Breaker Failure Protection – Standalone or Integrated With Zone Protection Relays?

Bogdan Kasztenny and Michael J. Thompson
Schweitzer Engineering Laboratories, Inc.

This paper was presented at the 64th Annual Conference for Protective Relay Engineers and can be accessed at: http://dx.doi.org/10.1109/CPRE.2011.6035639.

For the complete history of this paper, refer to the next page.

Published in the
proceedings of the 2nd Annual Protection, Automation and Control World Conference
Dublin, Ireland
June 27–30, 2011

Previously presented at the
65th Annual Georgia Tech Protective Relaying Conference, May 2011,
and 64th Annual Conference for Protective Relay Engineers, April 2011

Previous revised edition released October 2010

Originally presented at the
37th Annual Western Protective Relay Conference, October 2010

Breaker Failure Protection – Standalone or Integrated With Zone Protection Relays?

Bogdan Kasztenny and Michael J. Thompson, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—This paper discusses merits, advantages, and disadvantages of integrating breaker failure (BF) protection with zone protection relays (ZPRs). In this context, the paper considers cost savings, security and dependability, simplicity, the danger of human errors when testing bus configurations, overall relaying philosophy, and reliability of applied protection devices. Several ways of integrating BF protection are proposed, allowing different tradeoffs between the mentioned factors. This paper also reviews methods to improve the security of BF protection.**

I. Introduction

Breaker failure (BF) protection is a backup function substituting for breaker redundancy [1]. Historically, standalone BF relays have been used for a number of reasons, primarily as single-function relay technology, ease of maintenance, and the reduction of human errors due to the one-to-one association between breakers and BF relays. This architecture also provided security by separating the function of detecting power system faults and tripping the breaker from the function of determining that a fault is actually on the power system and the breaker has failed.

Today, BF functions are available in multifunction microprocessor-based relays and can be used at very little extra cost.

Normally, two zones of protection overlap at a breaker. With dual-redundant protection systems, up to four zone protection relays (ZPRs) that have access to the breaker current signal may integrate the BF protection for the breaker. How many integrated BF elements should be enabled for a given breaker? Is it safe to make trip and BF decisions based on the same current transformer (CT) output, wiring, and input circuitry of a relay? How do we keep the integrated BF simple enough to maintain and avoid unintended operation caused by human errors? How do we balance the rewards of avoiding external breaker failure initiation (BFI) signals prone to noise and test errors with the danger of using the same relay input data for primary zone tripping and BF tripping for a much bigger zone?

This paper reviews the merits of standalone and integrated BF protection. Further, it develops several architectures for BF protection integrated with multiple ZPRs.

Different bus configurations, local versus remote backup protection philosophies, application of breaker intelligent electronic devices (IEDs), reliability, security (in particular, of applied IEDs), and maintenance and testing practices are considered in the context of BF protection security and how the BF integration can impact the overall performance of the protection system.

Also included are examples of the various BF architectures, as applied to several typical bus configurations.

II. Basic Concepts of BF Protection

In a high-voltage substation, protective relays serve the function of fault detection. In this paper, we use a ZPR as a generic designation of protection functions (such as ANSI 21, 87, 51, or combinations thereof) as applied to a given zone of protection. Each relay is typically applied to be selective to a given power system zone. To provide redundancy and eliminate single points of failure, we often apply multiple (typically two [A and B]) relays to cover each zone of protection (Fig. 1). Alternatively, or in addition to, we can rely upon backup relays on adjacent zones that overreach the protected zone with time coordination.

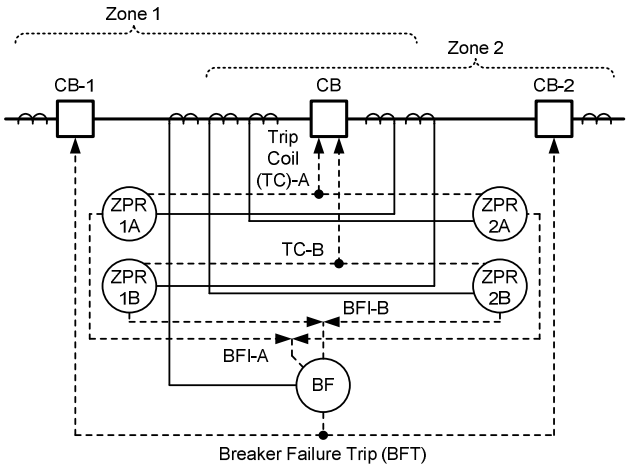

Fig. 1. ZPR and BF functions in a redundant protection scheme.

A circuit breaker (CB) serves the function of fault interruption. For cost and space reasons, we do not apply redundant circuit breakers. Instead, satisfactory backup for failure to interrupt a fault is provided by the BF protection system. If the BF protection system detects that a circuit breaker has failed to interrupt, it trips adjacent breakers to both clear the fault and isolate the failed breaker.

With reference to Fig. 1, ZPR-1A and ZPR-1B are the two redundant protection systems for Zone 1, and ZPR-2A and ZPR-2B are the two redundant systems for Zone 2. These systems typically use CTs that overlap at the common breaker to avoid any blind spots. They trip the common breaker, circuit breaker, and other breakers defining their respective zones of protection (CB-1 and CB-2). These breakers can be local or remote if the protected zones are transmission lines.

System A and System B are preferably supplied from two independent batteries, use separate protection panels and ac and dc wiring, and operate two independent trip coils of the breakers.

A BF function is initiated by all relays tripping the breaker, and as a backup function, it preferably uses a separate CT and ac wiring. Upon detecting a failure to interrupt, the BF function trips all breakers that connect sources of the fault current. This breaker failure trip (BFT) command is often distributed via a lockout relay to prevent accidental (automatic or manual) reclosing on the fault via the failed breaker.

It is also practical to trip from BF protection directly and to implement the lockout functionality in software when using microprocessor-based relays.

Remote breakers are tripped via direct transfer trip (DTT) using channels of adequate security (the received trip commands are not supervised with fault detection at the remote sites).

In applications with reconfigurable buses, such as double-bus single-breaker, the set of breakers to be tripped upon a BF is dynamic and depends on the present bus configuration as dictated by positions of disconnect and bypass switches [2]. For this reason, the BF trip commands are often routed via the bus protection system, which decides which breakers to trip [3].

