Case Study: Increasing Reliability, Dependability, and Security of Digital Signals Via Redundancy and Supervision

Paulo Franco, Geraldo Rocha, and David Dolezilek
Schweitzer Engineering Laboratories, Inc.

Presented at the
PAC World Africa Conference
Johannesburg, South Africa
November 12–13, 2015

Originally presented at the
5th International Scientific and Technical Conference: Actual Trends in Development of Power System Relay Protection and Automation, June 2015

Case Study: Increasing Reliability, Dependability, and Security of Digital Signals Via Redundancy and Supervision

Paulo Franco, Geraldo Rocha, and David Dolezilek, Schweitzer Engineering Laboratories, Inc.

Email: papers@selinc.com

USA

1 Introduction

Electrical substation information and control technology (ICT) systems use a variety of topologies, networks, and protocols to communicate between multiple nodes. Typical electrical substation nodes include the following:

- Intelligent electronic devices (IEDs), such as protective relays, meters, and dedicated controllers.
- Local computers, programmable logic controllers, or programmable automation controllers (PACs), providing data concentration and automatic control.
- Local displays or human-machine interfaces (HMIs).
- Local-area network (LAN) devices, such as Ethernet switches, radios, and serial-to-Ethernet converters.
- Wide-area network (WAN) devices, such as time-division multiplexers and radios.

The LANs and WANs provide local and remote connections to support the following applications:

- Peer-to-peer interlocking and high-speed automation.
- Substation data concentration, automation, protocol conversion, and local operator HMI.
- Supervisory control and data acquisition (SCADA) masters located in control centers.
- Wide-area measurement and control (synchrophasor) systems.
- Remote engineering access and maintenance workstations.
- Event report gathering and analysis systems.

This paper presents methods for supervising signal exchange via digital messages. Case studies that provide examples of improvements to applications, such as logic selectivity, circuit breaker failure (50/62BF), and automatic line transfer (ALT) based on signal message supervision, are discussed.

2 Signaling Methods for Teleprotection Applications

A hard-wired exchange of protection information uses an analog value at the receiver to indicate the status of the signal from the sender. Typically, an analog value set to zero indicates a status value of zero, and the maximum analog value represents a status value of one. This method creates a constant signal value at the receiver. However, if the signal wire is cut or disconnected, the receiving device cannot distinguish between this situation and a legitimate zero analog value. Digital messages convey the signal status each time they are received and, therefore, the signal exchange is not constant. Each time a digital message is received, the signal status is confirmed or a change of status is recognized. The receiver has no option but to assume that the signal status remains unchanged during the time between messages. However, the digital message exchange can be supervised, and the receiver will detect when the communications link is lost. MIRRORED BITS® communications publishes digital messages every 2 milliseconds over dedicated links, so the time between each signal confirmation is 2 milliseconds. A change of state is also detected within 2 milliseconds at the receiver. IEC 61850 GOOSE messages are configurable to be published at varying rates and are typically set to once per second over shared-bandwidth Ethernet networks. The time between signal confirmations at the receiver grows to once per second when GOOSE messages are used. A signal status change of state typically triggers an immediate GOOSE publication, so a change of state is also detected within 2 milliseconds at the receiver.

GOOSE messages are not published more rapidly so that the traffic on the shared-bandwidth Ethernet network is reduced. The consequence is that the time between confirmations is much longer, and the time to detect failed communications is much longer than with other digital messaging methods.

3 Application Redundancy

3.1 Benefits of IEC 61850 Ethernet LAN

A great benefit of the IEC 61850 standard is point-to-point communication through IEC 61850 Generic Object-Oriented Substation Event (GOOSE) messages to exchange signal information among several IEDs. This signal exchange is used in protection, automation, and interlocking logic, enabling the development of a decentralized automation system distributed among several IEDs.

Improvement of substation operating conditions via automation of actions previously performed by operators improves system reliability, security, and availability, which directly reduces downtime periods. In addition to operational and economic aspects, the decision to adopt this substation philosophy, through the use of IEC 61850 communications protocols, is also based on the following benefits:

- High-speed communication via Ethernet packet exchange.
- Interoperability among equipment from different manufacturers.
- Significant reduction in the quantity of cables.
- Reduced likelihood of undetected cable failure due to signal supervision.
- Faster and more automatic commissioning.
- Lower possibility of obsolescence in the near future, ensuring the return of the investment made.
- Guarantee of easy expandability.

3.2 Typical Substation Automation System Network

A substation automation system (SAS) consists of protective relays, controllers, communications networks, gateways to make integration with a SCADA system easier, disturbance recorders, meters, synchronized phasor measurement units, local and remote engineering workstations, and a local HMI.

