IEEE PSRC, WG I 19

Redundancy Considerations for Protective Relaying Systems

Members: Solveig Ward (Chair), Bryan Gwyn (Co-Chair), Galina Antonova, Alex Apostolov, Tom Austin, Phil Beaumont, Bob Beresh, Dave Bradt, Gustavo Brunello, Dac-Phuoc Bui, Matt Carden, Randy Cunico, Alla Deronja, Walt Elmore, Rafael Garcia, Bob Haas, Ameed Hanbali, Rob Harris, Pat Heavey, Gene Henneberg, Chris Huntley, Fred Ipock,Gerald Johnson, Sungsoo Kim, Gary Kobet, Jeff Long, Aaron Martin, Craig McClure, Jeff McElray, Michael Mendik, George Moskos, Chuck Mozina, Jim Niemira, Jim O'Brien, Neil Saia, Sam Sambasivan, Sinan Saygin, Tony Seegers, Don Sevcik, Mark Simon, Jack Soehren, Bob Stuart, Jonathan Sykes, Damien Tholomier, Steve Turner, Joe Uchiyama, James Wang, Don Ware, Tom Wiedman, Ray Young, John Zipp, Eric Udren

TABLE OF CONTENTS

1 Introduction

Reliability is always of concern for protective relay systems and redundancy plays an important role for reliability. Reliability is a compromise between security and dependability. Security is the ability to properly restrain from tripping when not called for. Dependability is the ability to trip when required. While security is not improved by increased redundancy, dependability is. Clearly, the impact on the power system when a protection device is not functioning when required is much less severe when there is a redundant device that takes over the job. If the two redundant devices are of equal performance, there should be no detrimental effect at all on power system operations, and a non-functioning device would just need to be repaired or replaced.

Local redundancy of components plays a major role in elevating the reliability of protection systems; however, it is not the only mitigation that can be used to improve the reliability. Remote protection systems may provide adequate protection system reliability in some situations, provided that remote protection can detect faults and provide clearing times that meet performance requirements. It is the task of the protection and the planning engineers to determine the proper solution for each element (lines, buses, transformers).

This report provides the relay engineer with information about what factors to consider when determining redundancy requirements. In addition, the report addresses differences depending on application area, present practices and provides real world examples.

Note. Different users have different terminology for referring to the redundant protection systems. They may be called "System 1" and "System 2," "System A" and "System B," "Primary" and "Secondary" or sometimes "Primary" and "Backup." This latter terminology, "Primary" and "Backup", implies, although unintentionally, that one of the two systems serves the main function of protection and the other serves to assist in the case of failure of the first system, analogous to carrying an undersized spare tire in the trunk of a car in case of a flat. In actual practice, the redundant systems are each fully capable, each system is able to detect and clear faults on its own, and each system serves as a backup to the other. For the purpose of the present report, the terms "System A" and "System B" will be used for referring to the redundant relaying systems. This selection of this terminology is intended to provide a consistent terminology to aid the reader's understanding of the topics of discussion in the remainder of the report, but is not intended to indicate a consensus or preference for this terminology throughout the industry.

2 What is redundancy?

2.1 Definitions

The following definitions are based on The Authoritative Dictionary of IEEE Standards Terms (IEEE 100-2000 seventh edition) and the International Electrotechnical Vocabulary (IEC 60050).

Redundancy is the existence of more than one means for performing a given function.

Dependability is the facet of reliability that relates to the degree of certainty that a relay or relay system will operate, or perform, correctly.

Reliability is a combination of dependability and security. Note that *reliability* denotes certainty of correct operation together with assurance against incorrect operation from all extraneous causes.

Security is that facet of reliability that relates to the degree of certainty that a relay or relay system will not operate incorrectly. Note that “cyber security” is a separate issue that relates to electronic access.

2.2 Purpose of redundancy

Redundancy is required for several reasons including governmental and regulatory requirements, ensure reliability, maintain customer satisfaction, increase system stability, and for maintenance purposes. These issues are dealt with in the remainder of this document.

