Advanced Protection, Automation, and Control Functions

Bogdan Kasztenny and Normann Fischer
Schweitzer Engineering Laboratories, Inc.

Revised edition released August 2010

Originally presented at the
1st Annual Protection, Automation and Control World Conference, June 2010

Advanced Protection, Automation, and Control Functions

Bogdan Kasztenny and Normann Fischer, *Schweitzer Engineering Laboratories, Inc.*

Abstract—**This paper reviews the historical background, present state, and future challenges and opportunities of microprocessor-based power system protection, control, and automation systems. The paper focuses on protection and control functions in terms of improved performance, new protection principles, addressing new challenges, and simplifying application. It excludes many associated fields, such as the role of communications, adaptive protection, or system integrity protection schemes.**

I. INTRODUCTION

This paper reviews advancements and the state of the art in power system protection, automation, and control. We focus on protection first and foremost and proceed briefly to automation and control. This paper covers progress in protection principles and ways of implementing them in microprocessor-based relays. Our intent is to summarize the evolution of the last few decades, the state of the art today, and some opportunities going forward. We narrow our discussion to just the protection and control (P&C) functions, leaving the many related topics such as IEC 61850 and the role of communication, synchrophasors, wide-area control, adaptive protection, and so on to the other reference papers of the inaugural Protection, Automation and Control World Conference.

II. PROTECTION

Shaping the operating characteristics via device construction substantially limited the electromechanical and static generations of P&C devices. Microprocessor-based relays brought freedom in forming the operating characteristics by way of real-time calculations and lifted other construction-driven constraints, inviting designers to go back to first principles and improve on existing protection functions, as well as to invent new ways of detecting faults and other abnormal conditions in power systems.

Microprocessor-based relays delivered a wealth of new functions—built-in digital fault recording, sequential event recording, metering, multiple settings groups, easier adaptivity to changing system conditions, fault location, and digital communication, to name only a few. Remarkable cost and space savings accelerated adoption of the new technology.

Early implementations were limited by the small amount of information available to the relays and their limited ability to process this information. Designers skillfully worked around the low sampling rates and scarce processing power in order to deliver sophisticated algorithms with many performance improvements over the older generations of relays. Adaptive directional elements, capacitive coupling voltage transformer (CCVT) transient detection logic for distance protection, load encroachment and blinders, and adaptive reactance elements for ground distance protection are good examples of protection enhancements that resulted from lifting the constraints of previous relay technologies.

Modern relay implementations have access to more information: higher sampling rates, more direct inputs, and more auxiliary signals delivered via communications from other devices. These relays have more processing power to utilize the available information, yielding better performance and facilitating new functions.

New microprocessor-based relays are designed for lower internal latencies, thus overcoming the inherent disadvantage of using sequential processing and incurring internal delays as compared with analog relays. Modern relays are designed with a fair amount of parallel processing, using field-programmable gate arrays (FPGAs) in order to speed up processing and provide for deterministic execution of computationally intensive functions. Internal relay architectures, while designed for simplicity, are heavily optimized for performance. Integrating protection, automation, recording, metering, human-machine interface (HMI), and communications functions, these devices are designed for guaranteed performance under a variety of activity patterns in any of the respective functional areas.

The change from the mechanical detection of problems to calculations and storage of values led to the possibility to perform self-tests, and the art of self-checking of microprocessor-based relays became a mature field of engineering. The abilities to detect an internal failure, fail gracefully ("fail-safe"), and alert the user of the problem are considerable benefits that have been available since the early days of microprocessor-based relays. Avoiding undesired operations and preventing hidden failures to operate have a significant and direct impact on the overall performance of the protection system. Today, a renewed attention is given to this aspect with the goal to improve and optimize periodic testing and maintenance activities for P&C systems. Relying on natural events, such as tests of current and voltage transformers (CTs and VTs) and circuit breakers, the enhanced relay self-monitoring can facilitate a "run-to-fail" maintenance strategy, where a P&C system is left operational until it reports problems. Avoiding human activities and associated errors would yield a potentially better performance than the periodic testing approach. This strategy is one of the new, yet to be fully realized advantages of microprocessor-based protection technology.

As human resources at user organizations become scarce, new emphasis is given to simplicity. While integration of the many traditional functions (from protection, through recording, metering, and remote terminal units [RTUs], to automation and control) in a single device brings size, cost, and performance benefits, the device itself appears more complex. Microprocessor-based technology opens new opportunities in this area. A power swing detection element that requires no settings to track the rate of change of the swing center voltage is a good example of a better protection principle that eliminates the need for some of the engineering required to apply the function.

In the following sections, we elaborate on several key dimensions of the progress in microprocessor-based power system protection.

A. More Information Enables Better Protection

Higher sampling rates with greater precision enable protection devices to obtain finer measurements more rapidly and more often. This leads to protection devices with faster and more secure elements. The following are a few examples of higher sampling rates leading to better protection algorithms.

