



GSM BASED INDUSTRY PROTECTION SYSTEM

¹Dr. B. Rambabu, ²S. Megha syam, ³B. Giri, ⁴K. Lakshmi Narayana

¹HOD&Professor, ²Student,
³Student, ⁴Student¹Electronics and
Instrumentation Engineering,

¹Lakkireddy Balireddy College of Engineering, Mylavaram, India

Abstract: Today, smart grid, smart homes, smart water networks, intelligent transportation, are infrastructure systems that connect our world more than we ever thought possible. The common vision of such systems is usually associated with one single concept, the Internet of Things (IoT), where using sensors, the entire physical infrastructure is closely coupled with information and communication technologies; where intelligent monitoring and management can be achieved via the usage of networked embedded devices. These devices will connect to internet to share different types of data. We have proposed an Industrial Monitoring System using WIFI module and sensing based applications for internet of things. By detecting the values of sensors, it can easily find out the Temperature, humidity, over load and gas present in the industrial area.

Index Terms – INTRODUCTION,LITERATURE REVIEW,COMPONENTS,RESULT,REFERENCES.

I. INTRODUCTION

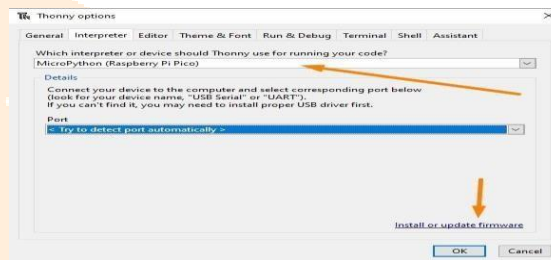
In recent years, there has been a significant increase in the usage of GSM technology in industrial applications. Today, several businesses employ GSM-based industry protection systems to increase their security and safety. This system enables remote equipment monitoring, notifies users of security breaches, and promptly responds to emergencies. An overview of the GSM-based industry protection system's components and operation will be given in this document. The sensors, control unit, and GSM module are the three main parts of the GSM-based industry protection system. To identify any unusual activity or failure, sensors are deployed in the industry's essential locations. Based on the predetermined parameters, the control unit analyses the data from the sensors and initiates the required action. In the event of any security breaches or crises, the GSM module is in charge of notifying the designated persons. The sensors that have been installed in the sector are made to pick up on environmental changes such changes in temperature, pressure, or movement. These sensors send data to the control unit continually, and the control unit is designed to examine the data and perform the required action.

II. LITERATURE REVIEW

Industrial security systems now offer a dependable and affordable communication method thanks to GSM technology. Researchers have created GSM-based systems that can combine many sensor types, such as motion detectors, smoke detectors, temperature sensors, and gas sensors, in order to identify any anomalies in the industrial environment. Several components have been included into GSM-based industry protection systems, according to the literature. For instance, sensors and communication modules have been combined in a single device using the low-cost microprocessor known as the Raspberry Pi Pico. A buzzer has also been incorporated into the system to give audible alerts to the staff in the event of any security breaches or crises. The various communication protocols utilized in GSM-based industry protection systems have also been examined in the literature. SMS, MMS, and GPRS are the most widely used protocols. To ensure the safe transmission of data between the control unit and the sensors, researchers have created algorithms.

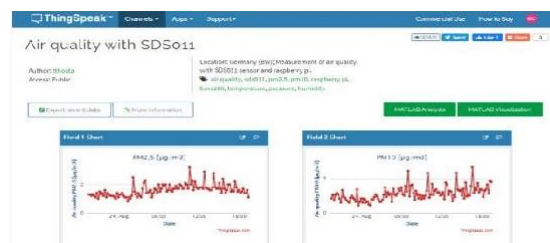
III. COMPONENTS

XILINX ISE: For the purpose of designing unique logic designs for use in the control unit of a GSM-based industry protection system, the Xilinx ISE software offers a potent FPGA design platform. Timer, counter,

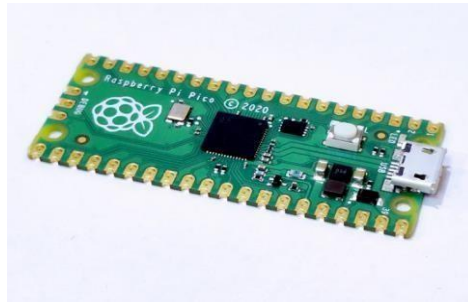


and state machine characteristics that can be utilised to regulate the system's functioning can be added to the FPGA architecture through customization.

