Station Integration for Reduced Costs and Improved Operational Efficiency

Ryan McMahon and Bill Winters
Con Edison (ConEd)
New York, NY

Cesar Guerriero and Farel Becker
Siemens
Wendell, NC

Abstract—Multi-vender protection and control integration has been performed in demonstration projects to show protocol capabilities, but rarely to provide a comprehensive station protection and control system. A new station, feeding power to lower Manhattan, provided an opportunity to use modern communications to reduce costs while providing advanced capabilities. This ConEd substation project applied the IEC 61850 protocol to provide a high reliability peer-to-peer network across fiber optic.

Index — Computer Network Reliability, Ethernet Networks, IEC61850 Standard, Substation Automation, Substation Protection.

I. INTRODUCTION

This paper will show how IEC 61850 provides greater flexibility for design implementation compared to a hardwired approach. Additionally, state-of-the-art cyber security tools were implemented to enable user compliance to NERC CIP standards.

The paper will describe design techniques and best engineering practices to avoid communication delays due to network routing and congestion. Field test results of the network traffic will be presented to support the understanding that when properly designed, a non-deterministic network can guarantee reliable data delivery for control and protection applications, therefore withstanding the effects of a “GOOSE Storm.” Also presented is a network design criteria for preventing Ethernet GOOSE messages from traveling outside the substation bus network. Various network design techniques are described which segmented the communication system in order to separately test the GOOSE messages within protection schemes. Considerations are taken into account to assure the system will operate without impacting the substation standard maintenance and testing procedures.

The ConEd substation uses an advance protection scheme with both GOOSE as well a conventional protection scheme. With the hesitation of the electrical utilities industry to migrate from a conventional protection scheme to an advanced IEC 61850 based GOOSE protocol protection scheme, this paper represents a good example of the interaction of conventional and GOOSE protection schemes in terms of system integration, HMI, testing and maintenance procedures.

As part of the integration process, Siemens and ConEd designed, manufactured, tested and commissioned a substation automation system with a redundant remote terminal unit (RTU) and Human Machine Interface (HMI). A special requirement requested by ConEd was the development of an advanced alarm processing system designed specifically for the utility’s substation operations.

It was important to ConEd that the system had the same look and feel that the operators were accustomed while also keeping the same standard ConEd testing and maintenance philosophy of the other conventional systems. These system enhancements accurately reflect data viewed at both the control center and substation but do not require the use of any special configuration tools and can be used by the operations staff without any special training. This and other features allowed for a savings of time and expense, helped with safety concerns and improved flexibility of the system.

The use of VLANs is an important aspect of designing reliable IEC 61850 networks. A VLAN is an Ethernet layer 2 construct that is comparable to layer 3 IP subnets. A unique VLAN ID is assigned to each GOOSE message which enables the switch to match a package to a specific set of port(s). Therefore a VLAN makes it possible to deliver GOOSE messages much faster. It is a method of partitioning a physical network, so that distinct broadcast domains or “tunnels” are created. In an IEC 61850 network it is sometimes used to control which ports specific GOOSE messages go to, to avoid sending more messages to a “slower” relay then it could possibly handle.

II. ETHERNET NETWORK CONCEPT OVERVIEW

The Ethernet standards comprise several wiring and signaling variants of the OSI physical layer in use with Ethernet. The original 10BASE5 Ethernet used coaxial cable as a shared medium. Later the coaxial cables were replaced by twisted pair and fiber optic links in conjunction with hubs or switches. Data rates were periodically increased from the original 10 megabits per second, to 100 gigabits per second. Systems communicating over Ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination addresses and error-checking data so that damaged data can be detected and re-transmitted. As per the OSI model Ethernet provides services up to and including the data link layer. The model was developed by ISO
(International Standards Organization) and OSI (Open Systems Interconnection). Fig. 1 demonstrates the model applied to the Internet as an example.

