

SECURITY FOR INDUSTRIAL COMMUNICATION SYSTEM USING ENCRYPTION / DECRYPTION MODULES

M.Jasmin¹, S.Beulah Hemalatha²

¹Assistant Professor, BIST, BIHER, Bharath University,

Assistant Professor, BIST, BIHER, Bharath University

¹jasmine.ece@bharathuniv.ac.in

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

1. 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[1-4].

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[6-11].

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[12-17].

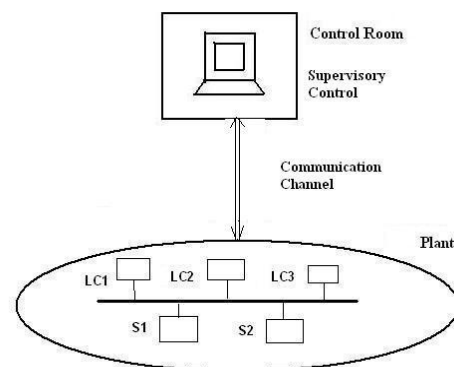


Figure 1. SCADA Network

A. 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 Security

B. 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[18-25].

These constraints complicate the implementation of complex cryptography in SCADA protocol.

C. 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 form. The key can be changed as per the needs[26-30].

2. 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

- 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

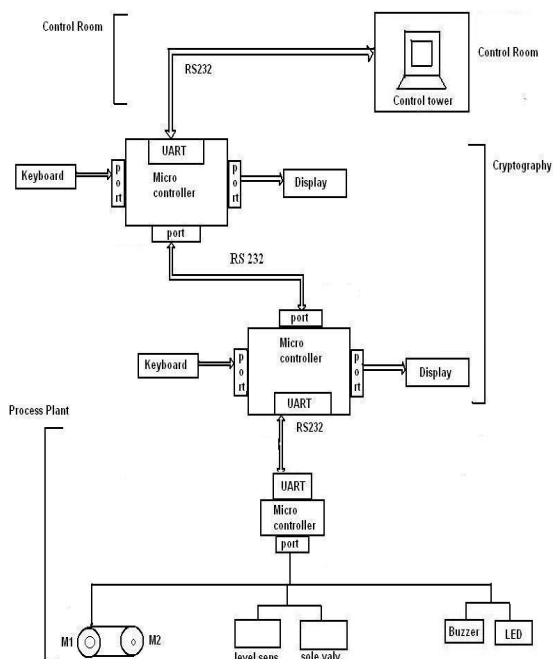


Figure 2. Simulation of Thermal Power Plant

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.

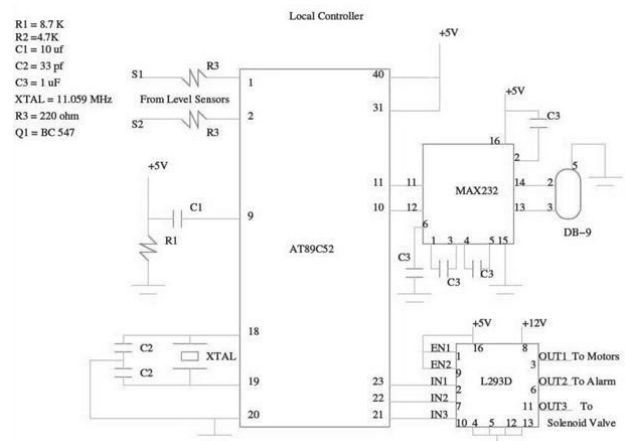


Figure 3. Local Controller

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.

