Holistic Security

Roy Moxley, William Credle – Siemens USA

moxleybr@gmail.com

USA

Abstract - Relay security has always been a concern to protection engineers. Recent data collected by the I-27 working group of the IEEE PSRC (regarding relay self monitoring) suggests that on the order of 3% of all relay trips are falsely caused by relay hardware issues. Setting errors and unanticipated system issues cause additional false trips. Because of the system impact of these misoperations, NERC has increased reporting requirements of false trips and with a changing generation mix, reclosing can no longer be counted on to "cure all ills".

Microprocessor technology has advanced to the point that proper protection design can greatly reduce or eliminate these misoperations. Improved hardware eliminates failure modes. Combined measurements can eliminate polarizing errors. Added measurement quantities provide new security techniques.

This paper discusses details of how security is improved by combining these and other advances. Changes in the power system dynamics put a premium on security to provide continuity of power to our end users. As engineers it is up to us to make the best use of new technology to maintain our traditional high level of service.

Introduction –

A relay misoperation is perhaps one of the worst things that can happen to an electric power system. First there is the direct element tripped by the relay (transmission line, transformer, generator, etc), then there may be an actual fault on the power system that caused the overtripping and will be cleared by another relay. The misoperation has a high probability of turning a single contingency into a double contingency. The majority of misoperations can be categorized into a few areas [1]:

Design errors/ Logic Incorrect/ settings

Relay failures / malfunctions

Communication failures

A systemic approach to correcting these issues would greatly reduce misoperations. Planning for the unexpected is part of any protection engineer's job description so each of these three areas can be addressed by a design approach.

Design / Logic / Settings

When it comes to relay design, it is important to recognize that a microprocessor is not limited to those techniques used in electromechanical relays. A modern relay can process information from multiple elements at the same time. It can "remember" quantities from cycles or seconds earlier. It can use remembered and combined quantities to create improved security without sacrificing sensitivity.

Line Protection –

One of the major causes of loss of directionality or overreaching in a line relay is an improper signal from the polarizing element. In electromechanical relays the selection of polarizing, ground current, negative

sequence voltage or current, was done in the design of the relay. In earlier microprocessor relays it was possible to select the polarizing quantity. This was somewhat improved by selecting the order in which the polarizing quantity was chosen. The problem with this system is that the first polarizing quantity with a sufficiently measurable signal is selected, whether it is the most accurate or stable is not a factor. The ability for a modern relay to evaluate multiple signals, and even combine them, can be used to improve this polarizing selection [2]. As discussed in the reference, this improved selection of polarizing quantity specifically reduces false tripping.

Differential line protection is a simple concept that has worked well as long as communications and current measurements are all correct. False trips from line differential relays occur when errors are not properly accommodated by the relay. Consider the actual and distorted waveform shown in figure 1.

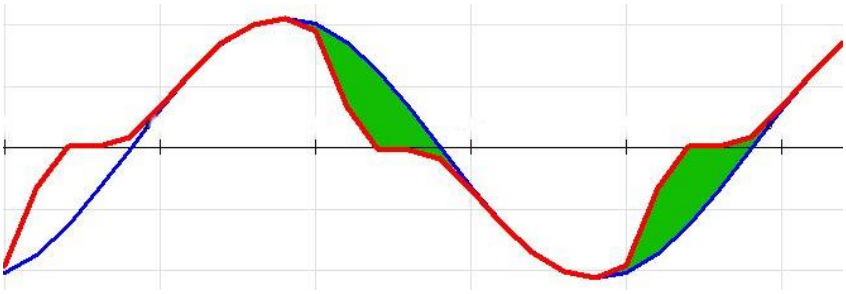

Fig. 1- Primary and Measured waveform.

An electromechanical relay can only "see" the measured waveform. It can use a harmonic restraint principle but it is difficult to accurately remove the error. Typically an electromechanical relay only removes one or two harmonics to approximate the error. Early microprocessor relays also only removed a subset of the harmonics present as they were limited by the sampling rate. A modern microprocessor relay does not have the same limitations. By removing error components caused by saturation or asymmetry of communications we can improve the differential relay performance as shown in figure 2.

