

Table of Contents

Purpose of This Document.....	2
Plant Data Network Fundamentals	2
Common Design Requirements	3
Design Basics.....	5
Physical Network Design Requirements	8
Network Electronics Requirements	9
Network Reliability.....	10
Network Security	11

Purpose of This Document

This document describes the functional requirements for the Plant Data Networks (PDN) that will be installed in two Nuclear Power Plants in the Southeastern United States.

Common functional requirements for the PDN as well as plant specific functional requirements are presented

Plant Data Network Fundamentals

The primary task of the PDN is to provide a common framework for the interconnection of dedicated plant information and control systems. The PDN provides a premises-wide “backbone” which can consist of fiber optic cabling (both single mode and multi-mode), copper cabling, and specialty cabling such as coaxial cable, where required.

A PDN has existed in various forms since the inception of instrument based process control. Initial systems utilized serial signaling technologies such as RS-232 and RS-485. These early protocols allowed a field instrument to communicate to a central computer system through modems. Serial based systems are limited both in the amount of data that can be passed over an individual connection and the need for direction connection between each instrument and the computer. As the field instrumentation advanced the need for more advanced communication methodologies developed. To meet this need many manufacturers developed proprietary network communication schemas to support their equipment. Most of these communication methods were efficient and reliable but limited the end user to using only that manufacturer's equipment. If the need arose to share information with another system a custom interconnection device, gateway, had to be installed. This solution added a great expense to the system and presented network management problems that were multiplied with every different manufacturer's equipment installed at the facility.

During the time that process control system vendors were developing their specialized systems the technology of networking was making huge leaps in performance and reliability. The advances in network technology led to corporations recognizing the value of process control data availability in real-time and near real-time. To meet this need the concept of an integrated control and information system was developed. These systems utilize standard network technology engineered to support the special needs of the control systems. Adoption of integrated systems allows the end user to reduce overall operating and maintenance cost by having a larger installed base of network equipment with many qualified technicians.

The base network infrastructure is referred to as the Plant Data Network and consists of the network cabling, switching equipment, and other support equipment. Like the older proprietary systems a PDN must be engineered to support the entire control and information process that is required by the facility installing the system. The engineering

design process includes the same steps as the older communication technologies because the base functions have remained the same. All networks must be analyzed for data load, reliability, maintainability, and failure.

The primary elements of the PDN are single mode and multi-mode fiber optic cable, and Unshielded Twisted Pair (UTP) cable. The use of a fiber optic backbone in the development of the PDN provides the capability for high-speed data applications. Fiber optic cable also supports a variety of applications that would require large copper cables and additional hardware. The fiber optic cable is dielectric and therefore immune to electrical surges and radio interference. Copper cabling is utilized for short connection runs from a Zone Switch to a field device. For the end user device the PDN provides physical connectivity to any other device on the system through the cabling infrastructure. Zone Switches are placed throughout the premises to provide the connection point for the end user devices. The Zone Switches typically has the capability to house fiber terminations, and RJ-45 terminations. The application at each location will determine the actual configuration of each IMO. The Zone Switch is then connected to the Core Switches for routing. This configuration provides the best mix of reliability through redundant connections and controlled bandwidth with

Common Design Requirements

Plant Data Network (PDN) shall be a fault tolerant switched Ethernet communication backbone. The PDN will consist of a core backbone that will allow connections at all locations of the plant when fully implemented. The PDN serves as a standardized network connection point for all information services that are required for operation of the power plant. Servers, workstations, and various other systems connect to the PDN through either a direct fiber-optic connection or RJ-45 copper connection interface to a remote “Zone” switch. Specialized systems that are not fully Ethernet compliant will be connected through a gateway computer providing protocol translation.