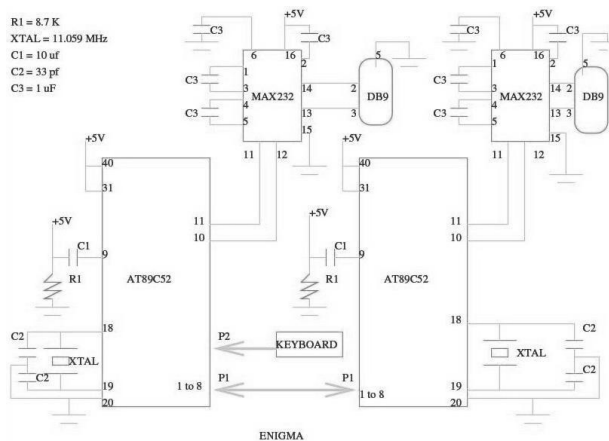


Figure 4. ENIGMA – Encryption/Decryption Module

3. Flow Diagram

A. Encryption/Decryption Module (ENIGMA) Flow Diagram

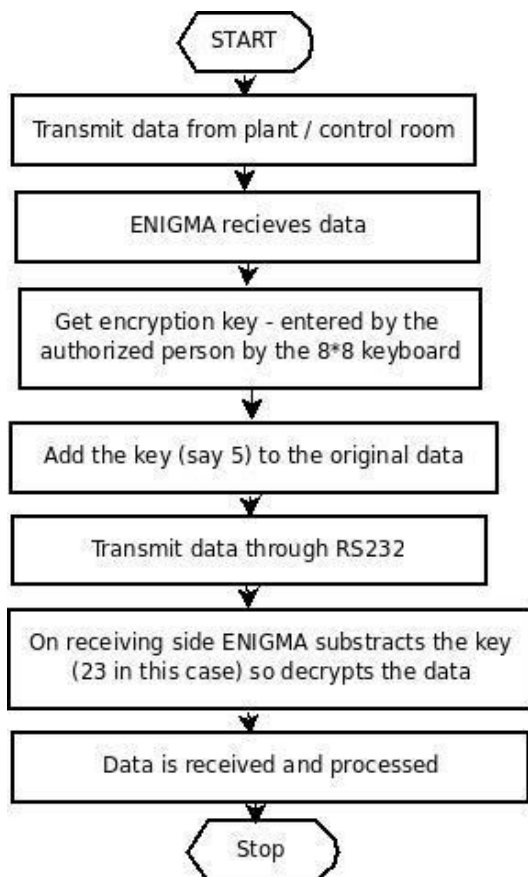


Figure 5. Process Flow Diagram of ENIGMA

B. Supervisory Control Mechanism Flow Diagram

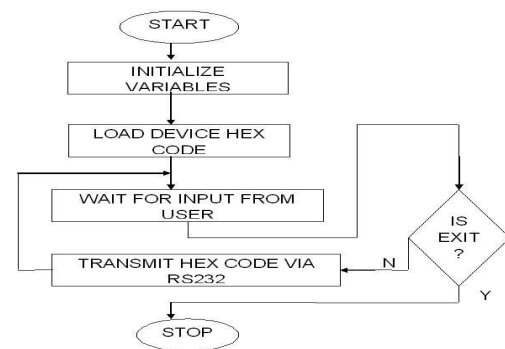


Figure 6. Supervisory Control Mechanism Flow Diagram

C. Encryption Flow Diagram

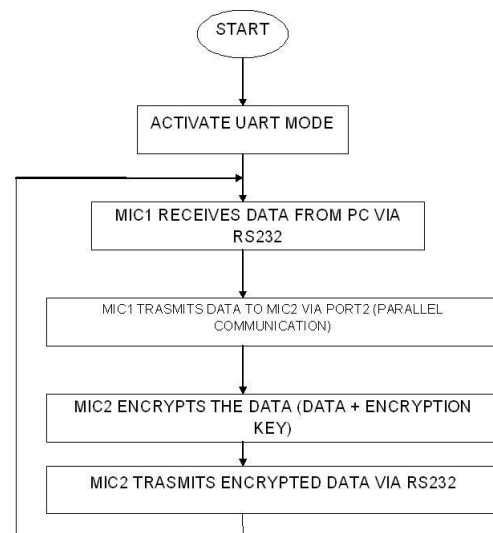


Figure 7. Encryption Flow Diagram

D. Decryption Flow Diagram

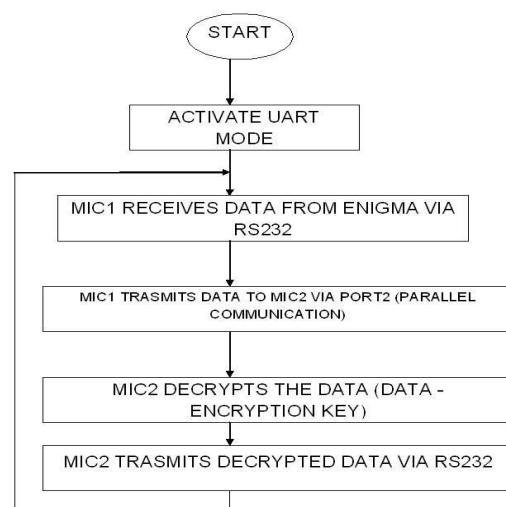


Figure 8. Decryption Flow Diagram
E. Local Controller Flow Diagram

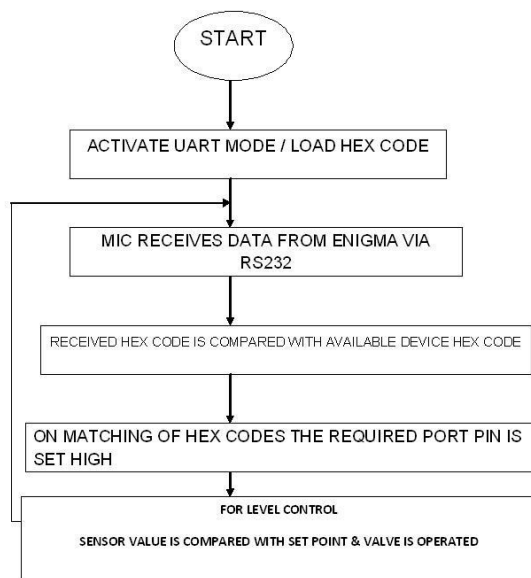


Figure 9. Local Controller Flow Diagram

4. 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.

References

- [1] Vijayaragavan S.P., Karthik B., Kiran T.V.U., Sundar Raj M., Robotic surveillance for patient care in hospitals, Middle - East Journal of Scientific Research, v-16, i-12, pp-1820-1824, 2013.
- [2] Vijayaragavan S.P., Karthik B., Kiran Kumar T.V.U., Sundar Raj M., Analysis of chaotic DC-DC converter using wavelet transform, Middle - East Journal of Scientific Research, v-16, i-12, pp-1813-1819, 2013.
- [3] Sundararajan M., Optical instrument for correlative analysis of human ECG and breathing signal, International Journal of Biomedical Engineering and Technology, v-6, i-4, pp-350-362, 2011.
- [4] Kiran Kumar T.V.U., Karthik B., Improving network life time using static cluster routing for wireless

sensor networks, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4642-4647, 2013.

- [5] Karthik B., Kumar T.K., Dorairangaswamy M.A., Logshanmugam E., Removal of high density salt and pepper noise through modified cascaded filter, Middle - East Journal of Scientific Research, v-20, i-10, pp-1222-1228, 2014.