Services are a set of operations. It is a vertical communication where the lower layer is the provider and the higher layer is the user. Protocols are set of rules. It is a horizontal communication which controls the format, packet meaning or messages. The protocol stack is an implementation of a computer networking protocol suite. The terms are often used interchangeably. Strictly speaking, the suite is the definition of the protocols, and the stack is the software implementation of them. Fig. 2 shows the complete layer 7 stack structure, where:

- HTTP – HyperText Transfer Protocol
- MMS – Manufacturing Message Specification
- TCP – Transport Control Protocol
- IP – Internet Protocol

Multicast is the delivery of a message or information to a group of destination computers simultaneously in a single transmission from the source.

Unicast messaging is used for all network processes in which a private or unique resource is requested.

Broadcast is transmitting a packet that will be received by every device on the network. In practice, the scope of the broadcast is limited to a broadcast domain. Broadcast of a message is in contrast to unicast addressing in which a host sends datagrams to another single host identified by a unique IP address.

III. CONCEPTS OF THE IEC 61850 STANDARD

According to the IEC 61850 standard the network LAN of a substation is divided into two parts. The first domain is the process bus, which consists of the interface of the process equipment at the instrument transformer level, such as breakers, switchgears, and digital protection relays. The second domain is the station bus which consists of the interface of the digital protection relays and the supervision equipment, including HMI and SCADA.

The IEC 61850 standard defines the three protocols for communication between the Process Bus and Station Bus:

- **Samples Values (SV)** are messages with stamps of the frequency (50 or 60 Hz) to build the phase vector (phasor) together with the amplitude of the measurement. This type of message is horizontal and it is used in the Process Bus level between IEC 61850 Servers. The protection intelligent electronic devices (IED) will use the current and potential transformers information to execute the protection algorithms. These messages contain phasor measurement magnitude data.

- **Alarms/Reports / Event Logging** are messages which are vital to the operation of the substation.
This message type contains all of the necessary information for supervision of the point. This type of message goes in the Station Bus between the IEC 61850 Client and Server, and the communication protocol used is MMS (Manufacturing Message Service). This is usually located between the control/IEDs and supervision systems, as HMIs and SCADAs.

- **GOOSE (Generic Object Oriented Substation Event) protocol** aims to replace the conventional hardwired logic necessary for intra-relay coordination with station-bus communications.

Upon detecting an event, the IED uses a multi-cast transmission to notify those devices that have registered to receive the data. The performance requirements are stringent – no more than 4 milliseconds is allowed to elapse from the time an event occurs to the time of message transmission. The number of IEDs, the network topology and the type of event will all contribute to the amount of data that will be generated after an event.

Collisions are quite possible in an Ethernet network in this scenario, so the GOOSE messages are re-transmitted multiple times by each IED. Three LAN configurations (10 MB switched hub, 100 MB shared hub, and 100 MB switched hub) are able to deliver 100 messages within 4 milliseconds. This architecture guarantees the speed, avoiding the degradations of a layer three network (Network Layer), used in WANs. GOOSE messages are digital or analog signals which contain Boolean or float point values.

The use of the GOOSE messages service of IEC 61850 is most often for protection and automation of electric systems. In this application they communicate horizontally and travel peer to peer between IEC 61850 servers, also called IEDs. At this level they pass commands and status data between breakers/switchgears and the IEDs which will execute the control/protection algorithms. Fig. 4 demonstrates how the services defined by the standard are applied to the ISO/OSI model.

**IV. NETWORK ARCHITECTURE**

The network designed for this substation includes redundant Ethernet switches connected in a Gigabit Fiber Optic Ring. The protection devices are connected in each one of the redundant Ethernet switches via fiber optic making a double star connection between switches and these devices.

Also the Redundant Data Concentrator (called RTU) is provided with two Ethernet channels each where each one of these channels is connected to one of the redundant switches. This system architecture is completely immune to a single point failure.

The Redundant Data Concentrator collects data at same time from all devices, called a hot-hot system, where both Data concentrators have updated information from the devices which are communicating with and provides this data to redundant control centers and Local HMIs. Everything is synchronized by redundant GPS clocks.

