Proceedings of the Korean Nuclear Society Autumn Meeting
Seoul, Korea, October 1995

A Study on LAN Applications in Nuclear Safety Systems

Sung Kim, Young Ryul Lee, Jun Mo Koo, Jai Bok Han

Korea Atomic Energy Research Institute

Abstract — It is a general tendency to digitalize the conventional relay based I&C systems in nuclear power plant. But, the digitalization of nuclear safety systems has many a difficulty to surmount. The typical one thing of many difficulties is the data communication problem between local controllers and systems. The network architecture built with LAN(Local Area Network) in digital systems of the other industries are general. But in case of nuclear safety systems many considerations in point of safety and license are required to implement it in the field. In this paper, some considerations for applying LAN in nuclear safety systems were reviewed.

I. Introduction

In safety systems in I&C of NPP, the old fashioned technology using relays and analog circuits have been used in point of safety and license, but nowadays the trend toward digitalization in safety systems of the conventional analog type is growing to form a total digital I&C in nuclear power plant(NPP). The conventional analog safety systems use point to point electro mechanical relay contacts for system interfaces. In this case, the signal transfer capability of each contcat is only one. It needs many cabling works and large space of the cabinets. To solve these problems, it is essential to introduce LAN(Local Area Network) in the plant. To do this, there are two ways. The first one is digitalization of the conventional analog systems, the second one is backfitting of LAN controllers between two systems.

1. OSI (Open Systems Interconnection) Reference Model of LAN

ISO(International Organization for Standardization) undertook development of a model for computer communication protocols in 1978, and published the OSI Reference Model in 1984. Figure 1 shows the familiar seven layer model

1). Physical Layer(PL)

The PL is responsible for the physical, electrical, and procedural specifications required to transmit the actual data across the physical medium or cables.

2). Data Link Layer(DLL)

The DLL must maintain a reliable connection between adjacent nodes, assuming an error-prone physical channel.

3). Network Layer(NL)

The NL is responsible for routing, switching, and controlling the flow of information between two hosts.

4). Transport Layer(TL)

The TL assures an error-free host-to-host connection. Said differently, the source to destination reliability is assured.

5). Session Layer(SL)

The SL provides for the establishment and termination of communication sessions between host processes.

6). Presentation Layer(PL)

The PL provides a mechanism to translate the data format of the sender to/from the data format of the receiver.

7). Application Layer(AL)

The AL provides protocols for common end-user functions or applications.

2. LAN Classification By Topology

The LAN classifications by topology are ring, bus, star.

1). Bus Network

Each compuer is tied in one transmission channel, all messages are exchanged through control nodes.

2). Ring Network

Transmitted message is moving around the ring in node unit base, each node is operated through RIU(Ring Interface Unit), and retransmits the addressed message to the other node in the received information.

3). Star Network

There is a central station in the center, the messages shold be routed through it The cental station will cause the phenomenon of bottle-neck.

3. LAN Classification By Access Method

1). CSMA/CD(Carrier Sense Multiple Access/Collision Detect)

While the received station is being responding, the other stations remain standby condition. The data collision is prohibited by priority, the characteristics of directive couplers.

2). Token Passing

a). Token Bus

Token is circulating, and the token is transmitted logically to the another station.

b). Token Ring

Token is circulating in the ring type circular network. Each node is operating through RIU, and retransmits the addressed message to the other node in the received information.

The performance comparision is as figure 1.

II. LAN Protocol Implementations

1. ARCNET(Attached Resource Computer Network)

Of all the major networks, ARCNET is the most flexible in its architecture. Both star and bus topology networks, or a combination that might be described as a distrubuted star with branches, are possible. There are many types of media, such as coax, single twisted pair and duplex fiber optic cable. A network requiring coax in the computer room, twisted pair through the office, and fiber optics outside to the guard station could be easily designed. The only major constraint on the transmission medium is that the signal propagation delay between any two workstations must not exceed 31 microseconds. In addition, the attenuation characteristics of the different types of cable affect the number of workstations that cab be attached in a bus topology.

A. ARCNET Software Considerations

1). Frame Formats

The ARCNET protocol implemented on the COM9026 is a character oriented protocol having five different types of frames. All ARCNET frames begin with an Alert Burst of six ONES. Each character within the frame consists of an 11 bit sequence : ONE + ONE + ZERO + 8 Bit Character. As a result, the network throughput is actually 1.8 Mbps (8/11 * 2.5 Mbps).

The five frame formats are defined as follows :

0. Invitation to Transmit(ITT)
Passes the token from one node to another

0. Free Buffer Enquiry(FBE)
Asks an intended destination node if it can accept a data packet from the node currently holding the token

0. Data packet (PAC)
The data itself, up to 508 octets, transmitted from the token holder to the intended destination. An octet is defined as eight bits.