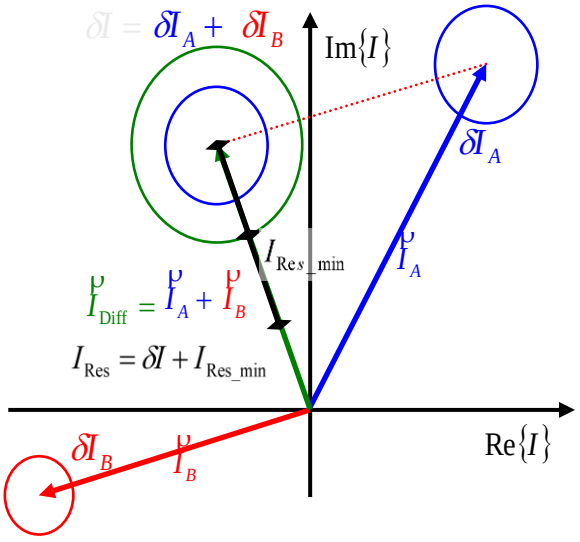

Fig 2- Resultant signal from the sum of two measurements including errors.

In the case shown in figure 2, a difficult line differential signal (2 currents almost out of phase, indicating an internal fault with significant outfeed) still results in a correct trip even with error signals subtracted

from the operate signal. Clearly subtracting error signals from the operating vector, in a way impossible with older relays, improves security.

Bus Protection –

Kirchoff's current law makes bus protection one of the simplest forms of high speed relaying. The problem, just as we see in figure 1 above, is that saturation causes an incorrect operate signal. The problem is compounded by the need for high speed tripping to maintain stability coupled with the need for high security, also to maintain stability. High impedance bus differential relaying provides both the high speed and security but comes at the "cost" of dedicated CTs all of the same ratio. Microprocessor relaying can solve the problem of high speed and security by using another capability not available in an electromechanical device; conditional logic and rate of change measurement[3]. Generally speaking CTs will not saturate in the first ¼ cycle. A microprocessor relay can use one set of logic for the first quarter cycle and another set of logic for the time after that.

