Fully Monitoring Protection and Control Systems

Craig Wester
Member, IEEE
GE Digital Energy Multilin
Norcross, GA
Craig.Wester@GE.com

Terrence Smith
Member, IEEE
GE Digital Energy Multilin
Birchwood, TN
Terrence. Smith@GE.com

Abstract -- Modern microprocessor-based IEDs offer many functions, which are underutilized by the industry. This paper will discuss using IED functionality to fully monitor the protection and control system, which will identify problems within the system before they manifest themselves by miss-operation. This paper will also discuss the use of these monitoring systems to lengthen the time intervals required for periodic testing of the protection and control system. Some of the monitoring techniques to be discussed include: trip coil, close coil, and lockout relay monitoring, usage of IED self-test alarm contacts, instrument transformer failure detection using analog GOOSE messaging & other level detection/comparison methods, breaker restrike detection, station battery monitoring, oscillography cross-triggering, automated contact input & output testing and natural testing by event analysis.

INTRODUCTION

Modern microprocessor based IEDs offer many advantages over their electro-mechanical counterparts. One of these advantages is the ability to monitor the IED health and the health of the protection and control system and raise an alarm if any monitored function is amiss. This ability to monitor the protection and control system gives the utility the capability to continuously insure the health of the protection and control system. The only way to insure confidence in an unmonitored protection and control system is to test the system. This includes not only testing the protective relay functions, but also testing the overall protection and control system.

As utilities look for low-hanging fruit to reduce their overhead expenses, the maintenance and testing of the protection system is an obvious target. The North American Reliability Council (NERC) has recognized that the reliability of an individual protection and control system can have dramatic effects on the overall electrical grid. To increase the reliability of the protection and control systems that could impact the grid, NERC has enacted reliability standards that ensure protection systems are maintained and tested [3]. PRC-005 defines requirements that NERC has enacted to ensure that protection systems are maintained. PRC-005 is under revision and the revisions to PRC-005, while maintaining the reliability of the electrical systems, gives utilities opportunities to utilize monitoring of the protection and control system to reduce maintenance costs. The primary mechanism that utilities can utilize to lower their maintenance costs is to increase the time interval required to test their protection systems. The draft version of PRC-005 recognizes that a fully monitored protection system does not need to be tested as frequently as an unmonitored protection system.

PRC-005, at the time of this writing, is in draft form. The draft document makes recommendations on time based maintenance intervals and allows a longer interval between testing for an unmonitored system verses a monitored system. For protective relays, the requirement for an unmonitored system is once every six years, while the requirement for fully monitored systems is once every twelve years. For a system to be considered fully monitored, it must meet the following minimum requirements [3]:

- Internal self diagnosis and alarming
- Voltage and current waveform sampling three or more times per power cycle and conversion of the samples to numeric values for measurement calculations by microprocessor electronics that are also performing self monitoring and alarming.
- Alarming for power supply failure.

For protective relays meeting the requirements above, the testing requirements of every twelve years are: verifying settings are as specified, verifying operation of the relay inputs and outputs that are essential to the proper function of the protection system, and verifying acceptable measurement of power system input values.

The testing requirements above can be reduced to: verifying only the unmonitored relay inputs and outputs that are essential to proper functioning of the protection system, if the relay meets the requirements above and:

- AC measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error.
- Some or all binary or status inputs and control outputs are monitored by a process that

continuously demonstrates ability to perform as designed, with alarming for failure.
- Alarming for change of settings.

The requirements and tests listed above pertain only to the IED or protective relay. Testing requirements and monitoring methods are also specified in PRC-005 for communications systems, voltage and current sensing devices, station DC supply, and control circuitry. Several of these requirements and monitoring methods are detailed in the remainder of this paper as well as methods to monitor the protective relay.

IED Alarming

One of the primary requirements for a protective relay to be considered as monitoring is that the relay has self-test diagnostics, be able to alarm for failure of those self-test diagnostics and also to be able to alarm for failure of the relay power supply. This is a critical function of the relay because failure of either self-diagnostics or failure of the power supply can prevent the relay from operating. Most microprocessor relays are equipped with a form-C contact, as shown in Figure 1 that is operated by a relay critical failure or loss of control power.

