Security for Industrial Communication System using Encryption / Decryption Modules

S. Arulselvi, B. Hemalatha, S. Balaji

Abstract*: The industrial communication systems of present time are to a large extent based on commercial operating systems, open protocol implementation & communication application which are not secure. By connecting to the internet or other public networks these risks are exposed to potential attacker and cause damage to the industries. The data send by the network can be tampered causing network failure. This results in an increase in the downtime of the industry causing major loss. The industrial communication channel can be accessed by unauthorized person and uncorrect information can be transmitted, i.e. the originality of the information is violated. Cryptography is the technique, which is used to improve SCADA security. Cryptography is hiding of actual information. But SCADA protocols do not support any type of cryptography due to limited computational capabilities of SCADA device and low rate data transmission in SCADA network. To tackle this situation we are introducing an encrypting/decrypting module (ENIGMA) which can be connected at one end of the plant and one end of the control room. The encrypting module encrypts the data at the transmitting end and transmits it through the communication channel. The decrypting module decrypts the data received via the communication channel.

Keywords*— industrial communication, encryption, serial communication, cryptography, microcontroller.

I. INTRODUCTION

Due to interconnectivity of the industrial networks a threat is imposed on the network. The threats can be explored by an attacker and cause damage to the industry. The data send by the network can be tampered with causing the failure of the network. This will result in an increase in downtime of the industry resulting in major loss [1-3].

Only authorized personnel must be allowed to access the network so as to ensure the safe working of the industrial equipments. The data being transmitted must maintain its originality. In case of an attack these security objectives are violated. Thus a security check must be implemented on the industrial network to ensure safe working of the industry [4-6].

A. SCADA network

SCADA network is a typical industrial network which connects various automated processes with a central supervisory controller (basically a computer) for remote control and monitoring of process [7, 8]

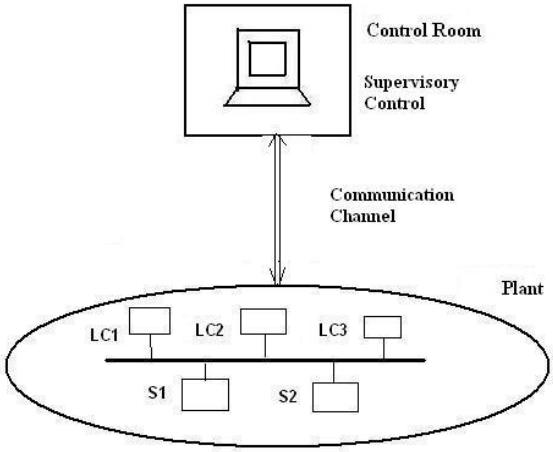


Fig. 1 SCADA Network

B. Security Issues in SCADA network

- Access Control
- The SCADA network must be secured from intruders.
- Firewall & Intrusion Detection system
- Cryptography and key management*
- Device and OS Securit

C. Cryptography and Key Management

SCADA protocol typically do not support any sort of cryptography due to limited computational capability of SCADA device, low rate data transmission on SCADA network, need of real time response.

These constrains complicate the implementation of complex cryptography in SCADA protocol [9-10].

D. ENIGMA - A cost effective solution

A technique can be implemented to ensure the integrity of the transmitted data. An additional cryptographic module (ENIGMA) can be connected at each end of the SCADA serial link. At the transmitting end the module encrypts the message and at the receiving end the encrypted message is decrypted by the module.

ENIGMA supports the SCADA protocol and plugs into the SCADA network without any hassle. ENIGMA is an embedded device; build up of 8051 microcontroller with minimum hardware requirements and flawless real time OS. The device is easy to use and needs very basic technical knowledge to operate.

Authorized personnel can feed in the encryption / decryption key from an 8X8 keyboard to transmit data in encrypted

Revised Manuscript Received on August 22, 2019.

S.Arulselvi, Department of Electronics and Communication Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India.

B. Hemalatha, Department of Electronics and Communication Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India.

S. Balaji, Department of Electronics and Communication Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India.

form. The key can be changed as per the needs [11-13].

II. DESIGN OF SYSTEM HARDWARE

A. SIMULATION – THERMAL POWER PLANT

To integrate the encryption routine we have simulated three basic processes of a thermal power plant, namely [14]

- Boiler Water Level Control
- Conveyor Control
- Alarm control.