Communication with the control center and the HMI is usually accomplished via connections to a communications gateway. This gateway collects data from the IEDs via IEC 61850 manufacturing message specification (MMS) protocol, concentrates the data in one database, and then converts them into protocols that the SCADA and HMI machines expect, including DNP3, DNP3 LAN/WAN, IEC 60870-5-101, and IEC 61870-5-104. Other information, such as synchrophasor data, sequential event records, event reports, and settings, is collected via direct connections to the IEDs. Time synchronization data are broadcast to the IEDs via a separate IRIG-B network that continues to work even if the Ethernet network is compromised. This keeps data among the protective relays synchronized for forensic analysis. Standards are being developed now for accurate time synchronization over the Ethernet network, but they are not yet mature and do not work at all if the LAN fails [1]. An example distribution substation one-line diagram is shown in Fig. 1a, and the corresponding architecture of the communications network of a distribution substation based on the IEC 61850 standard is shown in Fig. 1b.

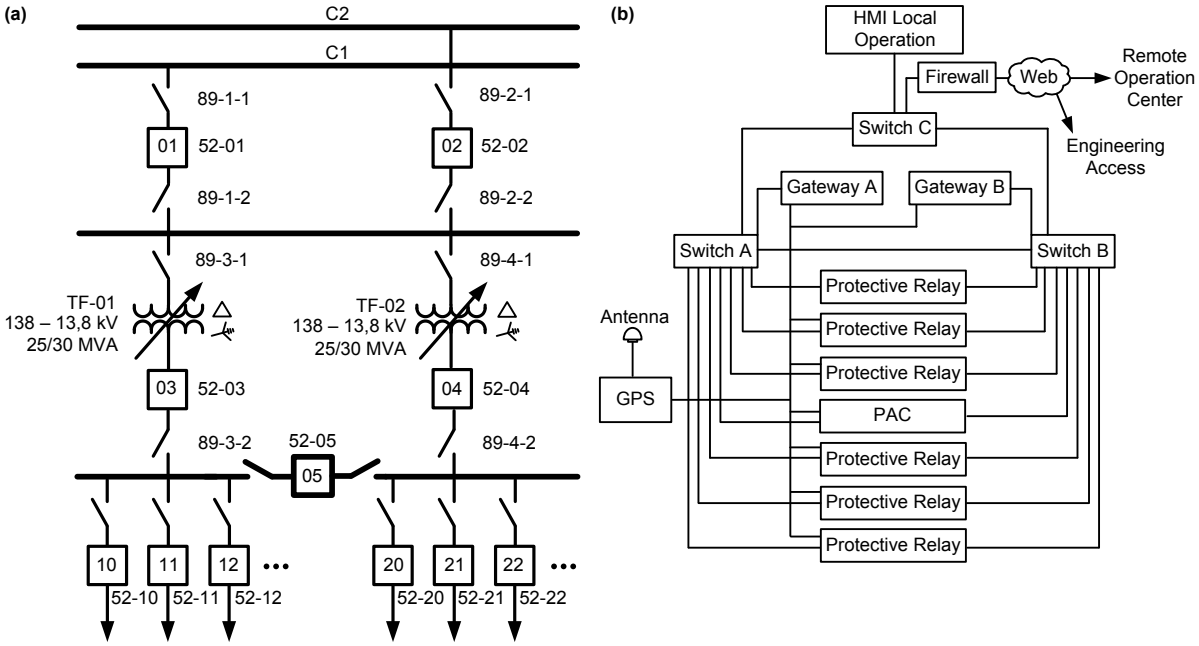


Fig. 1. Typical substation one-line diagram (a) and data communications network (b)

3.3 Managing Active Connections Within a Protection LAN

With the use of protection systems that depend on information exchanged over communications networks, it becomes essential that the network be designed and monitored for dependability, reliability, and availability.

Ethernet technology allows a single active connection to each physical device identified by a media access control (MAC) address. Protection and control IEDs now support multiple physical Ethernet connections and have an internal switch to manage their use. The Ethernet switch function inside the IED switches between the internal logic connection and the external physical connections. Two external connections can be physically attached to LAN switches, with one as an active primary and the other as an inactive failover. The failover connection can be in hot-standby mode, ready to be enabled immediately after detection of a loss of functionality of the primary port. High-performance Ethernet requires that this internal switch function manage traffic between the internal logic connection and one external physical connection. When the external physical connection fails, the internal switch manages traffic between the internal logic connection and the failover hot-standby physical connection. In this fashion, GOOSE messages to and from this IED travel through the LAN with the best possible performance and with minimal impact on other IEDs. These direct connections support the appropriate speed and reliability required for protection and interlocking, as shown in Fig. 2a, where Port A denotes primary and Port B denotes failover functionality.

