Communications-Assisted Schemes for Distributed Generation Protection

Edmund O. Schweitzer, III, Dale Finney, and Mangapathirao V. Mynam
Schweitzer Engineering Laboratories, Inc.

© 2012 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

This paper was presented at the 2012 IEEE PES Transmission and Distribution Conference and Exposition, Orlando, Florida, May 7–10, 2012, and can be accessed at: http://dx.doi.org/10.1109/TDC.2012.6281512.

Communications-Assisted Schemes for Distributed Generation Protection

Edmund O. Schweitzer, III, Dale Finney, and Mangapathirao V. Mynam

***Abstract*—Integrating generation into the distribution system presents several challenges. Distributed generation (DG) can affect the coordination between reclosers and fuses, compromising fuse-saving schemes and thereby reducing power quality and reliability. Nuisance tripping of distributed generators, either from local protection or from anti-islanding schemes, is also an issue. The use of communications-assisted schemes is well established at the transmission level. However, conventional communications links may not be cost-effective for use at the distribution level. With the advent of spread-spectrum radio, there is an opportunity to improve the performance of DG protection and anti-islanding schemes. Communications links based on wireless technology are much more cost-effective but have characteristics that can differ from conventional channels. This paper illustrates how teleprotection schemes can be designed to suit both the topology of the distribution network and the characteristics of the wireless channel, allowing DG to be integrated without compromising the reliability of the distribution network.**

***Index Terms*—Distributed generation, teleprotection schemes, distribution network, wireless communications, spread-spectrum radios, collocated radios, islanding schemes, fuse-saving schemes, recloser coordination.**

I. Introduction

A. Distributed Generation

A distributed generator is defined as an energy source that is connected directly to the distribution network. Distributed energy resources include both distributed generators and energy storage devices. Recently, renewable energy sources have been developed, such as solar, wind, and biofuels. Because of the scale of these sources, there is a tendency towards their integration at the distribution level. Distributed generation (DG) is gaining momentum, with governments all over the world pushing towards clean energy and carbon footprint reduction, causing a paradigm shift in the conventional generation, transmission, and distribution of electrical energy.

Distribution systems, which are conventionally radial, may now be equipped with energy sources, making them low-voltage transmission networks. There is a definite need to revisit the protection and operational philosophies associated with this new distribution network, along with available communications technologies.

E. O. Schweitzer, III, D. Finney, and M. V. Mynam are with Schweitzer Engineering Laboratories, Inc., Pullman, WA 99163 USA (email: papers@selinc.com).

B. Pertinent Characteristics of Distributed Generators

While virtually all generators connected into the transmission system are synchronous, DG systems can be synchronous, induction, or inverter based. A synchronous generator relies on the interaction of the rotor and stator fields to deliver real and reactive power to the system. An excitation system is used to create the rotor field, and as a result, a synchronous generator can produce stable power when islanded. Consequently, synchronous generators require synchronizing facilities and are at risk of severe damage due to out-of-phase reclosing. The initial fault current produced by a synchronous generator is a function of the subtransient reactance and typically is several times the rated current.

An induction generator differs from a synchronous generator in that it absorbs reactive power from the system in order to maintain the rotor field. Soft starters, rather than synchronizing facilities, are employed for bringing an induction generator online. An induction generator is, however, still subject to damage due to out-of-phase reclosing. Islanded operation of an induction generator is possible if the island can supply sufficient reactive power to maintain the field of the machine. This is known as self-excitation. An induction generator can supply significant fault current as long as there is reactive compensation available from the system.

An inverter-based distributed generator converts dc electricity from a power source to ac electricity. Inverters can be classified by their method of commutation. Most inverters used in DG applications are self-commutated. Self-commutated inverters require synchronizing facilities and can be damaged during out-of-phase reclosing. In contrast to synchronous and induction generators, the fault current of an inverter-based distributed generator is intentionally limited by its control system and may only marginally exceed the rated current.

II. Challenges Associated With DG Integration

This section reviews known issues that can occur on feeders with distributed generators [1] [2]. Systematic procedures have been developed to determine the extent of the impact, if any, for a particular DG installation [3].

A. Protection

1) Fuse Blowing Due to Slow DG Clearing

The percentage of transient faults can be as high as 80 percent in a distribution network. For many years, utilities have successfully employed fuse-saving schemes to achieve a high level of service availability for their customers [3]. However, increased fault contributions and slow fault clearing from the DG may result in fuses blowing for faults otherwise cleared by the fuse-saving scheme. This leads to extended customer outages. As a result, one major utility specifies a maximum DG clearing time based on a typical fuse melt time of 200 milliseconds [4]. This issue is unique to synchronous and induction distributed generators. Inverter fault contribution is typically limited to 150 to 200 percent of the thyristor rated current in magnitude and one-half cycle in duration.

2) Loss of Fuse/Recloser Coordination

Reclosers are typically coordinated with fuses, as shown in Fig. 1. In this example, a transformer is located on a branch circuit, as shown in Fig. 2. The branch circuit is downstream of a recloser. The fast recloser curve is set to be between the branch and transformer fuse curves. Under normal operation, the fast curve is active. A fault downstream of the branch fuse is interrupted by the recloser. Automatic reclosing is delayed to allow transient faults to extinguish. Upon reclosing, the fast curve is deactivated. If the fault is permanent, it will be cleared by the branch fuse. Effectively, the slow curve acts to back up the fuse.