Table 1 – Process Description

Process Name	Control Parameter	Sensor Used	Controller Used
Boiler Water Level Control	Water Level	Level Sensor	Level Controller
Conveyor Belt Control	Transportation	NIL	ON-OFF Controller
Alarm Control	Abnormality OR Industrial Accident	Fire Sensor	ON-OFF Controller

FIG. 2 SIMULATION OF THERMAL POWER PLANT

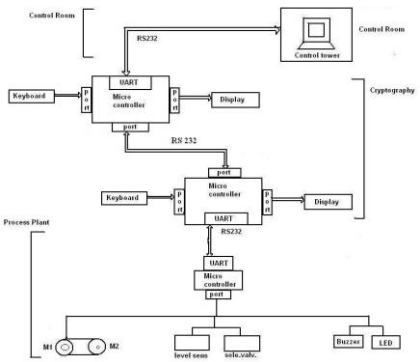
B. HARDWARE DESIGN

The single board is designed around three 8051 micro controller to accomplish the above mentioned system requirements

The major components which contribute to the hardware is as follows

- 8051Microcontroller
- RS232 – TTL Logic Converter
- Process Driver
- Power Supply Unit
- Fire Sensor
- Water Level sensor
- 555 Timer
- Local Controller
- ENIGMA – Encrypting/Decrypting Module

C. Local Controller



The local controller controls the three processes as per command it gets from the supervisory controller. The controller uses a process driver L293D for driving the three process which works on +12V.

The local controller gets the commands via RS232. The sensor inputs are given to the local controller which compares it with the set point and then takes desired action [14-18].

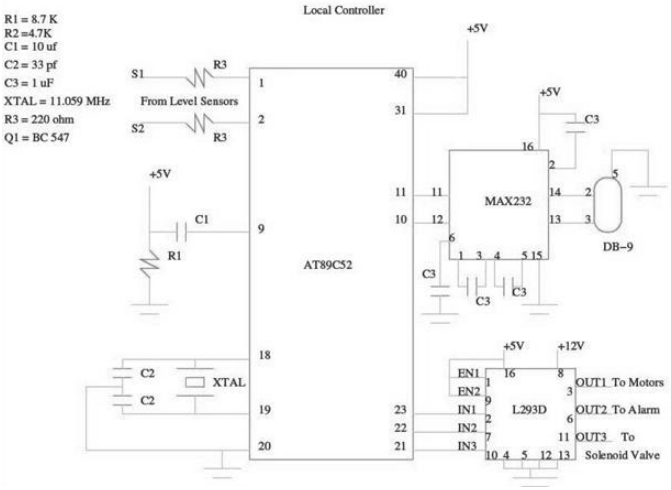


Fig 3. Local Controller

D. ENIGMA – Encrypting / Decrypting Module

The commands send from the supervisory controller is passed through ENIGMA. The first microcontroller gets the commands and after encrypting it passes on to the second microcontroller. The second microcontroller then transmits the message via RS232.

In the decrypting end the same technique is employed where the encrypted command is decrypted and then passed on to the local controller [19, 20].

