ETHERNET NETWORKS REDUNDANCY WITH FOCUS ON IEC 61850 APPLICATIONS

Rene MIDENCE
RuggedCom Inc. – Canada
ReneMidence@ruggedcom.com

Dominic IADONISI
RuggedCom Inc. – USA
DominicIadonis@ruggedcom.com

ABSTRACT

Today Ethernet is the predominant networking technology used in office and home environments. Because Ethernet networks are inexpensive and fairly well understood, their use is quickly becoming popular for industrial and utility applications including substation automation networks. A variety of flexible network architectures offering different levels of performance, cost and redundancy are achievable using managed Ethernet switches. This article looks at considerations when designing an Ethernet network for substation automation applications which may include IEC61850 Station or Process bus or a combination of both, with focus on redundancy. With Ethernet based networks and protocols, redundancy is needed to maintain maximum uptime and still be able to deal with minor outages and failures to the environment. This all gets rolled into the reliability of the entire system, from the very edge devices, through the network core, to the plant backbone. Understanding the relationships between the physical structure of a network and the protocols that run on the network is key to creating a truly maintainable and adaptable network that deals with issues effectively.

INTRODUCTION

The three main areas for Ethernet-based controls redundancy are physical, data link and network as show in Figure 1 below. The lower you look at the OSI model, the greater the impact of failures that occur. For example, if you lose a cable connecting an end device to a switch port, there is no data movement of any kind and there is an impact for the entire process, depending on the importance of that end device.

If there is an issue at layer 3 where a router may have experienced a loss of power and loses connection to the plant backbone, localized plant processes can still operate, but operation for distributed plant or business processes can be affected.

IEC61850 PROCESS - SYSTEM DESIGN

One of the most important functions of the substation automation system is the protection function. The majority of large Utilities design their protection with two independent protection systems called Protection A and Protection B. With a conventional protection and control systems, this is normally achieved by means of two protection relays, usually from different manufacturers that are individually connected to the process equipment.

The same level of redundancy needs of course to be achieved when designing an Ethernet network that will be used for IEC 61850 applications. That requires the duplication not only of the IEDs in the process equipment but also the communication system. This is considered in the architectural considerations for the use of IEC 61850 as process connection.

Substation automation consists commonly of three levels:

1. Station Level which may include a Human Machine Interface (HMI) and possibly a gateway (GW)
2. Bay Level consisting of protection and control IEDs
3. Process Level near the switchyard which includes instrument transformers, breakers, etc.

At each level, IEC61850 capable devices are connected to a communications network. The basic assumption is that this network is based on Ethernet switches that facilitate the distribution of functions and information to more than one IED. At the process level there are some real time requirements in addition to the station level requirements typically needed for operations and supervision.

BASIC COMMUNICATION ARCHITECTURES

The communications network may be one of the following:

1. Star Connection
2. Ring
3. Star or Ring Redundant
4. Multiple Redundancy

The overall Substation Automation system redundancy depends not only on the redundancy of the communication system but also on the IEDs, especially on the number of parallel communication ports determining the number of possible links to the switches.
IEC61850 IN REAL TIME

In a substation designed following IEC61850 standards, the information exchange between the process equipment and the substation automation is subject of high requirements regarding the real time behavior. The most critical information exchange is the one related to protection i.e. the transmission of the sampled values from the instrument transformers to the protection relay and the transmission of the trip command from the relay to the circuit breaker or transmission of interlocking commands between relays (peer-to-peer communications). According to IEC 61850-5, the acceptable maximal communication delay is for the highest class as few as 3 ms. This has to be achieved independent from the load of the communication network.

The communication stack for client-server communication specified in the mapping defined in IEC 61850-8-1 (Station Bus) and IEC 61850-9-2 (Process Bus) is MMS over TCP/IP and Ethernet. Ethernet as known from the office environment would not fulfill the requirements of a process connection. However, trends to use Ethernet as well in substation automation have lead to the development of Ethernet extensions that provide real time capabilities. IEC 61850 is using switched Ethernet to avoid collisions. The time-critical-messages are not routable and are directly mapped on the link layer. With the additional use of priority tagging and full duplex connections to the switch for the devices with time critical information, the real time requirements can be fulfilled.