2.3 Redundancy versus backup

Older documents, such as The Transmission and Distribution Electrical Reference Book do not make a distinction between backup and redundancy: “The measures employed in practice vary all the way from complete duplication of relays at one extreme to no backup at all at the other extreme.” However, common convention today is to define a redundant system as a second (or third) system that has essentially equal performance to the primary system applied. A backup system, while covering the zone protected by the primary equipment, will provide a lower degree of performance, e.g. less speed or less selectivity.

However, note that the two (or three) redundant systems do not always have to be of identical performance provided that any one of the redundant systems fulfill the requirements for the application with regards to operating time, selectivity, etc. For example, if stability studies have determined that a line can be adequately protected by stepped distance protection, a Main 1 distance pilot relay in combination with a Main 2 stepped distance relay can be considered a redundant protection system.

2.4 Redundancy’s influence on reliability

Reliability of a protection system is a combination of dependability and security. For protective relays, dependability is the ability to trip for a fault within its protective zone while security is the ability to refrain from tripping when there is no fault in the protective zone.
Redundancy will increase dependability since the required operation can be carried out by the redundant system. A failure of a single system will not affect operation.

Typically, redundancy will decrease security as the added device(s) will increase the risk for an unwanted operation. A failure (causing overtripping) of either system will produce a false trip. However, combining redundancy and duplicated devices, as in the voting scheme described in Section 4.5, will result in increased dependability and increased security.

Redundancy does not influence dependability and security to the same degree. The optimal degree of dependability and security, and consequently redundancy, has to be determined based on the impact of a false trip versus the impact of lack of trip for a fault. For example, the power system may not be greatly affected by a line protection’s incorrect tripping for a fault outside the protected line since automatic reclosing can quickly restore service. However, a false trip of a bus protection may not be as easily mitigated.

2.4.1 Dependability and security example

While not practical to use, it could be of interest to illustrate the concepts by looking at the two extremes; 100% dependability and 100% security. 100% dependability would be achieved by a protection system that is in a constantly tripped state, hence there is no possibility that there would be a fault that would not be detected. 100% security would be achieved by disabling the protection system entirely so that it could not trip. From this we can see that while high dependability and high security are desirable, they will both have to be less than 100%. Generally, an increase in dependability will decrease security, and vice versa. However, measures to increase dependability may not penalize security to an equal degree and the aim of a protection system design is to find the optimum combination of the two factors in order to provide adequate reliability.

In order to illustrate how redundancy influences dependability and security, data is borrowed from teleprotection standard IEC 60834-1 (1999). If a fault occurs and is isolated by a redundant protective system B, the fact that relay system A did not operate does not constitute a mis-operation; however, from an operational point of view this would be investigated in the chance that relay system A was defective in some respect.

In the following discussions, “redundant” refers to completely independent systems or components. The failure rate for each system or component is independent from the redundant system’s failure rate. A failure in one device does not influence the other and the failures are not triggered by a common cause[1].

[1] In actual fact, there may be common causes of failures in redundant protection systems, such as redundant schemes tripping a single trip coil or redundant schemes utilizing a single battery supply.

For our redundancy considerations, the requirements given for a Direct Transfer Trip Teleprotection System are used:

- 99.9999% security, or expressed as probability of a false trip (reciprocal of security) 10^{-6}
- 99.99% dependability, or expressed as probability of a missed trip (reciprocal of dependability) 10^{-4}

2.4.1.1 Security in a redundant system

If a redundant system is added, and the systems are equal and independent, the probability of a false trip will be the sum of the probability for each redundant system to give a false trip:

- Probability of a false trip for a redundant system 0.000002, or expressed as security: 99.9998%

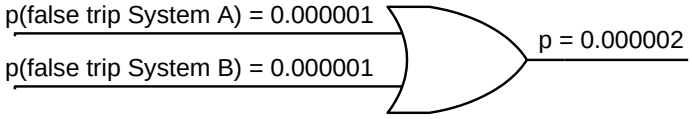


Figure 1. Probability of a false trip in a redundant system

Security is reduced from 99.9999% for a single system to 99.9998% for a redundant system, which is not a significant change.