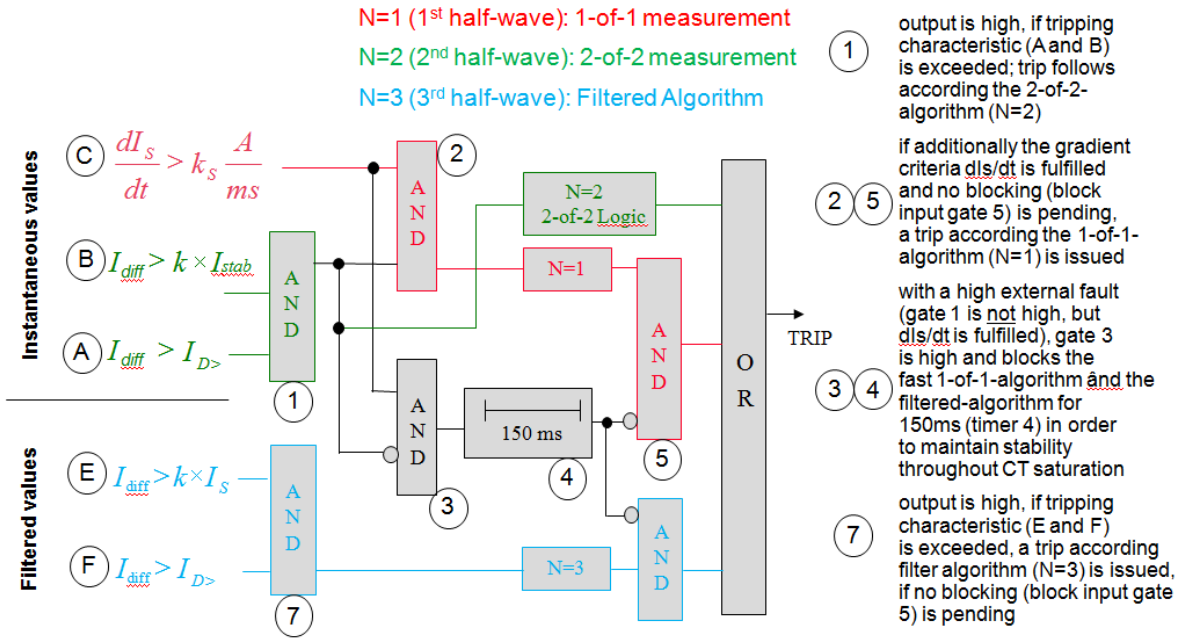

Fig.3- High Speed Bus Differential Logic.

This provides for fast tripping for severe faults without the risk of false tripping in a case of severe CT saturation. Figure 3 shows the complete logic for the different time periods used in a particular bus relay. Three different logics are used for each of the first three half cycles. While speed is one deliverable of this type of logic, security is the other. CT saturation could occur any time after the first quarter cycle and no trip would be produced. With electromechanical relays speed was purchased with the loss of security. Using microprocessor technology in ways that don't duplicate electromechanical logic, speed is improved by having security elements built into the measuring system.

Transformer Protection –

Microprocessor relays are typically not used for sudden pressure or other mechanical issues with transformers but differential relays are a major security concern. Consider the transformer inrush characteristic shown in Fig. 4[4]. Immediately after the transformer was energized it had 74.6% second harmonic current. After a few cycles the harmonics on B phase had reduced to just 6.8% second harmonic and the transformer relay misoperated. As transformers are being built with lower losses and

lower noise the amount of harmonics in the inrush has come down. The ongoing difficulty is that the inrush characteristic can change depending on the point of wave of the energization. In the case of the waveform of figure 4, the transformer had been in service for about ten years with no false trips. In electromechanical relays only harmonic blocking or restraint was available and that is what early microprocessor relays emulated. In more modern microprocessor relays the capability of pattern recognition is available. Notice in figure 4 that during an inrush there is a simultaneous "flat spot" in the current wave. This simultaneous flat spot is an indication that it is inrush being experienced and not a fault.

