Industrial Networking Basics and Ethernet Development for Industrial Applications

Michael G. Coffman
School of Information Systems & Applied Technologies
Southern Illinois University
1365 Douglas Drive, ASA Bldg. Mail code 6614
Carbondale, Illinois 62901

ABSTRACT

The basic characteristics of the four levels of industrial networking; informational, control, device, and safety are explained with general information, specific requirements, and application in the industrial setting given about each level. With the explanation of the safety network, an explanation of the SIL (Safety Integrity Level) required for industrial settings is presented. Then a comparison to standard (informational) Ethernet and the other levels is presented with information on why Ethernet is not adequate for these levels. In addition, developments in Ethernet to overcome these short comings and increase its viability on an industrial level are presented and reasons that Ethernet, while increasing its presence in the industrial environment, is still not the only type of network implemented.

Keywords: Industrial Networking, Ethernet IP, Device Network, Control Network, Safety Network

INTRODUCTION

Providing necessary information to be successful in networking in a manufacturing environment can be overwhelming do to the fact that several different levels of networks may be needed for task accomplishment. When most people think of a network it is in the context of a traditional informational network, and the transition to an industrial environment can appear to be a confusing and daunting task. A network that is more than sufficient for informational purposes may not be adequate for the networking levels required by a manufacturing facility. The information presented in this article is intended to make the transition to industrial networking less confusing.

INDUSTRIAL NETWORKING BASICS

An industrial network is formed when plant floor devices, controllers, and computers are networked together in any fashion. This may be everything from a network to allow a computer to program and monitor a Programmable Logic Controller (PLC) to real time plant floor process control and data collection. These applications may or may not include a traditional information network.

In an industrial setting there are four basic levels of networking. These levels are: informational, control, device, and safety [1]. Each level has unique requirements that affect which network is used for that particular level.

The informational level is where a traditional network such as standard Ethernet is used. For an industrial setting, a traditional network is one where data files are shared between computer systems. Standard Ethernet is a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) network. In this type of network, data transmission is performed on a first-come, first-served basis. Because of this, the more devices that are connected to the network, the slower the network performs.

The control level involves networking machines, work cells, and work areas. This is the level where Supervisory Control And Data Acquisition (SCADA) is implemented. If an automotive assembly plant is used as an example, this network level is where the individual control systems will be given information on the make, model, and options that are to be included on a vehicle so that the controllers can run the appropriate programs to assemble the vehicle correctly. Data such as cycle times, temperatures, pressures, volumes, etc. are also collected at this level [2]. The control level of the network must be deterministic and repeatable. Determinism is the ability to accurately predict when data will be delivered, and repeatability is the ability to ensure that transmit times are consistent and unaffected by devices connecting to the network. Because of the deterministic and repeatability issues, network access by CSMA/CD (traditional Ethernet) is inadequate, so a different type of network access is required. For example, Concurrent Time Domain Multiple Access (CTDMA) can be used. CTDMA is a time-slice algorithm that regulates each node's opportunity to transmit in a network interval. Adjustment of the amount of time for a network interval gives a consistent, predictable time for data transmission [3].

The device level involves networking I/O to the controller. This network connects devices such as limit switches, push buttons, photo eyes, various types of smart devices, etc. to a network. One of the advantages of this type of network is in cabling. All of the devices connect to a single cable. The cable usually has conductors for power, device signal, and a shield. The messages are usually small when compared to other networks. Because of deterministic and repeatability issues, CSMA/CD is inadequate; and a different type of network access is required. For example, Carrier Sense Multiple Access with Arbitration on Message Priority (CSMA/AMP) can be used. As the name implies, the messages can be prioritized so that the more critical information is transmitted first [3].

The last type of network is a safety network. A safety network is used to replace hardwired safety devices. The idea is to have a control structure (such as a Safety PLC) make decisions about what equipment needs to be shut down in an emergency situation [4]. The goal is to reduce downtime by limiting the shutdown to only the systems affected by the emergency.
The safety network must be highly deterministic and repeatable. It must be dual channel so that the messages can be

crosschecked, and the protocol must transmit each message twice. In addition, the necessary Safety Integrity Level (SIL) must be determined so that the appropriate network can be selected. SIL defines the average probability of failure on demand. The International Electronics Commission (IEC) standard 61508 defines the requirements of a safety system to comply with the appropriate SIL level. For example, a nuclear power plant will have critical systems that are at a SIL 4 (the highest level) while most traditional manufacturing facilities will have SIL 3 level applications [5]. Since the safety system is a network (as opposed to traditional hardwired relay), provisions must be made by the control system to place the equipment in a pre-determined safe state should a communications error occur. For example, the safe state on a robotic arm may be an immediate "power off" to prevent movement, while the safe state for an exhaust fan may be an immediate "power on" so that harmful or dangerous fumes can not accumulate. Because of these requirements, safety networks have not grown nearly as fast as the other types of networks.

ETHERNET DEVELOPMENT FOR INDUSTRIAL NETWORKING

Since Ethernet is so common in informational networks, efforts to bring it to the various levels of plant floor networking seem only natural. There are some problems with implementing standard Ethernet in a manufacturing environment. A lack of real-time determinism makes standard Ethernet inappropriate for the control level, lack of power delivery to devices makes standard Ethernet inappropriate for the device level, and an insufficient SIL level makes standard Ethernet inappropriate for the safety level. There are many variations of Ethernet that address some of these issues.