Figure 1 – Critical Fail Contact

The contact in Figure 1 is shown in its shelf-state. Shelf-state would mean that the relay is un-powered, so the shown state is how the relay would appear failed. To truly monitor this system, the contacts to wire to an alarming IED should be B1b-B1a. Wiring to B1b-B1a will give the receiving monitoring device a closed contact while the relay is healthy. Using a closed contact gives the alarming device the ability to not only monitor the relay health, but also the health of the alarm circuit, because if the circuit continuity is lost, an alarm is given. It is recommended to wire the self-test alarm contact to an adjacent relay and vice versa. This will allow the communicating relay to alert SCADA of a failure of a neighboring relay.

In addition to the critical failure alarm, there are also several other non-critical alarms that need to be monitored. These alarms include: when a communication path is lost, when a remote IEC61850 device is "offline", when the IRIG-B time signal is lost, or when the relay is experiencing an unusually high ambient temperature.

PRC-005 gives an exemption to some of the required testing if an alarm can be raised for a change of settings. Figure 2 illustrates an overall security alarm logic. In this logic the operand VO6 is asserted when a successful password has been entered and a setting is attempted. The operand VO6 could be mapped to an output contact or a communications point to raise an alarm for an attempted settings change. Additionally the operand VO5 is asserted when an incorrect password attempt is made on the relay. The combination of these two alarms could be used to raise a global security alarm for the IED.

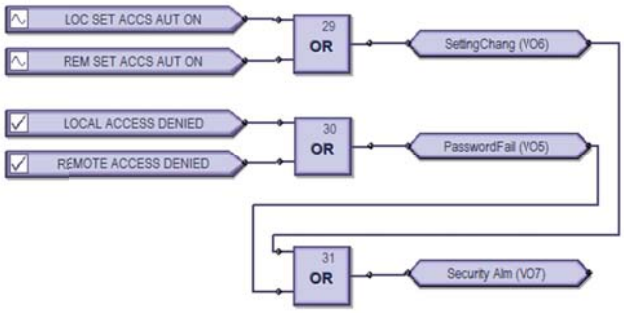

Figure 2 – Security Alarm

Trip Coil, Close Coil, and Lockout Continuity Monitoring

The monitoring of the dc continuity of trip circuits, close circuits and lockout relay circuits use the voltage across the circuitry as shown in Figure 3. This can be accomplished by using a spare contact input of a relay or the internal voltage monitoring circuitry of an available relay output contact (shown as V) in the below Figure 3. Logic can be created to monitor the trip circuit when the breaker is closed and the close circuit when the breaker is open. No need of monitoring the trip circuit when the

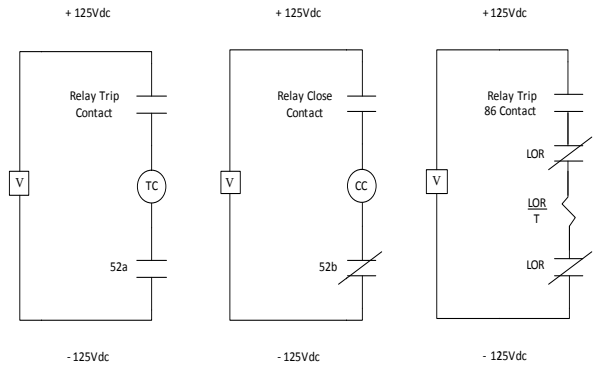

Figure 3 – Trip, Close & Lockout Circuit Monitoring

breaker is open nor monitoring the close circuit when the breaker is closed. For the trip circuit, the voltage monitor will be "on" or "Von" when the breaker is closed and indicates a healthy circuit. If the voltage is absent when the breaker is closed, an alarm will be given for a faulty trip circuit (i.e. "Voff"). For the close circuit, the voltage monitor will be "on" or "Von" when the breaker is open and indicates a healthy circuit. If the voltage is absent when the breaker is open, an alarm will be given for a faulty close circuit (i.e. "Voff"). Similarly an "open circuit" alarm can be created for the lockout relay circuitry (Figure 3) by monitoring the voltage across the circuit and alarming when the voltage is "off" or not present.