2.4.1.2 Dependability in a redundant system

The probability of a missed trip however, will be greatly reduced, resulting in much improved dependability. If the systems are equal and independent, both of them need to fail at the same time for a missed trip to occur. Therefore the resulting probability of a missed trip is the product of the individual probability:

- Probability of a missed trip for a redundant system is 0.00000001, or expressed as dependability: 99.999999%

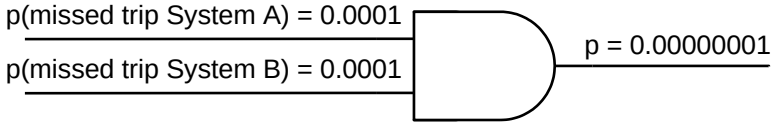


Figure 2. Probability of a missed trip in a redundant system

Consequently, dependability has increased from 99.99% to 99.999999% which is a great improvement.

2.4.1.3 Influence of redundancy on security and dependability

The table below summarizes the influence of redundancy on security and dependability for the example used with individual unit probability of a false trip of 10^{-6} and probability of a missed trip of 10^{-4}.

Table I. Redundancy Influence on Security and Dependability

Scheme	Probability of false trip	Security	Probability of missed trip	Dependability
Single	10^{-6}	99.9999%	10^{-4}	99.99%
Redundant	2×10^{-6}	99.9998%	10^{-8}	99.999999%

The above example explains why redundancy is important for protective relay system reliability. By adding a redundant system, the probability of a false trip increased by a factor of 2, while the probability of a missed trip decreased by a factor of 10,000.

2.4.1.4 Influence of redundancy on a voting scheme

One variation of redundancy is the voting scheme described in Section 4.5. The voting scheme does not only include redundant elements, but also duplicated elements. The connection of these elements in series and parallel and using a two-out-of-three operation criteria results in increased dependability without sacrificing security.

The logic is illustrated in Figure 3.

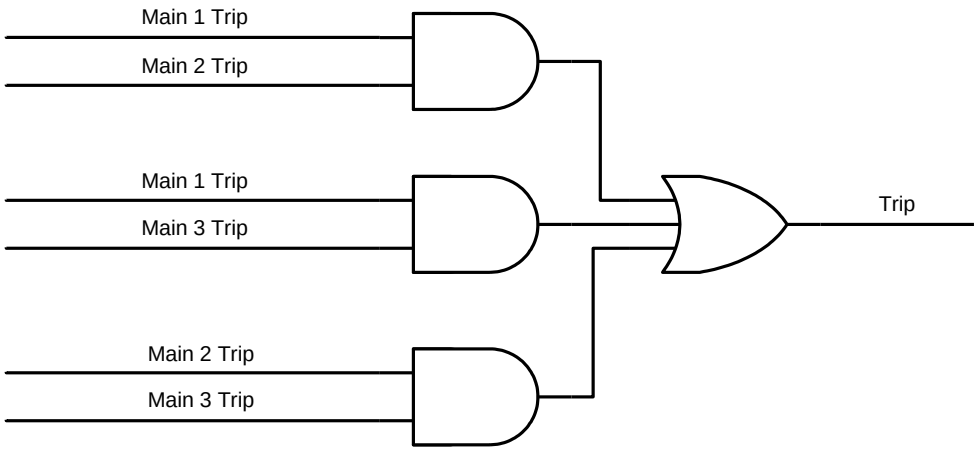


Figure 3. Two-out-of-three voting scheme

We can estimate the resulting improvement in security and dependability for the two-out-of-three scheme by applying the same principles as used for the dual scheme previously.