The basic network backbone design utilizes two (2) identical switches, one in the Cable Spreading Room (CSR) and one in the Computer Room (CR). Both switches are connected through redundant fiber-optic cabling to provide a secondary routing path for all signals. Remote locations connect to the network through a “Zone” switch that connects to the main switches through fiber-optic cables. The design separation between the PDN backbone and other systems is defined as the uplink interface on the Zone switch or the fiber-optic interface card on a gateway computer. Initial installation and operations will utilize the two (2) switch model. Full redundant operation can be implemented utilizing a four (4) switch model (Reference Figure 1). The logical operation of the two (2) and four (4) switch models are identical, with the change being in the level of redundancy. This general design is often referred to as a “STAR” topology.

Cable routed to the main switches will be terminated on a passive fiber-optic patch panel to facilitate ease of maintenance. The patch panels will be mounted in the racks with the switches. Direct connection from a device to a switch should be avoided because of the

increased probability of a system failure caused by a cable fault caused by movement of the attached equipment.

The PDN has two functional usage categories referred to as the “Information Network” and the “Control Network”. Both portions of the network have the same specifications and provide the same Quality of Service (QOS). The functions assigned to the various systems serve as the basis for the separation of these two networks. Systems that predominately supply support or archival information attach to the Information Network portion of the PDN. Workstations and systems that deal primarily with live time measurements and information gathering or have the potential to issue a control function to a plant system connect to the Control Network portion of the PDN. Information being sent to or received from an external source passes through a firewall connected to the Information Network portion of the PDN.

Separation of the Control and Information portions of the PDN is maintained using Virtual Private Networks in conjunction with Layer-3 routing and physical separation on the switches. This approach to separation allows easy routing of information between system's segments when necessary while allowing QOS monitoring and control.