The ConEd substation network consist basically of 40 protection devices, 5 Revenue Meters, 14 Ethernet switches, 2 Data Concentrators, 2 HMI Servers, 3 HMI Viewers and 2 GPSs. Also connected are 3 Auxiliary systems including fire protection, emergency diesel generator and building Management, as well as 29 merging unit devices connected to CTs/VTs installed in the substation yard. Fig. 5 shows the network diagram designed for the ConEd substation.

**V. APPLICATION DESCRIPTION – PROTECTION, CONTROL AND SUPERVISION SCHEMES**

This project is a 345 kV substation owned and operated by ConEd. It consists of an 8 breaker ring bus with 2 transformers, 2 reactors, 4 incoming lines and 1 generator feeder. Future expansion is planned to expand to a 12 breaker ring bus. The project included the coordination with two adjacent substations and monitoring of other site systems.
through the substation automation system. Fig. 6 shows the overview single line diagram:

![Figure 6 – Single Line Diagram Overview](image)

**Protection Scheme** – There are two redundant and independent lines of protection. The primary protection is hardwired (conventional) and the secondary uses IEC 61850 (GOOSE Messages) for protection. The primary line is hardwire connected to CTs, VTs, transformers, breakers, motor operated disconnect switches (MODs) while secondary line VTs and CTs are connected via Fiber Optic cable. The network designed for this substation made it possible for the final user (ConEd Operation and Maintenance personal) to keep their standard testing and maintenance procedures for different protection schemes (Conventional and GOOSE).

Types of protection includes: Overcurrent (50/51), Breaker Failure (50BF), Transformer Differential (87T), Busbar Differential (87B), Differential Line (87L), Reactor Differential (87R), Distance (21) and Directional (67).

On the secondary protection side, GOOSE messages are being used for the breaker failure initiation scheme and transfer trip. A flexitest switch, also used on the primary protection side, blocks the protection activation and isolates this relay from another protective relay if the flexitest switch is opened during test/maintenance. This way, GOOSE messages are also blocked, making it possible for testing/maintenance of single relay in an integrated protection scheme.

In addition to blocking GOOSE messages by a test switch, the use of VLANs enable testing of the entire protection scheme without having to disable any protection functions – for instance, testing of the distance function (21) without having to disable the line differential function (87L) which is in the same relay. In this case both the 21 and 87L functions are separate data items inside of the same GOOSE message frame and isolated further in a test VLAN. This method of testing a single protection element is possible by programming the AC injection equipment without changing the settings on the relay. This made it possible to perform testing and maintenance on a GOOSE protection scheme the same way the user is familiar with a conventional protection scheme.

**Control Scheme** – Breakers, Circuit Switches, Motorized Disconnects are controlled by 3 different levels:

- Local control at protection panel
- Local HMI at the substation in the control room
- Remote SCADA system via protocol communication serial DNP3 outside of the substation.

If the key switch is set to LOCAL, operations can only be initiated directly at the protection panel. In REMOTE position, control is only possible from higher levels as shown in Fig. 7. The key cannot be removed unless the key switch is in the REMOTE position.

![Figure 7 – Switching Control Authority Hierarchy](image)

An additional control feature was implemented as a special logic function, namely “Breaker Control Failover Logic.” It ensures that a breaker close or open command will be executed either by the relay protection or by the Data Concentrator in case the protection relay and/or merging unit fails. This is accomplished by developing logic in the data concentrator automation system (soft PLC) and remote I/O controller.

**Supervision Scheme** – This ConEd Substation is provided by a Local HMI system. For an efficient operation, a large amount of information needs to be handled and displayed quickly and clearly. At all times the station status is precisely displayed and recorded. Essential indications along with measured and metered values are archived, so that individual analyses in chart or table format are available at any time.
The controls via HMI follow the preconditions:

- The operator is authorized, for example, by logging in at the HMI via the combination of user and password.
- The switching authority is set to LOCAL/REMOTE.