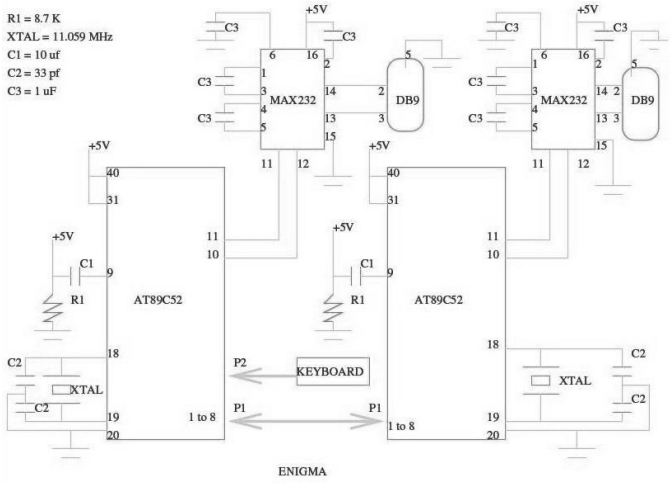


Fig. 4 ENIGMA – Encryption/Decryption Module

III. FLOW DIAGRAM

A. Encryption/Decryption Module (ENIGMA) Flow Diagram

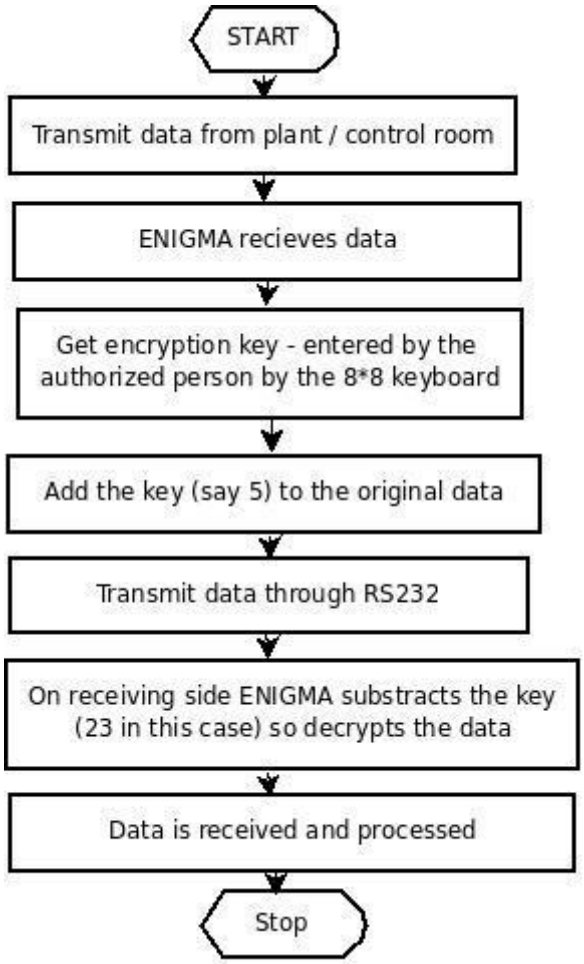


Fig. 5 Process Flow Diagram of ENIGMA

B. Supervisory Control Mechanism Flow Diagram

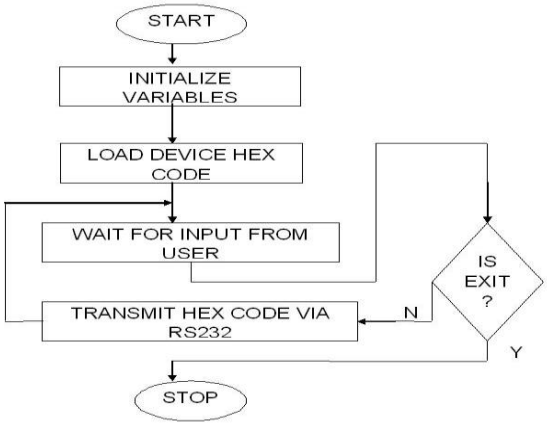


Fig. 6 Supervisory Control Mechanism Flow Diagram

C. Encryption Flow Diagram

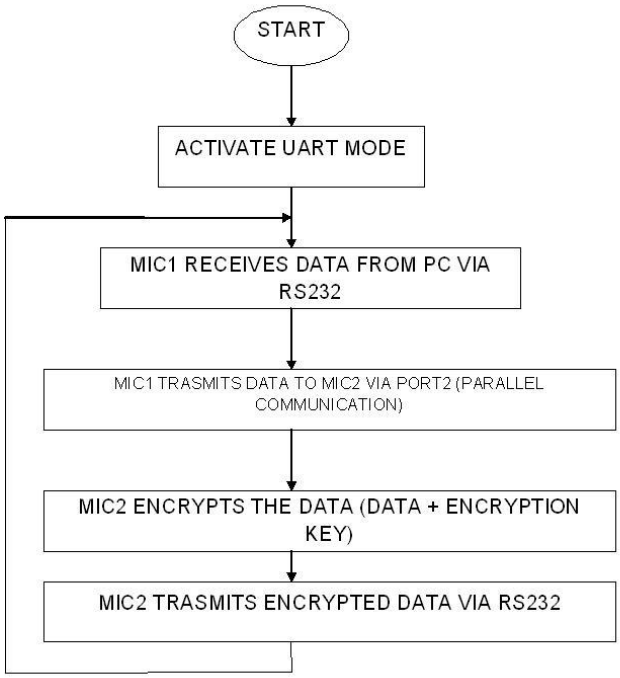


Fig. 7 Encryption Flow Diagram

D. Decryption Flow Diagram

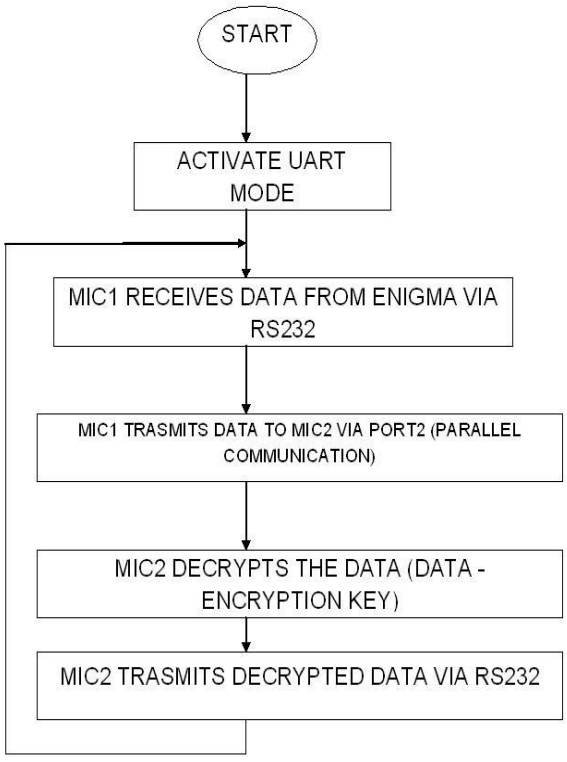


Fig. 8 Decryption Flow Diagram

E. Local Controller Flow Diagram

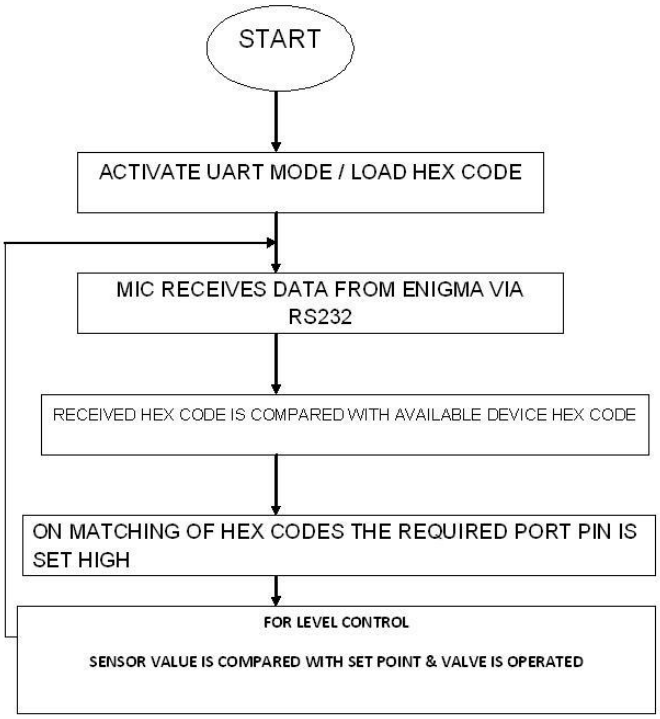


Fig. 9 Local Controller Flow Diagram

IV. CONCLUSION

ENIGMA provides a simple and cost effective mechanism to secure the network by just plugging in the device. The manufacturing cost of the device is low as compared to other security solutions. Since, ENIGMA is a plug and play device which connects to the network and not the process. Any kind of software installation or update on supervisory control machine is not required. Security can be enhanced by providing external encryption keypad.

Here, RS232 protocol has been implemented. Using the same hardware with few modifications Ethernet, USB or any other serial communication protocol can be secured.

AT89C52 is an 8 bit microcontroller. For higher speed and multiple encryptions 16 bit or 32 bit microcontroller can be used.

ACKNOWLEDGMENT

I express my profound gratitude to Dr. A. Vimla Juliet, M.E., Ph.D., HOD Instrumentation & Control Engineering, SRM University who was a constant source of encouragement and for readily approving this project when the concept was proposed. I am greatly indebted to my guide Mr.J. Sam Jeba Kumar, B.E., M.E., Lecturer, Instrumentation & Control Engineering., SRM University for his motivation, guidance throughout the courses of this project work.