INSTRUMENT TRANSFORMER VERIFICATION

PRC-005 requires testing of the voltage and current sensing devices without monitoring every twelve years. Devices that are monitored have no periodic maintenance interval specified and monitored is defined by: "Voltage and Current Sensing device connected to microprocessor relays with AC measurements are continuously verified by comparison of sensing input value as measured by the microprocessor relay to an independent ac measurement source, with alarming for unacceptable error or failure" [3].

Most critical protection systems have either redundant protective relaying or backup protective relaying. Typically, each set of relays is sourced from different instrument transformers. This type of redundancy is shown in Figure 4 where an "A" and "B" set relay protect each line. In this scheme, each relay is sourced from different three-phase current transformers. The "A" set relay could be configured to pass the RMS value of the current readings from the CTs that it is connected to, to the "B" set relay using an IEC61850 Analog GOOSE message and vice versa. The "A" and "B" set relays would use a comparator function to compare two RMS values and operate if the difference between the values is greater than a setting. The comparator could be used to raise an alarm if its RMS measured current is significantly different than the IEC61850 Analog GOOSE message it receives from the "A" set relay of RMS current. Since this is an alarm function, the time delay on the comparator could be set to accommodate any latency of the communication channel. These alarms would be blocked during fault conditions. This type of alarming should meet the requirement that the AC measurements are continuously verified by comparison with alarming for error or failure. This would also allow verification of correct CT and PT settings in each relay.

Monitoring the potential transformers in Figure 4 presents a challenge since the "A" set and "B" set relays

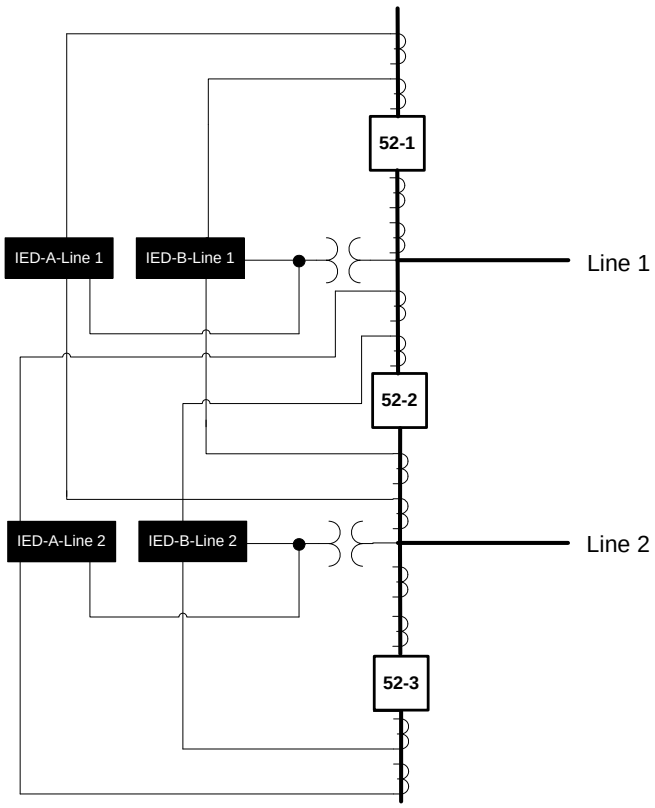

Figure 4 – Breaker and a Half Scheme

are both connected to the same potential transformers. In this instance, as long as the breaker 52-2 is closed, the voltage on the Line 1 relays should be the same as the voltage on the Line 2 relays. The Line 1 relays could send the RMS values of voltage to the Line 2 relays via an Analog IEC61850 GOOSE message. The comparator in the Line 2 relays could then be set to raise an alarm if the measured voltage values are different than the received RMS value (via Analog IEC61850 GOOSE) from Line 1 relay. These voltage comparison alarms would be blocked during fault conditions,

The microprocessor-based relay can also be used to monitor Capacitive Coupled Voltage Transformers (CCVTs). CCVT manufaturers state that if any phase voltage angle of the CCVT changes or drifts by 5 to 10 degrees it could be an indication of a CCVT problem brewing. Similarly, if any voltage magnitude changes by 5-10%, the CCVT could be experiencing a problem and the utility needs to investigate further. Figure 5 shows the CCVT alarm logic that can be created within the protective relay.

