Generator Protection Needs in a DG Environment

Generator Protection Needs in a DG Environment

DALE FINNEY
GE Power Management
Markham, Ontario

BOGDAN KASZTENNY
GE Power Management
Markham, Ontario

MARK ADAMIAK
GE Power Management
King of Prussia, Pennsylvania

Abstract
This paper will outline the features required for a multifunction protective relay or intelligent electrical device (IED) that meets the special requirements of the distributed generation environment.

Keywords
Distributed Generator, Protection, Electrical Power System, Virtual Private Network.

Introduction
A distributed generator (DG) may be defined as a power source that is connected to the Area Electrical Power System (EPS) and is not under the direct control of the EPS operator. This definition may ultimately include a very broad range of devices; some of which are now commercially available and others that are currently under development.

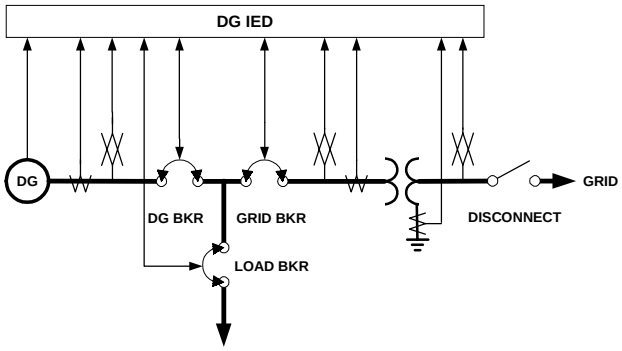

Fig. 1, Distributed Generator Single-Line

The following characteristics impact on the protection, monitoring and control requirements of the DG.

1. Configuration
This classification can be subdivided into two types: conventional and advanced. In a conventional DG, a rotating machine supplies power directly to the EPS. Conventional units may range from automotive-style, reciprocating engines to wind turbines.
Advanced units include micro-turbines, fuel cells, solar cells or advanced wind turbines. These systems interface to the grid through a single or three-phase inverter. The inverter may have the capability to regulate voltage.

2. Application
Typical applications include standby/emergency power, peak shaving and combined heat and power (CHP). Independent and parallel operation with the EPS including import and export capability may be required.

3. Size
Power ratings can be subdivided into small units (25 - 250 kVA) and large units (250 kVA – 30MVA).

EPS Interconnect Protection Requirements

Voltage/Frequency Protection
Voltage and frequency elements are required to detect deviations outside of the nominal operating ranges. This is usually the primary indicator that the DG has become islanded from the EPS.

Overcurrent Protection
Timed over-current protection is required for the detection of faults on the local EPS. The contribution from a rotating machine may decrement rapidly during the fault. Therefore a voltage-restrained characteristic is recommended. Improved selectivity may be obtained by supervising this element with a phase directional element.

Ground Fault Protection
The methods of detecting ground faults on the local EPS depend primarily on the connection of the interconnect transformer. For grounded primary connections, a timed overcurrent element connected in the transformer neutral will operate for system ground faults.
If the primary of the interconnect transformer is ungrounded, then ground fault protection can be provided by neutral displacement detection. Either a single phase-to-ground PT or a three-phase-grounded-wye PT connected at the primary of the interconnection transformer will be required. If a single phase PT is used then an undervoltage and an overvoltage element are required to detect the shift of the phase to ground voltage during a ground fault. If a three phase PT is used then a zero sequence overvoltage element can be used.

Loss of Synchronism
For larger units, loss of synchronism element may be required for rapid isolation of the DG from the EPS. This will depend on the size of the machine and the stiffness of the power system.

Directional Power
A directional power element will be required for installations where export of power is not permitted.

Anti-islanding
Anti-islanding protection is unique to DG applications. An island occurs when a section of the EPS to which a DG has been connected becomes isolated. After this section is isolated, the DG may continue to supply these local loads.