Consider a transformer differential relay. One of the greatest challenges for any differential relay is securing the differential element during external faults when one of the CTs goes into deep saturation. CTs that supply differential elements do not go into saturation immediately after fault inception but saturate sometime later. The first few milliseconds (< 4 milliseconds) after a fault, CTs will reproduce the primary current faithfully. A fault detection algorithm that uses high-rate data together with the fact that CTs do not saturate immediately determines whether a fault is internal or external to the protective zone within 2 milliseconds after fault inception. The algorithm uses the following principle to determine if the fault is outside the differential zone. If the fault is internal, both the differential and the restraint quantities change instantaneously (both quantities experience an incremental change). For an external fault, only the restraint quantity changes instantaneously; the differential quantity does not change. The differential quantity will experience a change only once one or more of the differential CTs go into saturation. When one or more CTs go into saturation, the differential element begins to measure a fictitious differential current. Therefore, it is essential that the relay determine if the fault is external before one or more CTs saturate. Once the fault detector detects an incremental change in the restraint quantity, it opens a 2-millisecond window and checks to see if the differential quantity changed during this time. If there is no incremental change in the differential current during this 2 millisecond window, the relay declares the fault external and switches the relay into a high-security mode. This means that if the CTs saturate after this time, the differential element is in a secure mode and any fictitious differential current will not negatively impact the security of the differential element.

System stability margins continue to become tighter, and this requires that faults be cleared as rapidly as possible. When a circuit breaker fails to operate, all sources that contribute to the fault have to be disconnected in order to maintain the integrity of the power system. Because disconnecting sources has a drastic effect on the system, it is best to delay this action as long as possible, giving the circuit breaker as much time as possible to clear the fault. Therefore, if the primary breaker operates, we want to reset the breaker failure initiate commands as rapidly as possible. Using current magnitude to reset the breaker failure typically introduces a delay in excess of one power cycle due to the latency of the filters. The reset time can be reduced by 0.5 to 0.75 cycles in modern relays via fast processing of the raw current samples. The algorithm uses the following principle to determine when the primary current has been interrupted. As current flows through the breaker, the current goes through a zero crossing every 0.5 cycle. The derivative of the current (di/dt) also has a zero crossing every 0.5 cycle, but the zero crossing of the current derivative is offset by 0.25 cycle (90 degrees) to that of the zero crossing of the current. Therefore, when current flows through a breaker, a zero crossing occurs in either the current or the derivative of the current at least once every 0.25 cycle. If there is no zero crossing for 0.5 cycle, then the primary current has been interrupted and the circuit breaker can be considered open. Using this method, it is possible to determine that a circuit breaker is open at least 0.5 cycle faster than using the traditional current magnitude method.

In addition, higher sampling rates of the analog quantities and access to more digital information (digital inputs) at a higher rate also create better and more flexible protection functions. The following are some examples of how access to more digital inputs helps achieve better protection performance.

Consider a multizone busbar system where zone reconfiguration occurs frequently by switching feeders from one zone to the next while the feeder is under load. One of the challenges for a busbar protective relay is to rapidly assign a transferring feeder to the correct zone or zones during the switching operation to maintain the integrity of the differential element. Earlier busbar protection schemes either disabled the protection during the switching procedure or switched the CT secondary current through auxiliary relays. If the relay could not correctly determine which zone or zones to assign the feeder to during the switching operation, the protective relay was disabled. This is not ideal, because some busbar faults are caused as a result of the switching. The idea behind switching the CT secondary current through auxiliary relays is to replicate the busbar configuration using the status from the isolator auxiliary switches. This is a good idea, except for the fact that this switches the CT secondary current. Should one of the auxiliary contacts fail, not only does the CT open-circuit but the bus relay also trips. The reason that these methods were employed was because these earlier busbar protective relays did not have enough digital inputs to replicate the busbar configuration in the relay itself. The newer busbar differential relays not only have enough digital inputs to monitor the status of the isolators, they also sample these inputs fast enough to replicate the busbar configuration in the protective relay in real time. This has the advantage that the relay always assigns the transferring feeder to the correct zone or zones and maintains high-speed bus protection, and the CT secondaries do not need to be switched.

Combining a higher sampling rate with a greater number of analog inputs allows for some very innovative protection schemes that not only offer greater flexibility but also provide system security while breakers are taken out of service and tested.

A breaker-and-a-half scheme is commonly used in transmission systems to provide greater feeder availability; however, it is often necessary to remove a breaker from service and test the specific breaker without interfering with the healthy breaker or the feeder. Newer protective relays no longer require the CTs from the individual breakers to be paralleled outside of the relay but allow them to be fed into the relay individually. These relays are equipped with source selection logic, where the logic determines how the currents from the two individual CTs are presented to the protection functions. In the combined mode, the logic combines the individual currents and presents them as the line currents to the relay. Should one of the breakers be taken out of service, an external input informs the source selection within the relay that the line current is no longer a combination of the breaker currents but rather a current from the remaining in-service breaker (this is a simple form of zone selection). The source selection logic then routes the current from the in-service breaker to the line protection function in the relay without interfering with the protection of the feeder. This allows the user to perform maintenance on the out-of-service breaker without interfering with the protection performance of the feeder. The user can inject current into the out-of-service CT and verify the CT measurements by using the meter function on the relay. Note the relay still monitors the current in the out-of-service breaker; it simply does not include it in the line protection functions. Once the maintenance is complete, the breaker can be simply switched back into service, and the source selection logic will once again combine the current from the two CTs and present it to the protection function. An added benefit of not combining the current external to the relay is that the relay can monitor the wear and tear on each individual breaker, as well as offer breaker failure protection to each individual breaker.