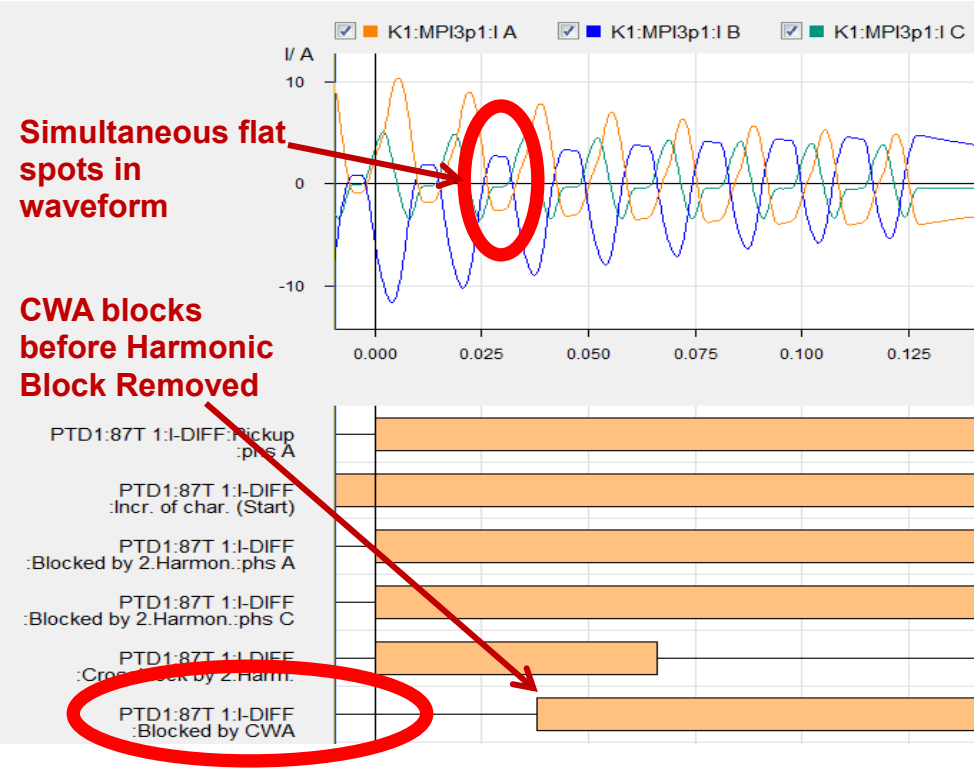

Fig. 4- Transformer inrush current

Having dual inrush detection system is clearly more secure than a single system, as demonstrated by replaying an actual trip event with a second blocking scheme and witnessing the elimination of the false trip.

Setting Issues -

Errors in settings have long been recognized as a significant security issue. Some setting calculations are so complex, or require so much system data, a correct setting is very difficult. Consider the power swings demonstrated in Fig. 5. These are simulations of the power swings resulting from a fault on a three machine system. The difficulties of setting a traditional blinder scheme have been compounded by non-traditional (and non-dispatchable) generation in remote locations. Based on the swings shown in figure 5 setting traditional blinders for power swing blocking is almost impossible.

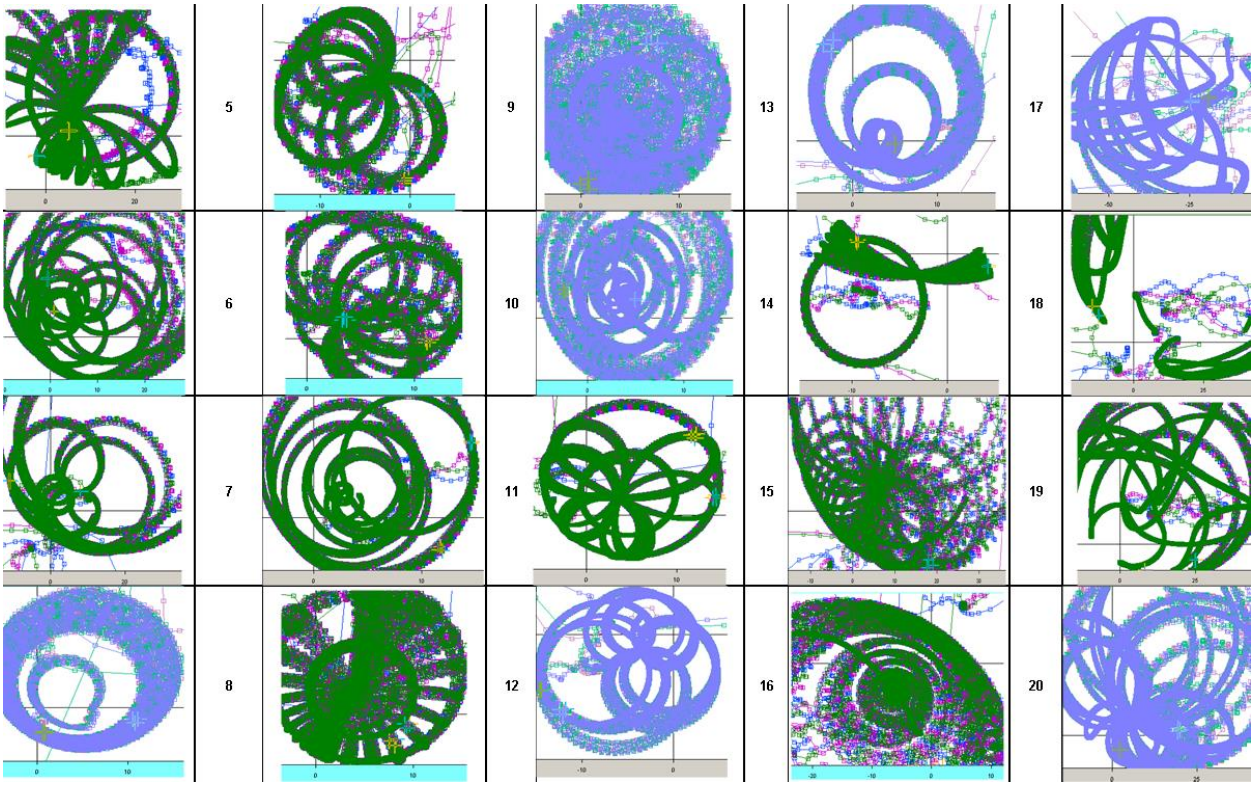

Fig 5- Out of step characteristics on a three machine system.