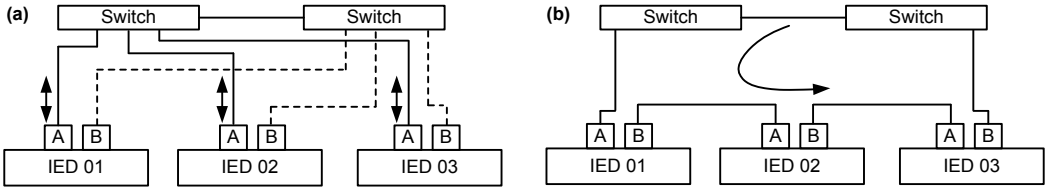


Fig. 2. Primary and failover hot-standby connections (a) and ring architecture (b)

The statuses of active connections are managed in the IEDs by link failure detection and failover. This works in conjunction with link supervision and activation within the LAN and is performed by the spanning tree algorithm (STA) within the switches (also referred to as bridges). The bridges within the spanning tree domain communicate with each other by broadcasting Ethernet packets that contain a special section devoted to carrying STA information. This portion of the packet is referred to as the bridge protocol data unit (BPDU). It contains LAN information that is used to determine which bridge controls the STA. This bridge, referred to as the root bridge, manages the active and hot-standby paths within the LAN. When a bridge starts up, it issues a BPDU in order to determine whether a root bridge has already been selected in the network. If no root bridge has been determined by

pre-engineering, then the lowest bridge priority number of all of the bridges becomes the root bridge. Best engineering practices include design and engineering of the root bridge in advance in order to optimize LAN performance. The root bridge periodically transmits a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes.

3.4 Low-Cost, Low-Performance Monitoring LAN

When IEDs are not performing protection or interlocking, some designers choose to sacrifice resilience and speed for cabling shortcuts. By having both physical Ethernet connections active simultaneously, all traffic passes in one physical port and back out the other. Traffic originating from, or directed to, the IED is managed between the physical connections and the internal logic connection via the IED switching function. In this mode, the IEDs can be cabled to one another in a ring or loop, as shown in Fig. 2b. Although possible, this creates a lot of unnecessary processing burden on the IEDs by forcing traffic through them. It also creates delivery bottlenecks because cables and IEDs become saturated with unwanted messages that consume processor and cable bandwidth. Due to poor speed and resilience, this connection method is not used for protection IEDs but may be acceptable for monitoring and control IEDs. The speed to detect failure and activate an alternate traffic path is dramatically reduced, but the installation requires two fewer IED cables than the best practice method in Fig. 2a.

3.5 Packet Duplication Mislabeled as Redundancy

Though out of the scope of this paper, there are numerous LAN technologies to create and deliver duplicate Ethernet packets. These methods, such as Parallel Redundancy Protocol (PRP) and High-Availability Seamless Redundancy (HSR), actually do not provide redundancy but rather perform packet duplication [2].

3.6 Signal Redundancy Via IEC 61850 GOOSE Retransmission

GOOSE messages are delivered inside a LAN via a unique virtual LAN (VLAN) based on IEEE 802.1Q. Also, each IED is responsible for surviving message loss, duplication, delay, out-of-order delivery, and loss of connectivity in case the LAN does not function as expected.

IEC 61850-8-1 specifies that GOOSE behavior signal exchange via Type 1 or 1A fast messages must be published immediately after the signal status changes. This is referred to as a state change, or change of state. IEC 61850-8-1 also specifies a retransmission scheme to achieve a highly dependable level of signal delivery. These retransmissions are redundant publications of the GOOSE message, each with a different sequence number and each containing the signal change-of-state information. This mechanism provides redundant delivery of each signal change (in case one or more packets are lost in the network) in order to improve the resilience of interlocking and protection via digital messaging. Fig. 3 shows this mechanism of retransmission of GOOSE messages. Once started, GOOSE messages are published constantly, containing a collection of data called a data set. During configuration, each GOOSE message is given a maximum time (MT) to wait between redundant message publications and the name of the data set to include in the message. The messages are published each time one of the data set elements changes or if the MT expires. After a data set element changes, a GOOSE message is published immediately and then published again after a short delay (often 4 milliseconds), represented by T1 in Fig. 3. These redundant publications are repeated very often to increase the likelihood that all subscribers will receive them across the nondeterministic Ethernet network. The minimum time between publications (TBP) is a configuration setting in the publisher used to determine how quickly to publish the second and third GOOSE message after the signal change of state. After several publications, the TBP grows longer, as illustrated by T2 and T3 in Fig. 3, until it reaches MT and is published as a steady state.