B. More Processing Power Enables New Protection Methods

Many original protection methods have been limited by construction of protection devices. Early microprocessor-based relays carried forward principles derived under limitations of electromechanical and static technologies. Today, increased processing power allows sophisticated protection principles, limited only by the laws of physics and imagination of the designers. Examples of how the power in newer microprocessor-based relays liberated the ideas of protective relay designers are discussed below.

Load current can significantly influence the performance of faulted phase selection logic and directional elements, which, in turn, influences the performance of the distance elements. Protection designers have known for some time that by using incremental quantities, the influence of load on these elements can be removed. To extract the pure fault current from the total fault current, the prefault current must be subtracted from the total fault current. In other words, the load current must be removed from the total fault current. To accomplish this, the distance relay stores the prefault voltages and currents. These prefault data are stored in buffers approximately 2 to 3 cycles deep. The information in these buffers is updated every processing interval so that the relay tracks the system load dynamically. The relay detects a fault if the incremental torque of any of the fault loops (produced by the product of the incremental voltage and current) exceeds a preset threshold. Once the relay detects a fault condition, the information in the buffers is frozen and stored as prefault values so that a reference point is maintained. The faulted phase or phases are determined by comparing the incremental torques against one another. The faulted phase (or phases) is typically the one with the greatest incremental torque. The fault direction is determined by the sign of the incremental torque; if the incremental torque is negative, the fault is declared forward, and if it is positive, the fault is declared reverse. In this manner, the fault direction and faulted phase(s) are readily identified, which results in a robust and faster protective relay.

With systems being pushed ever closer to their limits, a loss of a major transmission line may result in an unbalance in the power generated versus the power dissipated in a part of the power system, manifesting itself as a power swing (out of step). It is critical at this time to keep the power system from breaking apart and ending up with unstable islands. To accomplish this, protective relays employed on transmission systems are equipped with out-of-step protection that will detect this power swing and prevent the distance element from inadvertently tripping during this condition and leading to a further demise of the stability of the power system. Setting the out-of-step protection properly requires engineers to run extensive stability studies to determine the swing rate of the power system under different operating conditions so that the out-of-step logic can clearly distinguish between a fault condition and a swing condition. This task proves particularly challenging when long lines with heavy load are involved. Protection engineers have challenged themselves to develop new methods of detecting out-of-step conditions without the user having to run extensive system studies. Engineers came up with several solutions to this problem. One solution is to have the relay monitor the rate of change of the positive-sequence impedance. Under normal conditions, the positive impedance is stationary or varies very little; for a fault condition, the impedance changes suddenly and then reaches a steady-state value (the fault impedance). During a power swing, the impedance changes constantly. So to determine a power swing, the new logic takes the difference between the positive impedance now ($Z1_k$) and subtracts it from the positive-sequence impedance from the previous processing interval ($Z1_{k-1}$). It then computes the rate of change of impedance because the relay knows the time difference between processing intervals (Δt). If the rate of change is below a factory-optimized threshold, the relay declares an out-of-step condition and blocks the appropriate distance elements. The logic declares that the out-of-step condition has ended, once the rate of change drops below a threshold for a period of time.

Another method to detect a power swing is to monitor the swing center voltage. The swing center voltage is the voltage measured at the electrical center of a power system. Because a relay cannot be positioned at the electrical center of a power system (the swing center of a power system changes constantly because of changing system conditions), a direct relationship exists between the line current and the swing center voltage. Therefore, by monitoring the rate of change of the angular difference between the voltage and the current, we can monitor the rate of change of the swing center voltage (in other words, we are monitoring the power factor). Under steady-state conditions, the angle between the voltage and current remains approximately constant. When a fault occurs on the power system, the angle between the voltage and current approaches that of the line angle and remains there. When the system experiences a power swing, the angle between the voltage and current changes constantly; the relay uses this information to determine the presence of a power swing. The relay calculates the angular difference between the voltage and current for the present processing interval (Θ_k), and using the angular difference from the previous processing interval (Θ_{k-1}), it calculates the change in the angles ($\Delta\Theta$) between the processing intervals. Knowing the time difference between the processing interval (Δt), the relay can calculate the rate of change of the angle. If this rate of angle change is above a threshold, an out-of-step condition is declared and the appropriate distance elements are blocked. The relay removes the block condition once the rate of change falls below a threshold for a given period of time.

Series-compensated lines are becoming more and more prevalent in modern power systems as systems are pushed closer to their limits. One challenge for distance relays is how to detect and deal with a voltage inversion. A voltage inversion occurs when the impedance between the VT feeding the relay and the fault is capacitive instead of inductive. Under this condition, the voltage is 180 degrees out of phase (inverts) with the prefault voltage. One method of detecting that a voltage inversion occurred is to compare the phase angle of the present voltage (V_k) to that 1 cycle previous (V_{k-1} cycle). If no voltage inversion occurs, the angular difference between the two signals is small (typically a few degrees). If a voltage inversion does occur, the angular difference between these signals is greater than 90 degrees. What happens once the relay has detected a voltage inversion? Most modern distance relays use memory voltage to polarize distance elements. The memory voltage in state-of-the-art distance relays typically employs more than one time constant. For normal nonsymmetrical faults, the relays use memory voltage with a short time constant, meaning the relay uses a certain percentage (x) of actual voltage (V_k) and a certain percentage (1–x) of the memory voltage (V_{MEM}). If a symmetrical fault occurs and the voltage measured by the relay falls below a lower limit, the relay switches to the second time constant (long time constant) that almost exclusively uses memory voltage (V_{MEM}) to polarize the distance elements. This ensures that the distance elements remain directionally stable for three-phase faults close to the relay location. Similarly, when the relay detects that a voltage inversion has occurred, it switches the memory voltage to the long time constant, ensuring that the distance elements maintain their directional integrity.

