Arc-Flash Protection System Design Revisited

Matthew Watkins, Neel Shah, and Anurag Upadhyay
Schweitzer Engineering Laboratories, Inc.

Nilushan K. Mudugamuwa
Tengizchevroil

This paper was presented at the 72nd Annual Petroleum and Chemical Industry Technical Conference, Dallas, TX, September 22–24, 2025.

For the complete history of this paper, refer to the next page.

Presented at the
72nd Annual IEEE IAS Petroleum and Chemical Industry
Technical Conference (PCIC)
Dallas, Texas
September 22–24, 2025

ARC-FLASH PROTECTION SYSTEM DESIGN REVISITED

Matthew Watkins
Senior Member, IEEE
Schweitzer Engineering
Laboratories, Inc.
101 E Park Blvd, Ste 1180
Plano, TX 75074 USA
matt_watkins@selinc.com

Nilushan K.
Mudugamuwa
Tengizchevroil
9 Stockbridge Rd
Fleet, Hampshire
GU51 1AR UK
nmgn@chevron.com

Neel Shah
Schweitzer Engineering
Laboratories, Inc.
2900 Horizon Dr, Ste 100
King of Prussia, PA 19406
USA
neel_shah@selinc.com

Anurag Upadhyay
Schweitzer Engineering
Laboratories, Inc.
2900 Horizon Dr, Ste 100
King of Prussia, PA 19406
USA
anurag_upadhyay@selinc.com

Abstract—Engineers have applied arc-flash protection schemes to medium-voltage switchgear or low-voltage motor control centers for years. Modern devices are now able to sense light, supervise it with an ultra-high-speed overcurrent element, and issue a trip signal to a breaker in as little as 2 to 4 ms. Schemes taking a main-tie-main configuration into consideration require communications between the light-sensing, current-supervising, and tripping devices. While simple to implement and test, this communications path makes it difficult to ensure reliability. If done incorrectly, it can be susceptible to network storms or other communications issues that impact the reliability and speed of the arc-flash protection system.

This paper highlights the performance of an arc-flash protection system applied to switchgear and motor control centers around the world. The paper reviews various communications system designs available to engineers today when applying an arc-flash protection system to main-tie-main schemes. Options discussed include point-to-multipoint serial communications and Ethernet network design—including single Ethernet; dual Ethernet with failover mode, with switched mode using Rapid Spanning Tree Protocol, with failover using Rapid Spanning Tree Protocol, and with Parallel Redundancy Protocol; and operational technology software-defined networking using industry standard peer-to-peer protocols. The paper discusses the advantages and disadvantages of each option including relevant details on Ethernet communications protocols and presents the method the authors recommend if implementing an arc-flash protection system on a new main-tie-main scheme.

Index Terms—Arc-Flash Protection, IEC 61850 GOOSE, Ethernet Communications, RSTP, PRP, SDN, Network Storms.

I. INTRODUCTION

There are numerous papers associated with arc-flash protection covering topics that include prioritizing safety, limiting equipment damage, and minimizing loss-of-service impact. Some solutions can reduce arc-flash hazards using existing equipment [1]. While these solutions may lower incident energy by utilizing existing equipment, thus requiring very little capital cost, there may be alternatives to lower incident energy even further. Applying a protective relay—an application-specific intelligent electronic device (IED)—specifically designed to provide the fastest protection possible is covered in [2], and qualification testing of the system is covered in [3]. This paper expands on applying this technology to switchgear and motor control center (MCC) applications where main-tie-main transfer schemes are common and focuses on the advantages and disadvantages of various communications technologies available for use. Unlike standalone applications where the tripping IED is the same as the IED that senses both current and light, these applications add the complexity of a communications channel so that the light-sensing IED can send a digital status to the tripping and current-sensing IED.

II. CRITICAL SYSTEM COMPONENTS

Providing fast and secure arc-flash protection to a local breaker requires light sensors and current supervision. In a local breaker application, the arc-flash relay trips only its associated breaker. No communications is required, and tripping times of 2 to 4 ms are achievable. When this solution is applied to switchgear and MCCs where the light-sensing or current-supervising IED is not associated with the breaker that must trip, a communications channel is required. While the additional logic processing and communications from one device to another does add additional time, tripping in 6 to 15 ms is possible. The communications channel becomes as critical as the light-sensing and current-supervising elements. Determining how repeatable the system is for responding to an arc flash is very important. In [4], engineers studied arc-flash protection of a local system only and compared it to a system requiring communications. Each system applied 200 faults and highlighted the minimum, maximum, and standard deviation of each configuration. Often the goal is to reduce the arc-flash incident energy to a level of 8 cal/cm^2 or less.

Two common forms of light sensors are point and bare fiber. Point sensors are commonly applied to breaker compartments while bare fiber sensors are applied to bus sections. The IED may support the ability to sense light and support one or more sensors.

Overcurrent supervision is critical for security. Historically, users reported undesired operations (i.e., a breaker opened when not expected to) as the result of flashes of light, such as those from a camera. Configuring the system to provide current supervision to the sensitive light sensor eliminates this concern and improves dependability. If current is not available, undervoltage elements can also be used for supervision.

Last, dependability and reliability of the communications channel are critical to performance. Regardless of media (metallic versus fiber-optic), communications type (Ethernet versus serial), or protocol (Generic Object-Oriented Substation Event [GOOSE] versus other point-to-point protocols), the tripping time is impacted if the data cannot quickly and reliably get from the light-sensing devices to the current-supervising and tripping device.

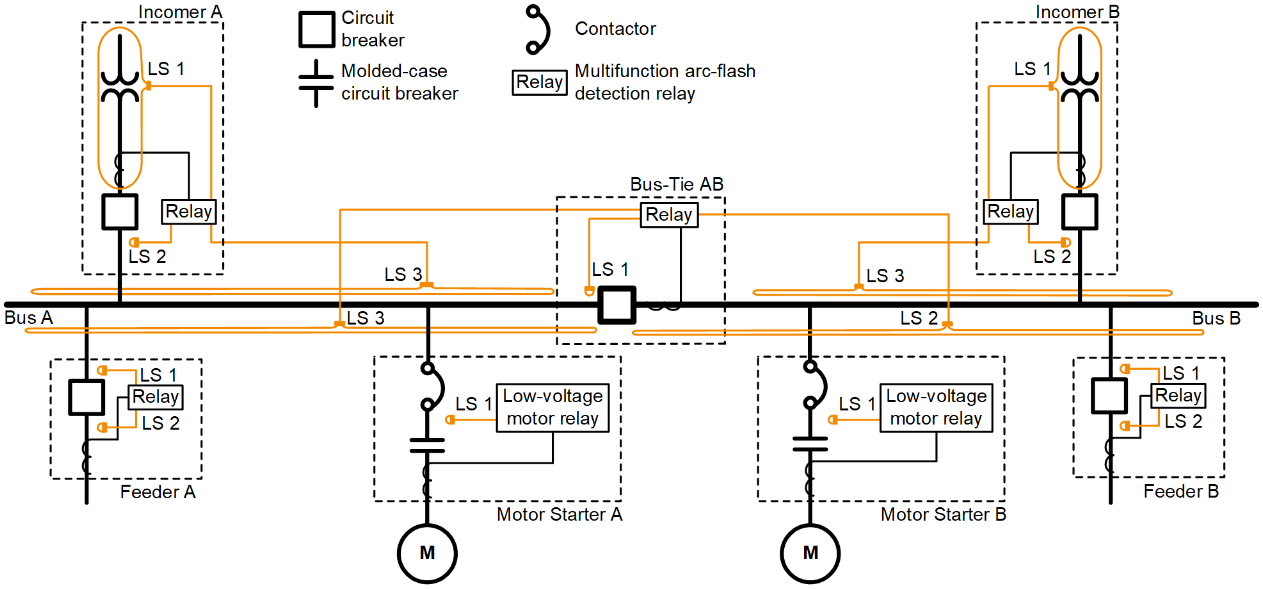


Figure 1 Example Main-Tie-Main Arc-Flash Protection Scheme [5]