By definition, BF protection is a backup function. Therefore, it is typically biased for security rather than dependability. A BF protection system will be called upon to not trip many more times than it will be called upon to trip. Because a BF operation results in tripping breakers that isolate all the adjacent zones of the power system, typically including the bus, the consequences of BF false operation are usually serious. BF protection security has the same importance as bus protection security.

Because of the desired bias for security, duplicated (redundant) BF protection is not common. However, it might be considered beneficial if the zone protection and BF functions are independent with respect to their input signals (CTs and wiring), hosting relays (hardware and firmware), and tripping outputs (relay output contacts). This strict approach does not prevent integration of the BF functionality with the ZPRs, as explained later in this paper.

One leading cause of BF misoperations is inadvertently initiating the BF protection. Spurious initiates often come from testing ZPRs that initiate BF timers. For this reason, it is important to make the system design as simple as possible and to be consistent in the design across the organization or at least throughout the substation.

Standalone BF protection has merits of simplicity and independence from the zone relays.

Integrated BF protection reduces cost by eliminating the extra device and the associated wiring, engineering, drafting, and construction costs. The integration can be done in a number of ways, yielding different balances between security and dependability. Referring to Fig. 1, four relays (ZPR-1A, ZPR-1B, ZPR-2A, and ZPR-2B) may be capable of integrating the BF function. Should all of them run the BF function, one of them, some of them? Should the allocation of the BF function be static or dynamic depending on availability of the hosting relays? This paper presents various alternative solutions and evaluates them in the context of their basic characteristics.

III. Merits and Design Criteria for BF Integration

From the redundancy and reliability points of view, relay failures and true BFs (excluding issues with the trip signaling path) are two nearly unrelated failures. Therefore, integrating BF protection in ZPRs does not inherently introduce any common-mode contingency issues.

A. Advantages of Integrating BF Protection

The advantages of integrating the BF function with the zone relays are twofold.

First, certain cost savings can be realized, primarily at the construction phase. This includes eliminating a standalone BF device; saving panel space by eliminating some panels and reducing requirements for the size of the control house; eliminating wiring and associated engineering, drafting, construction, and commissioning labor; and saving in engineering and period maintenance by having fewer devices to deal with. These savings may increase further if a user eliminates interposing tripping relays and/or reuses communications interfaces already available in line protection relays to execute DTT for remote breakers.

Second, additional gains can be realized, primarily in eliminating or reducing the amount of BFI wiring and frequency of spurious BFI events, increasing the availability of BF protection by having an opportunity to have it operational in several zone relays, and reducing the total fault clearance time under BF conditions [4] [5].

B. Design Criteria

Several factors impact the BF architecture and degree of integration. They include the following:

- General relaying philosophy and maintenance practice.
- Overall approach to a breaker IED.
- Bus arrangement.
- Types of ZPRs that are being used in the system.
- Preferred balance between security and dependability.
- Security record of the used protection devices.

These factors are reviewed in detail in the following sections.

C. General Relaying Philosophy

Relaying philosophy and maintenance practice significantly impact selection of a BF scheme. Factors to consider include the following:

- Preferred degree of security and reliance on remote versus local backup. With more reliance on remote backup, the BF function should be even more biased toward security. When a strict local backup approach is followed, we may consider increasing BF function availability, such as by having multiple instances of it operational in multiple relays.
- Willingness and capacity to adjust existing maintenance and periodic testing practices.
- Preferences with respect to simplicity and cost targets. In this respect, we need to remember that the total life-cycle cost has many components, not only the initial engineering and construction costs.

D. Breaker IED

An IED dedicated to the bulk of breaker functions is referred to as a breaker IED. The concept of a breaker IED is attractive because of the one-to-one correlation between breakers and associated IEDs.

The major protection functions provided in a breaker IED include BF, backup overcurrent protection, and pole discrepancy alarm and/or protection. Also, the lockout function can be implemented in a breaker IED if physical lockout relays are designed out of the system.

The major control functions include supervisory control and data acquisition (SCADA) open/close control for the breaker and associated motor-operated switches, SCADA interlocks, autoreclosing with synchronism check, and auxiliary functions (such as air compressor or heater on/off control). In dual-breaker applications, zone-oriented (instead of breaker-oriented) autoreclose architectures can be used, making the breaker IED concept less attractive.

The major monitoring functions include breaker alarms, breaker contact wear, operation counter, and cabinet intrusion alarms.

If cost is a main driver in integrating BF protection with zone relays, the key decision is not in integrating the BF function alone, but the concept of the breaker IED needs to be considered holistically. Placing the BF function only in the zone relays does not reduce cost, engineering, or wiring if the breaker IED is retained.

E. Bus Configuration

The bus arrangement influences how the BF protection system is designed in at least three ways.

First, a distinction needs to be made between static and reconfigurable buses. In reconfigurable buses, a given breaker may connect a given network element (e.g., line, transformer, capacitor bank) to multiple bus sections. Examples of reconfigurable buses include a double-bus single-breaker or main/transfer bus. This dynamic association of breakers complicates the BF tripping logic because the BF protection system must know which breakers are connected to the same bus as the failed breaker. For this reason, the BF function is often integrated with a low-impedance bus protection system, or the bus protection system receives the BFT signals from external BF elements and routes the BFT command adequately to the appropriate breakers [2] [3].

Second, dual-breaker terminations of network elements need to be considered (breaker-and-a-half, ring-bus, and double-bus double-breaker buses). In these configurations, the zone relays may or may not have access to individual breaker currents. If the zone relays are supplied from externally paralleled CTs, they cannot provide BF protection on a per-breaker basis.

Third, bus configuration impacts the tolerance of the system to BF protection misoperations. Substations with dual-breaker terminations arranged as breaker-and-a-half or double-bus double-breaker are less affected by an unwarranted BF trip—with one bus lost, the network elements are still energized via the other bus. In such cases, security of the BF system is not as critical as in the single-bus single-breaker arrangement, for example.

F. Types of ZPRs

Another major factor is the type of ZPRs being applied. With single-breaker arrangements, the ZPRs that trip the breaker typically also measure the current flowing through the breaker. For this configuration, the ZPRs that trip the breaker can also provide BF detection.