Protective relays depend on instrument transformers (VTs and CTs) for their data; therefore, any transient response by the instrument transformers impacts the performance of the protection device. CCVTs are known to not accurately replicate the primary voltage signal at the onset of a fault, because of the resonance between the stack capacitors (used for voltage division) and the tuning inductor. This transient causes the voltage output to be of a lower frequency than the system frequency, which ultimately translates into a voltage with a lower magnitude. For the distance relay, this voltage reduction translates into an overreaching phenomenon, meaning that a Zone 1 element may operate for an external fault. Protection engineers know that there is a direct relationship between the strength of the power system and the CCVT transient. In addition, they know that there is a direct relationship between the fault current and the fault voltage. For a protective relay to detect a CCVT transient, the relay looks at the relationship between the voltage and the current. If the relay detects that the voltage is lower than anticipated for a particular fault current, the relay sets the CCVT blocking signal, which holds back the Zone 1 element. However, the relay does not want to hold back the Zone 1 element indefinitely; studies have shown that CCVT transients last a maximum of 1.5 to 2 cycles. A transient may decay within 0.5 to 0.75 cycles, so it is desirable to reset the CCVT block signal as rapidly as possible once the CCVT transient has decayed sufficiently. This is done by computing the smoothness of the distance element calculation. The smoothness detector continually calculates the difference between the present distance calculation (m_calc_k) and the previous distance calculation (m_calc_{k-1}). During the transient condition, the difference is greater than 10 percent; once the transient decays sufficiently, this difference becomes less than 10 percent and tends towards zero (settles toward the steady fault value). Once the smoothness detector determines that the difference between three consecutive values is less than 10 percent, the block signal is removed and the Zone 1 element is allowed to operate.

C. Microprocessor-Based Technology Allows Easy Adaptation

Providing protection by means of calculations, microprocessor-based relays allow for adaptive behavior. The following are examples of how, by continuous calculation of certain parameters, protective relay sensitivity can be enhanced.

Detecting ground faults on an ungrounded power system is a trivial task when the fault resistance is low; however, as the fault resistance increases, this task becomes more complex because the unbalance caused by the fault begins to approach the standing unbalance of the power system. On an ungrounded power system, the standing unbalance is due to the nonsymmetrical capacitance per phase to ground. The standing unbalance of the power system varies as the system load varies. This unbalance manifests itself in the form of a neutral (residual) current. Most protective relays applied on these power systems use a fixed, user-settable threshold to monitor the magnitude of the residual current on specific feeders. If the magnitude exceeds the threshold, the relay declares a fault and either sets a local fault indication flag or sends it to a central location to indicate the presence of a fault on the system/feeder. However, if the load variation on the feeder is quite large, the sensitivity of the protection has to be compromised in order to prevent nuisance fault indications. This method has a further disadvantage in that if the fault was of such a nature that it caused the system to become balanced (i.e., the fault current canceled the standing unbalance), the relay would not detect the presence of the fault. Modern microprocessor-based relays are capable of measuring the actual unbalance at any instant in time and can determine the threshold by taking the average standing unbalance over a period of time. This means the relay has a dynamic threshold that adjusts to load and provides maximum sensitivity and security to the feeder at all times. On these systems, the load varies slowly and in a predictable manner (e.g., processes are switched on and off). Therefore, if the relay detects a sudden change in the neutral current (irrespective of if it increases or decreases), the relay can indicate the presence of a fault. Therefore, the relay can not only detect faults that result in the neutral current exceeding the dynamic threshold, it will also detect faults that create a large change in the neutral current.

In recent years, the detection of high-impedance ground faults on medium-voltage, solidly grounded power systems has become a priority. These faults do not cause a threat to the power system but do pose a large threat to human life and livestock alike. Because these faults cause very low ground current to flow, they are virtually indistinguishable from currents that flow because of normal load unbalance. Conventional algorithms based on the magnitude of the ground fault current cannot be used to detect these faults. One of the characteristics of these types of faults is that they arc. Arcing faults result in interharmonic currents; however, many power electronic loads also generate interharmonic currents. Therefore, for a protection device to distinguish between a normal condition and a fault, the relay must learn the feeder's normal interharmonic or noise current. One method used to learn the feeder's background or normal noise pattern uses the sum of the difference current. In essence, this method takes the current at time t (I_k) and subtracts it from the current 1 cycle previous ($I_{k-1cycle}$); essentially, it is a delta quantity calculation. This calculation removes all load current and harmonics from the signal and leaves only the interharmonics. The relay then averages these interharmonics over a period of time (e.g., 5 minutes) and uses it as a threshold. Because the relay updates this threshold every processing interval, the threshold adapts to loads. If an arcing fault occurs, the interharmonic content will be much larger than the normal feeder content, and the algorithm will count the number of times that the adaptive threshold is crossed. At the same time, the adaptive threshold is frozen, because the relay suspects the presence of a fault on the feeder and does not want to corrupt the threshold with fault data. Should the interharmonic content remain above the threshold, the relay will declare a fault on the feeder.