- [6] Karthik B., Kiran Kumar T.V.U., EMI developed test methodologies for short duration noises, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4615-4619, 2013.

- [7] Vijayaragavan S.P., Karthik B., Kiran Kumar T.V.U., Privacy conscious screening framework for frequently moving objects, Middle - East Journal of Scientific Research, v-20, i-8, pp-1000-1005, 2014.

- [8] Vijayaragavan S.P., Karthik B., Kiran Kumar T.V.U., A DFIG based wind generation system with unbalanced stator and grid condition, Middle - East Journal of Scientific Research, v-20, i-8, pp-913-917, 2014.

- [9] Arul Selvi S., Sundararajan M., A combined framework for routing and channel allocation for dynamic spectrum sharing using cognitive radio, International Journal of Applied Engineering Research, v-11, i-7, pp-4951-4953, 2016.

- [10] Arul Selvi S., Sundararajan M., SVM based two level authentication for primary user emulation attack detection, Indian Journal of Science and Technology, v-9, i-29, pp--, 2016.

- [11] Kanniga E., Sundararajan M., Kanembedded control of sub cyclic Ac chopper with high speed and low switching losses, Advanced Materials Research, v-717, i-, pp-579-584, 2013.

- [12] Kanniga E., Sundararajan M., Modelling and characterization of DCO using pass transistors, Lecture Notes in Electrical Engineering, v-86 LNEE, i-VOL. 1, pp-451-457, 2011.

- [13] Kanniga E., Selvamarathnam K., Sundararajan M., Embedded control using mems sensor with voice command and CCTV camera, Indian Journal of Science and Technology, v-6, i-SUPPL6, pp-4794-4796, 2013.

- [14] Lakshmi C., Ponnavaikko M., Sundararajan M., Improved kernel common vector method for face recognition, 2009 2nd International Conference on Machine Vision, ICMV 2009, pp-13-17, 2009.

