International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

Industrial Communication

Matthew N. O. Sadiku[1], Sarhan M. Musa[1], Osama M. Musa[2]

[1]Professor, [2]Vice President and Chief Technology Officer
[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View
[2]Ashland Inc – Bridgewater, Bridgewater Township, New Jersey

How to cite this paper: Matthew N. O. Sadiku | Sarhan M. Musa | Osama M. Musa "Industrial Communication" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.1362-1364, URL: https://www.ijtsrd.com/papers/ijtsrd24057.pdf

IJTSRD24057

ABSTRACT

Communication is the exchange of information between two or more parties or devices. The introduction of the Internet of Things (IoT) and Cyber Physical Systems (CPS) in the industrial environment have revolutionized the industrial world. Industrial communication networking is very important to the continued operation of all forms of industry. This paper provides a brief introduction to industrial communication.

Keywords: *industrial communication, industrial communication network, industrial computer networks*

INTRODUCTION

A communication network is one of the most important parts in promoting the effective use of industrial automation. In the past, industrial networks were not linked to each other and were not connected to public networks like the Internet. Today, industrial communication networks are increasingly based on open protocols that are also used in the Internet environment.

The use of local area networks (LANs) to interconnect computer and automation devices became popular in 1980s. It is now possible to extend the connection to a wide area network (WAN) through a gateway. Most industrial communication networks use serial data transfer which requires a limited number of wires to communicate or exchange data between devices.

In order to provide interconnection and communication between the devices, an effective communication network is required. In the environment of the automation of industrial processes, the communications between devices are carried out using various industrial communications protocols. A communication protocol is a set of rules that allows communication and transfer of data between the devices. Industrial communication protocols involve concurrency, timing, and resource constraints.

HIERARCHY OF AN INDUSTRIAL COMMUNICATION NETWORK

Due to their complexity, the industrial communication networks are typically built in hierarchical fashion. Based on functionality, industrial communication networks can be classified into three general levels: field-level networks, control-level networks, and information-level networks [1, 2]. These are illustrated in Figure 1 [2] and explained as follows.

- **Field Level:**

This lowest level consists of devices such as sensors, actuators, machines I/O modules, and drive units. This level is employed to transfer information between these devices. The common serial communication protocol standards used in this level include RS232, RS422, and RS485. Today, fieldbus technology is the most sophisticated communication network used in this level

- **Control Level:**

This level consists of industrial controllers such as programmable logic controllers (PLCs) and computer systems. The tasks of this level include configuring automation devices, loading of program data, and process variables data. LANs are often used as communication networks in this level.

- **Information Level:**

This top level of the industrial automation system gathers the information from the control level. It deals with large volumes of data. Ethernet and WANs are commonly used at this level.

COMMUNICATION NETWORK COMPONENTS

An industrial communications networks typically include a broad range of industrial wireless routers and modems, cellular 4G routers and gateways, hardened optical networks, multiplexers, broadband power line solutions, and Ethernet switches and converters. These components can be classified as follows.

- **Physical cables:**

These include twisted-pairs, coaxial cables, and fiber optical cables.

- **Network devices:**

These include repeaters, bridges, routers, gateways, hubs, switches, and transceivers.

- **Intelligent devices:**

These can be a programmable logic controller (PLC), PC, Distributed Control Systems (DCS), Supervisory Control, Data Acquisition Systems (SCADA), and Wireless Sensor networks (WSN).

The integration of these systems is carried out by distributing the communications in several layers: fieldbus, LAN networks, and LAN-WAN networks. Communication is the backbone of all industrial components for efficient automation production systems. The communication network connects all of the components so that they can work together effectively. The network is used to monitor and control physical equipment in industrial environments. Proprietary communication systems were supplemented and partially displaced by fieldbus and sensor bus systems [3].

Wireless communication is attractive for industrial networks because it serves as a substitute for cabling when using fieldbus standards and some industrial environments are too harsh for regular physical cabling. The penetration of wireless communication technology in industrial applications is steadily increasing. With the introduction of the Internet of things, SCADA, and cyberphysical system in industrial environment, industrial automation is undergoing a tremendous change.

APPLICATIONS

Industrial communication networks are employed in many industrial domains including manufacturing, electricity generation, food and beverage processing, transportation, water distribution, waste water disposal, and chemical refinement including oil and gas [4]. We will consider manufacturing as a typical example.

Today, manufacturing is expected to be more connected, reliable, more automated, more flexible, more agile, more responsive, more scalable, and more decentralized. Industrial communication networks span a wide range of manufacturing applications and provide a seamless integration of all networked devices. Typical examples are the assembly of automobiles and integrated circuits. Such networks enable seamless communication as well as greater speed and efficiency. A star topology is often used for communication in a manufacturing scenario.

CHALLENGES

A major challenge is connecting devices from different manufacturers and using proprietary digital communication networks. To address this challenge, several manufacturers have attempted to impose a standard that allows for simplifying and unifying industrial communications. Today, the trend is following Open Systems Interconnection (OSI) standards which allow interconnection of automation devices effectively irrespective of the manufacturer. Due to the presence of humans within the systems to be controlled, their safety requirement is high.