Ungrounded shunt capacitor banks are protected by measuring the potential difference between the voltage at the busbar and a tap point somewhere on the stack. With no fault condition on the system, the two ratio-matched voltages are the same. However, because of the unbalance of the power system and the tolerance in the capacitor cans, a potential difference exists between the two measuring points. Shunt capacitor bank protection detects the amount of capacitor cans that are either open- or short-circuited. To do this detection as sensitively and accurately as possible, the inherent difference between the two measuring voltages needs to be nulled out. This is often done by means of an adjustment factor (k); this factor adjusts the magnitude and phase of the tap point voltage. The adjustment factor is usually set when the capacitor bank is taken into service and is a settable static value. The issue with this setting is that it was determined based on the system conditions at that time; should system conditions change (i.e., the voltage at the busbar experiences a change in magnitude and phase due to a shift in load), the potential difference between the two VTs will now no longer be zero, even with the adjustment. So in order to prevent an incorrect indication of the number of cans lost in the stack, the pickup threshold of the alarming or tripping function has to be raised, compromising the overall sensitivity of the bank protection. To overcome this deficiency in the previous method, a third VT is introduced that measures the potential difference between the neutral point of the ungrounded capacitor bank and ground. Using this information and the voltage at the busbar, a shunt capacitor bank protective relay can now dynamically calculate the adjustment factor by measuring the standing unbalance of the system and compensating for it. In this manner, a user does not need to set this threshold, and the k factor calculation automatically adjusts for any system unbalance. This not only makes it easier for the user but also increases the sensitivity of the capacitor bank protection without compromising its security.

D. Design for Low Latencies Improves Protection Speed

Early microprocessor-based relays were limited by the available processing power, and having to process information sequentially, they were inherently disadvantaged compared with analog relays. Modern relays apply parallel processing and utilize powerful microprocessors and FPGAs, all within optimized internal data handling architectures, allowing for far shorter latencies.

An internal latency can be measured as the response time of the relay, not counting the data window required by the protection principle to maintain selectivity and security. For example, we may configure a relay to operate a contact from a highly sensitive disturbance detector and measure the response time between the change in the input current and the closure of a trip-rated output. This time delay is a good measure of the performance of the relay architecture in terms of processing latency.

The length of the data window required for selective operation is a measure of the power of the applied algorithms and logic constituting a given protection method. The shorter the data window, the less information it contains about the event, challenging the ability of the device to make the correct decision.

Today's algorithms are able to make reach-unconstrained decisions using between 0.25 and 0.5 cycles of data. These reach-unconstrained functions include directional elements, fault identification logic, starting elements and disturbance detectors (if applied), overreaching distance functions, external fault detectors, current detectors of a breaker failure element, and so on. Reach-constrained elements, meaning elements that require relatively precise reach accuracy, can be implemented using between 0.5 and 1 cycles of data. These reach-constrained elements include directly tripping under-reaching distance Zone 1, directly tripping instantaneous overcurrent elements, or differential elements.

Advancements in protection algorithms, such as external fault detection guarding against CT saturation errors in a differential function, allow shortening the data windows for decision making to 0.25 cycle or so, without impacting security.

More sophisticated protection algorithms require more processing power. The ability of the relay to execute its algorithms within a short scan cycle is a measure of the relay processing power.

Today's powerful relays optimize all three elements: internal architectures to limit latencies inherent in digital implementations, protection algorithms to respond correctly using shorter data windows, and processing power to enable more sophisticated algorithms.

The overall response time of the relay is the sum of the processing latency and the effective length of the data window required to make secure trip decisions. Both of these times asymptotically approach their limits with diminishing returns.

For example, the amount of research and extra processing power required to improve a 30-millisecond distance function to become a 28-millisecond distance function is negligible. But the amount of research and processing power required to improve the same distance function from a 10-millisecond operating time to an 8-millisecond trip time most likely doubles; going from 8 to 6 milliseconds probably quadruples the effort and processing power. The shorter the response time, the less guaranteed is the positive operation. Typically, short response times are achievable under best conditions, calling for a parallel, slower, but fully dependable algorithm.

Internal architectures of modern relays allow achieving latency times of 1 to 3 milliseconds.

Because of these diminishing returns, relay designers look for new ways to reduce the trip times. For example:

- A solid-state, trip-rated output can provide a response that is 2 to 3 milliseconds faster compared with a mechanical output and another 3 to 5 milliseconds faster if the interposing/lockout relays are eliminated.
- Because the critical fault-clearing time is of paramount importance, improving breaker failure reset time is a safe way to reduce the overall trip time, compared with attempting to make the trip decision faster in the first place.
- Moving critical signals via digital communication can be done faster compared with analog signals, considering the same level of security—as a result, integrating breaker failure and tripping functions in one relay or sending breaker failure initiate signals via communication can bring extra savings in the overall response time.

Early research into numerical protection focused on phasor estimation algorithms. Hundreds, if not thousands, of papers have been written in search of the "holy grail" of speed and accuracy. Today's design activities are multidimensional, involving analysis of power system phenomena and characteristics as a basis for new and improved protection principles, sophisticated signal processing, hardware and firmware co-design, and relay application practices.

E. Enhanced Self-Monitoring Improves Security and Availability

Protective relays are designed and manufactured to high standards of reliability. Mean time between failures (MTBF) reaches 300 to 400 years for best-in-class relays. Still, there is always a non-zero probability of internal component failure. Built-in self-monitoring is designed to maximize security and avoid unintended operation by detecting internal problems under practical component failure scenarios. Therefore, the MTBF viewed from the security perspective, meaning considering only failures that lead to unintended operations, is considerably better than 400 years for best-in-class relays.