Another monitoring method is to detect voltage transformer fuse failure (or VTFF) and raise an alarm and/or block elements that may operate incorrectly for a full or partial loss of AC potential caused by one or more

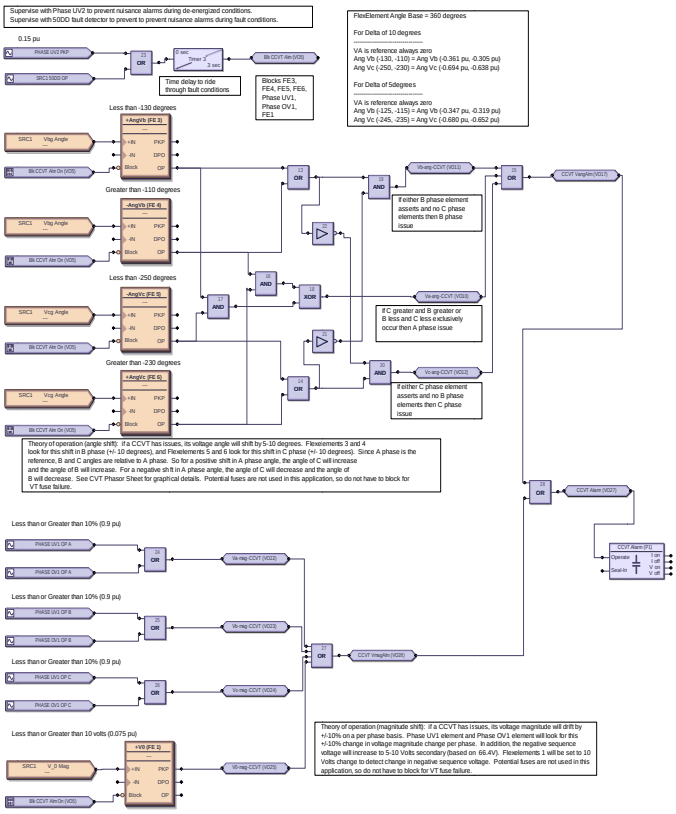

Figure 5 – CCVT Failure Monitoring

blown fuses. Some protective elements that might be blocked are distance, voltage restrained overcurrent and directional current. There are two classes of voltage transformer fuse failure that may occur; Class A - loss of one or two phases and Class B - loss of all three phases. Different means of detection are required for each class. An indication of Class A failure is a significant level of negative sequence voltage, whereas an indication of Class B failure is when positive sequence current is present and there is an insignificant amount of positive sequence voltage. These noted indications of fuse failure could also occur when faults are present on the system, so a means of detecting faults and inhibiting fuse failure declarations during these events is required. Once the fuse failure condition is declared, it should be sealed-in until the cause that generated it disappears. Also, the VTFF function is inhibited when the monitored circuit is de-energized, such as positive sequence voltage and current are both below threshold levels. Figure 6 shows an example of VTFF logic.

The microprocessor based relay can be configured to detect problems with system current transformers used to supply currents to the relay. The logic detects the presence of a zero-sequence current at the supervised

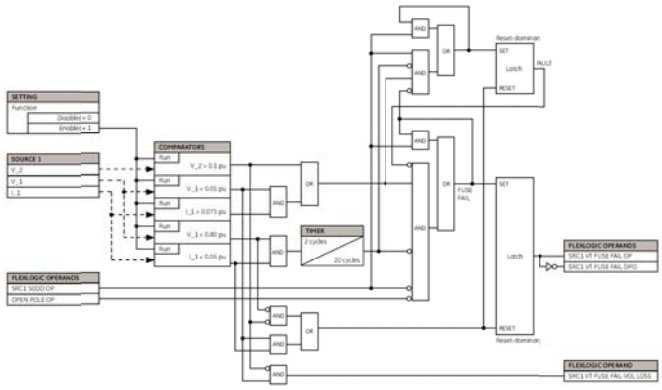

Figure 6 – VT Fuse Failure Logic

source of current without a simultaneous zero-sequence current at another source, zero-sequence voltage, or some protection element condition. This CT failure logic (Figure 7) is based on the presence of the zero-sequence current in the supervised CT source and the absence of one of three or all of the two following conditions:

- Zero-sequence current at different source current (may be different set of CTs or different CT core of the same CT).
- Zero-sequence voltage at the assigned source.