III. MCC APPLICATION EXAMPLE

A typical main-tie-main MCC configuration with arc flash applied is shown in Figure 1. This same example can apply to switchgear as well. Arc-flash protection for the incomers comprises two loop sensors—one covering the dry-type transformer and incoming cable compartment (Light Sensor 1 [LS 1]) and the second covering the bus (LS 3)—and a point sensor in the breaker compartment (LS 2). In this application, any arc detected by the point light sensor or loop sensor covering the incoming cable and transformer will trip the upstream breaker. The normally open bus-tie relay also has three arc-flash sensors—one point sensor covering the breaker compartment (LS 1) and two loop sensors, one for each adjacent bus section (LS 2 and LS 3). In the normally open configuration, these light sensors provide backup to the incomer's light sensor and can initiate a trip of the appropriate incomer by sending its light pickup status, which is then supervised by the incomer relay's current element. The outgoing feeders have two arc-flash point sensors applied—the first sensor is used to detect light in the breaker compartment to trip the incomer and tie (LS 1) and the second is located in the feeder cable compartment (LS 2) to trip its local breaker. Lastly, motor control cubicles can have a built-in arc-flash sensor (LS 1) that can trigger the incomer and tie to trip for light sensed in the bucket. While light can be sensed by any of these relays, if current supervision is enabled, the tripping relay would need to detect an overcurrent to qualify the trip. The use of an arc-flash zone tripping matrix, as described in [5], can further assist in understanding the scheme.

Figure 2 illustrates the arc-flash trip logic in the incomer relay, which is triggered by an arc flash in the motor control cubicle. This logic uses light sensed by and communications with the low-voltage motor relay. The arc-flash tripping logic would OR all cubicles' Cubicle_*x*_AF light element with the cubicle's Good Communications status. The 50PAF element provides the overcurrent supervision performed by the incomer relay.

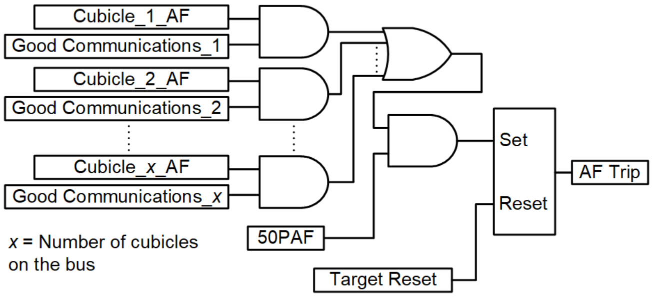


Figure 2 Example Communications Arc-Flash Trip Logic

Beyond arc-flash protection, it is common for each IED in a main-tie-main configuration to report data into a human-machine interface (HMI) for operator and process visibility. Engineers also want engineering access to the IEDs for remote data capture, settings verification, and settings updates. A time sync may also be provided across the network to synchronize event report and other data. As a result, many of these applications contain more than one protocol that the communications infrastructure must support. Reference [6] provides a good overview of the communications and protocols expected on more complex MCC applications.

IV. COMMUNICATIONS OPTIONS

Several communications options exist to transmit a light signal from the sensing relay to the tripping relay. Depending on the complexity of the design, communications may need to pass through multiple devices prior to a trip decision and a trip to the proper breaker. Other papers have considered the protocol design for user logic over protection channels [7]. Communications options include point-to-multipoint serial, single-channel Ethernet, dual-channel Ethernet with failover, dual-channel Ethernet switched mode using Rapid Spanning Tree Protocol (RSTP), dual-channel Ethernet failover using RSTP, dual-channel Ethernet with Parallel Redundancy Protocol (PRP), and software-defined networking (SDN). Each option should be carefully analyzed and evaluated based on the specific application. As shown in [8], communications-based events can delay receipt of a light-sensed signal and significantly compromise arc-flash protection as compared with a local, single-device solution. Beyond a description and diagram of each communications architecture, this paper provides an overview of the scheme with its expected performance, along with a list of advantages and disadvantages. This will help system designers evaluate each option and know what to guard against.

A. *Point-to-Multipoint Serial*

System architecture for a point-to-multipoint system is shown in Figure 3. Each IED requires a serial connection to a logic processor, and serial connections are also provided between adjacent logic processors. The configuration is scalable based on the number of arc-flash IEDs required and the maximum number of serial ports each logic processor supports. In Figure 3, the logic processor supports up to 33 serial ports. A serial connection exists between each logic processor and each arc-flash IED. In this configuration, each logic processor can support either 31 or 32 arc-flash IEDs. A specially designed point-to-point protocol is used in this configuration. The protocol must be specifically designed for speed, reliability, and subcycle communications capability.

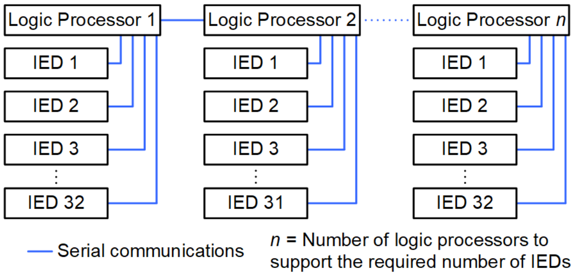


Figure 3 Multipoint Serial Communications Architecture

1) *Advantages:* For simplicity, a single protocol over a single point-to-point communications link connects the IED to the logic processor. As few as four settings in each device are required to enable this link. Both transmitting and receiving devices have a variety of tools available to analyze communications channel performance. These monitors can create alarm conditions to alert operators of any issues that arise. Lastly, protection can be enabled or disabled based on healthy communications.

Troubleshooting and testing this channel is simple. Technicians can use a test device to simulate both transmitting and receiving data to either end of the link. If the link is not available at a specific stage in commissioning, the test device can be directly applied to the transmitting or receiving IED and simulate transmission and reception of various signals. Channel status reports keep track of recent channel errors and provide an excellent history from either end.