Detection and alarming on internal relay failures maximize availability by reducing hidden failures to operate and shortening the mean time to repair (MTTR). A combination of high MTBF numbers, low MTTR numbers, and enhanced security (bias to fail gracefully) brings exceptional availability and security to the field of microprocessor-based protection.

While early generations of microprocessor-based relays operated more slowly because of processing latencies and were considered to be at a relative disadvantage compared with analog technologies, self-monitoring is an inherent advantage of the microprocessor-based technology. Both processing capability and self-monitoring capabilities have improved dramatically.

Digital systems fail gracefully by nature and by design. Data and code integrity checks, watchdogs, and other standard and optimized integrity monitors ensure fail-safe operation of the digital subsystems of a microprocessor-based relay. Internal data buses are protected with strong data integrity (redundancy) codes. Power supply rails are constantly monitored to ensure digital subsystems remain digital and never brown-out into a nondeterministic state where the built-in safety mechanisms could be defeated. Tripping and control outputs are actuated using digital techniques, ensuring fail-safe behavior even if the driving subsystem misbehaves. Communications ports are protected with data integrity checks and often include monitoring circuitries for fiber transceivers, if used.

The analog interface of a modern relay is designed for maximum reliability, with clean design and low component counts. Some degree of redundant measurements is often employed to ensure failures in this area can be detected in a timely fashion to prevent undesired operations.

Robust self-monitoring, combined with state-of-the-art MTBF characteristics and tracking of natural events to prove CTs, VTs, cabling, and circuit breakers, enables a run-to-fail maintenance strategy. Either the periodic testing or maintenance is considerably relaxed or even eliminated, delivering considerable savings to the user organizations, addressing the human resources gap, and improving protection system performance by avoiding human errors introduced while maintaining the system.

III. AUTOMATION AND CONTROL

Automation and control functions benefited from many of the same advancements as protection (more information available to the devices, more processing power). The fundamental progress, however, is in communication—the ability to share more information among multiple devices to gain a better understanding of the situation when deriving control actions.

A. Integration of Protection and Control

Modern multifunction devices integrate protection and many control and automation functions. This allows multiple savings (device count, engineering, documentation, wiring, and commissioning).

As far as performance is considered, integration brings extra advantages. The automation and control functions residing in a device that performs protection and measurements have natural access to a wealth of internally generated information and can benefit from it. For example, fault location information may aid restoration.

Complexity and user acceptance are the primary factors deciding on the degree of integration. Setup and commissioning tools address this concern.

B. Cost-Effective Communication

Local intersubstation communication is a norm, including both point-to-point serial and Ethernet networks. Cost-efficient intrasubstation means become available primarily through multiple (shared) usage of high-bandwidth channels. Modern radio solutions (spread spectrum) play an increasing role in short-haul communication and access to pole-top devices outside of the substation environment.

The ability to communicate information over a wider area enables sophisticated automation and control functions. Distribution automation is the key application example.

C. Increased Role of Time-Synchronized Data

New applications are possible when utilizing time-aligned data. Synchronized measurements (synchrophasors for ac quantities and time-stamped measurements for other data) allow new applications.

Fast load-shedding schemes for industrial facilities measuring and controlling the actual power balance in real time are good examples of acting upon time-synchronized measurements in automation and control functions.

The ability to execute a time-coordinated control action is another novel application of time. Instead of executing a series of manual and automated control actions in an uncoordinated fashion, an intelligent control system can precalculate an optimum control action, assuming all control commands will be executed simultaneously, preload those actions (“recipes”) via communications to the appropriate controllers, and launch them based on time. For example, taking a line out of service manually causes overvoltage or undervoltage conditions. Upon opening the breaker, tap changers and other controllers will eventually respond to maintain the voltage at lower levels. Subsequently, the operator may take action to rectify the voltage excursions on the high-voltage level, causing the reversal of the previous actions of tap changers, capacitor banks, and so on. All this can be avoided by launching the circuit breaker open command and the associated control actions simultaneously based on time. The net effect is lower wear of tap changers and other controllers and better power quality.

D. Availability of Computing Platforms

Powerful computing platforms allow deployment of sophisticated control and automation schemes, such as distribution automation. A combination of information from multiple devices giving visibility to the system state, affordable communication, and computing capabilities opens new opportunities.

Distributed schemes are also possible and used. In these schemes, individual devices that collect the data and execute commands run the automation and control algorithms, typically within their programmable logic. Modern programmable logic engines embedded in protective relays allow mathematical calculations, including unsynchronized and time-synchronized data (precise time alignment based on time stamps).

E. System-Level Control

Special protection schemes are beginning to play bigger roles as countermeasures to lowering the stability margins in the power system. Following the trend of standardization of hardware and software, these schemes are recently built on standard protection devices instead of low volume, slowly maturing, special products. Applications of varying sizes emerge between the strictly local and system-wide functions. Examples are station reconfiguration, distribution automation, industrial plant control (including islanded operation), and system integrity protection schemes.