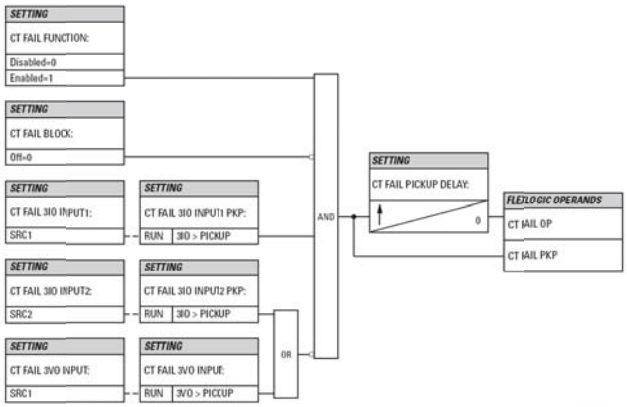

Figure 7 – CT Failure Logic

BREAKER RESTRIKE DETECTION

According to IEEE standard C37.100: IEEE Standard Definitions for Power Switchgear, restrike is defined as "a resumption of current between the contacts of a switching device during an opening operation after an interval of zero current of ¼ cycle at normal frequency or longer".

The protective relay with its connected 3 phase currents can detect breaker restrike. An indication can be provided to SCADA of the breaker restrike and logged by the relay for further analysis. Breaker restrike can be detected on several transmission applications, such as transmission line breakers, capacitor bank breakers and transmission breakers feeding large transformers. A typical restrike waveform and detection flag is shown in Figure 8.

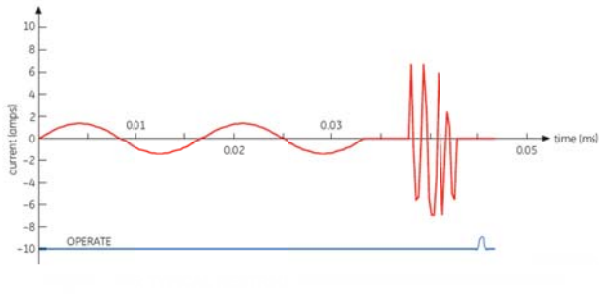

Figure 8 – Typical Restrike Waveform and Detection Flag

The breaker restrike algorithm responds to a successful interruption of the phase current following a declaration of an open breaker. If a high-frequency current with a magnitude greater than the threshold is resumed at least ¼ of a cycle later than the phase current interruption, then a breaker restrike has occurred in the corresponding phase.

A restrike event is declared if all of the following conditions are true: (1) the current is initially interrupted, (2) the breaker status is open, and (3) an elevated high frequency current condition occurs and the current subsequently drops out again. A distinction is made between a self-extinguishing restrike and permanent breaker failure condition. The latter can be detected by the breaker failure function or a regular instantaneous overcurrent element. Also, a fast succession of restrikes will be picked up by breaker failure or instantaneous overcurrent protection

The user can add counters and other logic to facilitate the decision making process as to the appropriate actions upon detecting a single restrike or a series of consecutive restrikes.

STATION BATTERY MONITORING

The protective relay can monitor the health of the station DC battery system. An analog indication of the current DC voltage derived from a contact input or dcMA transducer input wired between the positive and negative rails of the battery system can be provided to SCADA and on the relay display. This signal can be used to generate high and low DC voltage station battery alarms.

A high dc voltage alarm can be configured to indicate the battery DC voltage is greater than a maximum value. This can result in loss of life, loss of electrolyte, and thermal runaway. The maximum value should be set above the expected voltage during an equalization charge.

A low dc voltage alarm can be configured to indicate the battery DC voltage is less than a minimum value. This can be a sign of the battery undercharging, which can lead to reduced cell capacity and sulfation. An undervoltage condition will also occur due to a charger failure.