There are three basic ways to try to deal with real-time, deterministic communications. They are: switched Ethernet, IEEE1588 Precision Time Protocol, and time slicing. Switched Ethernet increases network speed but does not guarantee real-time, deterministic responses. It uses speed to try to overcome the problem. While the switched system does provide full-duplex operation between the switch and any of its nodes, the switch itself can be the source of bottlenecks as traffic increases and the switch's buffers try to keep up with the data flow. IEEE 1588 Precision Time Protocol defines methods to distribute and synchronize clocks in a network and time stamp the data. The clocks for the network are calibrated regularly with synchronization telegrams. Data is time stamped with information indicating when it was captured or when an operation needs to be initiated. Upon the receipt of the message, the receiver processes the time stamp according to a prescribed schedule and takes the appropriate action. Implementation of the clocks can be done by hardware or software depending on the level of precision required. It should be noted that the IEEE 1588 specification can be used in any network, not just Ethernet.

In a time slicing system, critical information is assigned a specific time slot to send data with non-critical data transmitted as time allows. In this type of network, data transmission is organized chronologically. The network requires one node on the network to manage time allocation and ensures that every node that has critical information can transmit data without interference. One problem that can arise with this solution is that not all IEEE 1588 and time slicing are implemented in the same way. For example, two IEEE 1588 networks may be implemented that are physically and electrically compatible with each other but the applications for file transfer may be different. While both networks are Ethernet and can send and receive data, they cannot process it correctly. There is another flavor of Ethernet that tries to addresses this problem, Ethernet/IP (Ethernet/Industrial Protocol). The idea is to establish and maintain standards to simplify implementation [6]. So, if a network is implemented using Ethernet/IP, all aspects of the network will be implemented in the same fashion thus eliminating the data interpretation problem.

Another interesting form of Ethernet is Ethernet Powerlink (EPL). EPL uses time slicing for a real-time, deterministic response when data is critical. EPL complies with standard Ethernet 802.3. This means that it can be implemented on any standard Ethernet interface card. EPL can also be implemented at the device level by using CAN (Controller Area Network) device profiles. EPL uses the CANopen EN50325-4 standard for automation [7].

One of the drawbacks to implementing device level Ethernet has been providing power to the devices. In 2003 Power over Ethernet (PoE) became an international standard, specifically IEEE 802.3af [8]. A standard Ethernet cable has four wire pairs and presently only two pairs are used to data in 10BaseT and 100BaseT communications. PoE uses the unused pairs in the Ethernet connector and cable to provide up to 48 volts DC for powering devices. Also, the Ethernet Powerlink Standardization Group recently introduced EPL Safety which has a SIL-4 rating, making it more than adequate for most industrial safety networks. Based on the preceding discussion, it would seem that EPL is the one network that would standardize everything in the industrial networking world; but this has not happened. There are still many hurdles to overcome which have prevented wide spread adaptation. As an example, the power available is presently limited to 13 watts at the receiving device [9]. More power interferes with the Ethernet data signals. Another example is that the standards are relatively new and there are currently few compatible devices available. So EPL is still not the answer to one network for everything in a manufacturing environment.

CONCLUSION

There are many different network levels used in industrial settings; and currently a single networking system that integrates all the levels does not exist. Perhaps in the future as Ethernet becomes more and more prevalent, all of the networks may migrate to Ethernet but for the present, network engineers will be faced with a wide range of networks from which to choose and implement.

REFERENCES

[1] Brooks, P. (2001, October), Ethernet/IP: Industrial protocol. Retrieved January 10, 2005, from http://literature.rockwellautomation.com/idc/groups /literature/documents/wp/enet-wp001_-en-p.pdf

[2] Stenerson, J. (1999). Industrial networks. In Charles E. Stewart, Jr. (Ed.), *Sensors and communications fundamentals of programmable logic controllers* (2nd ed.). (pp. 367-392) Upper Saddle River, New Jersey: Prentice Hall

[3] Bettendorf, B. (2004, Fall). *Which industrial network for you* (Industrial Networking). Putman Media Publications, p. 34

[4] Merritt, R. (2004, Winter). *Converge on safety* (Industrial Networking), Putman Media Publications. pp. 14-21

[5] Open DeviceNet Vendor Association, Inc. (2003) Safety networks. Retrieved January 12, 2005, from http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00110_DeviceNet_Safety_White_Paper.pdf

[6] Labs, W. (2005, Summer). *What's your taste in ethernet*? (Industrial Networking). Putman Media Publications. pp. 14-19

[7] Pfieffer, A. (2005, Winter). *Deterministic networking on ethernet* (Industrial Networking). Putman Media Publications. p. 34

[8] Hebert, D. (2004, Spring). *Almost Pperfect* (Industrial Networking), Putman Media Publications. pp. 12-21

[9] Merritt, R. (2005, Spring). *PoE: not ready for prime time … yet* (Industrial Networking). Putman Media Publications. p. 34