A system using a single communications link with only one protocol is very dependable. It is not influenced by communications into either device by other protocols. Based on IED design, this peer-to-peer protocol has priority in processing over other external communications including Ethernet protocols. This allows the system to maintain functionality even during network storms that may appear to slow the processing of other non-protection-based IED functions.

2) *Disadvantages:* Customers have to design in a second communications channel if communications to an electrical control system (ECS), engineering workstation, etc., is required. Unlike Ethernet communications, which permits multiple protocols over the same link, the point-to-multipoint connection by definition is single-protocol. The need for extra cabling to permit additional communications capabilities is the single largest disadvantage with this option.

As defined in Figure 3, only a single serial connection is used by the scheme. There is no inherent backup or redundant communications channel. Some relays do support the peer-to-peer protocol over multiple serial channels. However, this requires additional point-to-point serial cables and logic processors. With the nonredundant nature of the design, all logic processors become single points of failure; if one device fails, all communications into that device and out of that device are impacted.

For larger systems with more than 32 IEDs, an additional logic processor is required. As described in the following subsection, each additional logic processor requires the device to process the signal and pass it to the next adjacent logic processor. This adds 4 to 6 ms per logic processor and ultimately delays tripping.

3) *Performance:* Reference [9] provides details on the peer-to-peer link, covering topics of security, dependability, and performance. The typical back-to-back operating time (defined as the measure of time from an initiating element to assert in a transmitting IED to the time it takes to assert an element in the receiving IED) is 4.2–6.3 ms using a baud rate of 9,600 or 19,200 bits per second. For smaller systems with one logic processor, the time is approximately doubled, as the system requires peer-to-peer communications from one IED to the logic processor and a second link to the tripping IED. In addition, engineers need to account for the processing time in the logic processor, typically between 1–4 ms depending on the specific IED and logic processor.

For larger systems that contain multiple logic processors, the overall communications time delay needs to account for these additional links and required processing. As a result, the expected maximum communications delay in milliseconds can be derived according to (1).

$$(n + 1) \cdot 6.3 + n \cdot 4 \qquad (1)$$

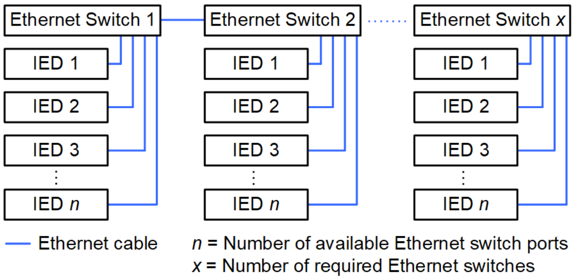
where n is the number of logic processors on the MCC.

A typical MCC covering up to 62 IEDs would require two logic processors and would have a maximum delay of 27 ms. To summarize this expected delay, there are three peer-to-peer communications links—two between logic processors and arc-flash IEDs and a third between the two logic processors. Each logic processor adds an additional 4 ms of processing depending on the process interval.

Using a similar peer-to-peer serial protocol with this technology, [8] includes an arc-flash incident where the IED took 4 ms to detect light, the peer-to-peer protocol took 10 ms to assert a trip in the receiving relay, and the breaker clearing time was 44 ms. The fault was sensed and cleared in 58 ms. Due to the specific application to trip a remote feeder breaker, a logic processor was not used. But this does illustrate the expected back-to-back IED operating time using a serial communications channel.

B. Single Ethernet

As discussed, IEDs can support different communications mediums, such as copper or fiber, and communications protocols. The simplest and most common Ethernet communications is shown in Figure 4, where each device is connected to the network via single fiber, Cat 5E cable, or Cat 6 cable. These devices communicate data frames complying to the Open Systems Interconnection (OSI) model [10] into the network, which is distributed by devices, such as routers and switches, that form the network. The devices are configured for Internet Protocol (IP) addressing, networking modes, and network speeds using device configuration software.



Ethernet Switch 1
Ethernet Switch 2
Ethernet Switch x
IED 1
IED 2
IED 3
IED n
Ethernet cable
n = Number of available Ethernet switch ports
x = Number of required Ethernet switches

Figure 4 Communications Network With Single Ethernet Port

Ethernet offers faster data transfer speeds compared with serial communications. However, it does have greater message overhead and processing costs. Ethernet also serves as a medium to transfer data to meet different application needs. Networks carry information about time using protocols, such as Network Time Protocol (NTP) or Precision Time Protocol (PTP), or synchronized phasor measurements using IEEE C37.118 or a time-critical protection element state, such as a time-overlight (TOL) arc-flash element, in the form of a GOOSE message.

GOOSE is a multicast peer-to-peer protocol in which data are transmitted and received through a publication and subscription method. Such data are exchanged at relatively high speeds compared with other protocols such as Modbus or DNP3, thus making it suitable to use for time-critical protection applications. Each IED configured to transmit GOOSE messages contains a set of protection element bits in which a change in state triggers a GOOSE message. The first transmission occurs immediately following the state change and subsequent transmissions occur at predefined intervals and continue to transmit a message at every maximum-time interval until another state change occurs. As indicated in Figure 5, the IED continues to transmit the messages at various intervals, which reduces the probability of the message not being received. While the repetition rate varies somewhat per manufacturer and IED model, several messages are sent within a power cycle interval.

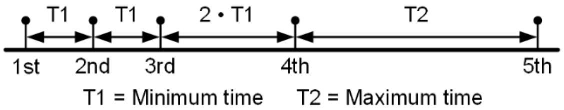


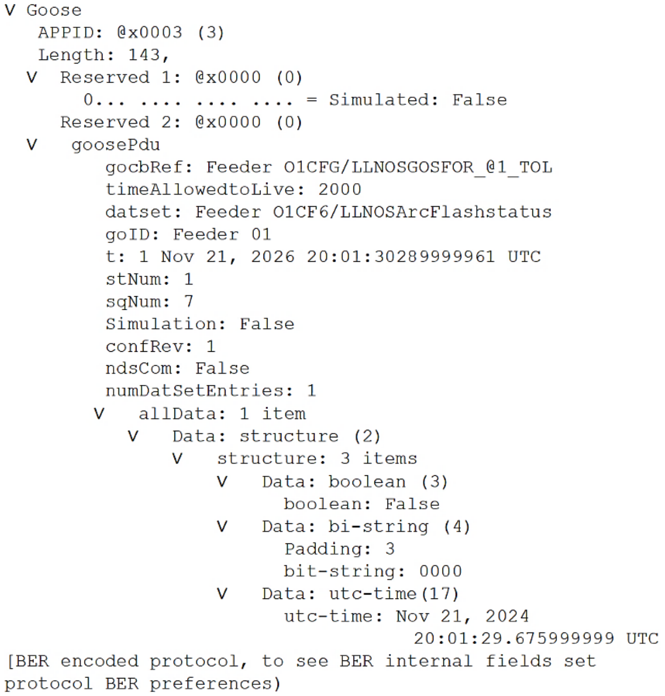
Figure 5 Example of GOOSE Message Retransmission Intervals

On the receiving side, IEDs subscribe to and process individual GOOSE messages. The details, such as the data set contents, transmit intervals, and IEDs subscribed to a GOOSE message, are contained in the Configured IED Description file (.CID). This file is stored in each IED that communicates via GOOSE message. The GOOSE message contains attributes like Time Allowed to Live (TAL), a Simulation bit, and a Quality bit for each data attribute. TAL can be used to check the network or availability of the publishing IED. This attribute tells the subscribing IEDs how long they should wait for the next message. The IED processes the information and gives statistics or options to customize in logic that can be used to create alarms, warnings, or LED indications.

