Improving Reliability and Security of Protection Algorithms Via Signal Message Supervision

P. Franco, G. Rocha, and D. Dolezilek
Schweitzer Engineering Laboratories, Inc.

Presented at the
13th International Conference on Developments in Power System Protection
Edinburgh, United Kingdom
March 7–10, 2016

Improving reliability and security of protection algorithms via signal message supervision

P. Franco*, G. Rocha*, D. Dolezilek*

**Schweitzer Engineering Laboratories, Inc., 2350 NE Hopkins Court, Pullman, WA 99163 USA, dave_dolezilek@selinc.com*

Keywords: Generic Object-Oriented Substation Event (GOOSE), time to live (TTL), message quality, digital signal supervision.

Abstract

Communications-assisted protection and automation logic is capable of accelerated and highly discriminate decision making via signal exchange using digital messages. However, each receiving intelligent electronic device (IED) must supervise the required communications and immediately detect failures in order to adapt the logic to work correctly in the absence of these communications. This paper illustrates the need and benefits of using the status of the signal message exchange in protection and automation logic.

1 Introduction

Innovative supervision of the successful exchange of digital messages being used to communicate protection signal information provides immediate detection upon failure. Knowledge of failure is used to adapt protection logic in real time to change from faster-operating communications-assisted algorithms back to traditional methods such as timers. This is a clear advantage over using hard-wired contacts between devices, where it is not always possible to distinguish between an "off" signal represented as an analog value of zero and failure as a result of an open circuit. Failure of digital message delivery is detectable regardless of the quantity of signals and their values. Correct operation of protection and interlocking applications requires secure and reliable signaling and immediate failure detection. This paper (an adaptation of [1]) explains the standard features of the IEC 61850 Generic Object-Oriented Substation Event (GOOSE) message and how to configure them correctly for use in exchanging protection signals.

Protection system applications include protective relays, voltage- and current-sensing inputs, dc control circuitry, station dc supply, and the communications network. Self-tests within the relays determine the health of firmware execution and communications port functions. Other diagnostics provide the status of communications interfaces and out-of-range warnings for input signals and dc power. Self-testing of the receipt of protection signals via digital messages (described in this paper as message quality) is performed by supervising the correct and constant receipt of the digital messages. Message quality is calculated individually for each subscriber and for each GOOSE message exchange. Message quality self-testing confirms the correct operation of the protection devices, dc control circuitry, station dc supply, and the communications network. It cannot verify voltage- and current-sensing inputs, but these diagnostics can be delivered as part of message contents.

Best engineering practices maximize the ability of the communications network to correctly deliver digital messages between devices. However, because communications networks are not fail-safe, internal relay message receipt self-tests, such as message quality, are necessary to indicate failure. Failure is detected and message quality set to bad when monitoring detects that messages are not received as expected, are received out of sequence, or are corrupted. The 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 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. 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 is 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 in order to reduce traffic on the shared-bandwidth Ethernet network. 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.

2.1 Typical substation automation system network

An example distribution substation one-line diagram is shown in Fig. 1a, and the corresponding architecture of the communications network based on the IEC 61850 standard is shown in Fig. 1b.

2.2 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 intelligent electronic devices (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 local-area network (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.

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.

