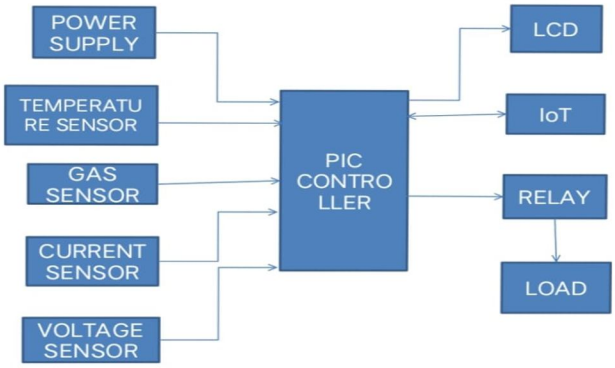
The development of an IoT network to connect and control industrial devices over a wireless network involves several steps. Firstly, the network must be designed and deployed. This involves selecting the right hardware and software components such as routers, switches, gateway devices, and sensors. The network must also be secured using encryption and authentication protocols to prevent malicious access. Secondly, the network must be configured to allow for the communication between devices. This requires the selection of the right communication protocols, such as Bluetooth and Wi-Fi, and the deployment of the necessary infrastructure. Thirdly, the devices must be connected and the application must be developed to enable the control and monitoring of the devices. This typically involves the integration of the application with the devices, and the development of the user interface.

Once the network is set up and the application is developed, the system can be tested and deployed. This involves testing the network and the application to ensure proper connectivity and communication between the devices and the application. Additionally, the system must be monitored and maintained to ensure that it remains secure and functioning properly.

Developing an IoT network to connect and control industrial devices over a wireless network is an exciting and potentially rewarding endeavor. By leveraging the power of IoT, businesses can reduce costs, improve safety and efficiency, and open up new ways of working.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com



II. METHODOLOGY

1) Phase 1: Establishing Requirements

The first step in developing an IoT network for industrial devices is to establish the requirements for the network. This should include the number of devices that are to be connected, the type of data that will be transmitted, the necessary bandwidth, and any potential security concerns. Additionally, this step should consider the physical layout of the network, such as the distance between the devices and the ability to access them from remote locations.

2) Phase 2: Evaluating Existing Infrastructure

The next step is to evaluate the existing infrastructure. This includes assessing the current network infrastructure, the existing wireless network, and the types of devices that will be connected. This evaluation is necessary to ensure that the current infrastructure is suitable for the IoT network.

3) Phase 3: Designing the Network

Once the requirements and existing infrastructure have been established, the next step is to design the network. This includes choosing the type of network, the hardware and software, and the protocols that will be used. Additionally, this step should include the selection of any necessary security measures.

4) Phase 4: Deployment

Once the network has been designed and the necessary hardware and software have been obtained, the next step is to deploy the network. This includes configuring the network, connecting the devices, and testing the network to ensure that it meets the requirements.

5) Phase 5: Maintenance

Finally, once the network has been deployed, the last step is to ensure that the network is maintained. This includes keeping the software and hardware up-to-date, monitoring the network for any security threats, and troubleshooting any issues that may arise.

III. DATA COLLECTION SOURCE

1) *Surveys and Interviews:* Conduct surveys and interviews with industrial users and professionals to get a better understanding of their needs and expectations for an industrial IoT network.
2) *User Testing:* Test the user experience of existing industrial IoT networks to gain insight into user preferences and needs.
3) *Log Analysis:* Analyze log data from existing industrial IoT networks to identify potential areas for improvement.
4) *Market Research:* Conduct market research to understand the competitive landscape and identify potential opportunities for product differentiation.
5) *Performance Analysis:* Analyze the performance of existing industrial IoT networks to identify potential areas for improvement.
6) *Security Analysis:* Analyze the security of existing industrial IoT networks to identify potential areas for improvement.
7) *Cost Analysis:* Analyze the cost of existing industrial IoT networks to identify potential areas for improvement.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

IV. DATA ANALYSIS

A. IoT Network Infrastructure

The first step in developing an IoT network to connect and control industrial devices is to determine the IoT network infrastructure that is needed. This includes hardware such as routers, switches, and access points. It may also include software such as a cloud-based platform, analytics software, and other applications.

B. Connection Protocols

The next step is to determine the connection protocols that will be used for the network. This includes determining the type of network (e.g., wired or wireless) and the specific technology (e.g., Bluetooth, Wi-Fi, or Zigbee) that will be used.