The transmission by a publisher and reception by subscriber of the GOOSE message take at least the minimum processing interval of an IED. Additional delays could occur due to the network configuration and other traffic on the Ethernet network. Factors like these need to be considered while designing an arc-flash solution based on a communications network. GOOSE messages are never confirmed as received by the subscribing IED to the publisher.

1) *Advantages:* IEDs can be easily connected to form a network. Due to a single point of connection, troubleshooting for link-down status is easily identified. Additionally, most IEDs offer binary status elements for link failures, which could alarm on a local HMI, as well as LEDs on Ethernet ports, which allow for a visual indication of a healthy communications link. Healthy communications links do not necessarily equate to valid GOOSE messages. A GOOSE message comprises a Quality attribute that checks the quality of data based on validity, detailed quality, source, and test, as well as whether the operator blocked. Message quality could be mapped in custom logic to reject invalid GOOSE messages indicated by a FALSE value of its quality attribute.

Network monitoring tools allow for viewing traffic on Ethernet networks, which is helpful in isolating issues related to incorrect configuration or delays in messages. A GOOSE frame capture is shown in Figure 6.



```
V Goose
   APPID: @x0003 (3)
   Length: 143,
  V  Reserved 1: @x0000 (0)
        0... .... .... .... = Simulated: False
     Reserved 2: @x0000 (0)
  V   goosePdu
         gocbRef: Feeder 01CFG/LLNOSGOSFOR_@1_TOL
         timeAllowedtoLive: 2000
         datset: Feeder 01CF6/LLNOSArcFlashstatus
         goID: Feeder 01
         t: 1 Nov 21, 2026 20:01:30289999961 UTC
         stNum: 1
         sqNum: 7
         Simulation: False
         confRev: 1
         ndsCom: False
         numDatSetEntries: 1
        V   allData: 1 item
           V   Data: structure (2)
               V   structure: 3 items
                   V   Data: boolean (3)
                         boolean: False
                   V   Data: bi-string (4)
                         Padding: 3
                         bit-string: 0000
                   V   Data: utc-time(17)
                         utc-time: Nov 21, 2024
                                   20:01:29.675999999 UTC
[BER encoded protocol, to see BER internal fields set
protocol BER preferences)
```

Figure 6 GOOSE Message Frame

The goosePdu contains the details about the GOOSE message, such as those identified in TABLE I.

TABLE I
goosePdu DETAILED OPTIONS

Attributes	Description
gocbRef	is the reference to the control block that is contained in LLN0
datSet	is the reference of the data set whose contents are transmitted
goID	allows a user to identify the GOOSE message
stNum	is a counter that increments when a state change is detected
sqNum	is a counter that increments with every transmission of a GOOSE message without an stNum update
Simulation	is a true value that indicates that the message contains simulated data
confRev	is the configuration revision, which updates every time the data set is modified
ndsCom	needs commissioning. If true, then gocb requires further configuration
numDatSetEntries	is the number of data sets in the GOOSE message
allData	is the values of all the mapped data

Owing to the simplicity and connection requirements of a single Ethernet configuration, the likelihood of forming network loops that create a harmful network storm is very limited. A network storm is an event in which a large number of broadcast, multicast, or unicast packets continuously flood the Ethernet network and unexpectedly overload the network, limiting available bandwidth and total system functionality. Additionally, the reliability of such a network is very high since the failure of a network cable or an IED in the network does not disrupt the entire communications. However, the failure of the central connection (the Ethernet switch) could bring down the entire network.

2) *Disadvantages:* Although the single-port devices are easy to work with, their biggest challenge is their limitation on the number of devices that can be connected to form a network. Most switches offer a limited number of ports to connect with either 5, 10, or 24 IEDs depending on the hardware selection. The network topology needs to be redesigned to consider additional devices. It is also not redundant, making it unreliable for time-critical messages.

3) *Performance:* As mentioned earlier, today's microprocessor-based IEDs offer Ethernet speeds up to 100 Mbps, allowing very high data speeds that enable fast transfer of data. However, communications-assisted arc-flash protection schemes could introduce communications delays of 6 to 13.4 ms in addition to fault clearance delays [4]. These additional delays need to be accounted for in the design of the arc-flash protection system.

C. *Dual Ethernet With Failover*

IED manufacturers now offer devices with more than one Ethernet port due to the wide adoption of Ethernet infrastructure. As the name of this configuration suggests, to provide redundancy, the network switches to another local-area network (LAN) should the primary LAN fail. Figure 7 shows devices connected in this network. Each device has two ports and connects to both LAN A and LAN B.

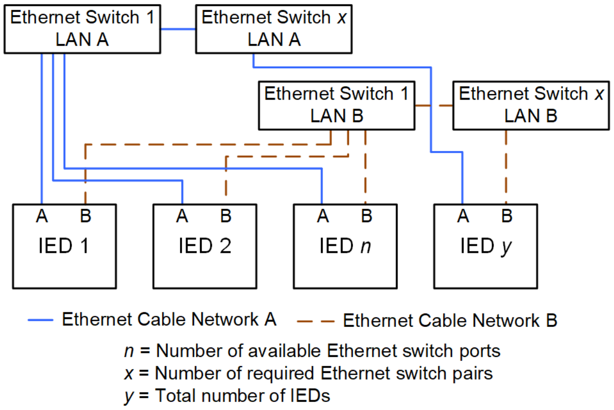


Figure 7 Communications Network With Dual Ethernet Ports

IEDs communicate via a primary LAN. As soon as the communications or the link fails in the primary LAN, the IED switches to the backup LAN. Also, IEDs can offer custom logic to switch between LANs. Typically, such a switchover can cause delays in transmission or reception of messages and should be accounted for when used to transmit arc-flash GOOSE messages. Switchovers should be done with no intentional delays.

1) *Advantages:* As discussed, failover is easy to configure when compared with an RSTP network since its settings, such as choosing a primary network, custom logic to switch between LANs, and time, are easy to configure. A failover network provides improved availability compared with fixed mode. Since the transition is slower, it is best suited for noncritical applications, such as supervisory control and data acquisition (SCADA), that are developed to collect periodic binary status, analog metering data, and event reports from IEDs in a substation.

2) *Disadvantages:* Many Ethernet cables and the maintenance of two network infrastructures are required. When multiple switches are involved in the network, the IED cannot readily detect the failure of an intermediate link.

3) *Performance:* The performance of a dual Ethernet with failover configuration is similar to that of a single Ethernet connection unless the network failover occurs at the same time as the arc-flash incident. This could delay receipt of critical messages.