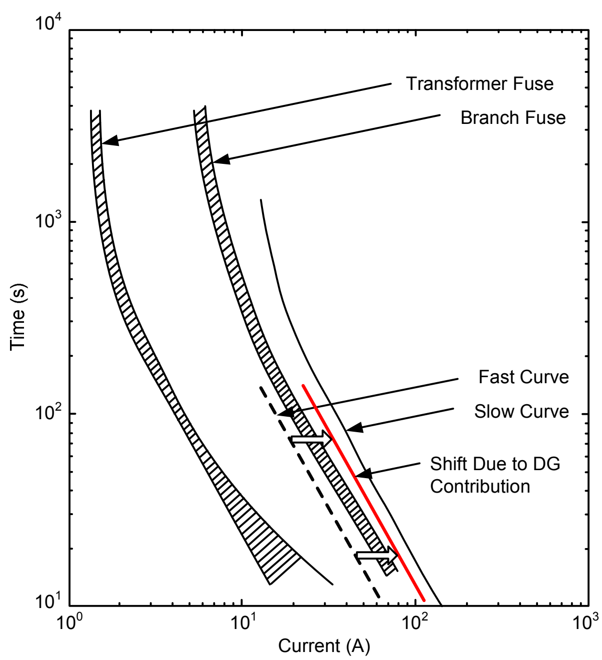

Fig. 1. DG may cause loss of coordination.

Fuse-saving schemes depend on the coordination of inverse-time characteristics between the fuse and recloser. The fundamental premise is that both see the same current. Fig. 1 illustrates the issue introduced by DG. The fuse will always see more current when the DG is connected. This will have the effect of moving the fast curve to the right. The result is that the fuse can operate before the recloser. The curves respond to the current squared, amplifying the effect of shrinking coordination time margins. As DG penetration increases, the discrepancy between the recloser and fuse currents increases, and the potential for loss of coordination grows as DG penetration grows.

3) Loss of Protection Sensitivity

The addition of a distributed generator to the feeder can lead to a reduction in the available fault current contribution from the system. Fig. 2 shows a feeder with a connected synchronous or induction distributed generator. The equivalent source representing the power system (SYS) feeds the distribution network. The circuit breakers (CBs) represent switching elements that are capable of interrupting fault current. Adding impedances and redrawing yield the circuit in Fig. 3. The variable x represents the location of the DG expressed as a percentage of feeder length. Inspection of this equivalent circuit shows that Fault 1 current splits between the two sources.

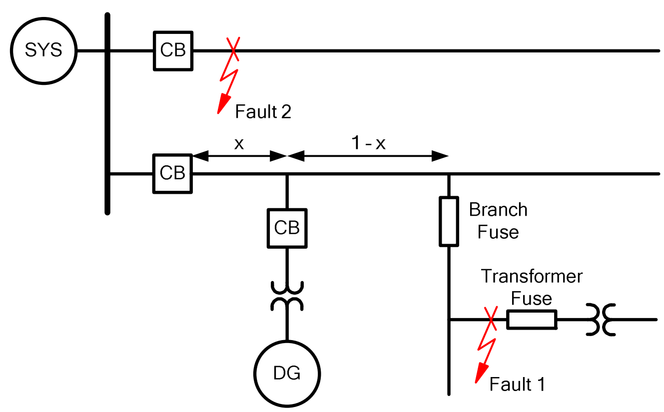

Fig. 2. A faulted feeder with DG.

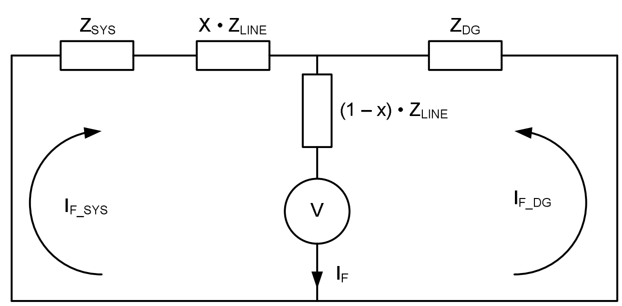

Fig. 3. Faulted feeder equivalent circuit.

We can apply circuit analysis to develop expressions for the fault currents both with and without the generator. Using these expressions, a plot can be produced that shows the available fault current at the feeder end expressed as a ratio of fault current without DG (see Fig. 4). Inspection of this plot shows that fault current varies as a function of DG penetration and location (x in Fig. 3). For this example, the circuit parameters have been arbitrarily selected. The penetration level is defined as the ratio of (capacity factor • DG rated kVA)/(peak load on the feeder).

Note that for high levels of DG penetration, the reduction in fault current is significant.