For a false trip, two protections need to misoperate at the same time. Consequently, the probability of a false trip is the product of the probability of false trip for the individual schemes. Assuming that they are equal, independent and using the 10-6 figure, the combined probability for a false trip is 10^{-12}.

For a missed trip, two of the three relays need to fail to operate for an in-zone fault. This means that the dependability is exactly the same as for a redundant system with two relays, assuming that they have equal and independent probability of a missed trip. Using the 10^{-4} figure from earlier, the combined probability of a missed trip is 10^{-8}.

The results for the voting scheme are summarized in Table II.

Table II. Two-out-of-three voting scheme

Scheme	Probability of false trip	Probability of missed trip
Two-out-of-three	10^{-12}	10^{-8}
Redundant	2×10^{-6}	10^{-8}

The two-out-of-three configuration shows an equal improvement of dependability and a considerable increase in security as compared to the redundant scheme using two protections only. However, this increase in security may not justify the extra cost of one more protection scheme.

2.5 Good engineering practices

All other considerations aside, it makes good sense to design protective relay systems that are inherently resilient. This means that the scheme design is optimized for cost and best meets the requirements for dependability and security. Further, the loss of one or more scheme components will have minimal impact on meeting those requirements. It is the task of the designer to strike a balance in meeting the

technical requirements, addressing reliability concerns, considering costs, and maintaining consistency in design standards with the goal of achieving a robust design that is also simple to operate and maintain.

2.6 Economic considerations

Cost is an important factor in determining the level of redundancy to design into a relay scheme. The cost of the relay scheme is weighed in light of its impact on dependability, security, and reliability of the power system. The goal is to achieve optimal results at an acceptable cost. Generally, the appropriate amount of money to be allocated increases with the level of load impacted by the relay scheme, or the criticality of the load. The level of load considered increases with the system voltage of the facilities in question. Therefore, it is safe to expect that the higher the voltage class of the protection system, the greater its impact, which results in the need for increased levels of protection redundancy. It is worthwhile to allocate more money to achieve this requirement. There are of course exceptions to this "rule-of-thumb." For example, a large customer receiving power at a lower voltage distribution substation may apply funding to install a level of redundancy in order to achieve greater reliability of service. Aside from such special cases, the redundancy requirements may result in the accumulation of costs beyond those required for simply meeting the relay protection needs. The value of these additional costs cannot be understated.

2.7 Asset management

Asset management can be described as "a systematic process of maintaining, upgrading, and operating physical assets cost-effectively". It combines Engineering principles with sound business practices and economic theory, and it provides tools to facilitate a more organized, logical approach to decision-making. Thus, asset management provides a framework for handling both short-and long-range planning." [1] It is also considered "a business process allowing a utility to make the right decisions on the acquisition, maintenance, operation, rehabilitation, and disposal of assets used for customer service." [2]

2.8 Outage time

Asset management provides input to the planning and operation of the power system. A vital consideration in this regard is that of redundancy and the impact on equipment outages. Outages may be either planned or forced. Planned outages are typically taken for maintenance and operating reasons and all precautions are used to minimize disruption to the system, whereas forced outages are a result of system disturbances and are highly undesirable.

A thorough examination of the utility's system and consideration for reliability, system security, and adherence to government regulations must be considered from an asset management point of view. Outages that impact system performance need to be minimized or penalties may be levied, customer satisfaction compromised, and equipment performance impacted – all of which can lead to financial costs and public embarrassment to the utility.

Asset managers seek to minimize the impact of outages to the performance of the utility's system by considering the need for redundancy. This may take the form of multiple feeds to substations, duplicate protection systems, and increased flexibility in operating configuration (design) to allow for multiple configurations of system operation (under both normal and abnormal operating conditions).