D. *Dual Ethernet Switched Mode Using RSTP*

Another feasible network topology with dual ports on IEDs is a ring topology in which participating IEDs also participate in network reconfiguration. The devices in this network contain dual Ethernet connections configured in a switched mode and are daisy-chained, as indicated in Figure 8.

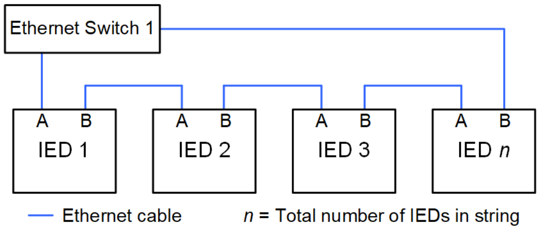


Figure 8 Ring Topology With Dual Ethernet Ports

Figure 8 shows a network loop that could cause network storms and collapse the entire network. The role of RSTP is to identify and prevent formation of such network loops. To prevent these loops in the network, an RSTP-enabled device sends the Bridge Protocol Data Units (BPDUs) to adjacent devices. An exchange of BPDUs between adjacent devices provides the necessary data to RSTP-enabled devices for deciding the route for communications. Information in BPDUs helps devices set their own communications ports to the appropriate roles and state. The three port states supported in RSTP are discarding, learning, and forwarding. The discarding state discards all Ethernet traffic except BPDUs. If any link breaks in the network, BPDUs are exchanged and a port in a discarding state transitions to a forwarding state, thus enabling an alternate route of communications. This is called network reconvergence. Root, designated, alternate, backup, and disabled are different port roles supported in RSTP.

Consider the network of three switches shown in Figure 9 connected in a ring with RSTP enabled. Based on the set bridge ID, the lower bridge ID switch becomes the root switch in the network. The root switch ports are in a designated role that forwards traffic.

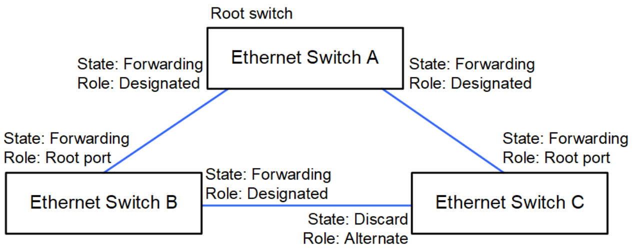
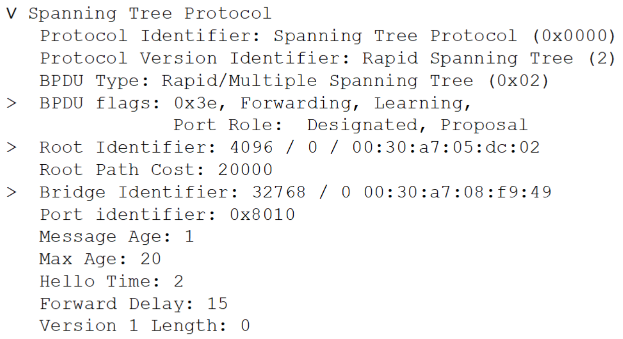


Figure 9 Three-Switch Network Configuration With RSTP

For every other switch in the network, there exists alternate paths to reach the root switch. Each switch with their respective connected ports calculates the path cost to reach the root switch. The port that has the least expensive path to reach the root switch becomes the root port and remains in a forwarding state while the other port's role becomes designated. The switch port in the loop with the highest path cost to reach the root switch becomes the alternate port instead of the designated port.

Each port has its own path cost, which is a numerical value, usually set based on the speed of the link. If the path cost is the same from both ports of the switch to reach the root switch, then the port that is connected to the root switch's lowest port priority becomes the root port. By changing the bridge priority of the device, path cost value, and port priority of the ports, the topology (logical break) can be set to the desired configuration. See [11] for further detailed information on path costs.

BPDUs exchanged by the devices contain the information shown in Figure 10. BPDUs are sent every 2 seconds per hello time after the network is configured.



```
v Spanning Tree Protocol
   Protocol Identifier: Spanning Tree Protocol (0x0000)
   Protocol Version Identifier: Rapid Spanning Tree (2)
   BPDU Type: Rapid/Multiple Spanning Tree (0x02)
>  BPDU flags: 0x3e, Forwarding, Learning,
               Port Role:  Designated, Proposal
>  Root Identifier: 4096 / 0 / 00:30:a7:05:dc:02
   Root Path Cost: 20000
>  Bridge Identifier: 32768 / 0 00:30:a7:08:f9:49
   Port identifier: 0x8010
   Message Age: 1
   Max Age: 20
   Hello Time: 2
   Forward Delay: 15
   Version 1 Length: 0
```

Figure 10 RSTP BPDU Message Frame

Following a network event such as a disconnected cable, BPDUs are exchanged to determine a new state and roles of the participating devices, and thus, the network converges to a stable configuration. Depending on the number of devices participating in the RSTP ring, the network could be flooded with BPDUs, which could impact the delivery of other time-critical messages, such as GOOSE messages, on the network. Hence, testing should be done to determine the worst-case performance of network convergence.

Moreover, the convergence time of the network depends not only on the IEDs but also on factors such as the location of the link failure, the number of IEDs and switches connected in a daisy chain, and network traffic.

1) *Advantages:* Rapid convergence of networks (within milliseconds [12]) is one of the main advantages of RSTP networks. This contributes to a reliable, redundant network. Moreover, creating the RSTP network is much easier than creating a serial communications network, and the cost of building the network is low when compared with PRP or a failover mode network.

2) *Disadvantages:* Designing the system with loops achieves cost-effective redundancy. However, the network completely depends on the RSTP algorithm to break the loop, correct the network, and prevent a crippling network storm. This brings the risk of losing not only redundancy but also any communications. Unexpected or loose cable connections, high network traffic, or even the small amounts of traffic with broadcast and multicast messages can create network storms during network link-up events. This may hinder the exchange of BPDUs and affect the performance of RSTP.

In the worst-case scenario, a network storm does not let the IEDs process BPDUs, which leads to a bigger storm, and thus, the entire RSTP system becomes unreliable and difficult to troubleshoot. Before choosing to use RSTP in a network, engineers must consider the worst-case network traffic scenarios with device capability to process the traffic. If all devices are not capable of handling the worst-case traffic, another network architecture should be employed.

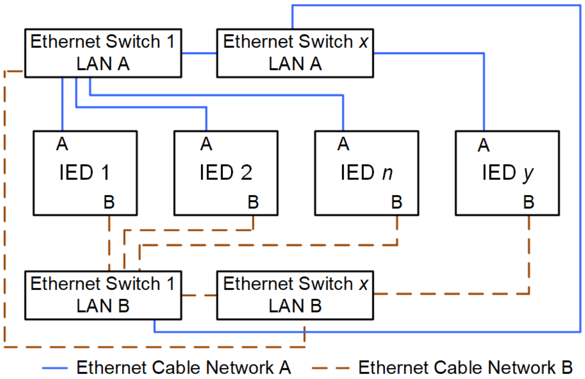
And if multiple IEDs are out of service (IEDs or cubicle turned off), the network is segmented, which may result in a loss of communications to multiple devices.