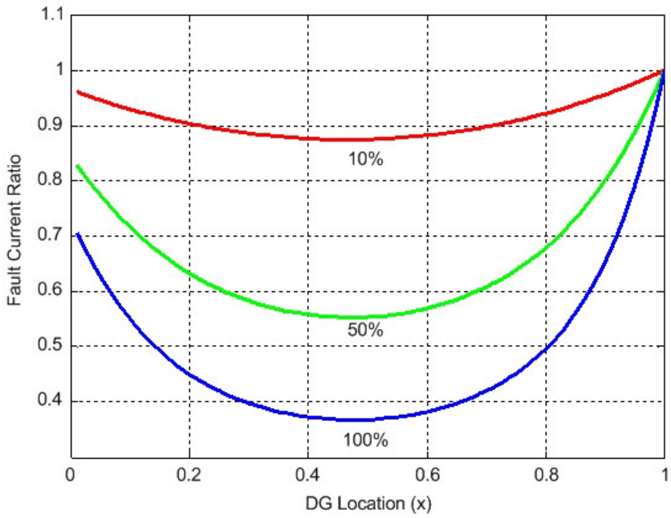

Fig. 4. Feeder fault current contribution expressed as a ratio of available fault current without DG for various DG penetration levels and locations (sample feeder and DG data used).

Ground fault current levels at the end of a feeder may be less than the load current. Ground fault protection must be set greater than the maximum current unbalance under normal operation. As a consequence of the reduction in fault current due to DG being online, feeder protection may be unable to detect ground faults over the entire feeder.

4) DG Step-Up Transformer Grounding

The DG transformer connection must be compatible with the distribution network to which it is connected, and therefore, the method of transformer grounding is typically mandated by the utility. Both the three-wire network and the four-wire multigrounded network are commonly used.

A four-wire network can supply single-phase loads, so transient overvoltages are a concern. In a four-wire network, the DG step-up transformer will be effectively grounded on the high side to limit overvoltages to a safe value. A solidly grounded connection is often avoided because it may produce excessive ground fault levels. Conversely, three-wire networks feed phase-to-phase and three-phase loads. Equipment may be rated for full phase-to-phase voltage, alleviating overvoltage concerns. Sensitive ground fault protection may be applied. In some systems, a grounded DG transformer high-side connection is not permitted, and as a result, current-based ground fault protection cannot be applied at the DG. In other distribution systems, the available ground fault current at the DG is restricted. Fig. 5 shows the sequence network for a single-line-to-ground fault for a feeder with connected DG. The DG transformer has a grounded-wye connection on the system side and a delta connection on the generator side. The transformer impedances that appear in the zero-sequence network act to shunt the available ground fault current. Consequently, on an effectively grounded system, increasing the penetration of DG can adversely impact the sensitivity of feeder ground fault protection.

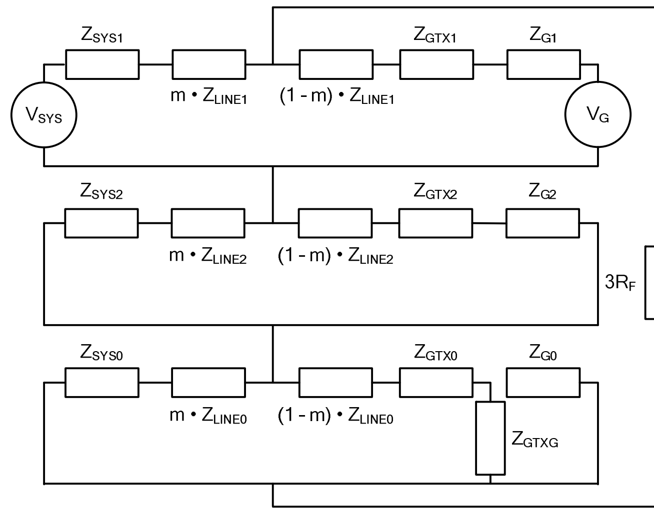

Fig. 5. Sequence network diagram for a ground fault with a grounded DG interconnect.

5) Nuisance Tripping

The addition of DG creates a contribution to upstream faults, as is evident for Fault 2 in Fig. 2. This creates a possibility that upstream reclosers and feeder protection that are typically nondirectional could operate for faults on the adjacent circuit. In addition, the DG interconnect protection (in particular, the voltage elements or the DG transformer fuses) could operate for faults on adjacent feeders.

6) Increased Fault Duty

Inspection of Fig. 2 also reveals that, with the addition of DG, the available fault current seen by downstream equipment increases. At high levels of DG penetration, the interrupting rating of downstream devices may be compromised.

B. DG Islanding

An island is a section of the distribution network that has been isolated from the remainder of the network. Stable islanding requires that load and generation be matched within the island. Islanding is not new to power system operators; transmission networks operate in islanding conditions during contingencies. Load- or generation-shedding schemes are typically triggered following island conditions to balance load to generation. However, for systems with DG, it is not recommended to operate networks in an islanded state [5]. Various anti-islanding schemes exist that detect islanding conditions and send a trip command to disconnect the distributed generator.

1) Existing Anti-Islanding Schemes

Anti-islanding schemes can be mainly categorized as passive, active, and communications-based. Passive schemes use the measured voltage and/or current quantities at the interconnect to detect the islanding condition. One type of active scheme injects signals at the DG location and detects the islanding condition by measuring the system response to the injected signal or modulation. Another type of active scheme introduces an intentional positive feedback into the inverter controls. As a result, the inverter is intentionally unable to regulate voltage or frequency when islanded, allowing detection of the islanding condition.