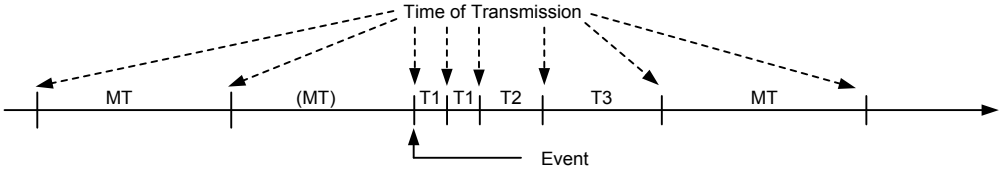


Fig. 3. Example of changing time between message publications (from IEC 61850-5)

For each message, publishing IEDs create and include a time to live (TTL), calculated based on the TBP. The publishers calculate TTL to be multiples of TBP to prevent nuisance alarms caused by the frequent and small Ethernet network delays. TTL is 2(TBP) when TBP is equal to MT and 3(TBP) when TBP is any value other than MT. For the first few messages after a protection signal element in

a data set changes state, the message is sent every 4 milliseconds, and then less rapidly. Each message includes the TTL, which forecasts the time delay before the next message will be published so that subscribers can monitor correct data flow.

When the next change of state occurs, a new message is created and published. The new data set event information is transmitted and repeated in the shortest TBP (T1), as shown in Fig. 3. The retransmission time gradually increases from T2 to T3 and eventually settles at a stable retransmission time of TBP = MT.

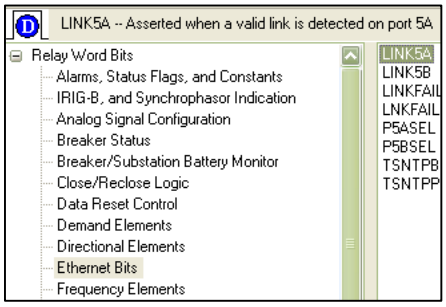
Subscribing IEDs constantly calculate time to wait (TTW) based on the TTL within each message. The subscriber considers data “stale” when the TTW expires and the IEDs have not received a new replacement message from the publisher.

If the subscribing IED detects expiration of the TTW, it assumes that the communication is lost and modifies its relay logic accordingly. The message redundant retransmission scheme is necessary to perform transmission from one to many and to allow each subscriber to know that the communications channel is healthy. However, depending on the choice of final stable retransmission time, it may not be sufficient to guarantee the reliability of mission-critical tasks.

3.7 IED Communications Supervision and Status

Protection, monitoring, and control IEDs have internal binary variables, as illustrated in Fig. 4a, that identify and monitor communications parameters. In the screenshot of a software engineering tool shown in Fig. 4a, an engineer has selected and highlighted the status value LINK5A, which is asserted when Ethernet Port 5A has a valid LAN link status. These binary variables are used in internal logic to dynamically modify algorithms and are published to SCADA systems and HMIs to provide network status information. Alarms based on these statuses are used to dispatch maintenance teams for actions at the communications network in order to correct defective situations in the network. This supervision and alarming increases the availability and reliability of the substation Ethernet network, which in turn increases the availability and reliability of the protection and control system accordingly.

(a)



(b)

```
=>>GOOSE <Enter>

GOOSE Transmit Status

   MultiCastAddr  Ptag:Vlan  StNum   SqNum  TTL  Code
------------------------------------------------------------
Device_OtterCFG/LLNO$GO$GooseDSet13
   01-0C-CD-01-00-10 4:1     1       166    457
   Data Set: Device_OtterCFG/LLNO$DSet13

GOOSE Receive Status

   MultiCastAddr  Ptag:Vlan  StNum   SqNum  TTL  Code
------------------------------------------------------------
Device_1CFG/LLNO$GO$GooseDSet13
   01-0C-CD-01-00-04   :      0       0      0    TTL EXPIRED
   Data Set: Device_1CFG/LLNO$DSet13

Device_1CFG/LLNO$GO$GooseDSet13
   01-0C-CD-01-00-0A  4:0     1      98531   120
   Data Set: Device_1CFG/LLNO$DSet13
```

Fig. 4. Engineering tool display of available internal IED Ethernet supervisory status (a) and an internal IED GOOSE report (b)

3.8 Subscriber IED Supervision of GOOSE Performance

The commissioning and maintenance of traditional IEDs using hard-wired copper conductors to convey signals is done with multimeters and oscilloscopes. In automation systems using signaling via digital messages based on the IEC 61850 standard, traditional maintenance and commissioning tools are replaced with tools developed by IED manufacturers. Fig. 4b shows an example of an IED GOOSE report that displays the status and configuration of published and subscribed GOOSE messages. This report supports the monitoring of which messages the IED is transmitting and receiving and whether there is some failure in the network that hinders the communication among the IEDs. This feature helps the technical team identify connection and settings errors by displaying the active configuration, including the following:

- *MultiCastAddr* indicates the MAC multicast address of the GOOSE message.

- *Ptag* indicates the message priority level.
- *Vlan* identifies the IEEE 802.1Q VLAN configured for the message.
- *Code* indicates the type of errors and failures in the network or in the message, if any.

Error codes include *out of sequence* (OOS) when one or more packets are not delivered and the sequence number of the next received packet is not consecutive. If the delay between messages becomes large, the TTL is set to *expired* because the link is considered disabled. Other errors include *message corrupted*, *configuration changes*, *commissioning needed*, and *test mode*.