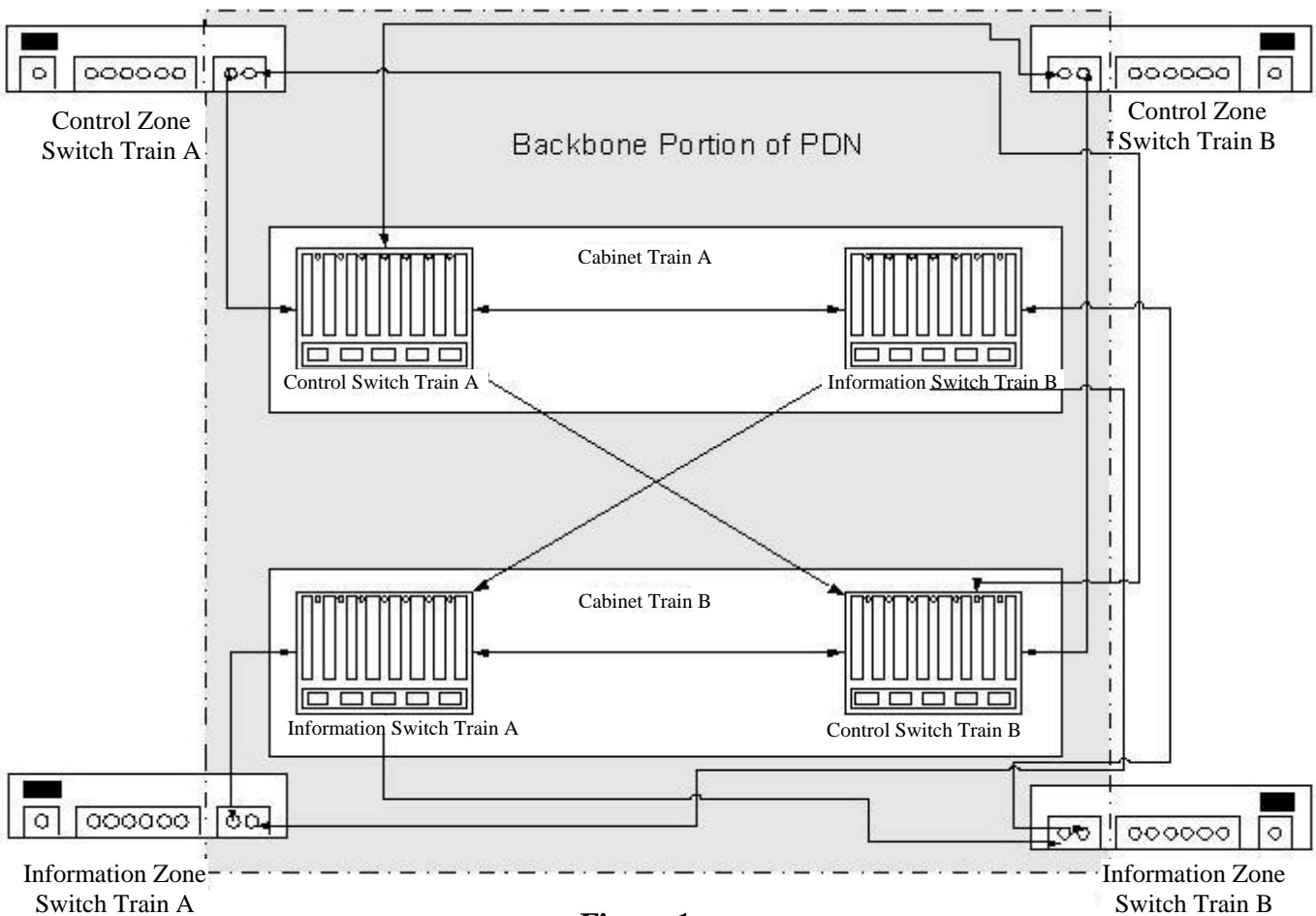
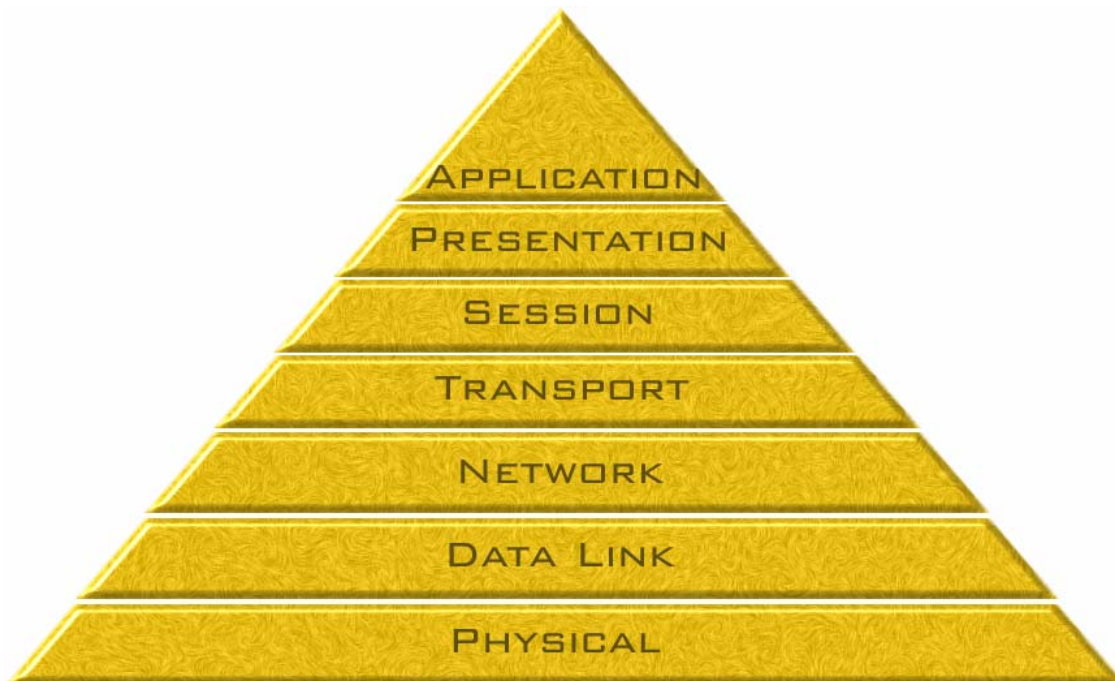