2) Performance of Anti-Islanding Schemes

The performance of the passive schemes that are based on frequency is dependent on the real power mismatch between the local generation and the load. Higher mismatches typically result in faster response times. Lower mismatches can result in restraining the operation of the scheme or slower responses. This zone of lower mismatch is termed a nondetection zone. Because the power output of the DG is typically constant, the load requirement prior to the island dictates the performance of the frequency-based islanding schemes. Fig. 6 shows an example of the operating times of frequency elements for a specific distribution system with different load-to-generation ratios.

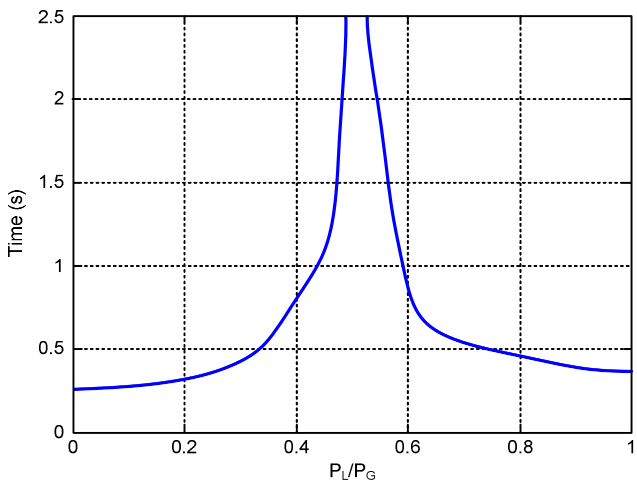

Fig. 6. Islanding detection time when using frequency elements increases as the power exchange decreases.

Similarly, islanding schemes based on the voltage magnitude depend on the reactive power mismatch in the island.

The possibility of nondetection of the island condition has led many utilities to adopt a two-to-one rule—meaning that the minimum islanded load must be twice as large as the total available DG within the island. If this limit cannot be guaranteed, passive schemes are not permitted.

The performance of the active schemes is not dependent on the power mismatch in the island. However, one of the main concerns with the active injection-based schemes is the interference introduced when multiple distributed generators are connected with the injection systems to detect islanding.

III. Teleprotection

We can define teleprotection as the use of communication to improve the performance of protection schemes. In transmission networks, teleprotection has been used for many years to achieve improvements in speed, selectivity, and sensitivity.

These schemes require a communications channel. In the following discussion, we refer to a channel as the physical medium used to convey a signal. Terminal equipment is the hardware connected at the ends of the channel. Examples of terminal equipment include modems, fiber-optic transceivers, and radios. We use the term link to refer to the channel together with its terminal equipment.

Varieties of communications links have been used for teleprotection at the transmission level. These links include power line carrier, leased phone lines, microwave radio, and fiber-optic cable. These links may be dedicated or, when bandwidth permits, be multiplexed to allow other applications to share the link.

In the following discussion, we review the characteristics of a communications link that are important when applied for teleprotection. We focus on unlicensed spread-spectrum radio and compare this link with two others that may also be considered as candidates in a distribution network—namely the leased telephone link and the fiber-optic link.

A. Security

Security is a measure of the ability of a link to not operate when it is not required to operate. The security of a link is a function of the channel characteristics and the error correction methods employed by the terminal equipment.

The signal-to-noise ratio (SNR) is one measure of channel quality. The SNR goes down when channel noise increases but also goes down when the signal level decreases. A decrease in signal level can result from increased path loss, weather, or a failing hardware component.

The bit error rate (BER) is the ratio of erroneous bits to total bits transmitted on a digital channel. BER is related to SNR and is also dependent on the modulation scheme and type of noise. In general, as SNR drops, BER goes up.

The attenuation of a radio channel increases with length. This property is known as path loss. The basic relationship for the path loss between two antennas in free space is given by the following equation.

$$\mathrm{LP(db)} = 20\log \bullet \left(\frac{4 \bullet \mathrm{d}}{\lambda}\right) \tag{1}$$

where:

LP is the path loss in db.

d is the distance between the transmitter and receiver.

λ is the carrier wavelength in the same units as *d*.

The receiver sensitivity is the signal level at which a receiver can reliably recover data. Manufacturers will typically specify the receiver sensitivity for a specified value of BER, which may range from 10^{-3} to 10^{-6}.

Radio channels share an important advantage with fiber-optic channels in that they are unaffected by the electrical transients or ground potential rise (GPR) associated with a power system fault. The same cannot be said for leased telephone channels, which may be forced out of service during a fault.

Terminal equipment typically employs error control coding to improve the security of a communications link. Some error control coding methods may detect and correct errors where others may simply detect errors. The cyclic redundancy check

(CRC) is a commonly used method. During encoding, extra (check) bits are added to the payload. When the message is received, the CRC is recalculated from the received payload and compared to the received check bits. A discrepancy indicates that the payload (or the CRC) has been corrupted. The check bits are redundant because they add no additional information to the message. The effectiveness of error control coding is a function of the relative number of check bits as compared to the payload. Increasing the number of check bits makes for a more secure message at the expense of message length, thus bandwidth.