With double-breaker arrangements, the current in the protected zone on at least one side of the breaker will be the summation of the current flowing through two breakers. In the past, this summation was always done external to the ZPR. For this configuration, the ZPR cannot provide BF detection. With some modern relays, the currents from each of the two breakers are brought into the relay, and the current entering the zone of protection is summed internally to the relay. This type of relay can provide BF detection for dual-breaker arrangements. In this respect, we could have three scenarios:

- All ZPRs that trip the breaker can see the current through the breaker.
- All ZPRs that trip the breaker have the currents summed external to the relay.
- A combination of both types of relays trip the breaker.

The above scenarios may create a permanent or temporary inconsistency of the applied BF solution when the protection systems are being retrofitted.

In many configurations, at least one side of the breaker is connected to a power system bus. Thus we need to consider the type of bus protection relay.

Multirestraint, low-impedance bus relays that measure the current in each of the breakers around the bus zone can integrate the BF function.

Bus relays fed from currents summed externally (high-impedance or differentially connected overcurrent) cannot integrate the BF function.

G. Balance Between Security and Dependability

With security taking precedence over dependability for BF protection, two key aspects need to be considered when designing a BF scheme.

Because it is a backup function for the breaker (including its tripping path), some may prefer the BF protection to use hardware and firmware independent from the zone relay and a separate tripping path. This preference is naturally met when using a standalone BF relay.

Dependability is directly proportional, while security is inversely proportional, to the number of operational copies of a given protection function. Today, we predominately deploy one BF function per breaker with external BFI signaling and physical lockout relays. The observed performance in terms of the frequency of unwarranted BF operations is a reflection of this practice. A scheme with multiple BF function elements for a given breaker, with each initiated from all the associated zone relays, would potentially multiply the probability of BF misoperation. This danger can be alleviated in a number of ways, while integrating the BF function as explained later. Most importantly, the danger can be alleviated by not having all zone relays initiate all operational copies of the BF function.

Integrating the BF function in multiple zone relays allows biasing the scheme for more security or more dependability compared with standalone BF protection, depending on the specific architecture selected and willingness to accept extra inter-relay signaling and associated complexity.

H. Security of the ZPRs Integrating the BF Function

1) Failure of the ZPR Hardware and Firmware

If the integrated BF function is initiated internally, there is a danger that the same relay hardware and firmware make the trip decision in the first place and the BF determination shortly afterwards. This creates a danger of unwarranted BF operations if the ZPRs are of poor security. Section V elaborates more on this decision factor.

In general, the BF function should not be integrated and directly initiated when using relays of poor or unknown field security records.

The BF determination is made a few tens of milliseconds after the trip decision. As a result, there is a chance that the relay diagnostics (self-tests) will prevent the unwarranted BF trip even when they allowed a false trip of the primary zone in the first place. Also, we may use BF architectures that minimize the danger of common-mode relay failures, as explained in Section IV.

2) Current Injection Testing

A second issue can affect security when the BF function is integrated with the ZPR such that both functions operate on the same signal representing the current through the breaker. If the false BF initiation is due to injection testing or a wiring error, both the ZPR functions and the BF functions will operate on this false measurement. In a system with standalone BF relays, these will not be the same signal, which can mitigate this common false current reading. Whether this impacts security or not depends on a number of factors:

- Design of the test switches in an integrated system to ensure that both the zone protection tripping outputs and the BF tripping outputs are isolated when performing injection testing.
- Use of the retrip function in the standalone BF function to ensure that, if it is inadvertently initiated while working with actual breaker current, it opens the breaker instead of timing out.
- Fault detectors in the standalone BF function set to ensure that they are not picked up on load.

IV. BF Architecture

This section reviews several possible architectures for BF protection [6] and discusses their advantages and disadvantages. It also provides a comparison table using the selection criteria introduced in Section III.

A. Standalone BF Protection

With reference to Fig. 2, a separate device is used to provide BF protection. The BF device works with a separate CT, is initiated by all the devices tripping the monitored breaker, and, upon declaring a BF condition, issues trip signals to all local and remote breakers required to open in order to isolate the failed breaker.

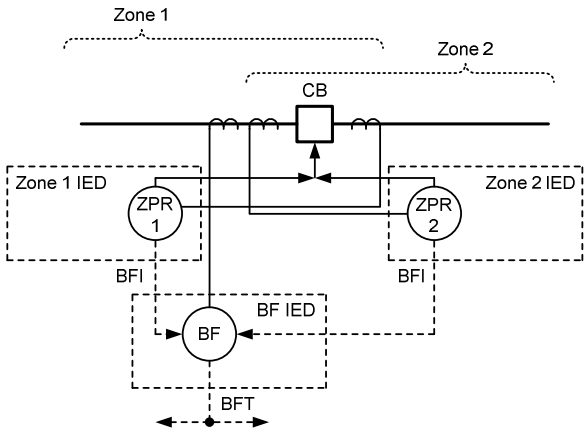

Fig. 2. Standalone BF scheme.

The BF device typically provides other functions for the breaker, as outlined in Section III, Subsection D, and becomes a logical implementation point for most, if not all, functions related to the breaker.

If the BF device is duplicated, System A initiates its own BF device and System B initiates its own BF device. If a nonredundant BF device is used, the initiate signals from both System A and System B are routed to the same BF device. This calls for careful engineering of the dc circuits in order to ensure independence and separation of the two battery systems as required. The issue of separation of the dc circuits is alleviated if the initiate signals are provided via digital peer-to-peer communication over fiber.

The standalone BF device can use dedicated DTT means to trip remote breakers, or it can issue DTT commands via the zone IEDs if the latter already have access to the teleprotection equipment.

Maintenance of the Fig. 2 scheme is relatively simple due to clarity of the zone protection location and BF functions and the design symmetry (none of the zone IEDs provide the BF function; the BF function resides in a device logically associated with the breaker).

Still, existence of external BFI signals may contribute to spurious BF operations when testing the ZPR (a human error of not isolating the BFI signals) or loss of BF protection dependability (a human error of not restoring the BFI signals after testing). These errors can be more or less likely, depending on the location of the cut-out switches (outputs from zone IEDs versus inputs to BF IED) and the applied test procedure.

B. Fully Integrated BF Protection

With reference to Fig. 3, each ZPR incorporates an internal BF function. This scheme increases dependability by allowing multiple instances of the BF function to be operational at any given time. The BF function is not lost upon a failure or an out-of-service condition of any individual device (the scheme provides the BF function as long as it provides zone protection).

