IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⋇ Impact Factor 7.047 ⋇ Vol. 10, Issue 5, May 2022

DOI: 10.17148/IJIREEICE.2022.10585

IOT BASED DEVICE FAILURE DETECTIOUSING MULTI SENSOR DATA FUSION FOR INDUSTRIAL CONTROL SYSTEM

Ms. S. kiruthiga M.E.[1], Mohamed shafiqur Rahman j[2], Sanjai M[3], Shankar V[4], Suresh R[5]

[1]Assistant professor, Saranathan college of Engineering, Trichy, Tamil Nadu, India

[2-5]Saranathan college of Engineering, Trichy, Tamil Nadu, India

Abstract: Industrial Control Systems monitor, automate, and operate complex infrastructure and processes that integrate into critical industrial sectors that affect our daily lives. With the increasing deployment of data network technologies in industrial control systems (ICSs), cybersecurity becomes a challenging problem in ICSs. During these ICS operation dangerous attacks, like machines malfunctions, increasing ambient temperature and unwanted gas particles may be released into the air also the attacks hazards. This project based on continuous monitoring ICS parameter such as load voltage-current, load condition (no-load/over-load), temperature, humidity and gas leakage, fire detection are monitored by wireless Zigbee technology. A microcontroller based system is used for collecting and storing data and making decision accordingly the data cyber-attacks machines and environmental malfunction. Extreme environment conditions are detrimental for human health. The communication system is reliable based on Zigbee, IEEE 802.15.4 standard. This is used for transmission between the hardware circuit fitted in the local site and the remote monitoring site (computer) through wireless devices. This project focuses on the use of process analytics to detect attacks in the industrial control infrastructure systems and compares the effectiveness of threshold value signature-based detection methods. The proposed work presents a pattern recognition algorithm aptly named as ‘‘Capturing-the-Invisible (CTI)’’ to find the hidden process in industrial control device logs and detect Behavior-based attacks being performed in real-time. This system is highly beneficial for rescue and protection of ICS and Industrial workers and equipment’s.

1. INTRODUCTION:

Smart sensor interfaces have evolved through the Internet of Things (IoT) which acquires heterogeneous sensor signals and connects them to the Internet, providing intelligent services in various applications such as healthcare systems, automotive systems and industrial monitoring systems. More specifically, healthcare systems have pursued the utilization of physiological and biomedical sensor data to improve the efficiency of health management of healthy subjects and patients.

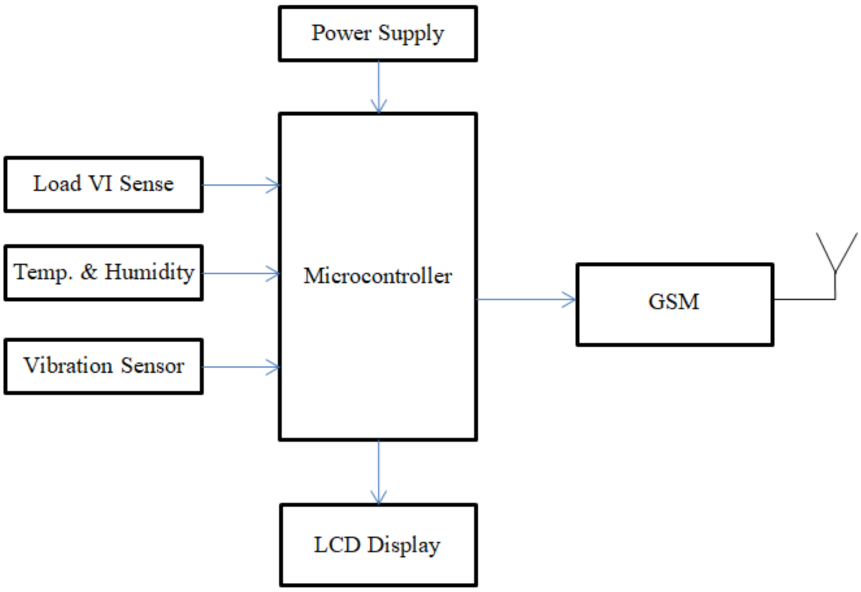
Automotive systems have introduced new vehicular services to connect various sensors and GPS-based location information to communication networks. The industrial manufacturing environment is also embedding new functions in the form of safety monitoring or smart factories. One recent trend of interest is the combination of heterogeneous systems and services from different fields such as by providing automated healthcare services in automotive environments.