Relays can also add additional security in the form of duplicate messages and parity checks. The resulting level of security provided approaches the level required for transmission applications [6].

B. Speed

The speed of a communications channel depends on the data rate of the channel, the size of the message, and the existence of any additional latency in the equipment at each terminal. Routing the communication directly from the terminal equipment to the relay avoids any delays associated with auxiliary teleprotection equipment.

Currently, point-to-point spread-spectrum radios are available with data rates as high as 38400 bps. Assuming a message size of 36 bits, the transmission time for a message at 38400 bps is approximately 1 millisecond. This assumes that the radio does not add any overhead for error control. Transmission times in the range of 4 to 5 milliseconds are typical when error control is taken into account.

Unlicensed radios operate primarily in the 915 MHz frequency band and have a range of around 10 to 20 miles with line-of-sight operation. A repeater is required when line of sight between the ends of the link is obscured or when the length of the path exceeds the range of the radio. The addition of a repeater effectively doubles the latency of the radio link.

Radios are available that can also apply data encryption. Encryption adds overhead to the message and, as a result, can add up to 10 milliseconds of additional latency. Note that the purpose of encryption is to protect the privacy of data, whereas error control coding addresses security. Encryption is therefore not considered necessary on a teleprotection link.

Finally, delays associated with the relay itself must be considered. Depending on the relay, the rate at which messages are processed can vary from two to eight times per power system cycle.

The data rates and error control on leased telephone circuits are similar to that of radio, so we can expect similar channel latencies on these links.

Optical fiber has the lowest latency of any of the links due to its immunity to electrical interference and high bandwidth. The delay on a fiber-optic channel can be less than 1 millisecond [7].

C. Availability

The availability of a link can be defined as the amount of time that the link is capable of successfully transmitting data expressed as a percentage of total time. A link will become unavailable if either its terminal equipment or channel fails. Assuming similar reliability of terminal equipment, the difference in availability of various links depends mainly on the channel characteristics.

The availability of a radio channel can be degraded because of such issues as weather, growth of trees, or erection of structures within the path of the radio link. Additionally, because the band is unlicensed, there is always the possibility of interference of another radio in the vicinity.

Spread-spectrum radios deliberately distribute their signals across a wide frequency band. As a result, these radios have very good immunity to interference and are difficult to jam. Spread-spectrum radios generally do a very good job of rejecting narrowband sources of interference; however, degradation can occur when multiple spread-spectrum systems are operating in the same vicinity.

Radios are available that can synchronize their frequency hopping behavior to allow the placement of multiple radios at a location without interference (Fig. 7).

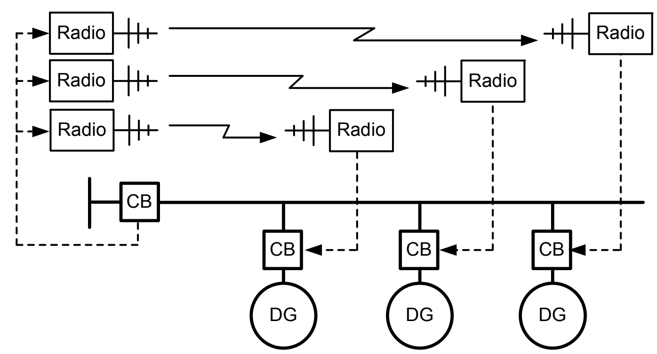

Fig. 7. Collocated radios.

The availability of leased telephone channels can be characterized by long periods of operation interrupted by brief bursts of noise [6]. Other causes of failure include reconfiguration of circuits at the telephone company central office or damage of a buried cable through inadvertent excavation.

Fiber-optic cable is expected to have the highest level of availability because it is immune to electrical interference. However, buried fiber is also subject to inadvertent excavation.

Protective relays are now designed to interface directly with terminal equipment. These relays are capable of measuring the availability and the current status of the link. This creates the ability to design better protection schemes, which adapt according to the status of the channel.

D. Cost

As previously mentioned, a 915 MHz spread-spectrum radio can operate at distances of up to 20 miles if there is an unobstructed electromagnetic line of sight between antennas (electromagnetic line of sight is more generous than optical line of sight). Installed cost is now on the order of a few thousand dollars per terminal. If the terrain is not adequately flat, towers and/or repeaters will be required, and this can result in a significant escalation in cost. On the plus side, there are no additional recurring licensing or leasing costs.

The terminal equipment cost for leased telephone links is similar to that of radio. These links will have additional costs associated with GPR isolation. In addition, leasing costs in the United States can be upwards of several hundred dollars per month.

Fiber-optic transceiver costs range from several hundred dollars for multimode transceivers to over one thousand dollars for single-mode transceivers. By far, the largest cost is to buy and install the fiber. This cost can run into thousands of dollars per mile [8].

IV. Communications-Based Feeder Protection Schemes

Some of the issues identified in Section II may be dealt with during the project planning phase through selection of the optimum location and/or size of the DG. Coordination studies can resolve other issues [3] [9]. The use of communication is not seen as a replacement for good engineering practices. Instead, it can be considered for issues that cannot be resolved by a simpler approach or for a higher level of DG penetration than might otherwise be possible.