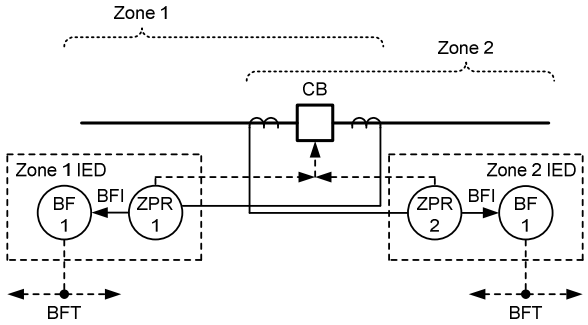

Fig. 3. BF function integrated with each zone protection device.

The scheme does not use external BFI signaling and therefore reduces the risk of human errors and noise-induced spurious BFI signals.

Wiring of the BFT signals is more extensive as compared with the standalone scheme because multiple relays issue the trip and lockout signals for any given breaker.

On the other hand, DTT for remote breakers can be easier to engineer if the zone devices have the DTT capability in the first place. However, we should notice that when issuing a BFT, the Zone 1 IED needs to reach all remote breakers, including remote breakers in Zone 2, and vice versa. As a result, the built-in DTT signaling needs to be cross-wired between the two ZPRs.

Maintenance of the Fig. 3 scheme is relatively simple due to clarity of the zone protection location and BF functions and the design symmetry (all of the zone IEDs provide the internally initiated BF function; no external BFI signals or devices are used).

The Fig. 3 scheme uses the inputs (CT, wiring, relay input circuitry, and firmware) to issue the trip and to determine if the breaker actually failed. This combined with multiple operational copies of the BF function can potentially erode security of the BF protection. Some multi-input relays reduce this concern to a degree by allowing different CT, wiring, and relay inputs for the BF function, as shown in Fig. 4.

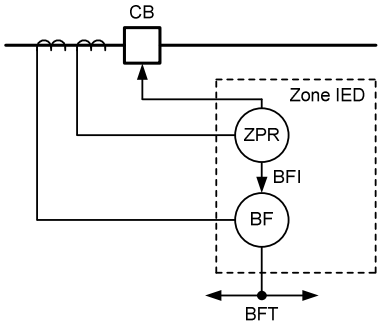

Fig. 4. Dual-input IED with separate CTs used for zone protection and BF protection.

C. Integrated BF Protection With Cross-Initiation

With reference to Fig. 5, this scheme integrates BF protection with each ZPR but applies cross-initiation to ensure the trip decision and the BF determination are performed by two independent devices based on two independent sets of current signals. This calls for external BFI signaling but increases the inherent security of the scheme from a false current measurement, as compared with the Fig. 3 solution.

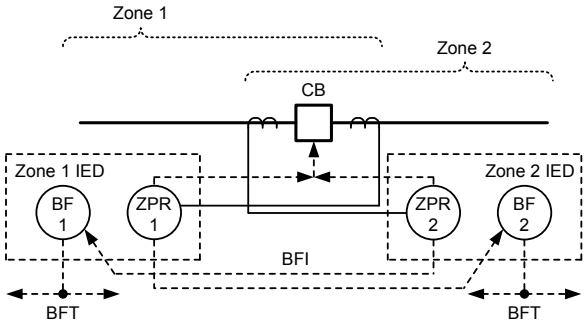

Fig. 5. BF function integrated with each zone protection device, with cross-initiation.

The scheme shown in Fig. 5 is symmetrical, simplifying maintenance and testing (each ZPR initiates a BF integrated in the adjacent zone overlapping at the monitored breaker). In practice, this symmetry can be difficult to implement. Often, the circuit breaker separates dissimilar zones with very dissimilar ZPRs involved in the cross-initiation architecture.

When applied with redundant protection, the Fig. 5 architecture would use cross-initiation within System A and System B devices separately. When only one system incorporates the BF protection, a failure or an out-of-service condition of one of the devices would lead to a loss of BF protection when initiated from the adjacent zone. This can be resolved by monitoring the out-of-service IED outputs between the two adjacent zones and allowing self-initiation should the BF protection in the adjacent device become unavailable.

D. BF Protection Integrated in One of the ZPRs

With reference to Fig. 6, one of the ZPRs protecting the two zones that overlap at the breaker provides BF protection for the breaker. This function is initiated internally from the hosting device and externally from the other device.

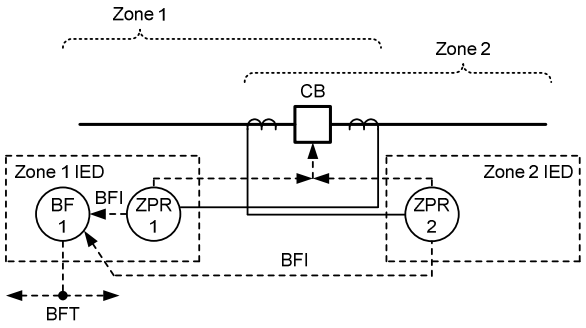

Fig. 6. BF element integrated with selected zone IED.

For trips generated in the hosting device, the same CT, wiring, hardware, and firmware are used to trip and determine BF, which erodes security from the device failure or injection testing points of view.

Dependability is not increased in this scheme either, as compared with the standalone BF configuration (should the hosting relay fail or be taken out of service, the BF function is lost). A solution to this disadvantage may be applied by monitoring the out-of-service output of the device hosting the BF function and, upon the BF unavailability, enabling an internally initiated BF function in the other device.

The scheme is not symmetrical because the two devices are configured differently with respect to the BF function. This lack of symmetry can result in an elevated number of human errors when maintaining and testing the scheme.

This scheme may be a preferred choice, however, when one of the protection zones in Fig. 6 is a bus. Assume the Zone 1 IED is a low-impedance bus relay measuring all individual bus currents and the bus is reconfigurable, calling for dynamic routing of the BFT signals. In this case, the BFT signals are naturally routed by the bus relay using the same input information and logic as for the main bus trips.

An alternative solution for a reconfigurable bus is to host the BF functions in the network element relays for the benefit of avoiding common-mode failures for the bus trip and BF trip decisions. In such a case, the bus relay receives a BFT command from individual BF elements and directs them accordingly, depending on the dynamic bus configuration at the time (Fig. 7). Section VI, Subsection C contains more details.