0. Acknowledegement (ACK)
Indicates correct receipt of a Packet or an affirmative response to a FBE

0. Negative Acknowledgement (NAK)
Negative response to a FBE

2. Token Ring Architecture

Its name implies a ring, however the token ring is physically a star, and electrically a ring. The serial transmission follows a complete ring or loop(hence the name token ring), with the sending station eventually receiving its transmission information back after this information completes one round trip around the ring. The token is merely a specific bit sequence that circulates among the nodes, giving permission to transmit. Token ring networks are often described as being distributed polling environments for this reason. When the node is in in possession of the token, it can transmit a messsage that is in its output buffer. Otherwise, the node is in bit repeat (and/or receive and process) mode. The token ring network adheres to the IEEE 802.5 Stamdard.

A. Token Ring Standard

1). Physical Layer

0. Symbol Encoding
Differential Manchester encoding with no DC component(therefore allowing inductive or capacitive coupling between cable and network interface) is used. The Differential Manchester code is defined as follows: a ZERO is represented by a transition at the beginning of the bit cell; a ONE has no beginning transition. In addition, a forced transition in the middle of the bit provides timing information

0. Signal Rate

0. Cable

0. Connector

0. Latency Buffer

0. Phantom Power

2). Medium Access Control Layer

0. Frame Formats
0. Error Control
0. Ring Maintenance Functions

3). Logical Link Control Layer

The LLC layer defines virtual data paths between communcating end points in collaboration with the physical data paths defined in the MAC and Physical layers.

0. Type 1(Unacknowledged Connectionless)
0. Type 2(Connection Oriented)
0. Type 3(Acknowledged Connectionless)

III. NETBIOS

NetBIOS(Network Basic Input Output System) was developed by Sytek, Inc., and IBM as a programming interface to IBM's PC NETWORK LAN. In its original release, NetBIOS was provided on the PC Network NIC itself; for the token ring network, NetBIOS is emulated within the PC. Many other vendor's also offer NetBIOS emulators. Many application programs are deemed "NetBIOS compatible", which is another way of saying that they rely upon the NetBIOS functions for network communication. When compared with the OSI model, the NetBIOS program would be defined as a Session layer protocol-one that is responsible for establishing and terminating the communication session between two users on the network, or between one user and the network server. Functions at the Transport and Network layers, specifically end-to-end reliability and internetworking, respectively, are not rigorously addressed by NetBIOS; and frequently other protocols, such as TCP/IP. When using NetBIOS, the Host machine builds a NCB(Network Control Block) and transmits the aprropriate NetBIOS frame.

IV. LAN Performance Metrics

0. Network Utilization

Network Utilization measures the gross level of activity on the network. Mathematically, this is defined as the ratio of the number of bits transmitted during a specific period of time to the total number of bits that could have been transmitted during that period.

0. Network Traffic

To measure network traffic you must first define the sources and destinations of the information transmitted over the LAN. The first metric to consider, sometimes referred to as Pair Counts, is the measurement of the number of frames exchanged between pairs of workstations, or between a workstation and a peripheral. This measurement determines which nodes are the busiest, who is communicating with whom, and can be useful in dividing the network into communities of interest. This determination is often required before adding a network bridge to create subnetworks.

A second, related benchmark is Throughput, which measures the number of frames or bits that have passed through the network.

A third benchmark, Frame Statistics, establishes the minimum, maximum, and average sizes of transmitted frames. These can prove useful for determining what type of activity are predominantly used on the LAN.

0. Network Delays

The channel Acquisition time is the time between when the frame is ready for transmission and when it is actually placed on the network. As such, it is a measure of the Media Access Control(MAC) delay, including delays, collisions, etc. Network Response Time measures the propagation delay from the transmitter to receiver and back.

0. Netwok Errors

Frame errors cause retransmissions, and generally degrade network performance. Five different frame error situations can occur :

-. A bad Frame Check Sequence(FCS) indicates that bit errors occurred that affected the Cyclic Redundancy Check (CRC).
-. Misaligned Frames occur when the number of bits in the received frame is not an integral number of octets, and the frame also has a bad FCS.
-. Jabbers are frames that exceed the maximum allowable frame length
-. Runts are frames that are less than the minimum frame length
-. Finally, Collisions result from the simultaneous transmission of two stations and occur in IEEE 802.3 networks.

Tracking down the sources of these network errors generally leads to a defective Network Interface Card (NIC) at one of the workstations.

V. Fault Analysis of LAN

Many LAN managers claim that that between 70 and 90 percent of their network failures are attributable to hardware failures. That means form 10 to 30 percent of these problems are to be blamed on software. Unfortunately, even though software difficulties occur less frequently, they are usually more difficult to diagnose. The following is a list of several failure modes including software and hardware faults to be considered for LAN implementations.