Fig. 5 illustrates an IED report that details the availability and the quality of an individual GOOSE subscription. These values help technicians to understand, diagnose, and troubleshoot any potential issues with each individual GOOSE exchange. Technicians can see records of when the exchange failed and for how long, as well as when GOOSE messages are dropped or received out of sequence. These data also reveal the frequency, time, and duration of LAN failures.

```
Ctrl Ref:   Device_1CFG/LLN0$GO$GOOSEOutPri7
AppID    : 4119
From     : 07/13/2012 09:15:40.992  To: 07/13/2012 10:26:47.660

Accumulated downtime duration                    : 0000:00:00
Maximum downtime duration                        : 0000:00:00
Date & time maximum downtime began               : 07/13/2012
Number of messages received out-of-sequence(OOS)   : 0
Number of time-to-live(TTL) violations detected    : 1
Number of messages incorrectly encoded or corrupted: 0
Number of messages lost due to receive overflow    : 0
Calculated max. sequential messages lost due to OOS: 0
Calculated number of messages lost due to OOS      : 0
```

Fig. 5. GOOSE message subscription statistics

3.9 IED GOOSE Message Quality Supervision

The major reason for failures in the protection and automation schemes of traditional systems is the inability to monitor the integrity of the metallic cable that transfers the signal information between the IEDs.

When, instead, the system uses digital GOOSE messages to convey signal status, any communications failure between the IEDs is monitored in real time as message quality. This status is used within the IEDs to perform blocking and/or change protection and automation logic to prevent incorrect performances.

Supervision is performed constantly, even when there is no change in the value of any variable inside the data set. This is possible because the GOOSE message is transmitted periodically at the MT as a heartbeat function. If the subscriber IED detects that the GOOSE message has not been received within the expected timeframe, the message quality variable is set to *failed*. Therefore, each subscriber calculates its own message quality for each GOOSE subscription.

Fig. 6 illustrates the use of message quality within a transformer relay subscribing to a feeder relay. The feeder relay data set includes a block signal when it detects the fault and attempts to trip the feeder breaker. The feeder relay data set also includes a breaker failure indication when the trip output is unsuccessful. The transformer relay detects the fault current locally and trips immediately upon receiving breaker failure indication. When the transformer relay either receives a block signal from the feeder relay or detects loss of communications from the feeder relay, it delays tripping for 100 milliseconds. This delay allows the feeder breaker to clear the fault. If, however, communications with the feeder are normal and the relay does not detect the fault, the transformer relay immediately trips.

The typical logic example in Fig. 6 shows how important immediate detection of message quality failure is to the protection of the transformer and the bus. As mentioned previously, message quality fails when the TTW expires and the relay has not received a new replacement message from the publisher. An accurate TTW is based on accurate TTL values calculated and published within each GOOSE message. Calculation of message quality is most critical immediately after a signal status change of state. This is also when the redundant GOOSE messages are published in the burst of retransmissions. TTW expires at 3(TTL) and message quality is set to *failed*.

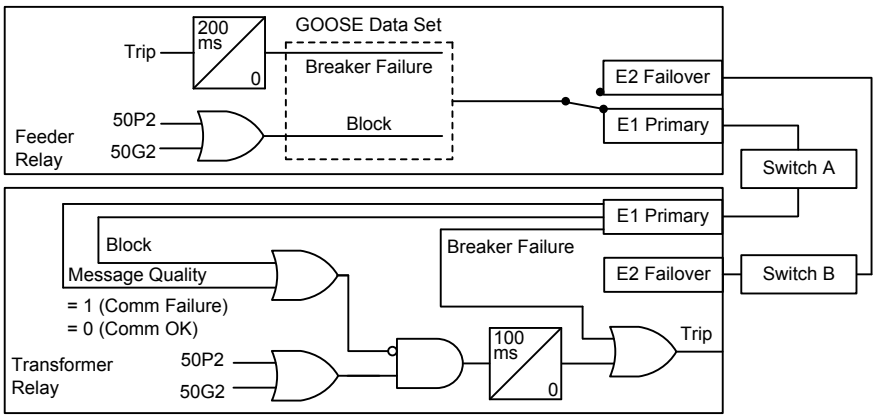


Fig. 6. Use of GOOSE message quality status in IED logic

As an example, consider IED1, which calculates TTW based on the actual TTL for a retransmission burst of 4, 4, and 8 milliseconds after the initial signal change-of-state message. IED2 never calculates TTL, but rather uses a fixed value of 500 milliseconds. IED3 never calculates TTL, but rather uses a fixed value of 2,000 milliseconds. When GOOSE exchange fails immediately following the first message with a signal change of state after a fault, the three IEDs have a very different detection of failure. Message quality for the immediately failed exchange with IED1 is set after 12 milliseconds. Message quality for the immediately failed exchange with IED2 is set after 1,500 milliseconds, and message quality for the immediately failed exchange with IED3 is set after 6,000 milliseconds. Therefore, logic operations are blind to failed communications with IED2 for 1.5 seconds and IED3 for 6 seconds, creating unwanted and unsafe conditions.