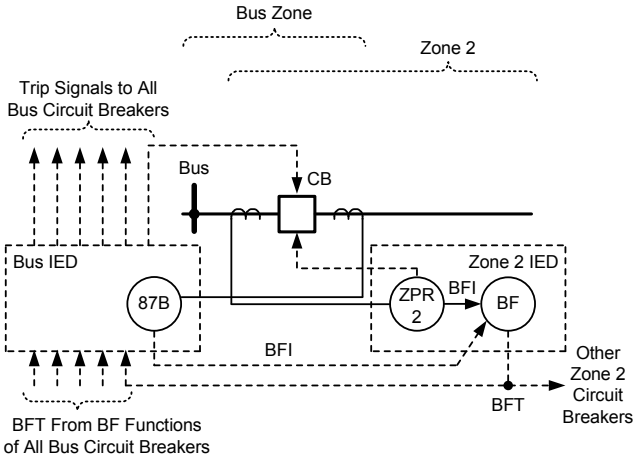

Fig. 7. A variant of the Fig. 6 scheme when Zone 1 is a reconfigurable bus.

Table I compares the outlined architectures.

TABLE I
COMPARISON OF THE BASIC BF SCHEMES

	Standalone (Fig. 2)	**Integrated With All Zone IEDs (Fig. 3)**	**Integrated With Cross-Initiation (Fig. 5)**	**Integrated in One IED Only (Fig. 6)**
Simplicity	Simple, symmetrical design	Simple, symmetrical design	Symmetrical design; external BFI required	Asymmetrical design; external BFI required
Human Errors When Testing	Moderate probability	Reduced by eliminating external BFI	Moderate probability	Moderate probability, potentially elevated by the design asymmetry
Security With Respect to Device Failures	High; independent devices initiate and determine BF	Potentially reduced; same device trips and determines BF condition	High; independent devices initiate and determine BF	Potentially reduced; device providing BF protection also initiates it
Dependability With Respect to Device Failures	Limited; unavailability of the BF device removes the BF function	Considerably increased; BF protection provided even with devices unavailable	Moderate; unless an internally initiated BF function turned on upon a failure of the other device	Limited; unavailability of the BF device removes the BF function
Security Versus Dependability (BF Function Count)	Biased for security	Biased for dependability	Biased for dependability	Biased for security
Applications With Reconfigurable Buses	Acceptable; bus relay routes trip signals (Fig. 7)	Less convenient	Less convenient	Convenient; BF integrated with bus or zone IEDs; bus relay routes trip signals (Fig. 7)

V. Security of BF Protection

This section discusses issues that can potentially impact the security of BF protection and ways to address them to improve security.

A. Spurious BFI Signals

BFI signals can assert spuriously due to noise conditions. Battery ground faults with a significant amount of cable capacitance are the primary concern, particularly when the BFI signals use seal-in logic in the BF function and microprocessor-based relays are applied with their relatively high input resistance of digital inputs.

Limiting the amount of cable capacitance, increasing the delay of a debounce security timer for the BFI input in the BF relay, selecting the appropriate pickup voltage level for a given battery voltage, or even installing burden resistors in parallel with the BFI digital input to better suppress the induced noise are practical means to improve security.

Another solution is to use two outputs to drive the BFI signal and keep both the positive and negative battery terminals isolated, as shown in Fig. 8. This arrangement requires one extra output in the ZPR but makes the signaling secure during battery ground faults.

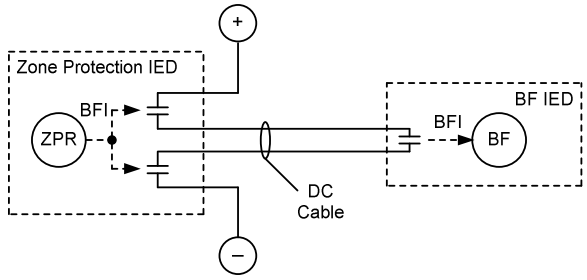

Fig. 8. Securing a hard-wired BFI signal against battery ground faults.

Using digital peer-to-peer communication increases security of BFI signaling through the application of embedded data integrity checks. When employing communications-based BFI and/or BFT signaling, we need to develop a proper strategy for isolation and testing [7] or else the benefits may be erased by the increased number of misoperations when testing or working on the protection system.

A retrip function, the BF function issuing a trip command to the breaker upon receiving a BFI signal for the breaker, is an efficient way to reduce the consequences of spurious BFI signals. If initiated spuriously, the BF function will not operate because the breaker normally opens in response to the retrip command. As a result, only the primary protection zone is impacted, as compared with much larger trip zones of BF protection. Automatic reclosing following a retrip can further limit the consequences of a spurious BFI. In order to increase effectiveness, the retrip function may use a diverse trip path compared with the trip path of the initiating ZPR.

The standalone BF protection and most of the presented architectures for integrated BF protection rely on external BFI signaling. As discussed here, we have multiple ways to secure the external BFI signal paths.

B. Human Errors When Testing

A human failure to isolate or restore external BFI signals when testing relays can result in unwarranted BF operations during testing or a failure to operate after restoration into service.

Test switches are used for isolation and as access points. For convenience of testing the ZPRs, the test switches should be applied at the outputs of the ZPRs. For convenience of testing the BF relays, the test switches should be applied at the inputs to the BF relays. This creates a problem if the zone protection and BF relays are located on different relay panels, unless the switches are installed in both places.

Proper application of test switches, clear and consistent test procedures, and application of the retrip function can reduce the impact of human errors on the security of BF protection.

C. Security of Applied IEDs

The security of applied IEDs has a major impact on the security of the integrated BF protection due to common signal paths for the zone protection and BF functions residing within the same IED.

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 [8] [9]. Still, there is always a non-zero probability of an 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 only considering failures that may lead to unintended operations) is considerably better than 400 years for best-in-class relays.

Self-monitoring is an inherent advantage of microprocessor-based relays. By nature and by design, digital relay components fail more securely compared with analog components. Data and code integrity checks, watchdogs, and other standard and optimized integrity functions 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 continually monitored to ensure digital relay subsystems are supplied with proper voltages to ensure the relay fails safely before any components start operating in 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.

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.

Current best practice in high-reliability products not only includes design for quality and reliability, as explained above, but also includes the following elements [8]:

- Testing products in a certified test laboratory to perform with margins well beyond the published standards or specifications.
- Tracking field product reliability and using data to continually increase reliability by:
  - Supporting products with an extended warranty and technical assistance.
  - Analyzing every product failure to root cause and applying the findings.
- Relying on high-quality suppliers.
- Manufacturing products under controlled conditions and to highest standards.