3) *Performance:* Measuring the performance of an RSTP network is challenging and depends on many factors. Even with the same network and traffic, the reconvergence time for different events varies based on the locations of the link failure and logical break in the system. Secondly, more IEDs in the loop take more time to exchange BPDUs and negotiate the new topology,

requiring more time for reconvergence. The number of IEDs employed should be based on the allowed delay of time-critical GOOSE messages. Also, GOOSE message minimum and maximum times can create additional delays. For example, if the arc-flash event and a cable break between publishing and subscribing devices occur simultaneously where network reconvergence time is 20 ms, minimum time is 4 ms, and maximum time is 1,000 ms, the receiving device will likely miss the first four messages due to network reconvergence. The fifth message will be received ~1,016 ms (reference Figure 5) after the event, long after it would need to act, even though the network was restored within 20 ms. In this case, a much shorter maximum time should be considered or the minimum time should be increased for the network to be capable of handling more traffic.

E. Dual Ethernet Failover Mode Using RSTP

So far, fundamental topologies that are widely used to establish communications networks have been discussed. It is possible to have a mix of these network topologies to take advantage of the merits of multiple configurations. One such arrangement is IEDs connected in failover mode and switches connected in a ring, as shown in Figure 11.



n = Number of available Ethernet switch ports
x = Number of required Ethernet switch pairs
y = Total number of IEDs

Figure 11 Dual Failover With RSTP

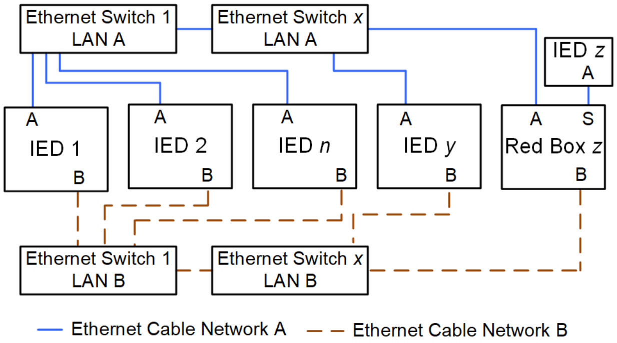
IEDs configured in failover mode reduce the burden when compared with RSTP or PRP modes due to reduced traffic. However, to have redundancy in such networks, the switches are configured with RSTP since they do not support link failover capability.

Large networks could cause challenges in the transmission of multicast GOOSE messages. Switches offer functionalities such as virtual LANs (VLANs) and priority-tagged message handling to improve upon delivery of GOOSE messages.

VLANs provide segregation of traffic into separate LANs and thus limit the traffic seen by the devices in the LAN. The priority-tagged messages egress switch ports based on set priorities.

F. Dual Ethernet With PRP

Network architecture for PRP is similar to failover network architecture. The only difference in PRP is that the IED continually sends duplicate messages in the parallel network instead of activating the backup port after the primary port fails. That means PRP provides active network redundancy by packet duplication over two independent networks [13]. In addition, IEDs that do not support dual Ethernet ports configured for PRP must use a device commonly referred to as a red box (redundancy box) to allow it to connect to the PRP network. See Figure 12.



n = Number of available Ethernet switch ports
x = Number of required Ethernet switch pairs
y = Total number of PRP-supported IEDs
z = Total number of non-PRP-supported IEDs

Figure 12 Parallel Redundancy Network

The deployment of a PRP system is as costly as the failover architecture and more expensive than RSTP system architecture but is the only one of the discussed arrangements that provides seamless active redundancy in the network. The cost of the system is impacted by the number of red boxes required, as well as if there are any additional costs associated with IEDs that have optional support for PRP.

In a PRP network, the devices transmit a supervision frame and append each frame with a redundancy control trailer (RCT). The supervision frames are transmitted periodically with a unique multicast address. It contains a sequence number, which increments with every new transmission. Additionally, it conveys if the mode of operation is duplicate accept or duplicate discard.

The RCT comprises a sequence number, a LAN identifier, a frame size, and a PRP suffix. Such details could be viewed using a network monitoring tool, as indicated in Figure 13 and Figure 14.

```
V HSR/PRP Supervision (IEC62439 Part 3)
   0000 .... .... .... = Path: 0
   .... 0000 0000 0001 = Version: 1
   Sequence number: 1720
   TVL type: PRP Node (Duplicate Discard) (20)
   TLV length: 6
   Source MAC Address: IED_MFG_55:47:89
                       (00:30:a7:55:47:89)
   TLV type: End of TLVs (0)
V Parallel Redundancy Protocol (IEC62439 Part 3)
   [PRP Version: PRP-1]
   Sequence number: 5135
   1010 .... .... .... = LAN: LAN A (10)
   LDSU size: 52 [correct]
   Suffix: 0x88fb
```

Figure 13 Network Capture of Supervision and RCT for LAN A

```
V HSR/PRP Supervision (IEC62439 Part 3)
   0000 .... .... .... = Path: 0
   .... 0000 0000 0001 = Version: 1
   Sequence number: 1720
   TVL type: PRP Node (Duplicate Discard) (20)
   TLV length: 6
   Source MAC Address: IED_MFG_55:47:89
                       (00:30:a7:55:47:89)
   TLV type: End of TLVs (0)
V Parallel Redundancy Protocol (IEC62439 Part 3)
   [PRP Version: PRP-1]
   Sequence number: 5135
   1011 .... .... .... = LAN: LAN B (11)
   LDSU size: 52 [correct]
   Suffix: 0x88fb
```

Figure 14 Network Capture of Supervision and RCT for LAN B

On reception, duplicate frames arrive at the device. The first frame that arrives is identified and accepted by the device, and the duplicate is discarded if the frame has arrived on a set PRP time-out.

1) *Advantages:* PRP is beneficial when a link break occurs between the switches as compared with failover mode. PRP offers fast redundancies compared with RSTP networks due to active redundant networks. The redundancies are achieved without path cost settings.

2) *Disadvantages:* The bandwidth in a PRP network increases since the network contains duplicate packets. IEDs participating in such networks perform additional processing to identify and discard duplicate messages. Additional hardware, such as redundant red boxes, is required to connect non-PRP-capable devices to a PRP network.

3) *Performance:* Although the packets are duplicated by IEDs in the network, one of the factors for engineers to consider while designing PRP networks is to have similar network latencies in the two LANs. Dissimilar LANs may cause delays in transmitting duplicate GOOSE messages, which could impact protection applications.

G. Operational Technology SDN

Software-defined networking (SDN) is a technological advancement that improves the performance and reliability associated with arc-flash protection schemes applied to switchgear applications. Purpose-engineered networking with ultra-fast healing times provides many advantages to the challenges associated with other networking architectures discussed so far. Unlike RSTP, which responds to a link failure and then determines an alternate path, SDN is proactively traffic-engineered so the switches already know how to respond to any network event.