THING SPEAK IOT PLATFORM: Data can be gathered from numerous sensors and devices in the industry protection system using Thing Speak. HTTP, MQTT, and TCP/IP are just a few of the protocols that can be used to send the data to Thing Speak. JSON, CSV, and XML are just a few of the different data types that Thing Speak supports.



RASPBERRY PI PICO: A microcontroller board appropriate for usage in GSM-based industrial protection systems is the Raspberry Pi Pico. It offers a wide range of capabilities and features that can improve the operation and performance of such systems. The Raspberry Pi Pico's ability to interface with GSM modules is one of its important characteristics. Serial communication, which is frequently used to interact with GSM modules, is hardware supported on the board.

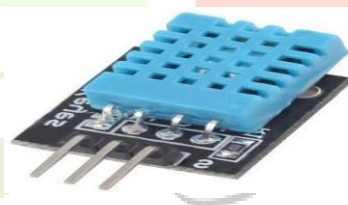


FIRE SENSOR: This tiny flame sensor infrared receiver module can detect flames or light sources with wavelengths between 760 and 1100 nm. It is also helpful for detecting lighter flames at a distance of 80 cm. The test distance increases as the flame size increases. It is extremely sensitive to the flame spectrum and has a detect angle of 60.



TEMPERATURE SENSOR:

A popular sensor for measuring humidity and temperature that is inexpensive is the DHT11. It is made up of a single chip that houses both a thermistor-based temperature sensor and a capacitive humidity sensor. A microcontroller or a Raspberry Pi can simply be interfaced with the DHT11 sensor's straightforward digital feed. The DHT11 sensor can be used to track the ambient temperature and humidity levels in the GSM-based industry protection system.



IV. RESULT:

The successful identification and avoidance of any dangerous or unacceptable circumstances in the industrial environment would be accomplished by a GSM-based industry protection system. An example of this might be early warning and alarms for gas leaks, smoke or fire, unusual temperature changes, and other environmental conditions that could endanger workers safety or the integrity of equipment. The system's usage of GSM technology, which enables quick and dependable communication, can assist prevent accidents and reduce damage in the event of an emergency.

V. REFERENCES:

- [1] "Integration of hybrid wireless networks in cloud services-oriented business information systems," *Enter. Inf. Syst.*, vol. 6, no.2, pp. 165–187, 2012; S. Li, L. Xu, Wang, and J. Wang.
- [2] Wang, and J. Wang.
- [3] Applications integration in a hybrid cloud computing environment: Modeling and platform, *Enter. Inf. Syst.*, vol. 7, no. 3, pp.237-271, 2013. Q. Li, Z. Wang, W. Li, J. Li, C. Wang, and R. Du.
- [4] "Data cleaning for RFID and WSN integration," *IEEE Trans. Ind. Informat.*, vol. 10,no. 1, pp. 408-418, Feb. 2014; L. Wang, L. D. Xu, Z. Bi, and Y. Xu.
- [5] "IoT based smart rehabilitation system," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2,pp. 1568–1577, 2014. Y. Fan, Y. Yin, L. Xu, Y. Zeng, and F. Wu.
- [6] Ali El Kouche Ad-hoc and Sensor Networking Symposium at the IEEE ICC 2012, "Towards a Wireless Sensor NetworkPlatform for the Internet of Things"
- [7] "Data-Gathering Wireless Sensor Networks: Organization and Capacity," E.J. Duarte-Melo and M. Liu, *Computer Networks*, vol. 43, pp. 519–537, 2003
- [8] "Capacity of Data Collecting in Arbitrary Wireless Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 1, January 2012. Siyuan Chen, Minsu Huang, Shaojie Tang, and Yu Wang.
- [9] *Inf. Technol. Manage.*, vol. 13, no. 4, pp. 205-216, 2012. Y. Li, M. Hou, H. Liu, and
- [10] Liu, "Towards a theoretical framework of strategic decision, supporting capacity, and information exchange under the context of Internet of Things."