Tripping the DG instantaneously has the potential to address coordination issues. IEEE 1547 requires that the DG be taken offline for all faults on the circuit to which it is connected. However, this can likely lead to DG trips for faults on adjacent feeders. Assuming that faults must be cleared within 200 milliseconds (see Section II, Subsection A) and the DG breaker takes 5 cycles or 83 milliseconds to operate, the DG protection must operate in less than 117 milliseconds. Assuming that it will take a minimum of 6 cycles or 100 milliseconds to clear a fault on an adjacent feeder (1 cycle for protection plus 5 cycles for the breaker), it becomes unlikely that fuse saving can be retained without tripping DG for faults on adjacent feeders.

A teleprotection scheme may be implemented to address DG overtripping. These schemes were designed for transmission lines. However, the underlying principles are applicable.

A. DG Directional Comparison Blocking Scheme

A directional comparison blocking (DCB) scheme is shown in Fig. 8. Directional elements in the substation are set to see upstream faults and transmit a blocking signal to the DG. The blocking signal is inverted and connected by an AND gate to the local protection. This reverse-looking element is also necessary to prevent tripping of the substation breaker.

Local protection is delayed to account for channel latency, and the time delay must be set longer than the longest anticipated delay of the channel. Thus particular radio links that have low average channel latency but high maximum channel latency should be avoided for use in DCB schemes.

DCB schemes that employ channels with deterministic latency can deliver DG clearing times that approach those of permissive overreaching transfer trip (POTT). In addition, the DCB scheme is not dependent on the ability of a forward-looking directional element to see all feeder faults.

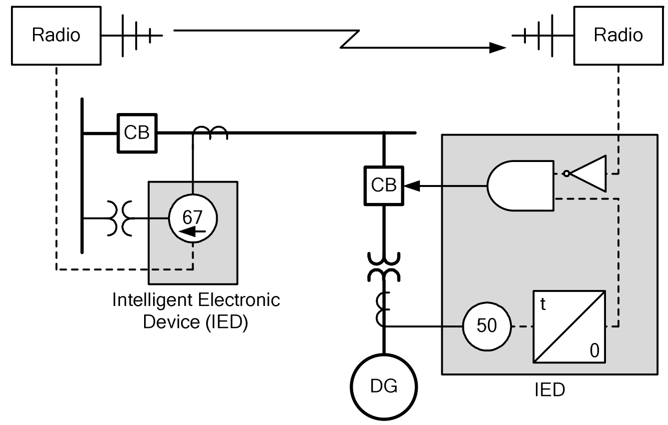

Fig. 8. DG DCB scheme.

Overtripping of the DG is possible for a channel failure or for a failure of the substation directional elements to pick up for a reverse fault. Again, this weakness demonstrates itself only under contingency conditions while allowing the use of a lesser performance channel, making the solution very attractive.

A common cause of DG overtripping is the operation of the intertie voltage element. This protection is specified in IEEE 1547 for detection of feeder problems [10]. However, it has been known to operate for faults on adjacent feeders. It is feasible to also supervise this function with the same blocking signal.

B. Adaptive Protection Coordination

The potential for loss of fuse/recloser coordination due to the contribution of the DG was explained and illustrated in Section II. In many cases, the fast curve may be adjusted to account for the DG contribution [1] [9]. However, the result of a permanent adjustment may be that the recloser is too fast when the DG is offline, resulting in recloser tripping for faults downstream of the transformer fuse. An alternative is the communications-based approach. The DG transmits its online indication to the upstream recloser. The recloser implements a settings group change whenever the DG is online. In the alternate settings group, the time dial of the fast curve is reduced to account for the difference between the recloser current and the fuse current. A fault study is required to determine the appropriate value for the multiplier setting.

The scheme is not dependent on the speed of the communications channel because the DG online indication will be present prior to the fault.

Protection is not lost in the event of a communications failure, although fuse/recloser coordination will be lost. This response under the contingency of lost communication is acceptable.

The proposed scheme may also be used to desensitize recloser protection, if necessary, during energization of the DG transformer.

V. Communications-Based Anti-Islanding Schemes

A. Transfer Tripping

Direct transfer trip (DTT) is one of the conceptually simple islanding schemes. In these schemes, islanding is typically detected based on breaker status or open phase detection logic by the upstream feeder relays or reclosers. Typically, there may be multiple breakers at different locations, any of which, when tripped, could create an island. Fig. 9 shows a programmable logic controller (PLC) receiving breaker statuses from feeder relays and reclosers.