C. Security

It is also important to consider security when developing an IoT network. This includes selecting the appropriate authentication protocols and encryption methods to ensure that the data is secure and private.

D. Device Management

The next step is to develop a device management system that will allow for the monitoring and control of the devices connected to the network. This includes features such as remote access, scheduling, and alerting.

E. Analytics

Finally, it is important to develop an analytics platform to analyze the data collected from the network. This includes the ability to track device usage, performance, and other metrics.

V. ALGORITHUM DEVELOPMENT

1) *Identify the Type of Devices and the Scope of the Project:* Determine the size and scope of the project, such as the number of devices, their locations, and the desired range of coverage.
2) *Design the Network Infrastructure:* Design the network architecture to accommodate the devices, such as the topology, protocols, and bandwidth requirements.
3) *Select the Appropriate Wireless Technology:* Choose the type of wireless technology, such as Wi-Fi, Bluetooth, and Zigbee, that best suits the particular network and devices.
4) *Implement the Network:* Install the necessary hardware and software components, such as routers, switches, sensors, and gateways, to create the wireless network.
5) *Test the Network:* Test the network to make sure it is working correctly and that it is able to handle the desired level of traffic and data throughput.
6) *Monitor and Manage the Network:* Monitor and manage the network to ensure that it is functioning properly and that it is secure from malicious attacks.

VI. TESTING

1) *Network Testing:* To test the network connection between the industrial devices and the IoT network, the network should be tested for latency, throughput, and reliability.
2) *Security Testing:* To ensure the security of the system, the network should be tested for vulnerabilities and the security protocols implemented should be tested for effectiveness.
3) *Compatibility Testing:* To test compatibility, the system should be tested against different versions of hardware and software to ensure they are compatible with the system.
4) *Performance Testing:* To test the performance of the system, the system should be tested for response time, scalability, and throughput.
5) *Usability Testing:* Usability testing should be conducted to make sure the network is user-friendly and easy to use.

VII. VALIDATION

1) *Efficient Functionality:* The system should be able to efficiently control the industrial devices over the wireless network.
2) *Error Handling:* The system should be able to handle errors and exceptions in a timely and efficient manner.

©IJRASET: All Rights are Reserved

3) *Compliance:* The system should be compliant with the necessary standards and regulations.
4) *Interoperability:* The system should be able to interoperate with existing systems and other networks.
5) *Security:* The system should be secure and prevent unauthorized access to the network and devices.

VIII. CONCLUSION

The development of an IoT network to connect and control industrial devices over a wireless network has the potential to revolutionize the way industries operate. With access to real-time data, predictive analytics, and automated processes, industrial operations can become more efficient, reliable, and cost-effective. The implementation of such a system can provide industry with the increased flexibility and scalability necessary to stay competitive in a rapidly changing environment. While there are still many security, data privacy, and infrastructure concerns to address before such a system can be deployed, the potential benefits far outweigh the risks.