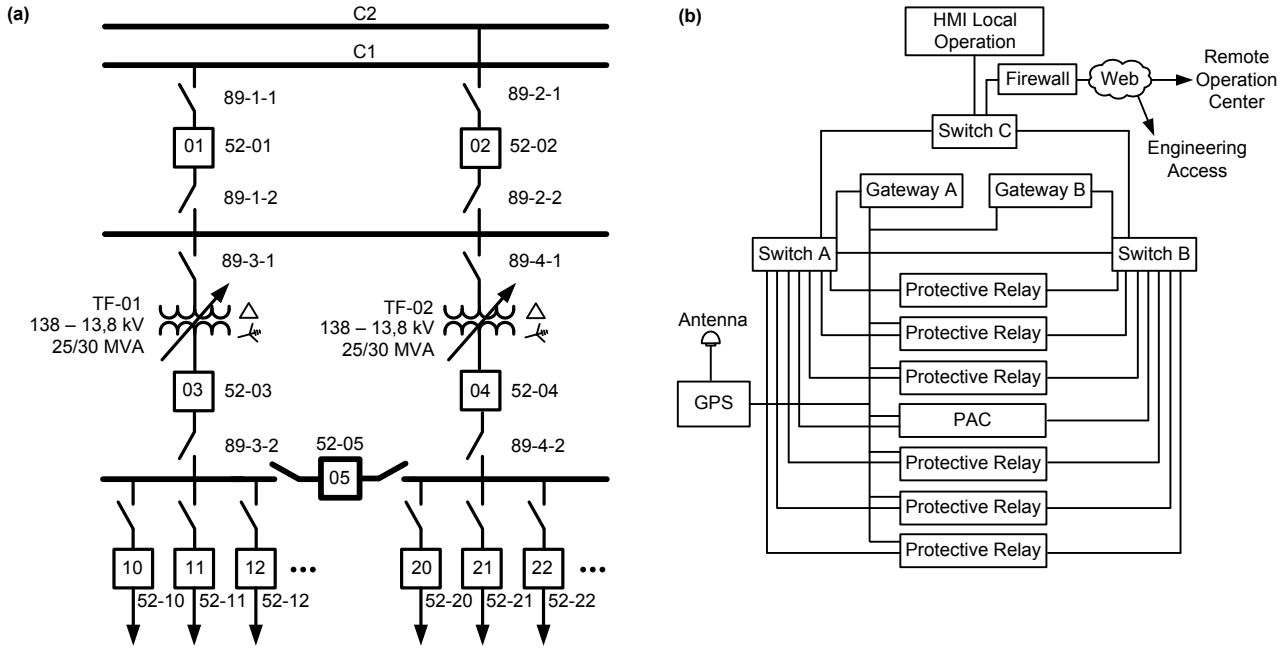

Fig. 1. Typical substation one-line diagram (a) and data communications network (b)

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.

2.3 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 signal exchange for protection must be done via the message classification Type 1 or Type 1A fast message. This requires that a message be published immediately after the signal status changes value, which 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 bursts of 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. 2 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 as well as 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. 2. 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. 2, until it reaches MT and is published as a steady state.

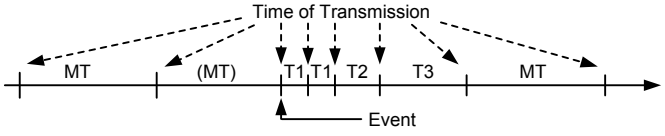

Fig. 2. Example of changing time between message publications (from IEC 61850-5)

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. 2. 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.

2.4 IED communications supervision and status

Protection, monitoring, and control IEDs have internal binary variables driven by the supervision of the GOOSE subscription process. Each GOOSE subscription has an associated logic variable called *message quality* that represents the success or failure of the GOOSE exchange. This binary logic value (0 for success and 1 for failure), in turn, represents the status of the signal exchange driving the communications-assisted logic. If the signal exchange fails, this failure must be detected immediately in order to adapt the logic to not misoperate in the absence of communications.

These binary variables are not only used in internal logic to dynamically modify algorithms but are also published to supervisory control and data acquisition (SCADA) systems and human-machine interfaces (HMIs) to provide network status information. Alarms based on these statuses are used to dispatch maintenance teams 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.

2.5 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. IED GOOSE reports display the status and configuration of published and subscribed GOOSE messages. These reports support 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 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*.

2.6 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. 3 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 a 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 a breaker failure indication. When the transformer relay either receives a block signal from the feeder relay or detects a 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.

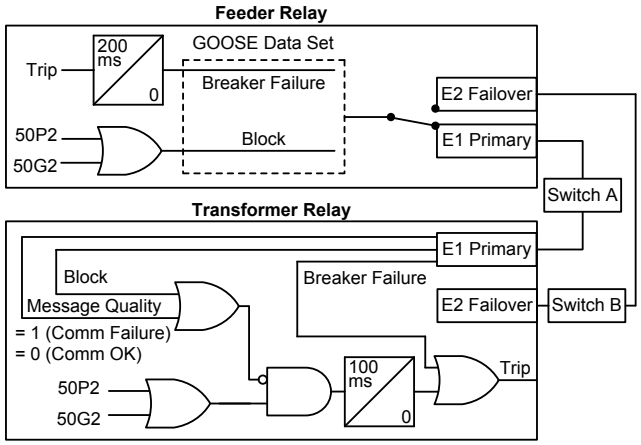

Fig. 3. Use of GOOSE message quality status in IED logic

The typical logic example in Fig. 3 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*.

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 a 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.

2.7 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 by supervising 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.

2.7.1 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. 4 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.

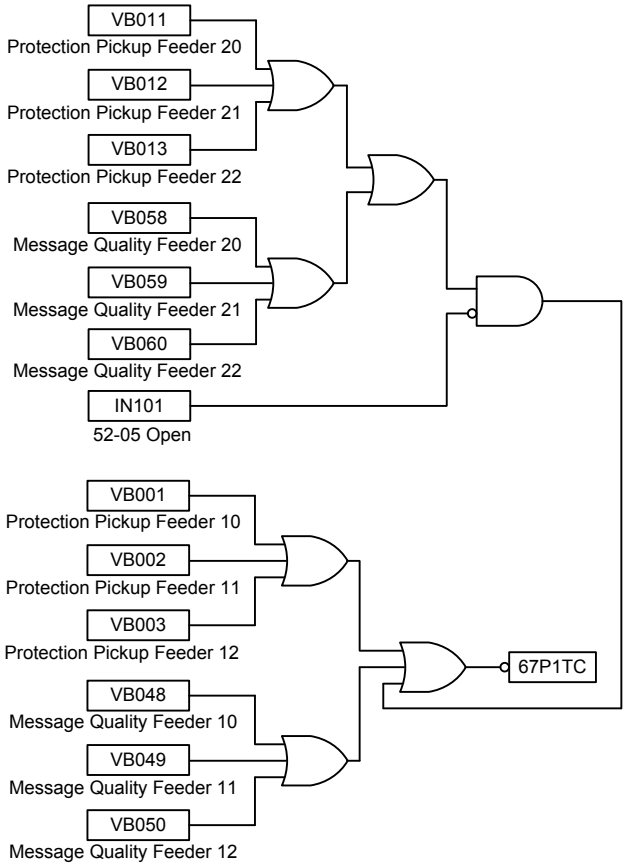

Fig. 4. Selectivity logic in Breaker 52-03 relay

In Fig. 5, 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. 5 illustrates the 52-03 breaker relay trip logic being conditioned by torque control (selectivity) or relying on coordination timers.