SDN is purpose-engineered using the OpenFlow 1.3 protocol to configure the SDN-capable switches. All network paths must be preprogrammed, including failover paths. Logical path programming and ultra-fast failover for failed network segments increase reliability of an arc-flash protection scheme. Network priority of traffic by application type is predefined, allowing GOOSE-related arc-flash protection to have higher priority over remote engineering access or SCADA communications.

Figure 15 shows an example of a software-defined network in a faulted state. Relays should be configured in dual interface modes, like failover, enabling both links to send and receive traffic. This simplifies the network architecture and flattens out the network without a performance tradeoff. SDN also ensures that each device only gets the traffic that is proactively traffic-engineered to be delivered to the device, microsegmenting the network to each conversation without the need for complicated VLAN configuration. Network loops are not a concern, and uncontrolled multicast or broadcast traffic is eliminated, resulting in improved network quality and end device performance increases since each device is only processing packets destined for itself.

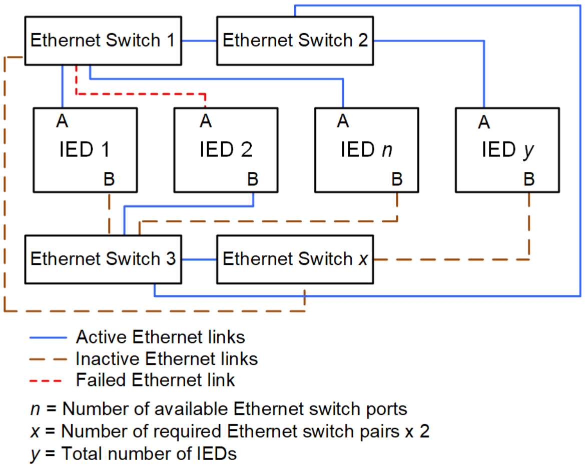


Figure 15 SDN

1) *Advantages:* With purpose-engineered communications paths, SDN is more efficient than other network architectures. Redundant messages and uncontrolled multicast and broadcast traffic are eliminated. And unlike RSTP, the network does not include unnecessary control plane traffic, like BPDU messages. In RSTP, this control plane traffic competes with the critical control messages for highest priority on the network, but in SDN, the control messages are the highest priority and there is no control plane traffic competition.

SDN allows for the prioritization of network communications based on message type and is no longer restricted to just the VLAN and port. Within an industrial MCC, the highest priority messages are associated with GOOSE communications for arc-flash protection, the second highest priority messages are process control system (PCS) communications—such as motor start and stop commands, the third highest priority messages are ECS communications, and the lowest priority messages are remote engineering access. Not only does SDN eliminate the risk of network loops leading to storms, but by prioritizing traffic, it ensures lifesaving arc-flash protection messages make it through a congested network.

SDN is a deny-by-default zero-trust switch fabric; no device or traffic is allowed until the authorized user provisions circuits to allow it. This strong network access control eliminates many cybersecurity risks.

2) *Disadvantages:* SDN does require pre-engineered data paths and may have additional upfront engineered costs. Historically, configuration was on a per-switch basis—each network path was individually engineered by application and message type. Recent advancements provide automated tools to configure network topology and provision communications circuits with the ability to create final state reports. In addition, modern technology can provide visual awareness by monitoring all paths and provide network level statistics of health and status.

These tools reduce the overall implementation and ongoing network maintenance costs of SDN.

3) *Performance:* SDN can achieve ultra-fast communications failover in the event of a link or switch failover. Communications can be reestablished within 100 µs [14]. This network restoration is over 100 times faster than that of a traditional RSTP scheme.

V. Other Considerations

With the serial-based protection scheme identified in Section IV.A, each additional protocol or connection type requires additional cables and equipment. Beyond the lack of redundancy, a dedicated point-to-point serial connection may not support passing IRIG-B synchronized time if this capability is available in the logic processor. While most modern IEDs support NTP and advanced IEDs support PTP, the advantage is that the simple network in Section IV.B eliminates the requirement for an extra cable to provide the capability to synchronize time. See [15] for the different options and advantages of each for time synchronization.

Obtaining engineering access to the system in Section IV.A requires an additional serial cable to a communications processor or an Ethernet cable and associated network equipment. In an all-Ethernet network, engineering access can use the same network and the additional bandwidth is negligible.

Other forms of communications, depending on the application, may include connections to an ECS and/or PCS. With an Ethernet-based solution, these data can use the same communication channel in the arc-flash protection system without the need for additional equipment.

VI. Conclusion

Performing local arc-flash detection—light sensing combined with overcurrent supervision—with an IED that can directly trip the appropriate breaker results in the fastest clearing time possible. This requires no communications and results in the lowest incident energy. Once the system configuration requires a light-sensing IED separate from the IED capable of tripping the appropriate breaker, a communications channel must be added, which adds additional processing, transmission delays, and communications-related risks.

The application of IEDs in MCCs or switchgear with Ethernet-based communications protocols is widely used due to its advanced features, reliability, and simplicity. As described in this paper, communications between IEDs may be configured in several ways, depending on the protocols and capabilities supported by the equipment being used. If IEDs are selected based on optimal network design at the beginning, the advantages, such as cost savings due to less cabling and physical space by not requiring additional input/output (I/O) units for arc-flash protection, will benefit the project.

Arc-flash protection is very important, both in saving lives and minimizing equipment damage. When applying this protection scheme to a main-tie-main configuration, communications is required to ensure proper equipment operation based on the location of the arc, supervising elements, and the configuration of the equipment. Engineers have many communications architectures to choose from, and while the speed of each instance under steady-state and no-fault conditions is similar, some network designs offer redundancy, which can lead to higher network availability. However, some common configurations increase the likelihood of unexpected loops, resulting in crippling network storms.

Critical arc-flash protection schemes have been compromised by network storms [8] due to certain network configurations. The increased traffic can also overload an IED trying to process each Ethernet message frame. Details of network storms and testing for a storm have been discussed elsewhere in [8] and [16]. These references clearly show several ways a storm can occur on a network and ways to mitigate it.

Dual Ethernet configured for failover with RSTP or dual Ethernet configured for PRP is an effective option that provides redundancy. SDN, however, offers superior networking and cybersecurity capabilities including ultra-fast failover, restoring network communications 100 times faster than other technologies while reducing Ethernet traffic and lowering the Ethernet message processing of each IED. In light of network storms, the single active network nature of SDN provides higher reliability and simpler configuration to house critical protection functions, such as arc-flash protection, using network switches.

Due to simplicity, the ability to have simultaneous communications protocols—including time synchronization—makes Ethernet-based solutions superior to serial-based options. A summary of each communications type along with a feature and performance comparison of each is shown in TABLE II.