The protective relay can monitor auxiliary alarm contacts from the battery charger system, such as:

- AC SUPPLY FAIL: Indicates the AC supply to the battery charger has failed.
- CHARGER FAIL: Connected to the charger critical failure contact and indicates the battery charger has failed.
- DC BREAKER TRIP: Indicates a DC distribution breaker has operated.
- DC GROUND FAULT: Indicates a battery DC ground fault.

The Sequence of Event (SOE) recorder of the relay can be used to record these alarms and the data logger of the relay can be used to record the station battery level or this value can be transmitted to SCADA for display and recording. An example of the wiring for the station battery monitoring is shown in Figure 9.

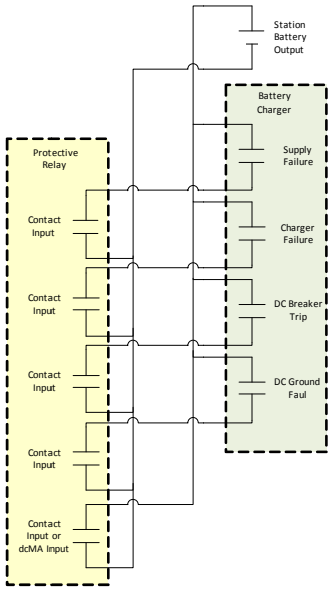

Figure 9 – Station Battery Monitoring

Oscillography Cross Triggering

Modern IEDs have the ability to record oscillography data and event data inside the relay. One of the most useful methods of testing is to analyze operations of the protective system to insure that the protective system operated as intended and identify and correct near misses. This method can be referred to as "natural testing". When using redundant relaying of different manufacturer as in Figure 4, an inappropriate operation or inappropriate non-operation often only involves one of the relays. It is impossible to analyze the forensics in the non-operating relay if the oscillography is not triggered and oscillography is typically only triggered on a trip. Therefore, it is necessary to cross-trigger the oscillography, so that a trip in one relay causes all the relays in the station to also trigger oscillography (i.e. an "oscillography trip bus" or station digital fault recorder). This can be accomplished with contact outputs and a wired oscillography trigger, but a better implementation of this type of multi-cast message would be to cross trigger with IEC61850 GOOSE messages.

The event shown in Figure 10 is an example of analysis using cross triggering. This event comes from a transmission line with redundant relaying. In this event, the B and C phase CCVTs developed a problem and the B-C phase voltage presented to the relay would have been zero. The "A" set relay operated appropriately, but not as intended since it was an undesired trip. With the voltages presented to the relay, the "A" set relay operated correctly. The "B" set relay did not operate for this event.

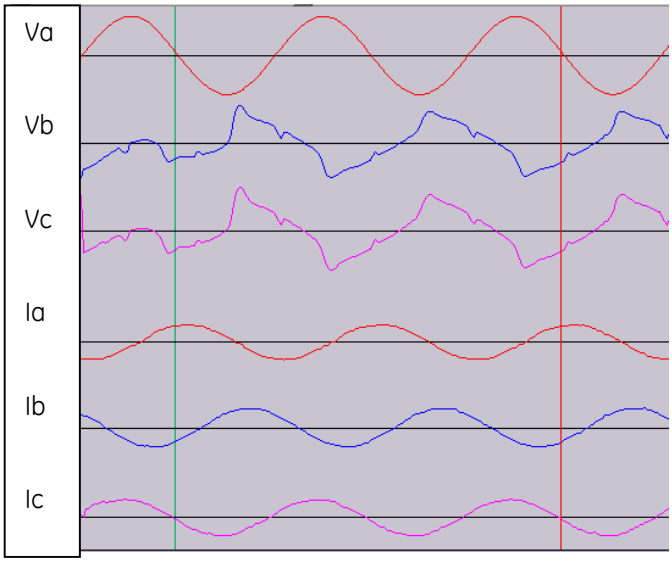

Figure 10 – Cross Triggered Event

In the event of Figure 10, the "B" set relay was cross triggered and the event could be analyzed restoring confidence in the "B" set relay. The analysis revealed that the phase distance element was supervised by a current detector and the current level was not above the supervision level.