IV. THE FUTURE

A. Present Trends

The trends outlined earlier will continue—more powerful relay platforms will emerge with more processing power, running more sophisticated algorithms and delivering better protection performance (speed, sensitivity, security, and dependability). Designers will more often go back to first principles in power engineering to extract more detailed characteristics of the protected and controlled apparatus to devise better P&C methods. This will bring improvements, but with diminishing returns as we approach the physical limits of what is possible when utilizing current and voltage measurements.

Protection functions geared toward speed will be more often implemented with parallel and complementary algorithms. Two or more algorithms may operate in parallel, each responding rapidly under certain, but not all, conditions. Quite often, these algorithms will be engaged only for a limited period of time to boost the speed of operation when it is safe to do that. As a result, a slower but dependable algorithm, typically based on the fundamental frequency components, needs to run in the background to ensure dependability and enforce the expected operating characteristic of the function.

Protection functions geared toward sensitivity will employ a fair amount of adaptivity. For example, capacitor bank unbalance protection may self-calibrate as the final stage of commissioning in order to null out all standing errors resulting from the natural bank unbalance and instrumentation errors. Disturbance detectors may monitor the level of the natural variation in their operating signals and adjust their pickup thresholds in proportion to this standing background noise.

Existing power system challenges will not disappear. For example, series compensation of transmission lines becomes applied with compensation levels exceeding 100 percent (as a result of splitting existing lines to connect new generation); or more phase-shifting transformers and power electronic-based devices will be installed to better control power flows in the system. All of this amplifies the associated protection challenges.

The trend of allowing relaxed CT ratings and compensating for the resulting errors with protection algorithms will also continue. Today, many differential functions for busbar, transformer, and line protection are stable on external faults with as short as 2 to 3 milliseconds of saturation-free CT operation. In metal-clad switchgear, poor CT dimensioning creates dependability problems for overcurrent protection. This too is being overcome by designing magnitude algorithms that work reasonably well under extreme saturation of low-ratio CTs.

The trend of integrating more functions in a protective relay started in the very early days of microprocessor-based technology and will continue into the future. Synchrophasors recently joined a long list of integrated functions. Integration of more functions brings multiplied benefits, not only by sharing the relay hardware and firmware to perform more tasks, but also by eliminating duplication in the construction, engineering, and maintenance areas.

B. New Challenges and Opportunities From the Relay Design Perspective

The trends of improving the performance of P&C functions while approaching limits of what is physically possible, integrating more functions into a single device, and improving reliability of the devices and schemes will continue.

There are new opportunities in the area of P&C system engineering and construction. Replacing labor-intensive copper wiring and switching to prefabricated components with more standardization in the physical domain, while moving variability into system configuration, have been recognized as key opportunities to reduce cost, speed up retrofit schedules, and deal with the shortage of skilled workers.

This architectural change involves communication for protection applications. Successful deployment of these systems will need to solve a number of practical considerations, such as isolation for testing and rework, test methodologies, and maintenance methodologies, in addition to solving performance challenges for the high-bandwidth, critical networks for protection applications.

Another opportunity is to address the maintenance challenge by designing much stronger self-tests with some degree of internal redundancy in order to virtually guarantee a fail-safe response of the P&C devices with a near 100 percent detection rate of internal failures. This would facilitate a run-to-fail maintenance strategy.

C. New Protection Principles

When utilizing information contained in the fundamental frequency components of voltages and currents, generated by the power system itself, and acquired via traditional VTs and CTs, we asymptotically approach what is possible in terms of speed and sensitivity of protection. Nontraditional VTs and CTs did not seem to deliver on their promise of reducing cost and size, and besides, it is still problematic whether the higher-fidelity measurements promised by the nonconventional instrument transformers can truly benefit protection functions.

We cannot rule out the invention of novel operating principles that would change the field of protection. One such opportunity would be a widespread deployment of next generation traveling wave devices. While the principle is known and applied in fault-locating devices, it has been mostly dismissed in protection applications. However, early implementations used very old technology compared to what is available today. Using modern analog-to-digital (A/D) converters, precise timing, and abundant processing power may lead to a rebirth of this ultra-fast line protection principle.

Another avenue is to deploy more instrumentation for P&C compared with what is traditionally used today. For example, wireless sensors embedded in rotors of large motors or generators improve thermal and short-circuit protection of the machines. Integrating electrical, thermal, mechanical, visual, and audio signatures will improve sensitivity and dependability of protection as well as—to a degree—speed and security.

Yet another way would be to apply active injection to monitor the health of protected primary devices, similar to the active injection methods for stator and rotor ground fault protection of generators and motors. The idea is to generate well-controlled signals and respond to them, instead of reacting to the fault-generated power system voltages and currents. This concept may not be practical for protection of transmission lines but may be useful for protection of machines, transformers, and capacitor banks.

D. Challenges of the Changing Power System

Power systems are on a trajectory to evolve considerably. The trend to connect renewable energy sources brings several changes:

- System configuration, power flows, and short-circuit levels may change very quickly, depending on the state of the nondispatchable generation.
- Short-circuit response of the new sources is different compared with traditional synchronous generators. Very often, new sources are effectively connected via converters and controlled quickly and aggressively by devices aimed at protecting the source. As a result, traditional fault signatures used to design protection algorithms for decades are violated. This poses new challenges to the existing protection principles and applications. For example, fault identification logic may be challenged when a power electronic source actively controls the negative-sequence current, while the zero-sequence current is driven passively by the grounding points in the network.
- Distribution networks evolve toward multisource configurations through deployment of distributed generation, defeating the classical time-graded overcurrent protection approach.
- Islanded operation of networks with distributed generation will most likely be allowed in the future, creating more challenges to control and automation schemes.