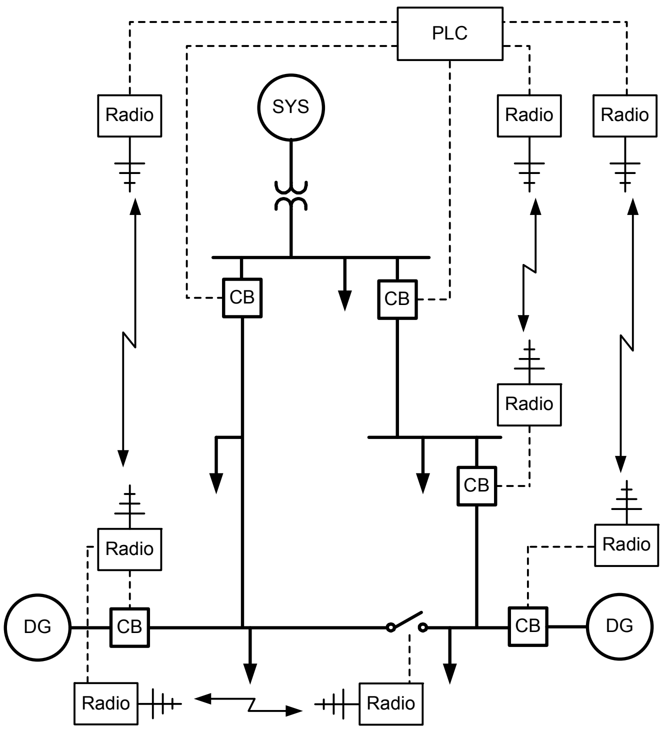

Fig. 9. DTT anti-islanding using a PLC and radios.

Based on preprogrammed logic, the PLC sends a trip command to the DG breaker. Radio communication and leased telephone lines are typically used as economical communications media for transfer tripping schemes. A radio at each monitoring location communicates the breaker status to the radio at the central location where the PLC is installed. It is recommended to use radios with collocation functionality to provide deterministic and dependable communication.

Utilities prefer to disconnect the DG when communication fails. This practice is acceptable to both the DG owner and the utility when highly reliable communication is in place. Spread-spectrum-based ISM band communication offers low-cost communication with lower availability. However, by performing path studies and implementing appropriate design practices, it is possible to take advantage of low-cost communication and achieve high availability. Tripping DG for communications failures is not appealing to DG owners. Therefore, DG protection designs must include logic to address communications failures without sacrificing protection for out-of-phase reclosing. It is recommended to supervise the feeder reclosing using standard practices; one such practice is dead line/live bus. Phase voltage on the line side of the breaker is required for this reclose supervision logic. Alternate schemes need to be implemented to prevent out-of-phase reclose when the line-side potential is not available.

Fig. 10a shows logic that can be implemented in the feeder relay to inhibit reclose if the communications link is down for more than 8 milliseconds. Reclosing is enabled if the communication is restored for longer than 1 second. This assumes that the autoreclose open interval delay expires before 1 second and drives the scheme to lockout.

Fig. 10b shows the logic to trip the DG if communication fails for over 5 seconds. This logic can be implemented in the protective relay at the DG site. The T1 and T2 timers in Fig. 10 are arbitrarily selected and can be changed per application requirements or practice. The communications okay (COMMOK) signal can be generated by using a watchdog mechanism, where the protective relay at the DG site periodically sends a digital bit to the upstream feeder relay. A communications failure is declared and the autoreclose is blocked by the feeder relay if the watchdog bit does not arrive for a programmable period of time.

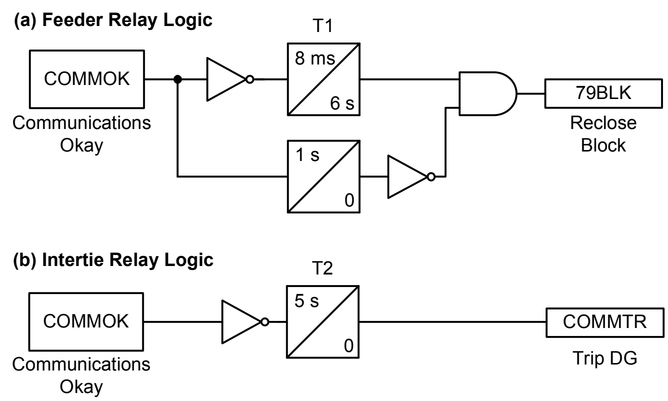

Fig. 10. Communications failure logic.

Implementation of transfer trip schemes is challenging when feeder reconfiguration and multiple distributed generators need to be considered.

B. Supervised Passive Anti-Islanding Scheme

Passive anti-islanding schemes can detect an island from local measurements of voltage and frequency. However, these schemes, specifically vector shift and rate of change of frequency (df/dt), are subject to nuisance tripping during disturbances. A communications channel can be used to supervise these schemes in order to improve security. An example is shown in Fig. 11.

The scheme requires df/dt elements located at the DG and substation using bus-side potential transformers. If an islanding event occurs by opening the substation breaker, the element at the DG will operate but the element at the substation will not. The DG will subsequently be disconnected. During a system disturbance, both elements may operate. The substation IED sends a block to the DG IED, preventing the DG from tripping. A short time delay at the DG is required to account for channel latency. Because islanding detection is carried out locally using passive protection elements, this scheme can still operate if the communications channel is unavailable, although false operations are more likely. A second advantage is that it does not require communications with midline reclosers. Because it is a passive scheme, it requires a power mismatch for guaranteed operation, as described in Section II, Subsection B.