Instead of setting calculations, in more modern relays it is possible to have a “zero setting” element for power swing detection. One of these advanced element’s logic is described in figure 6.

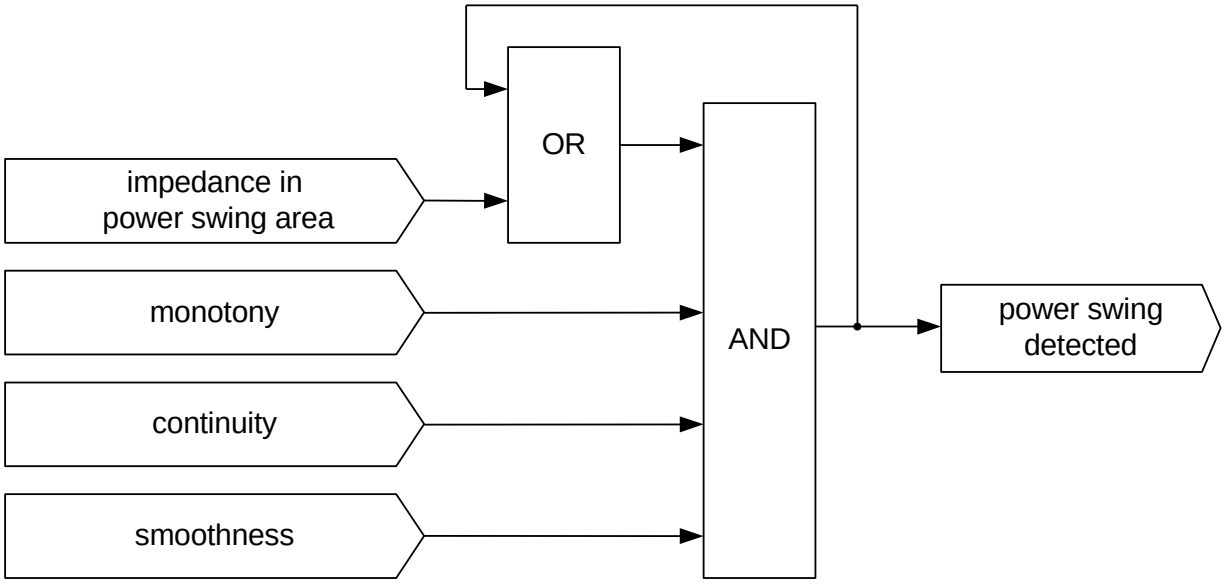

Fig. 6- Power swing detection logic.

The clear advantage of zero settings is that it eliminates the opportunity of a setting error causing a false trip. The polarizing logic, the transformer inrush detection , and the power swing logic described above are all zero setting elements (other than selecting them as “on”). While careful inspection and checking of

settings can reduce errors, it is a well-known saying that “quality cannot be inspected in”. The more we can eliminate settings, the more we can eliminate setting errors.

Relay failures and malfunctions -

Relays will fail; that’s just a fact of life. The best relays have greater than a 300 year MTBF but that means for every thousand relays a utility owns 3.3 will fail every year. The objective, from a security standpoint is to prevent any relay failure from causing a false trip. While self-monitoring of relays has improved there are still numerous reported instances of relays failing with a false trip [5]. The goal is to make the monitoring function of the relay faster than the fastest tripping element.

One method of accomplishing this is to use “fast current sum supervision”[3]. This method uses dual A/D converters, with the phase currents going to one converter and the neutral current going to another. The monitor performs a plausibility check whether the sum of the three phase currents is equal to the earth current. Or in other words:

$iA + iB + iC + iN = 0$

Of course inaccuracy has to be considered in order to avoid over sensibility and therefore
$IF = \left| iA + iB + iC + iN \right|$ is calculated.