A second example of natural testing by event analysis is shown in the event record of Figure 11. This record comes from the transformer relay of a distribution substation where a trip on any feeder breaker triggers oscillography on the transformer differential relay. During this event, one of the distribution breakers tripped on a B-phase overcurrent. The transformer had a Delta to Wye phase conversion and analysis of the event shows the A-B phase current on the transformer primary was correct and the B phase current on the transformer secondary was correct. Additionally, the oscillography from the distribution relay could be merged with the transformer relay oscillography to compare the magnitudes and waveforms between the two relays. This analysis verifies the current transformer, CT circuits, and the relay current inputs.

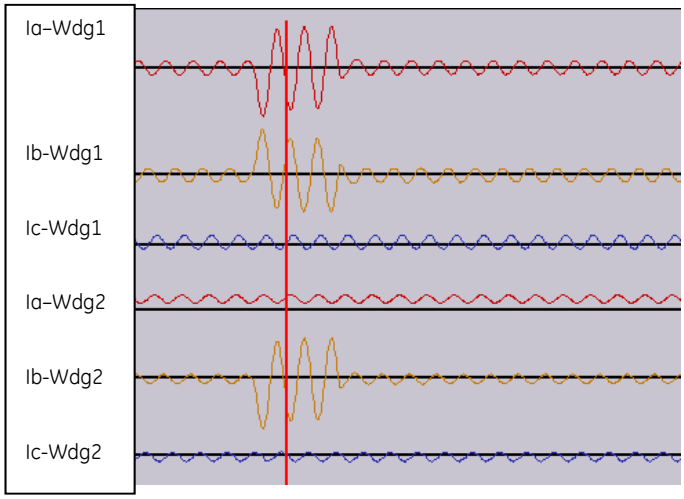

Figure 11 – Transformer Event Record

Setting Comparison

Another beneficial software tool to the utility industry is the comparison of settings in the relay "as found" to "as left". This comparison meets the PRC-005 requirement of "verifying settings are as specified" [3]. The function could be automated and provide an alarm if any settings have changed.

On-line Real-Time I/O Verification

With the use of creative wiring and form C contact outputs of the relay, on-line real-time testing can be

accomplished for critical or control relay contact outputs. Logic can be developed within the relay, to periodically test the actual working of an output contact and raise an alarm if the contact should fail. Protective relay trip and close outputs can be tested as shown in Figure 12 using the current coil monitoring of the relay output contact ("Ion"). For a trip circuit, logic can be developed to quickly connect the trip contact to DC battery negative through a resistance (such as 1000 Ohms) and energize the form C contact within milliseconds (within 2-4ms). If the contact is healthy, the current coil detector will operate (or "Ion"). If the contact does not close or is faulty, the current coil detector will not operate and an alarm can be issued. Similarly, logic can be developed for the relay close contact as shown in Figure 12.