Platform migration from bulky computers to smartphones is another important trend that has been accelerated by the proliferation of high-end mobile processors, but this is still limited in healthcare applications.

Therefore, the project proposes a smartphone-centric multi-sensor platform that supports heterogeneous sensor signals from different application fields, and particularly for environmental and healthcare signals. For this purpose, the proposed platform needs to be flexible for adding different kinds of signal processing or functions. The system-level flexibility was achieved by migrating most of the signal processing and computation burdens from the sensor module to a smart phone. Then, the smartphone can also provide various auxiliary functions including display, sound, and GPS to facilitate newly combined services.

2. RELATED WORKS

Traditionally, safety monitoring and automation systems were typically designed to meet the requirements of a single monitoring application. The industrial application has already gone beyond the interconnection of a few large back-end systems, and more and more underground physical devices make the state of objects and their surroundings seamlessly accessible to software systems. As a matter of fact, most works are based on monolithic system architectures, which are brittle and difficult to adapt.



3.1 Existing Block Diagram

The persons who are working in the industrial have to face various environmental parameters in their industrial. So to overcome that problem we are using Zigbee based intelligent helmet for coal miners.
Industrial incidents were unpredictable and it has many factors the event of an accident, not only causes huge economic losses, but a direct threat to the safety of miners
As an ICS is a cyber-physical system, the process of cybersecurity risk propagation in ICSs is different from that in general network systems.
Most ICS attacks aim to vandalize ICS assets, which include humans, environment, and equipment.

Traditionally, safety monitoring and automation systems were typically designed to meet the requirements of a single monitoring application.
The application has already gone beyond the interconnection of a few large back-end systems.

3.MULTI SENSOR DATA FUSION

Information Technologies (IT) & Operational Technology (OT) include critical software and hardware systems for the control and monitoring of physical sensor field devices. IT and OT provide essential, inherent integration and visibility for supply chain details about logistics, assets, processes, and completion times. This provides remote control and management units with information, thus keeping the ICS efficient and competitive. However, IT and OT are often targeted by cyber attackers, as most of the ICS do not have stringent security policies or the infrastructure to detect and monitor cyberattacks.
Human Machine Interface (HMI) provides a graphical user interface (GUI) application that assists the interaction of hardware, control system, human operators (staff).
HMI displays trends, historical and real-time status from data and logs gathered from the ICS environment. MI provides the dashboards to monitor, customize, set control points, and establish the operational parameters required for the day-to-day sensor and controller.
Micro Controller (MC) is the control component of the ICS ad that provides process management. MC provides supervisory, remote access, and control to devices such as actuators and sensors.
Remote Terminal Units (RTU) & Master Controller Units (MTU) are microprocessor-based field devices. RTU receives commands from the MTU and sends back the information from the field. Control Server &Loops host supervisory control systems, communicate with each low level, on-field control devices such as PLC and actuators to carry out tasks and complete processes. The control loop interprets sensor signals, motors, gears, control valves, breakers, and other electromechanical devices. Intelligent Electric Device (IED) are smart devices that acquire data, communicate with other

DOI: 10.17148/IJIREEICE.2022.10585

devices to control and perform local processing automatically. Remote Maintenance & Diagnostics identifies and prevents abnormal operations or failures and helps to prevent hardware and software related problems inside ICS.

RISK ANALYSIS IN INDUSTRIAL CONTROL SYSTEMS

With the increasing deployment of data network technologies in industrial control systems (ICSs), cybersecurity becomes a challenging problem in ICSs. Dynamic cybersecurity risk assessment plays a vital role in ICS cybersecurity protection. However, it is difficult to build a risk propagation model for ICSs due to the lack of sufficient historical data. In this paper, a fuzzy probability Bayesian network (FPBN) approach is presented for dynamic risk assessment. Firstly, an FPBN is established for analysis and prediction of the propagation of cybersecurity risks. To overcome the difficulty of limited historical data, the crisp probabilities used in standard Bayesian networks (BNs) are replaced in our approach by fuzzy probabilities. Then, an approximate dynamic inference algorithm is developed for dynamic assessment of ICS cybersecurity risk

In recent decades, Industrial Control Systems (ICS) have been affected by heterogeneous cyberattacks that have a huge impact on the physical world and the people's safety.