Manufacturing quality contributes significantly to the actual field-measured reliability and security of IEDs. Some of the key processes that contribute to reliability include the following [8]:

- Rigorous process controls. Each manufacturing step has clearly defined and displayed measures that support a practice to identify issues and achieve continuous improvement.
- Environmental stress screening at –40° to +85°C with rapid temperature cycling (each unit manufactured, not just random sampling).
- Ongoing reliability monitoring of production units.

From the user perspective, it is beneficial to monitor actual field performance, security in particular, of the IEDs intended for integrating the BF function. Devices with poor or undetermined security records should be avoided when integrating the BF function. They may be used as standalone relays to benefit from avoiding failures that simultaneously affect the zone protection and BF functions.

VI. Application Examples for Various Bus Configurations

In this section, three example scenarios are provided to illustrate some of the possible practices that might be followed in deciding how to integrate BF protection:

- Single-bus single-breaker as an example of a simple bus arrangement.
- Breaker-and-a-half bus as an example of a dual-breaker configuration.
- Double-bus single-breaker as an example of a complex bus arrangement.

The concepts presented can be applied in other similar applications. Each example includes a few alternative BF configurations.

In all of these examples, we assume that the line zone has both System A and System B relays. The bus zone has only a single (nonredundant) relay.

A. Single-Bus Single-Breaker Examples

We assume that the multifunction line relays are each capable of providing BF protection. Fig. 9 and Fig. 10 present the case where the bus relay is a multirestraint, low-impedance type capable of providing BF protection. Fig. 11 shows the bus relay as either a multirestraint type capable of integrating the BF function or a high-impedance type not capable of providing BF protection.

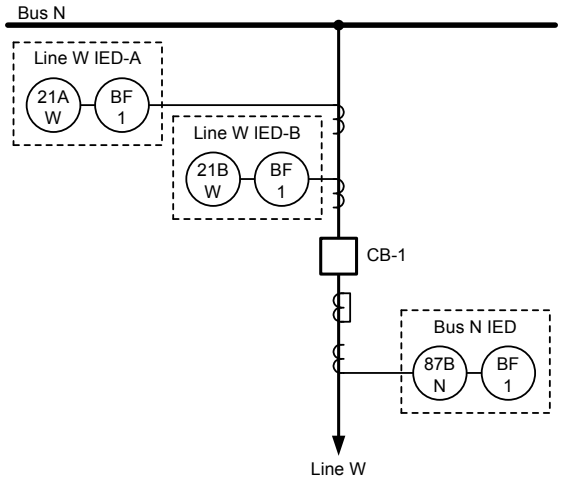

Fig. 9. Single-bus single-breaker configuration—BF integrated in all IEDs.

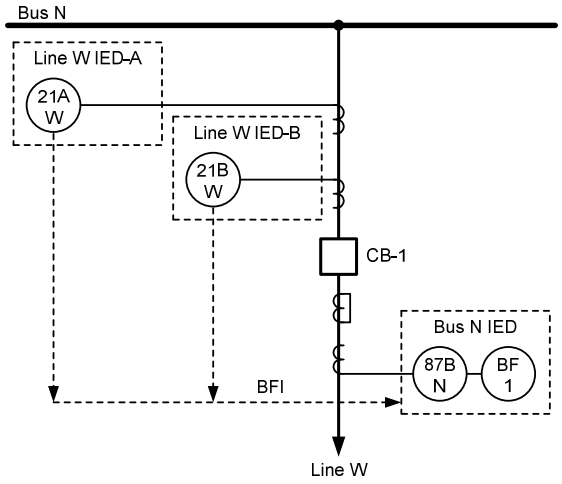

Fig. 10. Single-bus single-breaker configuration—BF integrated in the bus relay.

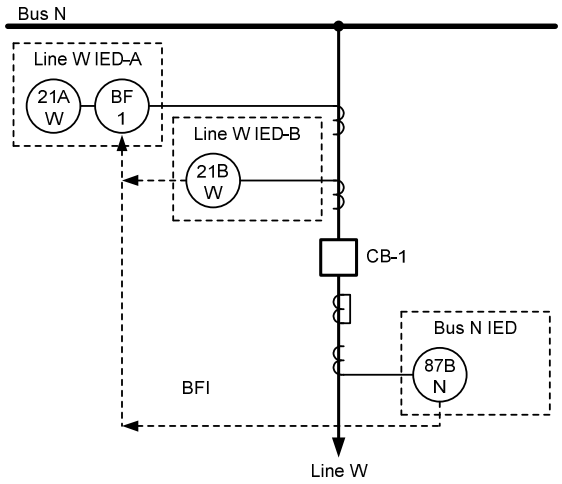

Fig. 11. Single-bus single-breaker configuration—BF integrated in the line relay. The bus relay is not capable or is not configured to provide BF protection.

Fig. 9 illustrates the simplest application, where each relay takes care of BF protection for all short-circuit trips that it initiates. There are no external BFI signals exposed to spurious initiation. In this configuration, when a relay is isolated for testing, there are no BFI signals to be concerned with from the human error point of view. When an individual relay is out of service or has failed, there is no loss of BF protection.

Fig. 10 and Fig. 11 are variations on the same approach. All three ZPRs that trip the breaker are capable of providing BF protection, but the function is enabled in only one of the relays. The configuration illustrated in Fig. 10 might be preferable because the security and trip-routing requirements for bus faults are nearly the same as the requirements for a BF.

Availability of DTT for the remote breaker needs to be considered. From this perspective, the configuration illustrated in Fig. 11 might be preferable because the line relay most likely already has direct access to the DTT equipment. In this configuration, there is external routing of the BFI signals, but the BF protection function is located in a single relay. If the single relay that provides BF protection is taken out of service or fails, there is no BF protection on that breaker. However, this only represents a single contingency because the primary system for fault interruption (the breaker) is still in service.

If the bus relay cannot provide BF protection, BF protection for bus faults will have to be initiated in one of the line relays. Fig. 11 shows the BFI signal going to only the System A relay. In this configuration, if that relay is out of service, there will be no BF protection for bus faults. Alternatively, the BFI signal could be wired to both line relays to eliminate this weakness.