3.10 The Use of Message Quality Within Protection Schemes

Protection and automation engineers seek the best methods to design secure logic schemes. With the use of IEC 61850 communications for protection and automation applications, best known methods now include the use of message quality supervision within protection signaling via GOOSE messages. In each example, the message quality logic input is calculated within the relay performing the logic based on the criteria listed previously for each GOOSE subscription.

Typical logic applications in a protection and control system for the substation illustrated in Fig. 1a include logic selectivity, circuit breaker failure (50/62BF) and ALT. The value of supervision of message quality within logic schemes is demonstrated in the following examples.

3.10.1 Logic Selectivity

Logic selectivity enables fast and secure real-time changes to the logic so that it adapts to changes in the substation infrastructure, communications network, and protection requirements. Fig. 7 illustrates logic in the relay protecting Breaker 52-03, which monitors the status from any of the feeder relays (10, 11, and 12). If none of these downstream feeder relays have a protection pickup and all have normal communications, the torque control (67P1TC) is set. Torque control equations control the operation of various levels of overcurrent elements. For example, the Level 1 phase-instantaneous and definite-time overcurrent elements (67P1/67P1T) are only enabled when feeder relays are communicating normally and report no faults indicated by 67P1TC = 1. In Fig. 8, when this is the case, 67P1TC = 1 is set, and then 67P1/67P1T follows 50P1 (which has been set to be fast and sensitive) to immediately trigger. If the tie breaker (52-05) is closed, this logic also includes Feeders 20, 21, and 22. If communications to any feeder relay are lost, the selectivity logic is not set because it is unknown if that relay is attempting a protective trip. In this case, if the upstream breaker relay sees fault current but has lost communications to one or more of the feeder relays, 67P1TC is not set and the trip equation waits for the 51S1T time-coordinated trigger. Fig. 8 illustrates the 52-03 breaker relay trip logic being conditioned by torque control (selectivity) or relying on coordination timers.

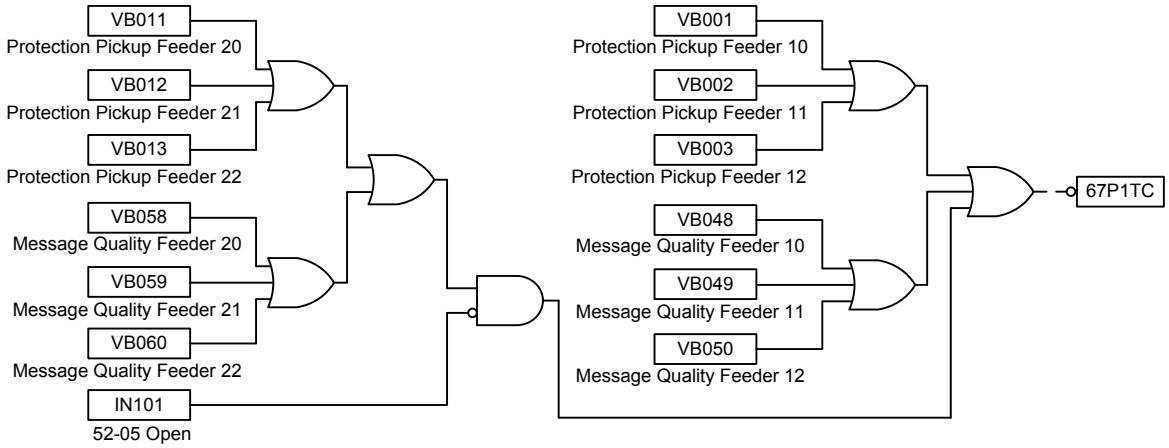


Fig. 7. Selectivity logic in Breaker 52-03 relay

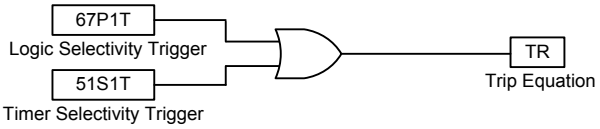


Fig. 8. Logic in Breaker 52-03 relay chooses coordination timer trigger only if 67P1T selectivity trigger is not set