TABLE II
COMMUNICATIONS OPTIONS—FEATURE AND PERFORMANCE COMPARISON

Connection Type	Multiprotocol Support	Redundant	Failover	Network Storm Susceptibility	Traffic Priority	Efficiency	Time Sync
Point-to-Multipoint Serial	No	No	N/A	N/A	N/A	High	IRIG*
Single Ethernet	Yes	No	N/A	N/A	VLAN	Medium	IRIG+, SNTP, PTP
Dual Ethernet With Failover	Yes	Yes	Seconds	High	VLAN	Medium	IRIG+, SNTP, PTP
Dual Ethernet Switched Mode Using RSTP	Yes	Yes	~100 ms	Medium	VLAN	Low	IRIG+, SNTP, PTP
Dual Ethernet Failover Mode Using RSTP	Yes	Yes	~10 ms	Low	VLAN	Medium	IRIG+, SNTP, PTP
Dual Ethernet With PRP	Yes	Yes	N/A	High	VLAN	Low	IRIG+, SNTP, PTP
Operational Technology SDN	Yes	Yes	Microseconds	N/A	Message Type	High	IRIG+, SNTP, PTP

* May require extra cable

+ Requires extra cable

VII. REFERENCES

[1] J. Buff and K. Zimmerman, “Application of Existing Technologies to Reduce Arc-Flash Hazards,” proceedings of the 33rd Annual Western Protective Relay Conference, Spokane, WA, October 2006.

[2] G. Rocha, E. Zanirato, F. Ayello, and R. Taninaga, “Arc-Flash Protection for Low- and Medium-Voltage Panels,” in *Record of Conference Papers Industry Applications Society 58th Annual IEEE Petroleum and Chemical Industry Conference (PCIC)*, 2011, pp. 1–8.

[3] B. Hughes, V. Skendzic, D. Das, and J. Carver, “High-Current Qualification Testing of an Arc-Flash Detection System,” proceedings of the 9th Annual Clemson University Power Systems Conference, Clemson, SC, March 2010.

[4] L. Napier, “The Need for Simplicity in Arc-Flash Protection Design,” proceedings of the CIGRE International Symposium, Cairns City, Queensland, Australia, September 2023.

[5] M. Cato, S. Manson, M. Watkins, and A. Gill, “Techniques for Commissioning Arc-Flash Mitigation Systems,” in *IEEE Petroleum and Chemical Industry Committee Conference (PCIC) Record*, 2019, pp. 249–258.

[6] P. Subramanian and S. Manson, “Case Study: Deployment of 300 Smart Motor Control Centers,” in *IEEE Petroleum and Chemical Industry Technical Conference (PCIC) Record*, 2018, pp. 179–188.

[7] Z. Eyasu, B. Le, T. Lee, K. Behrendt, and V. Skendzic, “Design and Application Considerations for User-Programmable Bits Over Protection Channels,” proceedings of the 67th Annual Georgia Tech Protective Relaying Conference, Atlanta, GA, May 2013.

[8] M. Watkins, K. Heshami, T. B. Chambers, N. K. Mudugamuwa, and A. S. Pandya, “Lessons Learned Through Commissioning, Livening, and Operating Switchgear: Part 2,” proceedings of the PCIC Europe Conference, Rotterdam, Netherlands, June 2024.

[9] K. C. Behrendt, “Relay-to-Relay Digital Logic Communication for Line Protection, Monitoring, and Control,” proceedings of the 32nd Annual Minnesota Power Systems Conference, Saint Paul, MN, October 1996.

[10] H. Zimmermann, “OSI Reference Model—The ISO Model of Architecture for Open Systems Interconnection,” *IEEE Transactions on Communications*, Vol. COM-28, No. 4, pp. 425–432, April 1980.

[11] ANSI/IEEE 802.1D-1998, *IEEE Standard for Local Area Network Media Access Control (MAC) Bridges*, New York, NY: IEEE.

[12] R. Pallos, J. Farkas, I. Moldován, and C. Lukovszki, “Performance of Rapid Spanning Tree Protocol in Access and Metro Networks,” in *Second International Conference on Access Networks & Workshops Record*, 2007, pp. 1–8.

[13] M. Rentschler and H. Heine, “The Parallel Redundancy Protocol for Industrial IP Networks,” in *IEEE International Conference on Industrial Technology (ICIT) Record*, 2013, pp. 1,404–1,409.

[14] Q. Yang and R. Smith, “Improve Protection Communications Network Reliability Through Software-Defined Process Bus,” proceedings of the Grid of the Future Symposium, Reston, VA, October 2018.

[15] E. O. Schweitzer, III, D. E. Whitehead, G. Zweigle, V. Skendzic, and S. V. Achanta, “Millisecond, Microsecond, Nanosecond: What Can We Do With More Precise Time?” in *69th Annual Conference for Protective Relay Engineers (CPRE) Record*, 2016, pp. 1–12.

[16] DNV GL, “Network Storm Testing” 2016. Online at https://mydnvglcdntqfjwwhej46g2.blob.core.windows.net/cdn/content/marketplace/docs/Network%20Storm%20Testing.pdf.

VIII. VITAE

Matthew Watkins, PE, received his BS, summa cum laude, from Michigan Technological University in 1996 and an MBA from Cardinal Stritch University, Wisconsin, in 2003. He worked for 5 years as a distribution protection engineer responsible for the application of reclosers throughout the distribution system. In 2005, Matthew joined Schweitzer Engineering Laboratories, Inc. (SEL) as a product manager and later served as a field application engineer. He presently holds the title of principal engineer in SEL Engineering Services, Inc. (SEL ES) in Plano, Texas. He is a senior member of IEEE and a registered professional engineer in the state of Texas.

Nilushan K. Mudugamuwa received his PhD in renewable energy from the University of Surrey, United Kingdom, in 2009 and BEng (honors) in electrical and electronic engineering at City University of London in 2004. He joined KBR London in 2010 as an electrical engineer and worked on a variety of projects. In 2015, he went on secondment to Azerbaijan and became responsible for onsite electrical engineering design for two offshore platforms. Since 2018, he has worked for Tengizchevroil (TCO) in Kazakhstan as a lead electrical protection engineer. He is a Member of the Institution of Engineering and Technology (MIET) and has been registered as a Chartered Engineer from the Institution of Engineering and Technology, United Kingdom (IET UK) since 2014.

Neel Shah received his MS in electrical and electronics engineering from the University of Texas at Arlington in 2023 and BTech in electrical engineering from BVM Engineering College, India, in 2020. He joined Schweitzer Engineering Laboratories, Inc. (SEL) as an engineering intern in 2022. During the internship, he worked on various communications functionality testing and testing tool developments for the SEL-700 series relays. He was hired as an associate integration and automation engineer at SEL after he completed his MS and now works on enhancement of IEC 61850 Edition 2.1 and communications protocols development for SEL relays.

Anurag Upadhyay received his MS in electrical engineering from Michigan Technological University in 2016 and BTech in electrical engineering from NIT Allahabad, India, in 2011. He joined Schweitzer Engineering Laboratories, Inc. (SEL) as a product engineer in 2020 and contributes toward the development of SEL-700 series protective relays.

Previously presented at the 72nd Annual Petroleum and Chemical
Industry Technical Conference, Dallas, Texas, September 2025.

20250401 • TP7194