In cases where DTT is not available, we could simplify the system and not provide BF protection for bus faults because the bus fault would have already caused tripping of all the local adjacent relays anyway. However, BF protection for a fault on the bus would provide direct indication of the failure and simplify troubleshooting (no need to determine if the remote relay overtripped or if the local breaker failed to interrupt).

B. Breaker-and-a-Half Examples

Fig. 12 shows how BF protection can be implemented if none of the relays are capable of providing BF protection for a double-breaker application. This is a common situation where the line relays require that the currents be summed external to the relay and the bus relay is a high-impedance type.

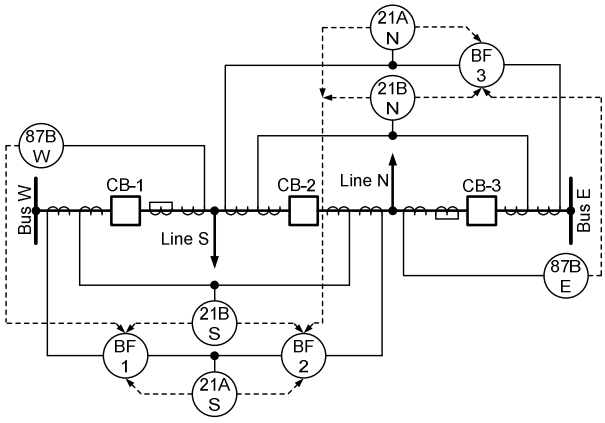

Fig. 12. Breaker-and-a-half configuration with standalone BF protection.

Fig. 13 illustrates an application where each relay takes care of BF protection for all short-circuit trips that it initiates. There are no external BFI signals exposed to spurious initiation. In this configuration, when a relay is isolated for testing, there are no BFI signals to be concerned with from the human error point of view. When an individual relay is out of service or has failed, there is no loss of BF protection.

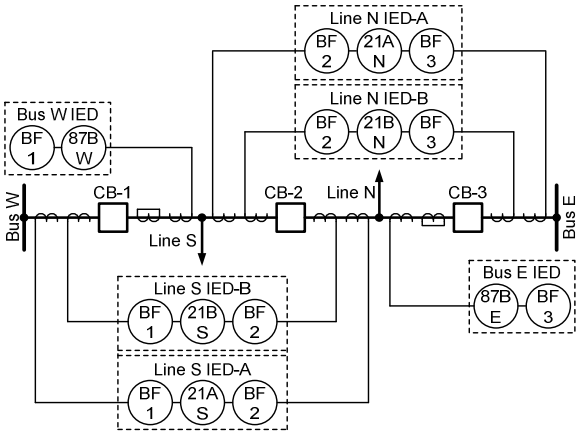

Fig. 13. Breaker-and-a-half configuration with BF protection integrated with all relays.

The scheme displays the same limitations as its counterpart for a single-bus single-breaker—zone protection and BF functions are codependent on the same hardware, firmware, and signal paths.

Fig. 14 illustrates a situation when only System A provides BF protection. BF protection in System B is not available or intentionally not applied. In this configuration, if the System A line relay is taken out of service or has failed, there is no BF protection on that breaker. However, this only represents a single contingency because the primary system for fault interruption (the breaker) is still in service.

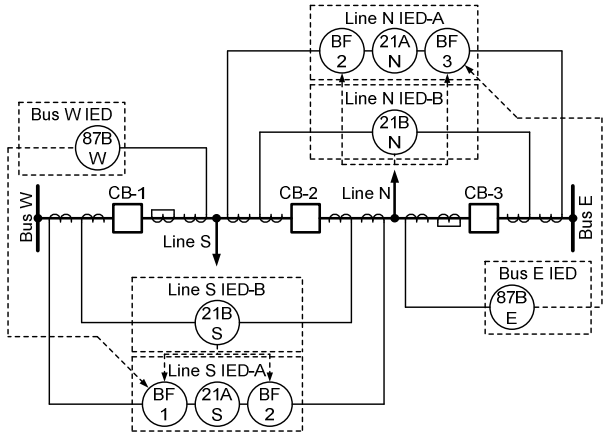

Fig. 14. Breaker-and-a-half configuration with BF protection integrated with System A relays.

Integrating BF protection in bus relays is not straightforward in the breaker-and-a-half configuration. BF protection for the two bus breakers can be symmetrically integrated with the two bus relays, but the middle breaker remains to be covered as a special case.

Either one or both bus relays provide BF protection for the middle breaker, one or more line relays provide BF protection, or a standalone device is used for the middle breaker.

However, bus relays normally do not measure any currents associated with the middle breaker, and therefore, integrating BF protection in bus relays is not natural and requires extra current inputs in the bus relays.

Integrating BF protection for the middle breaker with line relays while integrating BF protection for the bus breakers with bus relays creates a convoluted approach that requires a more careful approach to testing.

Using a standalone BF device for the middle breaker may be a good solution if the two bus breakers are protected by the two bus relays.

C. Double-Bus Single-Breaker Examples

For the purposes of examining a complex bus arrangement, this example looks at a double/transfer-bus single-breaker arrangement. In this bus configuration, each circuit can be connected to either bus. This can make BF tripping complex because the BF relay must know which breakers are connected to the same bus as the failed breaker in order to backup trip the correct breakers. For bus configurations like this, the bus protection relay must also have this information in order to make up the proper bus differential zones. Because of this commonality, BF protection is often combined with the bus protection system for this bus configuration.

The 21T relays are spare relays to substitute for the line relays with the breaker taken out of service and substituted with the transfer breaker (transferred to the transfer breaker).

Fig. 15 presents the preferred solution with BF protection integrated in the bus relay. This configuration has more complicated external initiation paths, but the BF tripping paths are simplified because they are common to the bus tripping paths. In this configuration, if the bus relay is out of service or has failed, there is no BF protection on that breaker. However, this only represents a single contingency because the primary system for fault interruption (the breaker) is still in service.

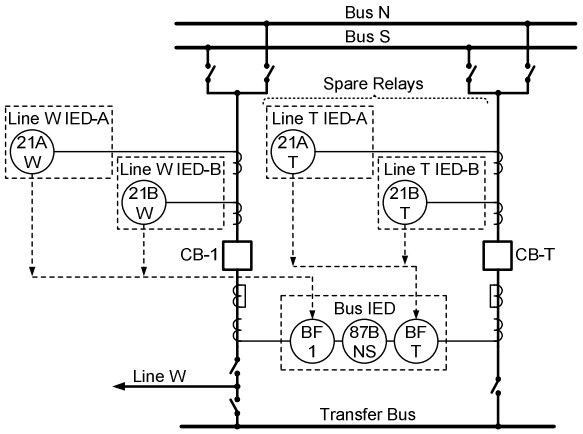

Fig. 15. Double/transfer-bus single-breaker configuration—BF protection integrated with the bus relay.