3.10.2 Circuit Breaker Failure

The circuit breaker failure scheme shown in Fig. 9 runs in each feeder breaker relay and reacts to the detected failure of a circuit breaker trip failure to operate (breaker failure), indicated as BFTRIP1. This defect is mitigated by sending a trip signal to the appropriate relay protecting and controlling a circuit breaker upstream. Fig. 9 illustrates logic in the relay controlling feeder Breaker 52-10, which is subscribing to GOOSE messages from other relays. Once the relay for 52-10 detects local breaker failure *and* has normal communications from the relay controlling 52-03 calculated as good message quality with a status value of zero, it sends a BF initiated trip for 52-03 (50/62BF 52-03). If the relay for 52-10 detects local breaker failure *and* communications have been lost from the relay controlling 52-03 and calculated as failed message quality with a status value of one, it sends a BF initiated trip for both 52-01 (50/62BF 52-01) and 52-02 (50/62BF 52-02). If the relay for 52-10 detects local breaker failure, Breaker 52-02 is closed, *and* communications are normal from the relay controlling Breaker 52-05, the relay sends a BF initiated trip for 52-05 (50/62BF 52-05). If the relay for 52-10 detects local breaker failure *and* communications have been lost from the relay controlling 52-05, it sends a BF initiated trip for 52-04 (50/62BF 52-04). The logic in Fig. 9 shows the use of communications supervision in the relay for 52-10 when forwarding the 50/62BF signal to the circuit breakers upstream in order to mitigate the communications failures, thus ensuring the correct and safe operation of the system.

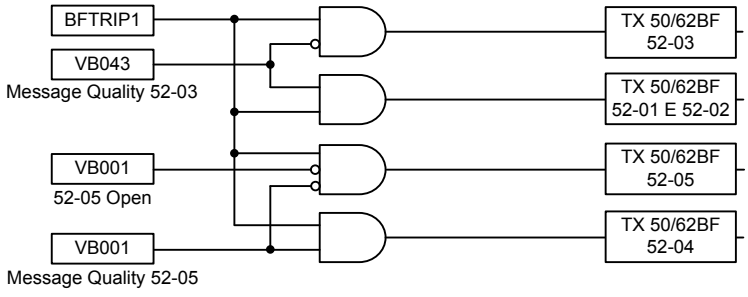


Fig. 9. Circuit breaker failure scheme

3.10.3 Automatic Line Transfer

The transfer between alternate lines is done automatically via the relays exchanging interlock signals within GOOSE messages. The line in operation is shut down and supply is reestablished to consumers through the automatic transfer to the backup line.

The relays protecting the feeds into the substation monitor the voltage of the line in operation (Fig. 10a). Absence of voltage on the active feed (C1) indicates Line 1 – Dead (Fig. 10a) and

presence on the other line (C2) indicates Line 2 – Live. The ALT logic (Fig. 10b) confirms correct operation of C2 and that the switches on either side of Breaker 52-02 are closed (Fig. 10b). This triggers the start of the ALT by setting ALT Start = 1 after the automation sequence timer expires.

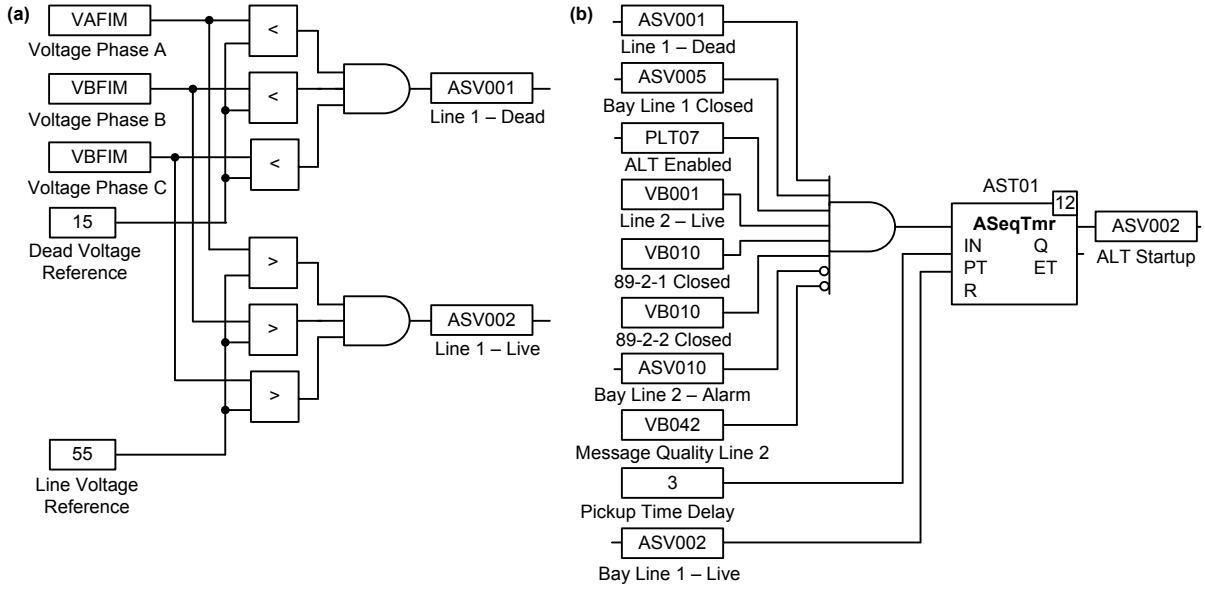


Fig. 10. Voltage monitoring (a) and ALT startup (b)