Wireless communication has posed additional challenge towards the security of industrial communication networks. The industrial communication systems of today are vulnerable to electronics attacks. This vulnerability presents an opportunity to cause malicious damage. Information system security can be described in terms of security objectives. In industrial communication networks, security objectives include confidentiality, integrity, availability, authentication, authorization, access control, auditability, nonrepudiability, and third-party protection. Currently, most industrial communication protocols have little or no security functionality [5].

CONCLUSIONS

We are presently in the stage of the deployment of the second generation of industrial communication networks. There is a trend within industrial communication networking to implement fieldbus protocols using wireless technologies. Wireless is quite suitable for hazardous and dynamic environments. Some courses have been offered to introduce students in this area [6]. More information about industrial communication can be found in [7,8].

REFERENCES

[1] "An overview of industrial communication systems & networks," https://www.electricaltechnology.org/2016/12/industrial-communication-networks-systems.html

[2] I. Belai and P. Drahos, "The industrial communication systems PROFIBUS AND PROFInet," Applied Natural Sciences, 2009, pp.329-336.

[3] P. Neumann, "Communication in industrial automation—What is going on?" Control Engineering Practice, vol. 15, 2007, pp. 1332–1347.

[4] B. Galloway and G. P. Hancke, "Introduction to industrial control networks," IEEE Communications Surveys & Tutorials, vol. 15, no. 2, Second Quarter 2013.

[5] D. Dzung et al., "Security for industrial communication systems," Proceedings of the IEEE, vol. 93, no. 6, June 2005, pp. 1152-1177.

[6] L. L. Bello, O. Mirabella, and A. Raucea, "Design and implementation of an educational testbed for experiencing with industrial communication networks," IEEE Transactions on Industrial Electronics, vol. 54, no. 6, December 2007, pp. 3122-3133.

[7] R. Zurawski (ed.), Industrial Communication Technology Handbook. Boca Raton, FL: CRC Press, 2nd edition, 2015.

[8] B. M. Wilamowski and J. D. Irwin, The Industrial Electronics Handbook: Industrial Communications Systems. Boca Raton, FL: CRC Press, 2nd edition, 2011.

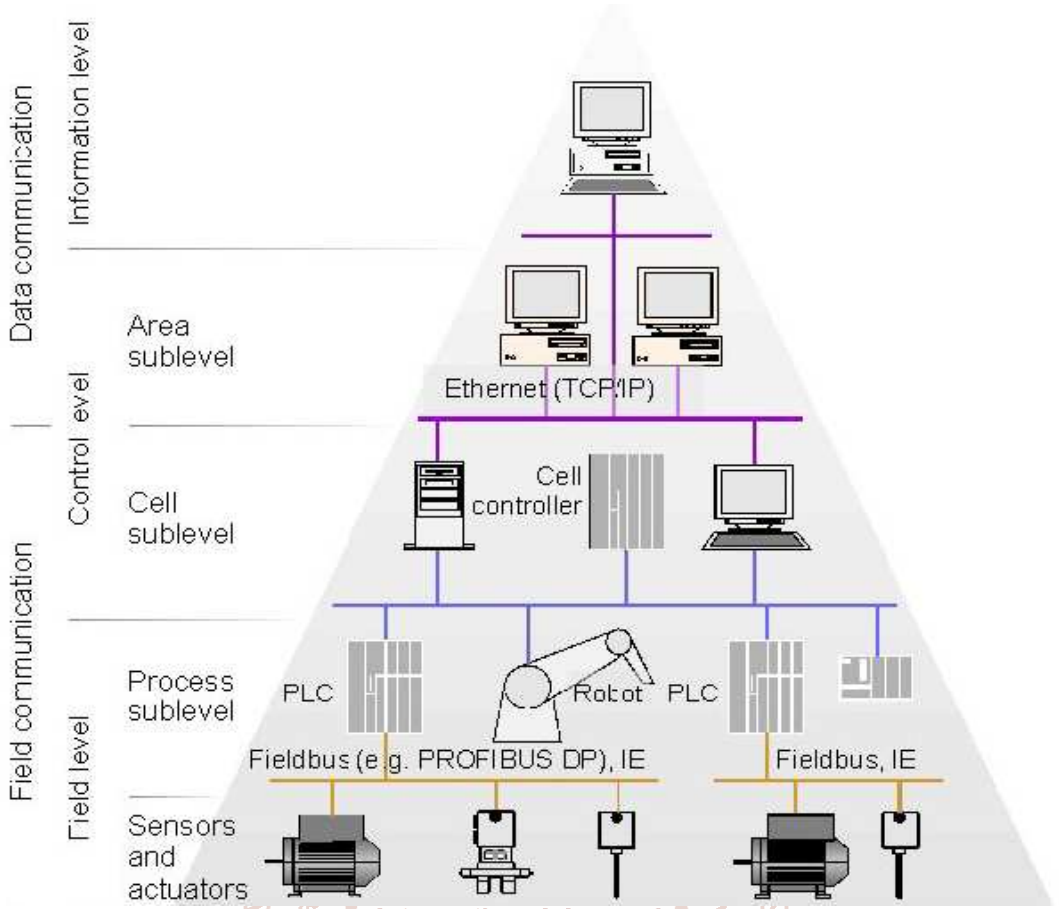

Figure1. Hierarchy of an industrial automation system [2]