The following measures increase the safety of the operator action at the HMI:

- Secured data transmission between the HMI and the substation controller
- Release only if operation authorization and switching authority exist
- Two-Stage Switching, where the confirmation must be given by the operator
- The window for command input closes automatically if the admissible time for operating equipment has been exceeded.

ConEd had a special requirement for local HMI that all the alarming processing must reside on the Data Concentrator or RTU. This way, in case of HMI failure, the Data Concentrator or RTU can still transmit alarm status to upper level of the ConEd SCADA system. The communications to the SCADA system only transmit a summary of alarms, grouped in categories. These categories should not depend on the local HMI – that is the main reason the Data Concentrator or RTU should process every single alarm as well its acknowledgement.

Another requirement was to provide fast alarm trouble detection. To meet this requirement, the alarms are grouped in small groups on the local HMI screen. These smaller groups imitate conventional annunciator tiles on the digital annunciator panel that are part of local HMI screens. This way, when the ConEd SCADA system receives an alarm group signal, the local operator can further determine the specific problem and notify the proper maintenance team. Fig. 8 below is an example of the alarm annunciator for HMI.

VI. NETWORK DESIGN TECHNIQUES AND BEST ENGINEERING PRACTICES

This project incorporated the use of several network design techniques to avoid data collisions and congestion including:

GOOSE Message Validity and Delivery – The IEC 61850 standard defines a mechanism of how GOOSE frames are exchanged between devices in the network. An event is sent cyclically every period, predefined as Tmax. The moment the status changes, the GOOSE message is sent immediately, switching from cyclic to spontaneous. The GOOSE frame starts to repeat at a predefined minimum time called Tmin. The repetition period is decreased until the Tmax. (N spontaneous repeats t = 2^N*Tmin). When the repetition time reaches Tmax again, it switches from spontaneous to cyclic.

In case the transmitter device does not send anything, this waiting time is bigger than a predefined time called TimeAllowedToLive, in most cases 1.5 times bigger than Tmax. The receiver waits for TimeAllowedToLive before invalidating this signal.

Mathematically, by repeating the same message in a short period of time, it will ensure delivery of the message. Besides, the receiving device verifies the message quality and checks if the transmitter device is there by usage of the TimeAllowToLive parameter.

Each frame sent by the transmitter devices is tagged with a number that increases every repeated frame. It is called Sequence Number. Every time there is a status change, when the transmitter device switches from cyclic to spontaneous, this new frame is also tagged with a sequential number that increases with every change. It is called State Sequence. To prevent frames from being lost, the GOOSE mechanism, shown in Fig. 9, uses the parameters Sequence Number and State Sequence where the receiver can reject GOOSE frames if it is out of the sequence. This mechanism is shown below in Fig. 9:

GOOSE Prioritization – The IEC 61850 standard allows for the prioritization of GOOSE messages over other Ethernet messages, thus allowing them to bypass the Ethernet data.
buffer. GOOSE frames use the extension of the layer 2 frame defined by IEEE called 802.1Q, as shown in Fig. 10. This frame extension has an extra parameter that defines priorities for Ethernet switches. Depending on the priority that is set, the switch will bypass a telegram buffer.

![Diagram of GOOSE frame](image)

**Figure 10 – GOOSE uses the 802.1Q Frame**

The parameter that defines the priority tag is called 802.1p. Fig. 11 shows GOOSE frames used to bypass the normal traffic.

![Diagram of priority tagging](image)

**Figure 11 – Priority Tagging of GOOSE Telegrams (Ethertype)**

By using only 2 layers from the ISO/OSI model, the GOOSE frames do not require the confirmation or connection of any other layer. GOOSE is a multicast message without connection or confirmation – that is why it is fast.

**Virtual LAN** – Commonly known as a VLAN, VLAN is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices. As indicated in Fig. 12, multiple devices can be connected at the same Ethernet switch, but logically in a different network segment.