- [15] Lakshmi C., Sundararajan M., Manikandan P., Hierarchical approach of discriminative common vectors for bio metric security, 2010 The 2nd International Conference on Computer and Automation Engineering, ICCAE 2010, v-2, i-, pp-784-790, 2010.

- [16] Venkataganesan K.A., Mohan Kumar R., Brinda G., The impact of the determinant factors in the career satisfaction of banking professionals, International Journal of Pharmacy and Technology, v-8, i-3, pp-17431-17436, 2016.

- [17] Sambantham M.C., Venkatramaraju D., Human resources management (HRM) practices in multinational companies with reference to knowledge transfer, *International Journal of Pharmacy and Technology*, v-8, i-3, pp-18565-18571, 2016.
- [18] Suganthi S., Senthilkumar C.B., A study on stress management of the staff of the co operative banks of Tamil Nadu, India, *International Journal of Pharmacy and Technology*, v-6, i-4, pp-7529-7533, 2015.
- [19] Thooyamani K.P., Udayakumar R., Khanaa V., Cooperative trust management scheme for wireless sensor networks, *World Applied Sciences Journal*, v-29, i-14, pp-253-258, 2014.
- [20] Nivethitha J., Brindha G., Management of Non-Performing Assets in Virudhunagar District Central Co-Operative Bank-An Overview, *Middle - East Journal of Scientific Research*, v-20, i-7, pp-851-855, 2014.
- [21] Ramachandran S., Venkatesh S., Performance measurement and management system-inter company case Study approach-Tamilnadu, India, *Middle - East Journal of Scientific Research*, v-20, i-9, pp-1162-1174, 2014.
- [22] Mathew S., Brindha G., Medical tourism – An avenue to attract foreign patients in Indian hospital industry, a study conducted in Chennai city, *International Journal of Applied Engineering Research*, v-9, i-22, pp-7508-7513, 2014.
- [23] Mathew S., Brindha G., An empirical study on competency mapping – A tool for talent management, *International Journal of Applied Engineering Research*, v-9, i-22, pp-7348-7354, 2014.
- [24] Mathew S., Brindha G., Quality of work life among the women it professionals in Chennai city, *International Journal of Applied Engineering Research*, v-9, i-22, pp-7434-7442, 2014.
- [25] Mathew S., Brindha G., Level of stress and its impact on job satisfaction among the employees of Air India limited, Chennai, *International Journal of Applied Engineering Research*, v-9, i-22, pp-7549-7559, 2014.
- [26] Brindha G., Emerging trends and issues in human resource management, *Middle - East Journal of Scientific Research*, v-14, i-12, pp-1727-1730, 2013.
- [27] Nivethitha J., Brindha G., Virudhunagar district Central Co-Operative Bank- An overview, *Middle - East Journal of Scientific Research*, v-12, i-12, pp-1663-1667, 2012.
- [28] Brindha G., Revamp of educational system-promoting entrepreneurship in India, *Middle - East Journal of Scientific Research*, v-12, i-12, pp-1668-1671, 2012.
- [29] Brindha G., Current role of human resources in health sector, *Middle - East Journal of Scientific Research*, v-12, i-12, pp-1649-1656, 2012.
- [30] Brindha G., A new approach for changes in health care, *Middle - East Journal of Scientific Research*, v-12, i-12, pp-1657-1662, 2012.
- [31] T.Padmapiya and V.Saminadan, "Utility based Vertical Handoff Decision Model for LTE-A networks", *International Journal of Computer Science and Information Security*, ISSN 1947-5500, vol.14, no.11, November 2016.
- [32] S.V.Manikanthan and V.Rama "Optimal Performance Of Key Predistribution Protocol In Wireless Sensor Networks" *International Innovative Research Journal of Engineering and Technology*, ISSN NO: 2456-1983, Vol-2, Issue –Special –March 2017.
- [33] Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL USING AODV PROTOCOL SCHEME FOR WIRELESS AD-HOC NETWORK." *Advances in Computer Science and Engineering* 16.1/2 (2016): 19.
- [34] Akhil Augustine , Manuel Johnson , Thomas Joseph, "EQUALIZATION OF THE CURRENT IN A THREE-PHASE ELECTRICAL POWER SYSTEM", *International Innovative Research Journal of Engineering and Technology*, Vol. 2, March 2017.