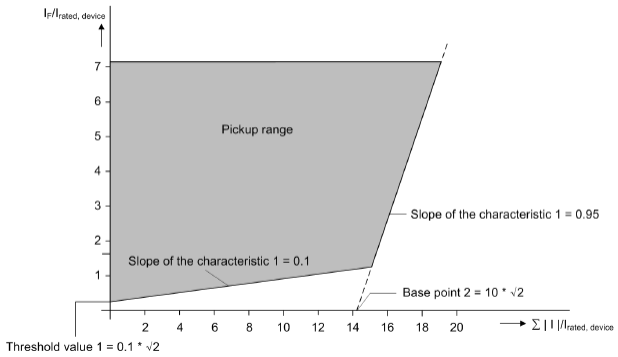

Fig. 1- Characteristic of fast current supervision

Whenever IF is in the pickup range, the protection is blocked immediately.

This calculation is done every millisecond based on instantaneous values and is only possible if the neutral point of the current is connected to an own current measuring input. This element can block tripping as fast as 2 ms which provides for securely tripping as fast as 3 ms for critical protections. While this element does not completely solve the problem of false trips on relay failures, it makes a major step forward.

Communication Failures –

If a blocking signal does not get through to an overreaching relay there may be a false trip. If a current differential signal is corrupted from one end of a transmission line to another there may be a false trip. If a direct transfer trip signal is incorrectly sent there may be a false trip. It is not surprising that communications problems are one of the leading causes of false trips given the many circumstances in today’s relay world that signals are exchanged between relays. The good news is that standards have been enhanced to provide for improved reliability of communications [6]. It is not enough to know that the signal has been sent. The system as a whole must establish that the signal has been received.

In IEC 61850 Edition 1 it was monitored that a message had been sent. In Edition 2 it is monitored that a message has been received. This is a major shift to improved signal reliability.

LGOS class				
Data object name	Common data class	Explanation	T	M/O/C
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22.		
Data objects				
Status information				
NdsCom	SPS	Subscription needs commissioning		O
St	SPS	Status of the subscription (True = active, False=not active)		M
SimSt	SPS	Status showing that really Sim messages are received and accepted		O
LastStNum	INS	Last state number received		O
ConfRevNum	INS	Expected configuration revision number		O
Settings				
GoCBRef	ORG	Reference to the subscribed GOOSE control block		O

Fig. 8- LGOS – GOOSE subscription supervision

In figure 8 we see that the status of a subscribed message is true if it is received within the time specified and false if the message timed out. By using this status in relay tripping logic, any system that uelies on communications can have improved security.

Conclusions

Improved relay algorithms add to security while reduced settings reduce setting errors. Both these advances lead to fewer false trips.

Newer relay designs, such as using dual A/D converters, improve security without compromising ultr-high speed protection.

New standards, such as IEC61850 Edition 2, improve communication security to enable more sharing of information between relays.

References:

[1] NERC Misoperations Report of April 1, 2013

[2] New Design of Directional Ground Fault Protection 67N, Joerg Blumschein- Siemens, Germany; presented at 2018 Conference for Protective Relay Engineers Texas A&M University

[3] “Ultra-High-Speed Bus Protection”, Roy Moxley, Christian Wallner, Rainer Goblirsch-Siemens; presented at 2016 Western Protective Relay Conference

[4] “False Trips on Transformer Inrush”, Raymond Ni, Peter Wang- ATCO Electric, Roy Moxley, Stefan Flemming- Siemens, presented at 2015 Georgia Tech Relay Conference

[5]Draft report of the I-27 working group of IEEE PSRC, “Relay Self Monitoring”

[6] “Recent Enhancements to System Reliability by Implementing IEC 61850 GOOSE and SV Monitoring via LGOS and LSVS Logical Nodes”, Rodrigo Munos, Cedric Haspiura, Farel Becker – Siemens, presented at 2018 PEAC conference