Figure 1

Design Basics

In an effort to standardize data communications between different types of systems, the International Standards Organization (ISO) developed a seven-layer information interchange model known as the Open Systems Interconnection (OSI) model. This model formed the basis for systems integration and communications between systems. The seven layers that make up the model are: 1-Physical, 2-Data Link, 3-Network, 4-Transport, 5-Session, 6-Presentation, and 7-Application. The premise behind the model is that communication cannot exist across a layer if the layers below it have not been established. For example, communication at the Network layer cannot exist without successful implementation of the Data Link and the Physical layers. The standard form of the OSI model and a brief discussion of the layers are given below:

OSI Model



Layer	Description
7- Application Layer	This layer provides the end user interface to services. This is where applications such as E-mail, terminal emulation, database display modules, etc., reside. (DCS)
6- Presentation	This layer performs the translation of data to isolate the lower layers of the model from the application layer. It is in this layer that “raw” data is transformed into a “readable” format. (DCS)
5- Session	This layer organizes and synchronizes the exchange of data between application processes. It is in this layer that timing and flow control are established. (DCS)
4- Transport	This layer provides the mechanism for transparent transfer of data from the source to the destination. This layer also ensures that the data sent matches the data received. (PDN)
3- Network	This layer provides the physical routing of the data, and determines the physical path between the source and destination. (PDN)
2- Data Link	This layer controls the transmission of data frames. This layer is responsible for correcting errors that occur in the actual transmission of the data (i.e., errors resulting from magnetic interference or faulty cabling). (PDN)
1- Physical	This layer is made up of the physical infrastructure (i.e., cabling and cable connections). (PDN)

The OSI model has been in existence since the late 1970's and is still embraced by the computer world as the basis for network design and implementation. The model has been very successful in accomplishing its initial task of providing the framework for systems interconnection and integration. Taking a closer look at the model it can be seen that the premise behind OSI can easily be applied to the implementation of an integrated information and control network at PDN. As noted above various layers are identified as being performed by the components contained in the DCS or components contained in the PDN. In general the first four layers of the model are supported by the PDN equipment, and the upper three layers are provided by the DCS equipment.

Using the OSI premise of a layered approach for the information exchange model at PDN, the following is a discussion of the layers that are required for implementation of an integrated system:

Note: The following discussion builds upon the principles of the OSI model and is intended to provide a successful “operational model” for PDN. Although the OSI model was used as the basis behind this business model, an exact interpretation or correlation to each OSI layer may not apply.

1.) Communications Infrastructure

The first layer in the PDN model is the Communications Infrastructure. Similar to the OSI model, PDN must have an effective physical layer to form the foundation for all communications in the plants. A PDN, this consists of the cabling infrastructure, included in the PDN design. It is at this layer that the physical connections are provided for those individuals or systems that are providing or receiving information.

2.) Design Redundancy/Resiliency

The second layer of the PDN model is tied very closely with the 1st layer (Communications Infrastructure). This layer will ensure that the physical design of the information exchange system is based on principles that provide for a system that is fully resilient. This provides assurance that all data that is transferred between systems will be received correctly. An example of this layer is to provide two physically separate routing paths from a mission critical server to system operators.

3.) Network

The third layer in the PDN model is the Network Layer. This layer will provide the infrastructure for the electronic routing of the data to be shared. It is at this layer that the “network” of electronic components such as the Core and Zone switches, Firewalls, and Gateways will be designed and installed to perform the actual routing of data. This layer cannot exist without the Communications Infrastructure layer and must employ the principles that have been established in the Design Redundancy layer.