Fig. 16 illustrates the application where each relay takes care of BF timing for all short-circuit trips that it initiates. There is no routing of external BF initiate signals. This scheme would provide simpler BFI logic but more complex tripping logic. Two solutions are possible for the BF tripping paths.

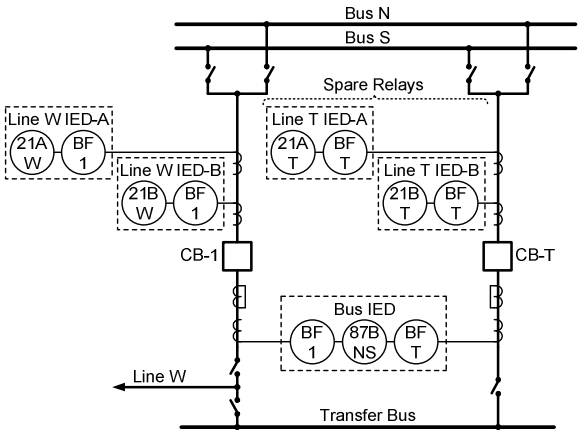

Fig. 16. Double/transfer-bus single-breaker configuration—BF protection integrated with all relays.

In the first approach, the line relays monitor the disconnect switches to identify which bus the failed breaker is connected to and which other breakers are connected to the said bus and need to be cleared. This solution is practical only for very

small buses, and when implemented, it should follow similar principles as bus protection [2].

In this configuration, when a relay is isolated from the system for testing, there are no external BFI signals to be concerned with.

The second approach is to let the line relays assert the BF trip command and indicate the failed breaker to the bus relay. The latter does not perform the BF timing but simply resolves the tripping matrix for the bus configuration at the time of BF.

In this approach, although there are no external BFI signals, the signals sent from the line relays to the bus relay are effectively direct trips. As such, they are arranged for maximum security (e.g., using the Fig. 8 solution or dual-point input/output wiring).

In this scheme, when an individual relay is out of service or has failed, there is no loss of BF protection.

VII. Conclusions

This paper considers the merits, advantages, and disadvantages of integrating BF protection with ZPRs. Major factors considered include the following:

- Preferred balance between security and dependability in the context of using multiple BF elements for a given breaker, designing out external BFI signal paths and therefore reducing the probability of human errors when testing, and overall security and reliability of applied IEDs.
- General protection philosophy in terms of the preferred degree of integration, application of dedicated breaker IEDs, remote versus local backup, lockout relays versus virtual lockout function in software, and maintenance and testing practices.
- Bus arrangements potentially impacting the complexity of the BF trip paths, as well as the overall security due to a varying tolerance to unwarranted BF operations.

Several alternative solutions have been presented for integrated BF protection. These solutions allow different tradeoffs between simplicity, amount of interdevice signaling, security, and dependability. The presented alternatives have been illustrated using three bus configurations in common use—single-bus single-breaker, breaker-and-a-half, and double/transfer-bus single-breaker reconfigurable bus.

Ways to improve the security of BF protection have been discussed, including better security of BFI signals under battery ground faults and noise, benefits of retrip in limiting the consequences of unintended BFI signals, and merits of cross-initiation of integrated BF protection in improving the overall security of the scheme.

VIII. References

[1] IEEE Guide for Breaker Failure Protection of Power Circuit Breakers, IEEE C37.119-2005, 2006.

[2] IEEE Guide for Protective Relay Applications to Power System Buses, IEEE C37.234, 2009.

[3] A. Guzmán, C. Labuschagne, and B. L. Qin, "Reliable Busbar and Breaker Failure Protection With Advanced Zone Selection," proceedings of the 31st Annual Western Protective Relay Conference, Spokane, WA, October 2004.

[4] E. Atienza and R. Moxley, "Improving Breaker Failure Clearing Times," proceedings of the 36th Annual Western Protective Relay Conference, Spokane, WA, October 2009.

[5] H. J. Altuve, M. J. Thompson, and J. Mooney, "Advances in Breaker-Failure Protection," proceedings of the 33rd Annual Western Protective Relay Conference, Spokane, WA, October 2006.

[6] "Ancillary Protective and Control Functions Common to Multiple Protective Relays," IEEE Power System Relaying Committee WG K5 Report, December 2009. Available: http://www.pes-psrc.org.

[7] M. Thompson, "The Power of Modern Relays Enables Fundamental Changes in Protection and Control System Design," proceedings of the 60th Annual Conference for Protective Relay Engineers, College Station, TX, March 2007.

[8] R. Kirby and R. Schwartz, "Microprocessor-Based Protective Relays Deliver More Information and Superior Reliability With Lower Maintenance Costs," proceedings of the 17th Annual DistribuTECH Conference and Exhibition, San Diego, CA, February 2007.

[9] Newton-Evans Research Company, *Worldwide Study of the Protective Relay Marketplace in Electric Utilities: 2006–2008, Volume 1: North American Market*, 2008.

IX. 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 Wrocław University of Technology, 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 IEEE Power System Relaying Committee and is a registered professional engineer in the province of Ontario.

Michael J. Thompson received his BS, magna cum laude, from Bradley University in 1981 and an MBA from Eastern Illinois University in 1991. He has broad experience in the field of power system operations and protection. Upon graduating, he served nearly 15 years at Central Illinois Public Service (now AMEREN), where he worked in distribution and substation field engineering before taking over responsibility for system protection engineering. Prior to joining Schweitzer Engineering Laboratories, Inc. (SEL) in 2001, he was involved in the development of several numerical protective relays while working at Basler Electric. He is presently a principal engineer in the engineering services division at SEL, a senior member of the IEEE, a main committee member of the IEEE PES Power System Relaying Committee, and a registered professional engineer. Michael was a contributor to the reference book *Modern Solutions for the Protection Control and Monitoring of Electric Power Systems*, has published numerous technical papers and holds a number of patents associated with power system protection and control.

Previously presented at the 2011 Texas A&M Conference for Protective Relay Engineers.

20110217 • TP6447-01