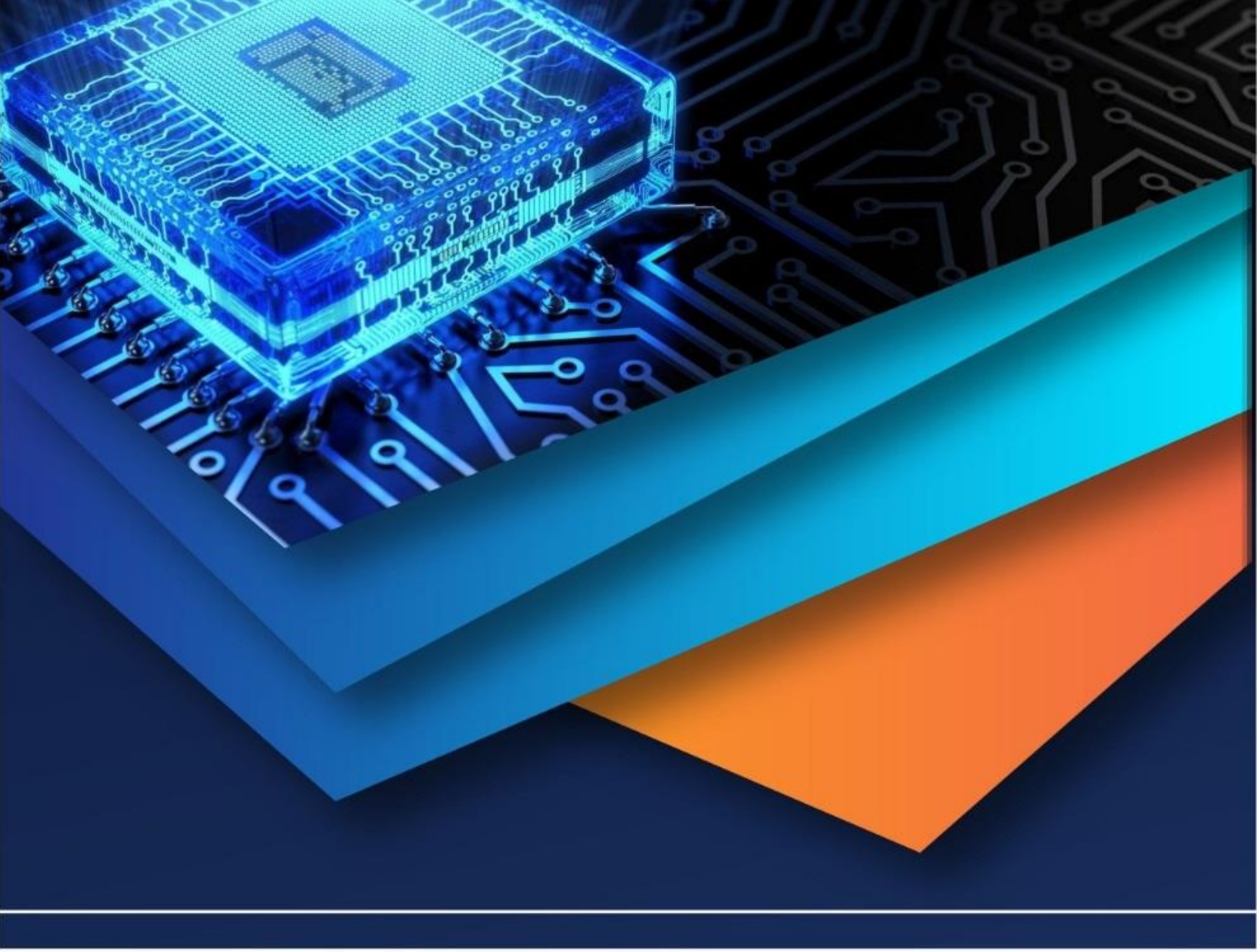
IX. ACKNOWLEDGMENT

We would like to thank the following people for their contributions to the development of this concept:
1) Professor Cesar Cerrudo, who provided his expertise in the field of industrial automation and control.
2) Professor Robert Metcalfe, who provided his insight into the development of an IoT network.
3) Professor David L. Tennenhouse, who provided his knowledge on wireless network protocols and architectures.
4) Professor Sanjay Jha, who provided his expertise in the field of embedded systems and computer architecture.
5) Mr. Robert L. Shostak, who provided his expertise in the field of industrial engineering and operations.
6) Mr. Steve Wozniak, who provided his expertise in the field of computer engineering and design.
We would also like to acknowledge the efforts of the engineers and technicians who have worked hard to develop the technology and make it available to the public.

REFERENCES

[1] Elizabeth Kadiala, Shravya Meda, Revathi Basani, S.Muthulakshmi, “Global Industrial Process Monitoring Through IoT Using Raspberry Pi”,2021.
[2] Gang Wang, Mark Nixon, Mike Boudreaux, “Toward Cloud-Assisted Indusrial IoT Platform for Large-Scale Continuous Condition Monitoring”,2019.
[3] M. M. Pandini , J. M. Neto , A. D. Spacek , O, H, Ando Junior , “Design of a Didatic Workbench of Industrial Automation Systems for Engineering Education” ,vol.15, pp. 1384-1391, 2017.
[4] Valeriy V. Vyatkin, James H. Christensen, Jose L. Martinez Lastra, “OOONEIDA: An Open , Object-Oriented Knowledge Economy for Intelligent Industrial Automation” , vol .1, pp. 4-17, 2005.
[5] Rahul N. Gore, Himahri Kour, Mihit Gandhi, Deepaknath Tandur, “Bluetooh based Sensor Monitoring in Industrial IoT Plants” 2020.
[6] Komal S. Shinde, “Industrial Process Monitoring Using IoT” , pp. 38-42, 2018.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)