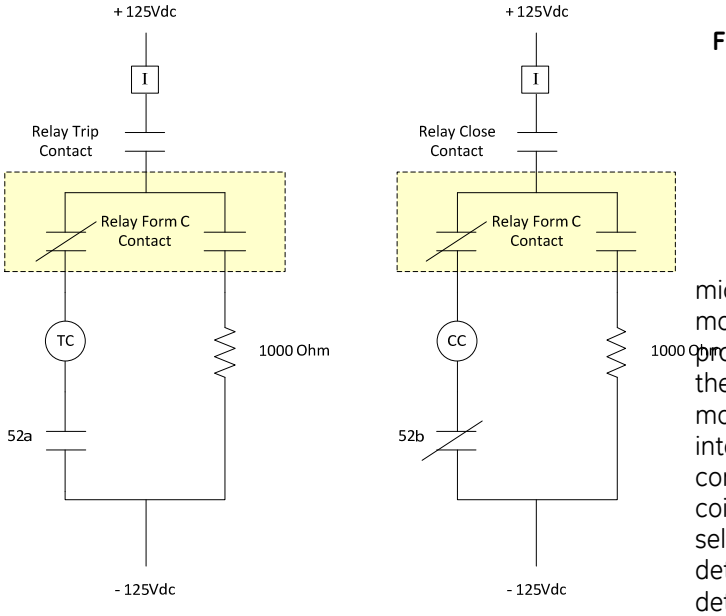

Figure 12 – Real Time Trip & Close Relay Contact Output Testing

In addition, critical relay contact inputs, such as breaker failure initiate, start carrier, etc. can be on-line real-time tested by using form A contact outputs of the relay. Logic can be developed to quickly connect the critical input contact to the relay and test if it is recognized by the relay. Necessary functions that are normally affected by the tested input contact would be temporarily disabled during the short test period (2-4ms). Figure 13 shows an example of the wiring to automatically test a critical input contact of the relay using programmable logic. The relay could be temporarily put into "test mode" such that all relay output contacts are disabled temporarily during the input contact tests.

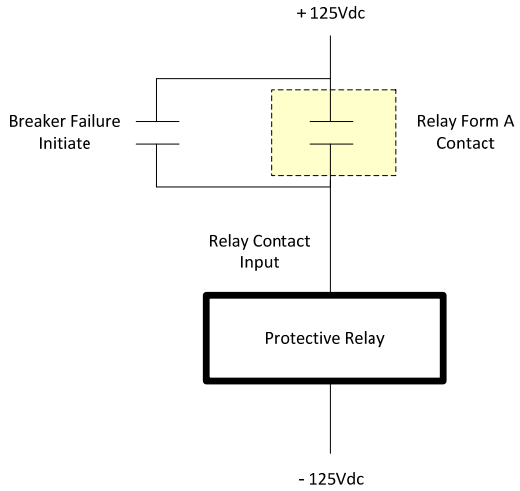

Figure 13 – Real Time Testing of Critical Relay Contact Inputs

CONCLUSIONS

The flexibility and configurability of today's microprocessor based protective relays allow a utility to monitor the protection and control system and identify problems within the system before they manifest themselves by miss-operation. With the use of these monitoring techniques a utility could lengthen the time intervals required for periodic testing of the protection and control system. The monitoring techniques include: trip coil, close coil, and lockout relay monitoring, usage of IED self-test alarm contacts, instrument transformer failure detection using analog GOOSE messaging & other level detection/comparison methods, breaker restrike detection, station battery monitoring, oscillography cross-triggering, and automated contact input & output testing. The relay sequence of event recorder (SOE) can be used to record the occurrence and time of these monitoring alarms of the protection and control system. In addition, these monitoring techniques increase the reliability of the protection and control system and enable the utility to have a smarter/intelligent protection and control system.

BIOGRAPHIES

Terrence Smith has been an Application Engineer with GE Digital Energy Multilin since 2008. Prior to joining GE, Terrence has been with the Tennessee Valley Authority as a Principal Engineer and MESA Associates as Program Manager. He received his Bachelor of Science in Engineering majoring in Electrical Engineering from the University of Tennessee at Chattanooga and is a professional Engineer registered in the state of Tennessee.

Craig Wester is the southeast US Regional Sales Manager for GE Digital Energy Multilin in Norcross, Georgia has been with GE for 21 years. He was born in Belgium, Wisconsin, and received a B.S. in Electrical Engineering with a strong emphasis on power systems from the University of Wisconsin-Madison in 1989. Craig joined General Electric in 1989 as a utility transmission and distribution application engineer. He is a member of the IEEE.

REFERENCES

[1] T. Smith and R. Hunt "Fully Utilizing IED Capacity to Reduce Wiring" 64th Georgia Tech Protective Relay Conf. May, 2010.

[2] C. Wester and M. Adamiak "Practical Applications of Ethernet in Substations and Industrial Facilities" 64th Georgia Tech Protective Relay Conf. May, 2010.

[3] North American Electric Reliability Corporation, *"Transmission and Generation Protection System Maintenance and Testing "*, Standard PRC-005-1. (Draft)

[4] *D60 Line Distance Protection System Instruction Manual*, GE Publication GEK-113519.

[5] *E. Udren and C. Rogers "The New NERC Protection System Maintenance Standard"* 64th Georgia Tech Protective Relay Conf. May, 2010.