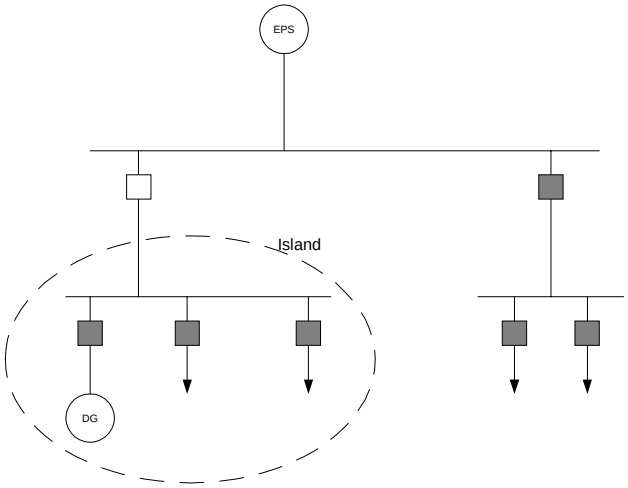

Fig. 2, EPS Islanding

This is a problem for several reasons:
- The isolated section remains energized and consequently presents a hazard to operations and maintenance personnel.
- EPS protections may not operate correctly to clear faults on the islanded section.
- The DG may drift in phase or frequency during an autoreclose operation. The resulting out-of-phase closing can damage EPS or DG equipment.
- Customers on the islanded section can suffer from poor power quality leading to equipment damage.

Primary detection of anti-islanding is provided by frequency and voltage elements. However these methods will fail when the DG output closely matches the local EPS load. Consequently there is a need for more advanced methods that operate quickly and securely for all operating conditions.

Anti-islanding schemes can be divided into two types: active and passive. In general, an active scheme detects an island through the modulation of a power system parameter and the measurement of the corresponding system response. Active schemes are inherently more complex than passive schemes. Several of these schemes are only suitable for implementation on inverter-based DG systems. Other potential drawbacks of active schemes include possible degraded power quality and unwanted interaction between the anti-island schemes of multiple paralleled DGs.
Passive schemes, for the most part, operate on detection of a change or rate-of-change in a power system parameter. These parameters include rate-of-change of frequency, rate-of-change-of voltage and voltage vector jump. Some passive schemes are thought to be more prone to false operation than active schemes. Others are thought to be less sensitive. Figure 3 contains a list of algorithms that have either been implemented or are the subject of current research [1].

Active	Passive
Asymmetrical Waveform	Voltage Harmonic Monitoring
Active Frequency Drift	Voltage Vector Jump
High Frequency Signal	Frequency Rate of Change
Impedance Switching	Power Rate of Change
Impedance Insertion	Voltage & PF Rate of Change
PLC communication	Slide Mode Frequency Shift

Fig. 3, Survey of Anti-islanding Algorithms

DG Protection Requirements

Negative Sequence Overcurrent
The primary function for negative sequence protection is the detection of open phase possibly due either to the operation of a fuse on the distribution network or due to a faulty inverter.

Negative Sequence Overvoltage
This element can be used to prevent connection of the DG to the EPS when the phase rotation is incorrect.

Loss of Field
Protection is required for a failure of the excitation system of a conventional synchronous generator. Poor power factor detection may be necessary for induction machines

Directional Power
Conventional DGs will require a directional power element is to detect a loss of the prime mover.

Stator Differential
On the largest conventional units, a differential element will be required to provide sensitive, high-speed detection of stator faults.

Overexcitation
On conventional units, overexcitation protection will be required to protect the machine from core damage.

Control

Local Interface
A local interface is necessary to provide easy access to protection settings. The local interface should also allow the display of voltage, current, energy, power factor, protection target information, breaker and disconnect status, etc. The local interface can also be used to perform control actions such as manual trip & close. Password protection for both settings and control functions is required for security.

Synchronizing
Economic considerations favor the integration of the automatic synchronizer into the DG IED. The element must be capable of sending speed and voltage matching commands to the DG controls. In the case that auto-synchronizing is done elsewhere, a synchrocheck function should be included in the DG IED with the ability to compare voltage, phase, and frequency difference. This function must also have the capability to block closing of the DG breaker when the EPS is de-energized.

Autorestoration
When the DG has been disconnected after a fault on the EPS. The DG should have the capability to automatically reconnect once the EPS has been re-energized, and system parameters have returned to normal. Programmable logic functionality can be utilized to generate the necessary permissive signal for the DG.