![Diagram of VLAN segregation](image)

**Figure 12 – VLAN Segregation on a Network – RuggedCom Manual**

Depending on the type of GOOSE dataset transmitted, it can be attached to a VLAN priority. In all protection GOOSE messages, it is preferable to set VLAN priority to 0-2, which is a higher priority. For all other indications it can be set from 0-7 priority.

**Subnet Mask** is used to define a sub network of a larger network. It uses a mask to determine which subnet an IP address belongs. An IP address has two components, the network address and the host address. VLANs and Subnets are network segregation techniques that when used in combination will increase network efficiency. The subnet defines the LAN (Local Area Network), while VLANs are network segregation LOWER layer than subnets. Subnets are in layer 3 of the ISO/OSI model, while VLANs are in layer 2. Computers, such as HMI and RTUs, have IP addresses. That is why they need Subnets in order to separate networks from other equipment. On the other hand, GOOSE messages have no IP address – they are in the lower layer on the ISO/OSI model using only Multicast Addresses. To separate or contain these GOOSE messages in a certain area of the network, it is necessary to use VLANs.

**Network Switch Configurations** – Switches improve Ethernet performance by eliminating collisions. With Ethernet LANs playing such a critical role in protection and control systems, new standards such as IEEE 802.1W Rapid Spanning Tree Protocol, which are used to implement network redundancy and ring architectures, are of critical importance. If switches in the network are connected in a loop (Ring Topology) a “broadcast storm,” it will result in a single broadcast frame that will circulate endlessly. This condition consumes all available bandwidth in the loop making the network unusable. The Spanning Tree Protocol is used to prevent this situation.

A ring topology offers built-in redundancy and is often the most economical in terms of interconnection costs. Two popular methods of implementing rings are collapsed backbone and distributed switch. From the distributed switch a double star connection is conducted in order to interconnect to the devices.

A VLAN, as mentioned before, is a way of grouping switch ports together to create a separate logical LAN. This is useful for limiting the effects of broadcasts and providing some security at Layer 2, as each VLAN is given a numerical Identifier, and broadcasts cannot be forwarded between VLANs. Also, devices on one VLAN cannot
communicate with devices on another VLAN without a Layer 3 device such as a router.

The ConEd substation network design VLAN was used to avoid GOOSE frames going to other parts of the network, like HMI level, as well to avoid mixing GOOSE frames between different protection systems. VLANs in this project design were also used in order to create a separated logical network where the test equipment (AC injection equipment) is connected, making possible a protection test in a GOOSE protection scheme without having to disable or change any protection setting. Fig. 13 below shows the VLAN configuration for the ConEd substation.

VII. PROJECT REQUIREMENTS – TESTING OF PROTECTION GOOSE MESSAGES

In this ConEd substation project, by using segregation techniques described previously, the network usage is substantially reduced. As shown in Fig. 14, GOOSE messages and other captured packets (excluding TCP/UDP messages), were only 10% of the network capacity.

One of the project requirements was that all individual protection elements of the relays should be mapped to a published GOOSE message to allow an IEC 61850 test set to sense the individual protection element operations. This way, when testing a protection GOOSE scheme, the test set equipment (AC injection equipment) would be programmed to identify individual protection elements inside of the GOOSE data set and isolate the protection element to be tested without having to disable or change any protection setting. The secondary protection relays were programmed to send GOOSE data sets with each one of the protection elements, as well each one of the phases, as shown in Table 1.

This exceeds the requirements of Paragraph 3.6 of Appendix B of the NPCC D3 document dated July 11, 2008.