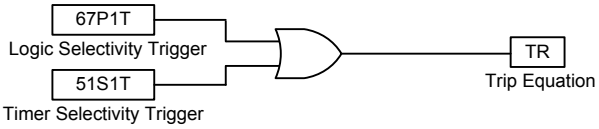

Fig. 5. Logic in Breaker 52-03 relay chooses coordination timer trigger only if 67P1T selectivity trigger is not set

2.7.2 Circuit breaker failure

The circuit breaker failure scheme shown in Fig. 6 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. 6 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. 6 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.

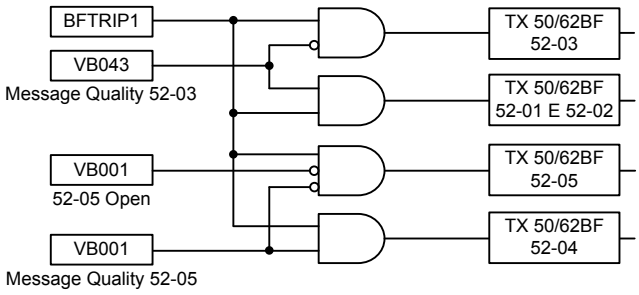

Fig. 6. Circuit breaker failure scheme

2.7.3 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 automatic transfer to the backup line.

The relays protecting the feeds into the substation monitor the voltage of the line in operation (Fig. 7a). Absence of voltage on the active feed (C1) indicates Line 1 – Dead (Fig. 7a) and presence on the other line (C2) indicates Line 2 – Live. The ALT logic (Fig. 7b) confirms correct operation of C2 and that the switches on either side of Breaker 52-02 are closed. This triggers the start of the ALT by setting ALT Start = 1 after the automation sequence timer expires.

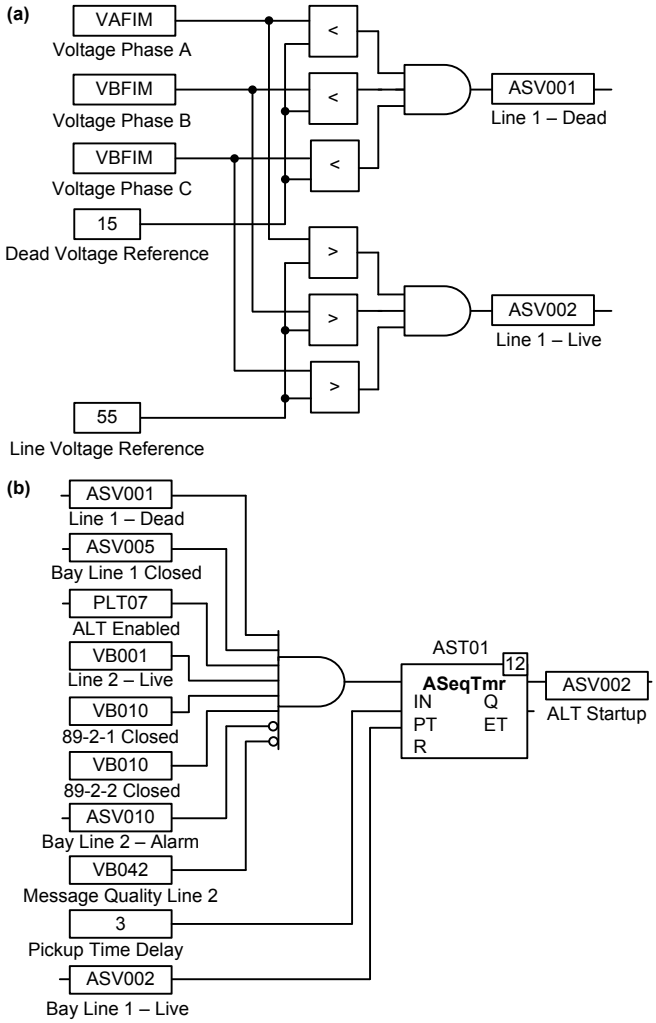

Fig. 7. Voltage monitoring (a) and ALT startup (b)

3 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.

Reference

[1] P. Franco, G. Rocha, and D. Dolezilek, "Case Study: Increasing Reliability, Dependability, and Security of Digital Signals Via Redundancy and Supervision," proceedings of the 5th International Scientific and Technical Conference, Actual Trends in Development of Power System Relay Protection and Automation, Sochi, Russia, June 2015.