Nowadays, the techniques achieving the best performance in the detection of cyber anomalies are based on Machine Learning and, more recently, Deep Learning

Measuring parameters **HUMIDITY SENSOR**

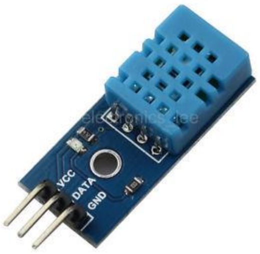


Fig 5.9 Humidity sensor

Humidity is the presence of water in air. The amount of water vapor in air can affect human comfort as well as many manufacturing processes in industries. The presence of water vapor also influences various physical, chemical, and biological processes. Humidity measurement in industries is critical because it may affect the business cost of the product and the health and safety of the personnel. Hence, **humidity sensing** is very important, especially in the control systems for industrial processes and human comfort.

Controlling or monitoring humidity is of paramount importance in many industrial & domestic applications. In semiconductor industry, humidity or moisture levels needs to be properly controlled & monitored during wafer processing. In medical applications, humidity control is required for respiratory equipments, sterilizers, incubators, pharmaceutical processing, and biological products. Humidity control is also necessary in chemical gas purification, dryers, ovens, film desiccation, paper and textile production, and food processing. In agriculture, measurement of humidity is important for plantation protection (dew prevention), soil moisture monitoring, etc. For domestic applications, humidity control is required for living environment in buildings, cooking control for microwave ovens, etc. In all such applications and many others, **humidity sensors** are employed to provide an indication of the moisture levels in the environment.

Relevant Moisture Terms

To mention moisture levels, variety of terminologies are used. The study of water vapour concentration in air as a function of temperature and pressure falls under the area of psychometrics. Psychometrics deals with the thermodynamic properties of moist gases while the term "humidity' simply refers to the presence of water vapour in air or other carrier gas.

Humidity measurement determines the amount of water vapor present in a gas that can be a mixture, such as air, or a pure gas, such as nitrogen or argon. Various terms used to indicate moisture levels are tabulated in the table below:

Most commonly used units for humidity measurement are Relative Humidity (RH), Dew/Frost point (D/F PT) and Parts Per Million (PPM). RH is a function of temperature, and thus it is a relative measurement. Dew/Frost point is a function of the pressure of the gas but is independent of temperature and is therefore defined as absolute humidity measurement. PPM is also an absolute measurement.

Dew points and frost points are often used when the dryness of the gas is important. Dew point is also used as an indicator of water vapor in high temperature processes, such as industrial drying.

Mixing ratios, volume percent, and specific humidity are usually used when water vapor is either an impurity or a defined component of a process gas mixture used in manufacturing.

DOI: 10.17148/IJIREEICE.2022.10585

Humidity Sensing – Classification & Principles

According to the measurement units, humidity sensors are divided into two types: Relative humidity(RH)sensors and absolute humidity(moisture) sensors. Most humidity sensors are relative humidity sensors and use **different sensing principles**.

Sensing Principle

Humidity measurement can be done using dry and wet bulb hygrometers, dew point hygrometers, and electronic hygrometers. There has been a surge in the demand of electronic hygrometers, often called humidity sensors.

Electronic type hygrometers or humidity sensors can be broadly divided into two categories: one employs capacitive sensing principle, while other use resistive effects

Sensors based on capacitive effect: Humidity sensors relying on this principle consists of a hygroscopic dielectric material sandwiched between a pair of electrodes forming a small capacitor.

Most capacitive sensors use a plastic or polymer as the dielectric material, with a typical dielectric constant ranging from 2 to 15. In absence of moisture, the dielectric constant of the hygroscopic dielectric material and the sensor geometry determine the value of capacitance.