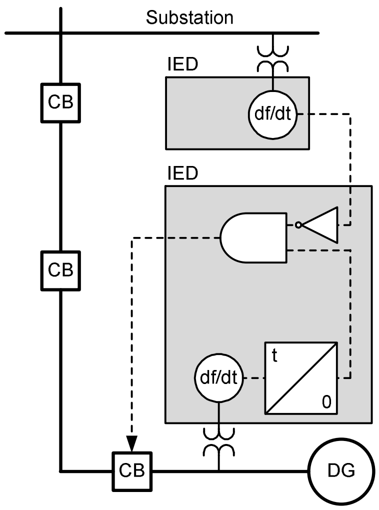

Fig. 11. Supervised df/dt scheme.

With cost being an important factor for DG projects, spread-spectrum-based ISM communication offers a great solution to provide security for passive islanding detection schemes. A low-cost communications channel to minimize nuisance tripping is a viable option that DG owners could implement. As the DG penetration increases, dedicated fiber communication might be justifiable.

VI. Conclusion

This paper reviews the challenges of integrating generation at the distribution level. It presents several schemes that use communication to improve protection and anti-islanding performance in distribution networks with distributed generation but are not completely dependent on the availability of the communication. The schemes are well-suited to the characteristics of a radio link. Specifically, the security of a radio link approaches that of links used in transmission applications. Radio links also compare very well in terms of speed, which is more than adequate for the schemes presented in this paper. The availability of a radio link can be more difficult to quantify. As a result, schemes that are biased towards dependability are favored whenever radio links are employed.

VII. References

[1] R. A. Walling, R. Saint, R. C. Dugan, J. Burke, and L. A. Kojovic, "Summary of Distributed Resources Impact on Power Delivery Systems," *IEEE Transactions on Power Delivery, Vol. 23*, Issue 3, pp. 1636–1644, July 2008.

[2] IEEE Power System Relay Committee WG D3, "Impact of Distributed Resources on Distribution Relay Protection," August 2004.

[3] Qualsys Engco. Inc., *Protection Coordination Planning With Distributed Generation*, presented to Natural Resources Canada, June 2007.

[4] Hydro One Networks Inc., *Distributed Generation Technical Interconnection Requirements*, DT-10-015 R2, 2011.

[5] J. Mulhausen, J. Schaefer, M. Mynam, A. Guzmán, and M. Donolo, "Anti-Islanding Today, Successful Islanding in the Future," proceedings of the 63rd Annual Conference for Protective Relay Engineers, College Station, TX, March 2010.

[6] E. O. Schweitzer, III, K. Behrendt, and T. Lee, "Digital Communications for Power System Protection: Security, Availability, and Speed," proceedings of the 25th Annual Western Protective Relay Conference, Spokane, WA, October 1998.

[7] R. Moxley and K. Fodero, "High-Speed Distribution Protection Made Easy: Communications-Assisted Protection Schemes for Distribution Applications," proceedings of the 31st Annual Western Protective Relay Conference, Spokane, WA, October 2004.

[8] S. V. Achanta, B. MacLeod, E. Sagen, and H. Loehner, "Apply Radios to Improve the Operation of Electrical Protection," proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.

[9] A. Zamani, T. Sidhu, and A. Yazdani, "A Strategy for Protection Coordination in Radial Distribution Networks With Distributed Generators," IEEE Power and Energy Society General Meeting, July 2010.

[10] IEEE Standard 1547-2003, IEEE Standard for Interconnecting Distributed Resources With Electric Power Systems.

VIII. Biographies

Dr. Edmund O. Schweitzer, III is recognized as a pioneer in digital protection and holds the grade of Fellow of the IEEE, a title bestowed on less than one percent of IEEE members. In 2002, he was elected a member of the National Academy of Engineering. Dr. Schweitzer received his BSEE and MSEE from Purdue University, and his PhD from Washington State University. He served on the electrical engineering faculties of Ohio University and Washington State University, and in 1982 he founded Schweitzer Engineering Laboratories, Inc. (SEL) to develop and manufacture digital protective relays and related products and services. Today, SEL is an employee-owned company, which serves the electric power industry worldwide, and is certified to the international quality standard ISO-9001.

Dale Finney received his Bachelor's degree from Lakehead University and Master's degree from the University of Toronto, both in electrical engineering. He began his career with Ontario Hydro, where he worked as a protection and control engineer. Currently, Mr. Finney is employed as a senior power engineer with Schweitzer Engineering Laboratories, Inc. His areas of interest include generator protection, line protection, and substation automation. Mr. Finney holds several patents and has authored more than a dozen papers in the area of power system protection. He is a member of the main committee of the IEEE PSRC, a member of the rotating machinery subcommittee, and a registered professional engineer in the province of Ontario.

Mangapathirao V. Mynam received his MSEE from the University of Idaho in 2003 and his BE in electrical and electronics engineering from Andhra University College of Engineering, India, in 2000. He joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2003 as an associate protection engineer in the engineering services division. He is presently working as a lead research engineer in SEL research and development. He was selected to participate in the U.S. National Academy of Engineering (NAE) 15th Annual U.S. Frontiers of Engineering Symposium. He is a member of IEEE.

Previously presented at the 2012 IEEE PES Transmission and Distribution Conference and Exposition, Orlando, FL, May 2012.
© 2012 IEEE – All rights reserved.
20110915 • TP6520