4.) Data Management

The fourth layer of the PDN model is the Data Management layer. This layer will effectively manage the transfer of data between systems and/or users. It is in this layer that the priority and access rights of systems and users will be established. This layer will ensure that those with top priority and the correct authorization have first access to the required data and those systems without authorizations are refused access. Also, it is at this layer that all users of the system shall be defined. At this level the components that are the DCS are connected to the network. The controllers, I/O, and workstations have their network configurations specified and become an operational part of the network. Some functions such as base level network security are still accomplished by the PDN components.

5.) Communications Standards

The fifth layer of the PDN model is the Communications Standards layer. This layer will establish the rules for communication between users and/or systems. At this layer, the format for data exchange must be standardized. Standards must be established which meet all individual needs and which allow for efficient data transfer between systems. It is in this layer that protocol standards such as TCP/IP are established.

6.) Software Standards

The sixth layer of the PDN model is the Software Standards layer. This layer will establish software standards for providing services to the end users. This layer will be closely coordinated with the Communications Standards layer to ensure compatibility. The standards that will be established will be applicable to both “off the shelf” software packages, and customized software as required to provide information and control to all plant components required to share information. One of the most critical decisions for design at this level is the selection and standardization on the database access method to be used for the network based storage.

7.) Integration

The seventh layer of the PDN model is the Integration layer. It is at this layer that the software and communications standards that have been developed in layers 5 and 6 are utilized to provide shared information to all that require it. This layer will provide the capability of such things as allowing an authorized employee in the maintenance department to be able to view equipment history versus current operational parameters as well as providing customizable displays to operators in the control room. This layer will also specify the type of user interface that must be present for end user applications (i.e., graphical user interface such as Windows). Training and documentation are additional factors that affect the overall system; therefore, they have also been included in layer 7. It must be noted that to achieve this layer, all the layers below must first be established.

Physical Network Design Requirements

To provide the reliability required of the DCS and other systems that will utilize the PDN for communications a few basic design requirements must be met.

- Where possible the connecting cables should be fiber optic. This provides total electrical isolation between various components increasing overall network reliability.
- All critical connections should have redundant cable paths available. This basic design requirement is identical to other electrical systems design requirements in an industrial environment. The separate cable, routed through separate paths, provide physical security as well as supporting protection against failure of electronic components impacting network operations.
- When design the basic PDN growth assumptions should be made that prevent the need to install additional cabling. One of the major costs of the PDN is the labor associated with installing the cabling. Installation of

excess cable, Dark Fiber, minimally increases the cost of the overall project and ends up being a cost savings as subsequent projects require additional fiber. A minimum of 25% additional fiber should be designed into the PDN backbone.

Network Electronics Requirements

Network electronics handle the actual communication routing between the individual devices utilizing the PDN. Historically, communication processes were controlled by the computers actually being connected to each device. This was an expensive option and severely limited the capabilities of the DCS and other systems. In newer designs the network communications are relegated to routers, switches, and hubs. Each of these devices is designed to control communication between network devices and allow management of the overall communication process.

As with all network technology the routing equipment has advanced and multiple vendors supply industrial grade equipment suitable for the PDN.

The network electronics selected for the PDN should be selected based on standard engineering design practices that include the following requirements.

- All network communication should be switched. This is the best overall method for controlling network communications based on the utilization of the PDN and the reliability requirements. A switch electronically connects the devices connected to it as required. Each connection creates a separate electrical path for the signal. In a hub, the other possible choice, each signal must compete for the available routing resources in the hub. This competition results in collisions between data transmissions that reduce the overall network performance and introduce a potential failure point if a single device begins transmitting continually, referred to as a network storm.
- All switches must be capable of Layer 3 routing. A network is made up of two components, the physical and logical. The physical network is defined by the cabling, switches, and other devices that are installed. The logical network is the configuration of method in which the devices are identified. A basic logical definition is with the protocol that is used to control the communication between devices. All protocols have limitations that define the members of a network and communication to another network requires a standardized method to move individual communication packets between the networks. This function was historically performed by a router. Routers are specialized devices that are optimized for connecting different logical networks. The PDN will be composed of multiple logical networks to enhance performance and reliability so will require routing. Current technology switches can act as a router in this type of design. By allowing the switches to perform the

routing process a separate piece of equipment isn't required reducing the overall cost of the network.