This requirement was achieved, besides GOOSE data sets with individual protection element, by creating a VLAN where all the GOOSE for testing proposes would be configured. Since GOOSE messages are multicast messages, a different VLAN was created to avoid GOOSE messages going to other places of the network which are not required, like the HMI level, as shown in Fig. 15:

In order to keep similar test procedures between primary protection (hardwire conventional) and secondary protection (IEC 61850 GOOSE messages) schemes, another requirement of this project was having a flexitest blade wired to a digital input on the relay to logically disable GOOSE messages going to other places of the network which are not required, like the HMI level, as shown in Fig. 15:
To prove that a network design can improve performance, avoiding network overloads, one of the tests in this project was to measure the GOOSE performance for a breaker failure (50BF) scheme. Field tests were performed by generating a reactor differential (87R) fault. The breaker was prevented from opening, thus initiating the 50BF function. The upstream breaker receives the 50BF initiate signal and trips. Below is the BF INIT signal sent by Reactor 16 (87R-2/R16) to initiate the breaker failure scheme:

**TABLE 2 – SEQUENCE OF EVENTS FROM REACTOR’S PROTECTION RELAY**

<table>
<thead>
<tr>
<th>Event Number</th>
<th>Event Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>2011-04-29T08:56:23</td>
<td>BF INIT Off</td>
</tr>
<tr>
<td>02</td>
<td>2011-04-29T08:56:27</td>
<td>BF INIT On</td>
</tr>
<tr>
<td>03</td>
<td>2011-04-29T08:56:30</td>
<td>TRIP LED Off</td>
</tr>
<tr>
<td>04</td>
<td>2011-04-29T08:56:33</td>
<td>TRIP LED On</td>
</tr>
<tr>
<td>05</td>
<td>2011-04-29T08:56:38</td>
<td>SC音响 TRIGGER Off</td>
</tr>
<tr>
<td>06</td>
<td>2011-04-29T08:56:42</td>
<td>SC音响 TRIGGER On</td>
</tr>
<tr>
<td>07</td>
<td>2011-04-29T08:56:45</td>
<td>BUS 1</td>
</tr>
<tr>
<td>08</td>
<td>2011-04-29T08:56:50</td>
<td>BUS 1</td>
</tr>
<tr>
<td>09</td>
<td>2011-04-29T08:56:55</td>
<td>BUS 1</td>
</tr>
<tr>
<td>10</td>
<td>2011-04-29T08:57:00</td>
<td>BUS 1</td>
</tr>
<tr>
<td>11</td>
<td>2011-04-29T08:57:05</td>
<td>BUS 1</td>
</tr>
<tr>
<td>12</td>
<td>2011-04-29T08:57:10</td>
<td>BUS 1</td>
</tr>
<tr>
<td>13</td>
<td>2011-04-29T08:57:15</td>
<td>BUS 1</td>
</tr>
<tr>
<td>14</td>
<td>2011-04-29T08:57:20</td>
<td>BUS 1</td>
</tr>
<tr>
<td>15</td>
<td>2011-04-29T08:57:25</td>
<td>BUS 1</td>
</tr>
<tr>
<td>16</td>
<td>2011-04-29T08:57:30</td>
<td>BUS 1</td>
</tr>
<tr>
<td>17</td>
<td>2011-04-29T08:57:35</td>
<td>BUS 1</td>
</tr>
<tr>
<td>18</td>
<td>2011-04-29T08:57:40</td>
<td>BUS 1</td>
</tr>
<tr>
<td>19</td>
<td>2011-04-29T08:57:45</td>
<td>BUS 1</td>
</tr>
<tr>
<td>20</td>
<td>2011-04-29T08:57:50</td>
<td>BUS 1</td>
</tr>
</tbody>
</table>