1. Cable Faults
   0. Cable short, open, frayed
   0. Connector is bad or improperly seated
   0. Miswiring
   0. Cable Tap Faulty
   0. Improperly grounded

2. Hardware Faults
   0. Workstation that can transmit but not receive
   0. Excessive data packet collisions
   0. Improperly framed transmissions, known as fragments or jabbers
   0. High error rates resulting from a failure of the CRC calculation at transmitter or receiver

3. Software Faults
   0. Failure of the S/W itself (as a bug)
   0. Parameters (such as workstation cache buffers) that are improperly configured

0. Incompatibilities between two nodes, such as transmit and receive buffers or window sizes

4. Routing Faults

0. Duplicate node address

0. Network congestion at a bridge, router, or gateway

0. Broadcast storms where nodes broadcast queries for routing information and do not allow sufficient time for a response

VI. Real considerations about LAN in safety systems

There are two steps to implement LAN in safety systems. The first step is to digitalize the system, and the second step is to replace the abundant interface wires between two other systems witho one coaxial cable or optical fiber . The important point to be considered here is a response time between node to node. The three factors related to the response time are (1). PLC scan time or controller's one loop execution time (2). Network token rotation time (3). Hot standby failover. So, to reduce the response time, the following requirements should be satisified.

1). The program size should be small to reduce scan time or one loop execution time.

2). The node numbers be small to reduce the network token rotation time.

3). The conecpt of hot standby is not good because it takes much time in case of failover.

The other considerations are as the followings.

0. The Frame should be short (40 % margin), and regular traffic in normal condition

0. Faster response in accident conditions

0. Fast recovery and reconfiguration in case of LAN faults

0. Distribution of propagation delay should be uniform

0. Network delay

Since data transaction is processed in high speed, the delay time which took for processing will cause network delay, review how much it will affect the network in applications.

0. Network Maintenance

-. Network Control Access Method, Routing, Protocol, Security consideration

-. Node and Link Hardware Failure

0. In case of node failure, should be considered for redundant data path(master, slave)

VII. CONCLUSION

To applay LAN in nuclear safety systems, many things should be considered. Fisrt of all, the suitability of applying LAN is considered. There are two points to do it. The first point is digitalization of the conventional analog systems, distribution of functions properly, and connection of the function modules with LAN, the second point is backfitting of the single LAN cable between two conventional systems instead of a bundle of wires. In case safety system has many nodes, the token passing protocol which is a deterministic protocol is more suitable to apply because it doesn't have the time dealy due to the data collision. But, In case of small system, if the traffic is not much, CSMA/CD protocol is more suitable to apply becasue it doesn't have overhead. In the actual design, the above real considerations in the safety systems should be checked.

REFERENCES

1. John E.McNamara, "Technical Aspects of Data Communication", Digital Press
2. Mark A.Miller, "LAN Troubleshooting Handbook", M&T Books
3. Mark A.Miller, "LAN Protocol Handbook", Prentice Hall
4. 이기종간의 LAN, mobico
5. EPRI URD Chapeter 10, MMIS
6. Framatome Equipment Document

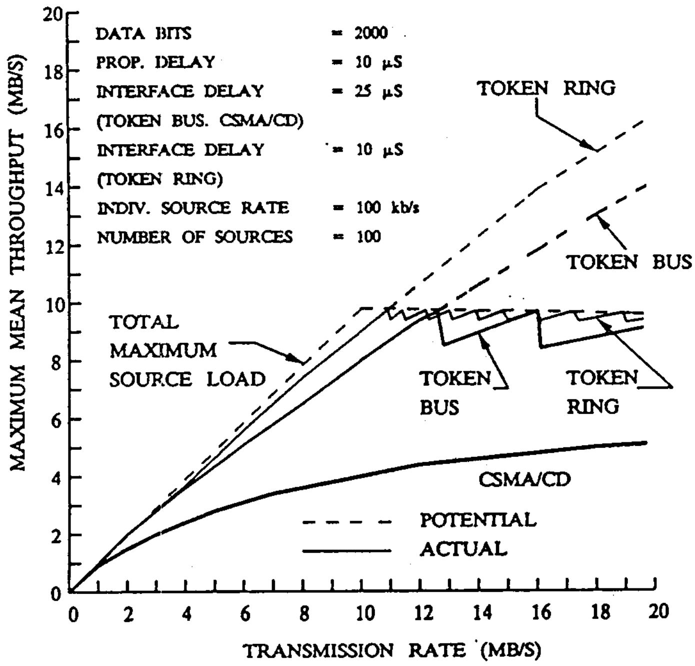

Fig.1. Maximum mean throughput rate as a function of the LAN transmission rate