REFERENCES

[1] Kongkham, D. & Sundararajan, M. 2019, "Distributed wideband sensing method for faded dynamic spectrum access", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 4309-4312.

[2] Balaji, S., John Paul Praveen, A. & Mohanraj, R. 2019, "Recognizable proof and analysis of palm print in biometric authentication system using bayes techniques", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1126-1129.

[3] Kavitha, G., Priya, N., Velvizhi, R. & Allin Geo, A.V. 2019, "Parallel computation in correspondence and signal processing", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1136-1139.

[4] Hema, R., Sundararajan, M. & Balaji, S. 2019, "Smartphone control robot with automatic firing gun", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 625-627.

[5] Kaliyamurthie, K.P., Sundar Raj, B., Velvizhi, R. & Shanmugapriya, K. 2019, "Dual band paper substrate CPW antenna for wireless applications", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 605-608.

[6] Geo, A.V.A., Arunachalam, A.R., Michael, G. & Elankavi, R. 2019, "Evaluating architecture using compact modalities", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 836-838.

[7] Theivasigamani, S., Jeyapriya, D. & Anita Davamani, K. 2019, "Anamoly analyzing and exploring for wireless sensor networks", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1116-1118.

[8] Jeyapriya, D., Theivasigamani, S., Velvizhi, R. & Nandhini, P. 2019, "Program detection in wireless feeler networks", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1194-1195.

[9] Gowri Sankaran, B., Karthik, B. & Vijayaragavan, S.P. 2019, "Image compression utilizing wavelet transform", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 4305-4308.

[10] Gowri Sankaran, B., Karthik, B. & Vijayaragavan, S.P. 2019, "Weight ward change region plummeting change for square based image huffman coding", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 4313-4316.

[11] Hema, R., Sundararajan, M. & Balaji, S. 2019, "Smartphone control robot with automatic firing gun", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 625-627.

[12] Rangaswamy, K. & Rajabhushanam, C. 2019, "Congestion control in wireless network using TCP friendly rate control (TFRC)", International Journal of Recent Technology and Engineering, vol. 8, no. 2 Special issue 3, pp. 1598-1602.

[13] Tamil Selvan, S. & Sundararajan, M. 2019, "Performance Parameters of 3 Value 8t Cntfet Based Sram Cell Design Using H-Spice", International Journal of Recent Technology and Engineering, vol. 8, no. 2 Special issue 5, pp. 22-27.

[14] Vinoth, V.V. & Kanniga, E. 2019, "Steganographical techniques in hiding text images – system", International Journal of Recent Technology and Engineering, vol. 8, no. 2, pp. 6535-6537.

[15] Saravana, S., Balaji, S., Arulselvi, S. & John Paul Praveen, A. 2019, "Reliable power quality monitoring and protection system", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 644-645.

[16] Sundaramoorthy, A. & John Wiselin, M.C. 2019, "Single patch antenna with multiple feed", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9, pp. 1743-1747.

[17] Velavan, R., Bharanidharan, S. & Sheeba, B. 2019, "EMF pollution - Causes, effects and protection", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1166-1168.

[18] Veer, R.A., Arulselvi, S. & Karthik, B. 2019, "Construction of ensemble square classification approaches in MIMO OFDM", International Journal of Engineering and Advanced Technology, vol. 8, no. 5, pp. 2039-2041.

[19] Agitha, W. & Kaliyamurthie, K.P. 2019, "Improved energy efficient in WBAN using MAC with cloud computing", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 8, pp. 2405-2408.

[20] Kastro, G.G. & Wiselin, M.C.J. 2019, "Design and analysis of stub loaded resonator", International Journal of Recent Technology and Engineering, vol. 8, no. 1 Special Issue4, pp. 272-283.

AUTHORS PROFILE

S.Arulselvi Associate Professor, Department of Electronics and Communication Engineering, Bharath Institute of Higher Education and Research, Chennai, India

B. Hemalatha, Assistant Professor, Department of Electronics and Communication Engineering, Bharath Institute of Higher Education and Research, Chennai, India

S. Balaji, Assistant Professor, Department of Electronics and Communication Engineering, Bharath Institute of Higher Education and Research, Chennai, India