**BF INIT received by the device to execute BF on Breaker 16 (50/62-2/16):**

**TABLE 3 – SEQUENCE OF EVENTS FROM BREAKER’S PROTECTION RELAY**

<table>
<thead>
<tr>
<th>Event Number</th>
<th>Event Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>2011-04-29T08:56:23</td>
<td>BF INIT Off</td>
</tr>
<tr>
<td>02</td>
<td>2011-04-29T08:56:27</td>
<td>BF INIT On</td>
</tr>
<tr>
<td>03</td>
<td>2011-04-29T08:56:30</td>
<td>TRIP LED Off</td>
</tr>
<tr>
<td>04</td>
<td>2011-04-29T08:56:33</td>
<td>TRIP LED On</td>
</tr>
<tr>
<td>05</td>
<td>2011-04-29T08:56:38</td>
<td>SC音响 TRIGGER Off</td>
</tr>
<tr>
<td>06</td>
<td>2011-04-29T08:56:42</td>
<td>SC音响 TRIGGER On</td>
</tr>
<tr>
<td>07</td>
<td>2011-04-29T08:56:45</td>
<td>BUS 1</td>
</tr>
<tr>
<td>08</td>
<td>2011-04-29T08:56:50</td>
<td>BUS 1</td>
</tr>
<tr>
<td>09</td>
<td>2011-04-29T08:56:55</td>
<td>BUS 1</td>
</tr>
<tr>
<td>10</td>
<td>2011-04-29T08:57:00</td>
<td>BUS 1</td>
</tr>
<tr>
<td>11</td>
<td>2011-04-29T08:57:05</td>
<td>BUS 1</td>
</tr>
<tr>
<td>12</td>
<td>2011-04-29T08:57:10</td>
<td>BUS 1</td>
</tr>
<tr>
<td>13</td>
<td>2011-04-29T08:57:15</td>
<td>BUS 1</td>
</tr>
<tr>
<td>14</td>
<td>2011-04-29T08:57:20</td>
<td>BUS 1</td>
</tr>
<tr>
<td>15</td>
<td>2011-04-29T08:57:25</td>
<td>BUS 1</td>
</tr>
<tr>
<td>16</td>
<td>2011-04-29T08:57:30</td>
<td>BUS 1</td>
</tr>
<tr>
<td>17</td>
<td>2011-04-29T08:57:35</td>
<td>BUS 1</td>
</tr>
<tr>
<td>18</td>
<td>2011-04-29T08:57:40</td>
<td>BUS 1</td>
</tr>
<tr>
<td>19</td>
<td>2011-04-29T08:57:45</td>
<td>BUS 1</td>
</tr>
<tr>
<td>20</td>
<td>2011-04-29T08:57:50</td>
<td>BUS 1</td>
</tr>
</tbody>
</table>

Comparing the timestamps between the sender and the receiver device for 50BF scheme:

**TABLE 4 – GOOSE PERFORMANCE COMPARISON TABLE**

<table>
<thead>
<tr>
<th>IED SENDER</th>
<th>IED RECEIVER</th>
<th>Timestamp 1</th>
<th>Timestamp 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>87R-2/R16</td>
<td>87R-2/R16</td>
<td>Apr 29 2011</td>
<td>Apr 29 2011</td>
</tr>
<tr>
<td>87R-2/R16</td>
<td>87R-2/R16</td>
<td>08:56:23</td>
<td>08:56:23</td>
</tr>
<tr>
<td>50BF</td>
<td>50BF</td>
<td>08:56:23</td>
<td>08:56:23</td>
</tr>
<tr>
<td>50BF</td>
<td>50BF</td>
<td>08:56:27</td>
<td>08:56:27</td>
</tr>
</tbody>
</table>

Total Performance: 3.315 ms

**VIII. CONCLUSION**

The paper demonstrates design techniques and best engineering practices for reduced cost and operational efficiency when designing a substation automation system with Ethernet-based protection schemes. Design techniques, such as the use of VLANs and subnets to improve network performance, were implemented, tested and measured. Operational efficiency was enhanced by the implementation of a flextest scheme, control failover logic, separate VLAN for testing and digital alarm annunciator.

Field test results and the project design have demonstrated that a network protection scheme properly designed can guarantee reliable data delivery for protection applications, as well provide mechanisms for testing and maintenance, fulfilling utility company needs for better and more efficient operation.

This paper also has demonstrated the ability of the substation automation system to supervise and control both a conventional and Ethernet-based protection system. This duel engineering approach provides the utility with the ability to pilot the Ethernet-based protection scheme.

**REFERENCES**