At normal room temperature, the dielectric constant of water vapor has a value of about 80, a value much larger than the constant of the sensor dielectric material. Therefore, absorption of water vapor by the sensor results in an increase in sensor capacitance.

At equilibrium conditions, the amount of moisture present in a hygroscopic material depends on both the ambient temperature and the ambient water vapor pressure. This is true also for the hygroscopic dielectric material used on the sensor.

By definition, relative humidity is a function of both the ambient temperature and water vapor pressure. Therefore there is a relationship between relative humidity, the amount of moisture present in the sensor, and sensor capacitance. This relationship governs the operation of a capacitive humidity instrument.

TEMPERATURE SENSOR

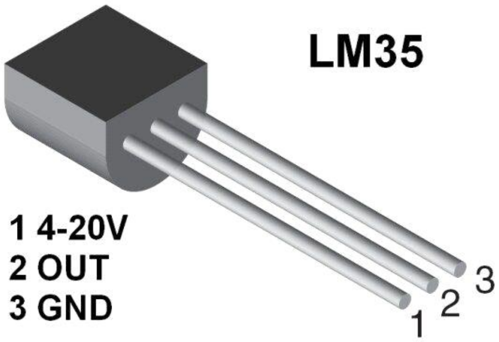


Fig 5.10 temperature sensor

- Calibrated directly in˚Celsius (Centigrade)
- Linear + 10.0 mV/℃ scale factor
- 0.5℃ accuracy guarantee able (at +25℃)
- Rated for full −55˚to +150℃ range
- Suitable for remote applications
- Low cost due to wafer-level trimming
- Operates from 4 to 30 volts
- Less than 60 µA current drain
- Low self-heating, 0.08℃ in still air
- Low impedance output

The LM35 series are precision integrated-circuit temperature sensors, whose output voltage is linearly proportional to the Celsius (Centigrade) temperature. The LM35 thus has an advantage over linear temperature sensors calibrated in˚Kelvin, as the user is not required to subtract a large constant voltage from its output to obtain convenient Centigrade scaling. The LM35 does not require any external calibration or trimming to provide typical accuracies at room temperature and over a full −55 to +150℃ temperature range. Low cost is assured by trimming and calibration at the wafer level. The LM35's low output impedance, linear output, and precise inherent calibration make interfacing to readout or control circuitry especially easy. It can be used with single power supplies, or with plus and minus supplies. As it draws only 60 µA from its supply, it has very low self-heating, less than 0.1℃ in still air. The LM35 is rated to operate over a −55˚to

DOI: 10.17148/IJIREEICE.2022.10585

+150℃ temperature range, while the LM35C is rated for a −40° to +110℃ range (−10° with improved accuracy). The LM35 series is available packaged in hermetic TO-46 transistor packages, while the LM35C, LM35CA, and LM35D are also available in the plastic TO-92 transistor package.

5.1.5 CO2 SENSOR

The gas sensor has high sensitity to Propane, Butane and LPG, also response to Natural gas. The sensor could be used to detect different combustible gas, especially it is used to detect all natural gases.

This smoking sensor is low in cost and low power consumption.

Fig 5.11 CO2 sensor

Sensitive material of MQ-6 gas sensor is SnO2, which with lower conductivity in clean air. When the target combustible gas exist, The sensor's conductivity is more higher along with the gas concentration rising. Please use simple electro circuit, Convert change of conductivity to correspond output signal of gas concentration.

MQ-6 gas sensor has high sensitivity to Propane, Butane and LPG, also response to Natural gas. The sensor could be used to detect different combustible gas, especially Methane; it is with low cost and suitable for different application.

Character Configuration

Good sensitivity to Combustible gas in wide range
High sensitivity to Propane, Butane and LPG
Long life and low cost
Simple drive circuit

Domestic gas leakage detector
Industrial Combustible gas detector
Portable gas detector. Home appliances Due to the incipient stage of cybersecurity research in ICS, the availability of datasets enabling the evaluation of anomaly detection techniques is insufficient. In this paper, we propose a methodology to generate reliable anomaly detection datasets in ICS that consists of four steps: attacks selection, attacks deployment, traffic capture and features computation. The proposed methodology has been used to generate the Electra Dataset, whose main goal is the evaluation of cybersecurity techniques in an electric traction substation used in the railway industry.