- All switches must support VLAN technology. A VLAN is an individual network that is created within a switch using a logical separation process. A device on the PDN can be assigned membership in one or more VLAN groups. Each group functions as a separate network even though the same physical cabling and switches are used. This capability enhances the security and performance of the network. An additional benefit is a dramatic increase in the flexibility of the network, often resulting in a cost reduction on future projects.
- All switches must be capable of being remotely managed. A modern complex network requires management just as any other complex system. If the switches have the capability of being remotely managed this function can be almost totally automated, requiring operator intervention only in the event of a detected problem. The management capabilities conform to established international standards through RFC, IEEE, and other documents.

Network Reliability

The measurement of network reliability has changed as networking technology has advanced. Older style measurements were based on the estimated Mean Time Between Failure (MTBF) of the individual network components. This measurement is still considered in the design of networks when individual components are selected, as in any other engineering process. The draw back to this measurement is that it can not analyze the logical component of the network. To address this limitation most designers expressed network reliability in terms of percent availability. Typically reliability is expressed as 99 plus some numbers of nines (99.9999) percent availability. This measurement was better, but in the basic network design utilized by the PDN it is not an accurate measurement.

The PDN utilizes a design that provides redundant routes and automatic load balancing and switching between these routes. To effectively express the reliability of a network of this type a new measurement approach must be used. The best approach is utilization of a probability based method that recognizes the flexibility of the network. In general the designer must define the types and numbers of failures that would result in the network being unable to perform its function. A basic statement is that no single failure will result in loss of full network function to an identified critical component.

To implement this approach the following design requirements are set for the PDN.

- All switches, switch operating systems, and network cards must support automatic transfer on failure and traffic load balancing.

- Individual devices that are determined to be critical must have redundant connections to the PDN.
- The overall network logical design must have sufficient separation to preclude a network storm from impacting both routes for any device.
- All routing devices must be capable of providing packet level performance data to the network management system through standard processes such as open MIBS.
- All routing equipment shall have redundant power supplies capable of individually powering the device, powered from separate secure power sources.
- Where possible all blades and power supplies on the routing equipment shall have the capability of being hot-swapped.

Network Security

There are two aspects to network security on the PDN, internal and external. Internal security deals with an attack from a careless or malicious user that has access to the physical devices on the PDN. The basic PDN supplied security is the capability of limiting functions to specific devices with the VLAN process. As an example a potential attacker plugs a laptop computer into the PDN at a remote point and attempts to access one of the main computers. The port the attacker is attached to is not configured as a member of the VLAN that the main computer exists in so access is denied at the switch level. In addition the network management system notices the attacker's attachment and alarms.

External security addresses the same attacker attempting to access the PDN from an outside network through a connection between the PDN and other networks. Security for this attack is provided by a firewall. Firewalls are basically specialized routers that limit the types of communication that is allowed into and out of a network based on a set of rules that the network owner specifies. A typical firewall configuration allows all traffic to leave a network but only traffic in specific response to an outgoing request to come back into the network. If desired a firewall can allow specific requests from outside the network to be sent to specific targets inside the network. This allows services such as Web servers or others to be made available but still protected to the greatest extent possible.

Requirements for the PDN firewall include:

- The firewall must be firmware based. This type of firewall is typically more efficient and has historically provided a greater level of security.

- The firewall must allow user defined access rules.
- The firewall should support a DMZ. A DMZ is basically an intermediate security level between the external network and the PDN.
- The firewall must provide intrusion detection capabilities and alarming to the network management system.
- The firewall must allow multiple network connections.