4 Conclusion

The protocols within the IEC 61850 standard have become an efficient method of communicating between IEDs to transmit information about statuses, measurements, interlocks, and protection signals. Correct design of a protection and automation system based on IEC 61850 protocols requires correct engineering of the Ethernet LAN for speed, reliability, dependability, and availability. The mission-critical nature of digital protection applications also requires a much higher level of dependability, security, and Ethernet network availability for delivery of the GOOSE packets. At the IED level, correct operation of peer-to-peer communications must be supervised and communications failures, once detected, must trigger blocking and/or change protection and automation schemes to prevent incorrect performances. These GOOSE subscription defects are communicated to operators at the HMI and SCADA systems as alarms. These alarms are also sent to technicians so that communications errors can be immediately found and corrected. The IED diagnostic reports support troubleshooting, diagnostics, and preventive maintenance.

5 References

[1] S. T. Watt, S. Achanta, H. Abubakari, and E. Sagen, “Understanding and Applying Precision Time Protocol,” proceedings of the 2014 Power and Energy Automation Conference, Spokane, WA, March 2014.

[2] S. Chelluri, D. Dolezilek, J. Dearien, and A. Kalra, “Understanding and Validating Ethernet Networks for Mission-Critical Protection, Automation, and Control Applications,” March 2014. Available: http://www.selinc.com.

6 Biographies

Paulo Franco is an automation engineer with Schweitzer Engineering Laboratories, Inc. He is located in Brazil.

Geraldo Rocha received his BSEE from Universidade Estadual Paulista Campus de Bauru, Brazil, in 2001 and specialized in electrical power systems protection at Universidade Federal do Rio de Janeiro. He worked as a protection and automation engineer for CPFL Geração de Energia S.A., where his responsibilities included maintenance, commissioning, specification, and studies of protection and automation of hydroelectric plants. In 2007, he joined Schweitzer Engineering Laboratories, Inc., where he is currently a marketing manager.

David Dolezilek received his BSEE from Montana State University and is the international technical director at Schweitzer Engineering Laboratories, Inc. He has experience in electric power protection, integration, automation, communication, control, SCADA, and EMS. He has authored numerous technical papers and continues to research innovative technology affecting the industry. David is a patented inventor and participates in numerous working groups and technical committees. He is a member of the IEEE, the IEEE Reliability Society, CIGRE working groups, and two International Electrotechnical Commission (IEC) technical committees tasked with the global standardization and security of communications networks and systems in substations.

Abstract—Protection and control functions within modern microprocessor-based intelligent electronic devices (IEDs) directly measure data representing the present state of the power system. Communications-assisted protection and control functions collect signal data from other IEDs via digital messaging. The contents of the digital messages are combined with the local measurements in the relay to perform accelerated and/or more selective protection and automation logic.

NERC PRC-005 describes a protection system application to include protective relays, voltage- and current-sensing inputs, dc control circuitry, station dc supply, and the communications media. Application redundancy is accomplished via multiple protection system components, such as IEDs, instrument transformers, dc circuits, and power sources. Communications media redundancy is accomplished via multiple communications connections, communications devices, and messaging protocols. Self-tests within the application and communications media perform supervision and immediate detection of failure.

Application and media system reliability and dependability are best improved via the use of robust devices and designs. Both application and communications media redundancy are performed via primary and backup devices, hot standby devices, or dual primary devices. Ethernet media is made resilient with technology designed to satisfy reliability standards, such as the IEEE 1613 standard for the environmental and testing requirements for communications networking devices in electric power substations. Ethernet media is made more robust via optimized redundant connections and hot standby reconfiguration algorithms. Dual primary message technologies provide redundant signaling with no common-mode failure.

Traditionally, protection and automation engineers search for the best and most secure logic designs. Security in applications using MIRRORED BITS® communications or IEC 61850 Generic Object-Oriented Substation Event (GOOSE) digital messaging is improved via the supervision of the message quality. Though designs intend to maximize good message quality, signaling message quality fails when monitoring detects that messages are not received as expected, are received out of sequence, or are corrupted. Status of system-wide digital messaging for protection and interlocking signaling, control, and monitoring is now easily displayed for quick review by operators similar to other system data. This provides 100 percent visibility for supervision and performance auditing. Failures are automatically time-stamped, logged, reported, and alarmed similar to other power system or control system malfunctions.

This paper presents a comparison of various application and communications media redundancy methods and redundant and duplicate connections. Finally, case studies provide examples of improvements to applications, such as logic selectivity, circuit breaker failure (50/62BF), and automatic line transfer (ALT) based on signal message supervision.

20150422 • TP6695