Figures 2, 3 and 4 show typical network topologies used in Ethernet networks servicing IEC61850 Station Bus implementations. In these networks, the IEDs are connected to a Human Machine Interface (HMI) or Gateway (GW) via new generation of Ethernet switches designed to meet the requirements of the standard.

PROCESS BUS REDUNDANCY

Possible process bus architectures are determined by the fact that the protection could be redundant (Protection A, Protection B) at least at the transmission level of the power system. Any new solutions or advances in technology are expected to preserve this possible redundancy. Redundancy at Control level is not normally implemented however it can not be consider typical.

An architecture fulfilling this requirement could be described as follows (refer to Figure 5):
- Bay protection units (IED1 & IED3) own independently from each other a process communication system with a switch
- Bay control unit (IED2) is connected to both switches for operation in conjunction with the protection units by means of possibly GOOSE messages
- Merging units (MU1 & MU2) as source of current and/or voltage according to IEC 61850
- Breaker IED (IED4 & IED5) representing the breaker controlling device, also the source of commands (trip or close)
- The station bus connectivity may be single or doubled.
SIMPLIFYING THE COMMUNICATION ARCHITECTURE

According to Figure 5 with the dashed part the redundant station bus and redundant process bus together require 4 switches per bay. By combination of the process bus and the station bus switches, their total number is reduced to 2 per bay (Figure 6). The segregation of Process and Station Bus traffic may be achieved by means of virtual local network (VLAN) as standard means of the Ethernet technology.

The combination of both Process Bus and Station Bus networks is conceivable and acceptable due to the further economic benefits it provides. However, the architecture of the network must be chosen such that it renders the highest availability possible. The following sections will focus on considerations of redundancy in the Ethernet network architecture design, with the objective of ensuring maximum network availability when the same will be used with IEC61850 in mind.

PHYSICAL REDUNDANCY: MORE THAN JUST THE CABLING.

Physical redundancy covers the physical Ethernet network connections (and control system equipment) AND the physical hardware the connections go between (the Ethernet Network). Network redundancy focuses upon the multiple routes that can be used between edge devices. Physical redundancy normally follows two scenarios:

1. Diverse routing of cabling- installing cabling in diverse conduits to prevent the total loss of connectivity if the conduit is damaged
2. Redundant hardware- having multiple connections on a controller or other hardware allows the controller reliable connectivity in cases where a connection or port has suffered a failure. This also involves having redundant network hardware in case of failures, including multiple power supplies, multiple CPU cards on controllers, etc.

When looking at redundancy for the Ethernet network, one need to first look at the application and the area of coverage, including the number of devices that are attaching to the Ethernet network. Answer to the following questions is required:

- Are they grouped according to location and function?
- Application performed?
- Device type?
- Will there be a requirement to connect to the existing Substation Backbone network?

Based on this knowledge you can begin to put together a picture of how the Ethernet network will look like and what the number of ports will be on the Ethernet switches that will be put in those areas. This is needed to determine number of cables, physical routing of the cables, and location of network nodes to connect the cables, and so on.

A popular way to look at system connectivity needs is the Zone/Cell view where you have a Zone of control divided up into functional Cells. Refer to Figure 7.

Looking at Figure 7, assuming that each line is a single cable connection, it would be very easy to isolate sections of the process with the loss of just 1 or 2 cables. At the physical layer, it is important to plan out redundant connections to devices that can support multiple connections. Many devices only have one data interface, but the Ethernet switches they connect to have multiple ports to support connections to other switches, forming redundant paths and being able to work around port and cabling failures.