Monitoring

Metering
A wide range of analog measurements are required for local display. On larger DGs, the EPS operator may require metering information for SCADA. In addition, metering values may be required by a local Energy Management System (EMS). Metered values will include voltage, current, real and reactive power, power factor, energy, etc. The ability to set thresholds to these quantities for alarm or control functions is also necessary.

Harmonics/THD
The ability to monitor local power quality and generate alarms is required to ensure that the DG has not impacted negatively on Area EPS power quality. For advanced DGs this will necessitate true RMS, THD, and harmonic metering capabilities.

Data Logger
The ability to locally store historical data on the operation of the DG and make this data available through a local or remote communications interface can provide valuable information to the DG stakeholders.

Oscillography
The DG IED will require the ability to record current and voltage waveforms during a fault. Ideally this data should be available over a communications network for remote analysis.

Communications

It is arguable that large-scale integration of DG will require a networked communication system. For large DGs a leased-circuit communications channel is cost justified. However, for small DGs the size and potential number of units makes a conventional leased-circuit scada implementation unattractive from a cost perspective. In addition there may be a number of stakeholders who required data from the DG unit. These include the DG owner, The EPS operator, The DG marketer, and the DG manufacturer/maintenance provider.

One solution worth consideration is the implementation of a virtual private network (VPN). A VPN provides a secure means of transfer of information across a public data network (internet). Inexpensive VPN routers are commercially available from companies such as Cisco, Checkpoint and Netscreen. In addition to the VPN function, these devices can negotiate with a DHCP server to obtain a dynamic IP address from the internet service provider. Packet firewall capability is also included.

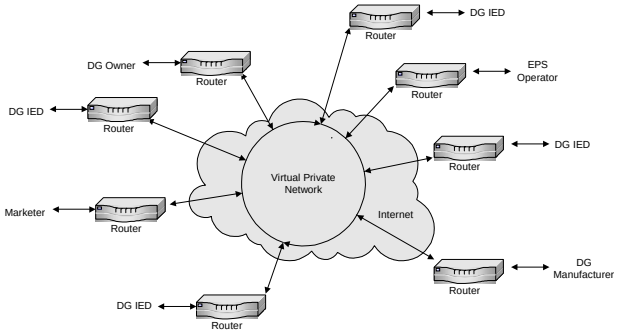

Fig. 4, Virtual Private Network

Ideally, this type of a communications solution would require that the DG IED support multiple sessions over TCP/IP. In instances where the DG is installed on the owners premises, the unit could share the customers internet connection.

VPNs can be subdivided into two types; IPSec – developed by the Internet Engineering Task force (IETF) and PPTP – developed by Microsoft. The following discussion outlines the features of IPSec.

IPSec
IPSec is essentially a set of open standard protocols designed to address the following security issues:
Confidentiality - prevents unauthorized access to information as it is transferred across a public data network.
Authenticity - Confirms the identity of the sender and receiver of the information.
Integrity - checks that information has not been altered during transmission
Anti-playback - Ensures that a data transaction is only carried out once unless there is authorization for retransmission.

IPSec can be broken down into three basic components: Authentication Header (AH),Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE).

Integrity is provided within the AH protocol through the use of a secure hash function. A hash function is an algorithm that operates on a message to produce a checksum. The algorithm is considered secure if it is highly improbable that two messages can produce the same checksum. The check sum is transmitted along with the data. Once received, the message is again passed through the hash function. If the checksums agree, then the data has not been corrupted in transit.
AH also includes anti-playback functionality. This is done by appending a sequence number to each transmitted message. On the receiving end, each message's sequence number is checked to see if it falls within a specified range. If the sequence number falls outside the range, then the message is blocked.

Confidentiality is provided within ESP using encryption. Encryption can be defined as the conversion of information into ciphertext. Unauthorized inspection of ciphertext will not reveal the original information. Encryption requires the use of an encryption algorithm and a unique key.