CONCLUSION:

Industrial Control Systems have migrated from being dedicated, air-gapped, centralized infrastructures and have adopted the distributed, corporate systems accessible via the Internet.

Although the efficiency, speed, precision quality is increased, this has exposed ICS to the unsecured Internet.

In this way, the proposed multi-sensor interface can achieve the compactness and the flexibility of the sensor module by utilizing two reconfigurable method for various sensor interfaces and also by migrating most of the burdens for signal calibration and analysis to a smartphone.

Thereby the sensor module itself can achieve a low-cost bill of materials (BOM) and can maximize the usage time of its internal battery by powering a minimal number of components and by optimally reconfiguring its internal operations.

The Industrial Internet of Things involves the use of IoT technologies in manufacturing processes and across supply chains.

Alongside data from devices and sensors, Industrial IoT strategies should incorporate machine learning and big data technology, harnessing that combination of existing sensor data, machine to machine (M2M) communication and automation technologies to provide more insight back to the business. For companies in the manufacturing and logistics sectors, the new era of instant demands can be better met through more use of Industrial Internet of Things (IoT).

DOI: 10.17148/IJIREEICE.2022.10585

REFERENCE

1.L. P. Gómez, L. F. Maimo, A. H. Celdran, F. J. G. Clemente, C. C. Sarmiento, C. J. Del Canto Masa, and R. M. Nistal, ‘‘On the generation of anomaly detection datasets in industrial control systems,’’ IEEE Access, vol. 7, pp. 177460–177473, 2019

2.X. Li, C. Zhou, Y.-C. Tian, and Y. Qin, ‘‘A dynamic decision-making approach for intrusion response in industrial control systems,’’ IEEE Trans. Ind. Informat., vol. 15, no. 5, pp. 2544–2554, May 2019

3.M. G. Angle, S. Madnick, J. L. Kirtley, and S. Khan, ‘‘Identifying and anticipating cyberattacks that could cause physical damage to industrial control systems,’’ IEEE Power Energy Technol. Syst. J., vol. 6, no. 4, pp. 172–182, Dec. 2019

4.Q. Zhang, C. Zhou, Y.-C. Tian, N. Xiong, Y. Qin, and B. Hu, ‘‘A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems,’’ IEEE Trans. Ind. Informat., vol. 14, no. 6, pp. 2497–2506, Jun. 2018

5.X. Li, C. Zhou, Y.-C. Tian, N. Xiong, and Y. Qin, ‘‘Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems,’’ IEEE Trans. Ind. Informat., vol. 14, no. 2, pp. 608–618, Feb. 2018

6.M. Banerjee, C. Borges, K. R. Choo, J. Lee, and C. Nicopoulos, “A hardware-assisted heartbeat mechanism for fault identification in large-scale iot systems,” IEEE Transactions on Dependable and Secure Computing, pp. 1–1, 2020.

7. S. Seshadri, D. Rodriguez, M. Subedi, K. R. Choo, S. Ahmed, Q. Chen, and J. Lee, “Iotcop: A blockchain-based monitoring framework for detection and isolation of malicious devices in internet-of-things systems,” IEEE Internet of Things Journal, 2020, in press.

8. J. Konecny, H. B. McMahan, F. X. Yu, P. Richt ´ arik, A. T. ´ Suresh, and D. Bacon, “Federated learning: Strategies for improving communication efficiency,” CoRR, vol. abs/1610.05492, 2016. [Online].

9.S. K. Lo, Q. Lu, C. Wang, H. Paik, and L. Zhu, “A systematic literature review on federated machine learning: From a software engineering perspective,” ArXiv, vol. abs/2007.11354, 2020.

10. H. Kim, J. Park, M. Bennis, and S. Kim, “Blockchained on-device federated learning,” IEEE Communications Letters, pp. 1–1, 2019.

11.J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, “Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive,” IEEE Transactions on Dependable and Secure Computing, pp. 1–1, 2019.