Once the connection of devices to the network has been decided, the next decision is the level of redundancy required to achieve maximum system uptime. This implies evaluating the cabling and Ethernet network hardware needs. Then, more questions need to be answered:

- Do we need redundant cabling between devices?
- Is it going to be redundant cable installation?
- Does it require physical segregation of the cabling?
- Is there more than one Ethernet interface on the device to be used (many controllers have multiple Ethernet interfaces in case of Ethernet port or module failure)?
DATA LINK LAYER REDUNDANCY

Ethernet switches in the network can be used to provide protocol redundancy and maintaining Ethernet network health. Layer 2 Redundancy protocols do two things: Identify all the possible paths amongst the networking devices and place the redundant extra paths in a blocking state to remove network loops. Loops in an Ethernet network cause data duplication and will bring a network to a quagmire. If a network segment becomes unreachable, spanning tree reconfigures and reestablishes link by activating the “Blocked” links.

Ethernet networks have redundancy protocols that are supported by identified Ethernet standards. These are supported in Layer 2 and Layer 3 of the OSI model. First we will look at Layer 2:

Standard Layer 2 Network Redundancy Protocols:

1. **Spanning Tree** - There are several flavors of Spanning Tree.
   a. STP (Spanning Tree Protocol) - Standardized in 1996 as IEEE 802.1D, it is the first and slowest of the Spanning Tree protocols. Average failover time for STP started at 30 seconds and went up. Way too slow for any industrial Process. Next came…
   b. RSTP (Rapid Spanning Tree Protocol) – Currently standardized as IEEE802.1D 2004, it is an evolutionary leap for STP. It is more rapid, with failover times from about 250msec to up to 12 seconds, so it was better than STP. Still an issue with the speed of failover for Industrial processes.
   c. MSTP (Multiple Spanning Tree Protocol) - Originally standardized as IEEE 802.1s and then incorporated into IEEE 802.1Q 2003, it allows multiple instances of Spanning Tree Protocol per Virtual LAN. This means that in a single physical network, there can be multiple virtual network groupings, each with their own instance of Spanning Tree Protocol.
   d. There are proprietary implementations of Spanning Tree that are optimized for use in Industrial Networks. They are based upon standard RSTP, but are not designated as a standard STP protocol.

2. **LACP (Link Aggregation Control Protocol)** - This protocol allows the user to configure multiple Ethernet ports between Ethernet switches into a Single virtual “Link”. This allows load sharing of information between the links and is extremely fast in moving data between a failed port and an adjacent port if there is a link failure. The amount in interconnections amongst the network elements dictates the amount of failures the network can take and still maintain the process. Refer to Figures 8 showing an example of these protocols.

Spanning Tree is a redundant topology in that it provides network redundancy instead of just path redundancy while preventing loops in a network. For Ethernet to function properly, only one active path can exist between devices. To provide redundancy, Spanning Tree relies on having multiple paths or connections to different switches and configures some of these paths into standby (Blocked) state. If a network segment becomes unreachable, spanning tree reconfigures and reestablishes link by activating the “Blocked” links.

**Figure 8 - Example of a Spanning Tree Ethernet Network**

Link Aggregation Control Protocol or LACP (IEEE 802.1ad) provides redundancy without the use of Spanning Tree. It enables users to be able to bundle groups of ports between switches to form 1 virtual link with the bandwidth of the member links. LACP provides several functions:
- Higher bandwidth
- Enhanced Bandwidth Granularity
- Load sharing across the member links to balance bandwidth across the member links
- Fault tolerance provided by offloading data to working member links when a member link fails

**SUMMARY**

Understanding the relationships between the physical structure of a network and the protocols that run on the network to provide is key to creating a truly maintainable and adaptable network that deals with issues effectively. Considering the basic communication architectures discussed above, for switches with reasonably high availability the ring is an acceptable and economical, i.e. a suitable solution. The reconfiguration time is a critical issue for safety suggesting that the Ethernet switches shall be chosen with fastest rapid spanning tree. This is a critical factor when the network will be the carrier of mission critical information such as GOOSE messages between IEDs. If higher availability is needed, doubled communication networks are recommended, which however need special handling at protocol level to run them in parallel. In HV substations, all bays are protected by redundant protection (Protection A, Protection B). Therefore, the related process bus has to be doubled by definition to avoid a single point of failure. Sharing the process bus switches with station bus connectivity reduces the number of switches and communication ports.