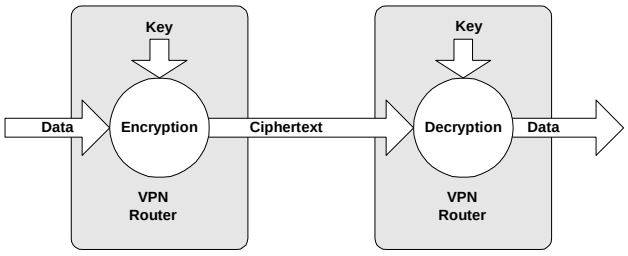

Fig. 5, Encryption Process

IPSec utilizes strong encryption techniques for which there are no known attacks on the algorithm itself. Consequently, unauthorized attempts to decipher encrypted data take the form of a brute-force attack. A brute-force attack is an attempt to use every possible key to decrypt the ciphertext. On average ½ the keys must be tried before the correct key is found. Therefore the key size relates directly to safety of the information from such an attack. The key size used in the DES encryption algorithm is 56 bits which yields 2^{55} or 3.6×10^{16} possible keys. The most secure IPSec encryption algorithm in use today (triple DES) uses a 168 bit key. ESP supports several encryption algorithms including ARCFour, DES, and Triple DES.

The methods used to ensure the confidentiality and integrity of the transmitted information rely on the use of keys. IKE provides the mechanisms for the secure exchange of key information.
Encryption techniques can be divided into two main types; private key encryption and public key encryption. In a private key encryption, both the sender and the receiver use the same key. To update the keys in a private key system, a different medium is required for secure transmission of the key information. In public key encryption, two keys are required (sometimes referred to as a key pair). Information encrypted with the first key can only be decrypted with the second key and vice versa. In a public key system, the parties at each end of the connection create unique keys. These keys are kept private. At the initiation of a VPN session, the private key is used to generate a public key using a one-way algorithm (the private key can not easily be deduced from the public key). The public keys are then exchanged between parties. The private and public key information are used to generate a session key that is used for the encryption process. In this way, IKE allows for key management and information transmission using the same communication channel. IKE also allows parties to authenticate one another and allows the specification of a lifetime for the IPSec session.

Conclusions

With the exception of anti-islanding, the protection elements required for DG are currently available with no major application restrictions [12]. Further research is necessary to develop an anti-islanding scheme that is fast, reliable, and secure for various operating modes and system configurations.
Adding more functionality to the DG (control, monitoring and communications) can reduce the overall cost of the DG and improve its commercial viability
Research into new communication strategies may lead to improvements in the way that DG are utilized, monitored and maintained.

References

[1] GE Research and Development Center, DG and Interconnect Improvements, Interconnect Requirements and Conceptual Design Report, Appendix A, Dec. 2001

[2] GE Research and Development Center, DG Power Quality, Protection and Reliability Case Studies, http://www.eren.doe.gov/distributedpower/PDFs/GE_DGCaseStudies.pdf, Sept. 2001

[3] Cisco Systems White Paper, IPSec, http://www.cisco.com/warp/public/cc/so/neso/sqso/eqso/ipsec_wp.htm, Nov. 2000

[4] Kent & Atkinson. Security Architecture for the Internet Protocol, RFC 2401, http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2401.html, Nov. 1998.

[5] Kent & Atkinson. IP Authentication Header, RFC 2402, http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2402.html, Nov. 1998.

[6] Kent & Atkinson. IP Encapsulating Security Payload, RFC 2406, http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2406.html, Nov. 1998.

[7] Harkins & Carrel, The Internet Key Exchange, RFC 2409, http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2409.html, Nov. 1998.

[8] Eric Maiwald, "Network Security: A Beginner's Guide" Berkeley California, (Osborne/McGraw-Hill, 2001)

[9] IEEE P1547/D08, Draft Standard for Interconnecting Distributed Resources with Electric Power Systems 2001.

[10] IEEE 1021–1988, IEEE Guide for Interfacing Dispersed Generation and Storage Facilities with Electric Utility Systems.

[11] IEEE C37.102-1987, IEEE Guide for AC Generator Protection.

[12] G60 – Generator Management Relay, Instruction Manual, General Electric, 2001.

GE Power Management

215 Anderson Avenue
Markham, Ontario
Canada L6E 1B3
Tel: (905) 294-6222
Fax: (905) 201-2098
www.GEindustrial.com/pm