The above changes appear immense and will most likely consume considerable resources and investment, but from the technical perspective, they should not be seen as overwhelming.

Tightly coupled networks with large variability in short-circuit levels, weak terminals, or aggressively controlled short-circuit sources can be reliably protected using differential protection or simpler communications-assisted schemes. Recent advancements in communications technologies for the power industry (Ethernet, spread-spectrum radio, WiMAX) facilitate wider applications of these premium protection principles. Reliable, cost-efficient, and easy-to-use communications technologies are key enablers.

New primary devices or unusual system configurations have been introduced in the past with little or no consideration for the protection aspect (series compensation, phase-shifting transformers, HVDC [high-voltage direct current], reconfigurable busbars). These devices have been conceived and driven by power system economics. Each time, the protection industry found ways to ensure proper protection of the new devices and the devices in the vicinity of their installation. This trend will only continue.

Multisource distribution networks can be protected with communications-assisted schemes acting in concert with the isolation and restoration (autoreclose) schemes used for decades in the higher voltage networks. Again, short-haul, low-latency, and cost-efficient communications solutions and reclosers are key enablers.

Islanded operation of a microgrid poses a challenge that is no different than running a bigger interconnection. State estimation, load flow, frequency control, load shedding, restoration, synchronization, black start, and so on are all applicable concepts with existing solutions. What is different is the scale, cost expectations, ease of use, and ability to run in a more autonomous mode, because human operators cannot be deployed at the scale typical for large systems.

At the transmission system level, new sources, rapidly changing power flow patterns, and interaction of multitudes of actively controlled schemes would change the dynamics from the high-inertia smooth operation of today to more hectic patterns with shorter time constants. Specific challenges and detailed system integrity algorithms are still to be defined for this area, but it is self-evident that the solution will be built on synchrophasors and high-speed, wide-area communication.

V. SUMMARY

When looking at the past, present state, and future challenges and opportunities for P&C, we offer the following observations:

- Microprocessor-based relays are not limited by their construction when it comes to the operating principles—we have enough processing power to run sophisticated algorithms. Laws of physics and the imagination of the designers are the only limiting factors.
- Going back to first principles allows enhancing the classical protection criteria and schemes. Running parallel algorithms brings an increase in speed and sensitivity, but we approach an asymptotic limit of what is possible when responding to classical protection signals.
- In addition to enhancing individual functions, we need to look at complete applications and target performance of the entire scheme. For example, reducing the reset time of a breaker failure overcurrent detector is much easier than speeding up a distance function by the equivalent margin—when considering a critical fault-clearing time, both have the same impact.

- Communications and time-synchronized measurements open new opportunities for wide-area schemes in protection and automation. These technologies, although not new, are being deployed at a massive scale today, owing to a wealth of new, cost-efficient products. It is fair to observe that the technical capacity (measure, communicate, calculate) of the existing devices exceeds their demonstrated applications. The industry can do much more with the new products.
- There are still some untapped opportunities to make relays more fail-safe and use self-monitoring and internal redundancy to eliminate all failure-related undesired operations. This would enable a shift toward a run-to-fail, optimized maintenance strategy.
- There are opportunities in the way P&C systems are put together (replace low-density copper signaling with all communications-based solutions), but substantial challenges need to be overcome first (maintenance, testing, determinism of the network, upgrades).
- More functions yield more complexity. The industry addresses this challenge with better configuration and test tools.
- The anticipated evolution of the power system toward distributed generation, intermittent (nondispatchable) generation, narrower margins, new power devices, and more autonomous distributed control creates new challenges for P&C. However, solutions to many of these challenges exist today as developed for high-voltage applications. Migrating the “high-end” solutions to lower voltage networks will required extra investment, primarily in communication, but we do have a solid starting point as far as the technology is considered. Cost-efficiency and simplicity will play a role when applying the high-end solution to distribution and subtransmission levels.

VI. BIOGRAPHIES

Bogdan Kasztenny is a principal systems engineer in the research and development division of Schweitzer Engineering Laboratories, Inc. He has 20 years of experience in protection and control, including his ten-year academic career at Wroclaw University of Technology, Poland, Southern Illinois University, and Texas A&M University. He also has ten years of industrial experience with General Electric, where he developed, promoted, and supported many protection and control products.

Bogdan is an IEEE Fellow, Senior Fulbright Fellow, Canadian member of CIGRE Study Committee B5, and an Adjunct Professor at the University of Western Ontario. He has authored about 200 technical papers and holds 16 patents. He is active in the Power System Relaying Committee of the IEEE and is a registered professional engineer in the province of Ontario.

Normann Fischer received a Higher Diploma in Technology, with honors, from Witwatersrand Technikon, Johannesburg in 1988, a BSEE, with honors, from the University of Cape Town in 1993, and an MSEE from the University of Idaho in 2005. He joined Eskom as a protection technician in 1984 and was a senior design engineer in the protection design department at Eskom for three years. He then joined IST Energy as a senior design engineer in 1996. In 1999, he joined Schweitzer Engineering Laboratories, Inc. as a power engineer in the research and development division. Normann was a registered professional engineer in South Africa and a member of the South Africa Institute of Electrical Engineers. He is currently a member of IEEE and ASEE.

20100811 • TP6440-01