Asset managers must also consider how the system can be maintained. This may require the need for redundancy in order to minimize outage times. For instance, if a bulk power protection system needs to be maintained on a specific cycle, the operating requirement to keep the protected system component in its normal operating state (while the protection equipment is being maintained) may necessitate the need for redundant protections. This would be in addition to and/or in conjunction with the fundamental requirement of having a redundant protection in case the primary protection fails.

2.9 Restoration time

If a protection is taken out of service, or forced out of service due to a problem, the reliability of the system protected is dependent on the time to repair that protection. If a certain level of reliability is required for the power system, then additional redundancy may be required in the protection system.

2.10 Mean Time to Repair (MTTR)

A factor called the Mean Time To Repair (MTTR) is a common measure used to indicate the maintainability and repairability of a device. The MTTR is the time required to restore a failed or non-operational piece of equipment back into service. Some devices may take more and some may take less, however, the MTTR is a mean value.
Mean Time to Repair (MTTR) is the average time required to restore a failed or non-operational piece of equipment into service.

2.10.1 Hardware MTTR

Often repair is considered to replace a faulty hardware module in an operational system; therefore hardware MTTR is the mean time to replace a failed hardware module. System design should allow for a high MTTR value and still achieve the system reliability goals. The table below demonstrates how a low MTTR requirement necessarily causes a high operational cost for the system. (The "Operator" in the table refers to a relay engineer/technician, i.e. a person capable of repairing the relay equipment.)

Table III. Estimating hardware MTTR

Hardware MTTR Estimates		
Where hardware spares are kept	**How is the site manned?**	**Estimated MTTR**
Onsite	24 hour/day	30 minutes
Onsite	Operator on call 24 hours/day	2 hours
Onsite	Regular working hours on week days, weekends and holidays	14 hours
Onsite	Regular working hours on week days only	3 days
Offsite *Shipped by courier when fault condition encountered*	Operator paged by system when a fault is detected	1 week
Offsite *Maintained in an operator controlled warehouse*	System is remotely located Operator needs to be flown in to replace the hardware	2 weeks

2.10.2 Software MTTR

One method used to calculate MTTR for a software module is the time taken to reboot after a software fault is detected; therefore possible software MTTR figures can be calculated from the mean time to reboot after a software fault has been detected. System design should keep the software MTTR as low as possible.

Software MTTR depends on several factors such as the following:

- Software fault tolerance techniques
- Operating System used (does the Operating System allow independent application reboot?)

Table IV. .Estimating software MTTR

Software MTTR Estimates		
Software fault recovery mechanism	**Software reboot upon fault detection**	**Estimated MTTR**
1) Software failure detected by: • Watchdog • Health message	Processor automatically reboots from a ROM resident image	30 seconds
2) Software failure detected by: • Watchdog • Health message	Processor automatically restarts the offending tasks without needing an operating system reboot	30 seconds
3) Software failure detected by: • Watchdog • Health message	Processor automatically reboots and the operating system reboots from disk image and restarts applications	Up to 3 minutes
4) No software failure detection	Manual reboot required	30 minutes - 2 weeks

Note that there may be undetected failure modes due to the possibility of unknown software bugs at the time of release. Often an intermediate solution is required for such cases until the vendor can fix the software and release a new revision. Class (4) failures in Table IV should immediately be reported to the manufacturer.

2.10.3 Time to repair dictates degree of redundancy required

As mentioned previously, protection equipment is typically made redundant in critical applications, however, the reliability of the protection system is impacted by the time required to repair a defective component. On few occasions protections (critical applications) may be triplicated, but in general, protection schemes are duplicated. In applications where reliability may not be as much of a concern, such as in feeders, protections may be based on a single scheme only.

Some aspects of the protection scheme, even if duplicated, may have common points of failure, such as two protections (“A” and “B”) tripping a single trip coil on a breaker or depending on the same battery supply. Where reliability is critical, it is important to have redundancy, however in some cases, such as with a single trip coil or a single battery, full redundancy may not be possible.

The availability of a device is typically given by the MTBF (Mean Time Between Failure) divided by (MTBF+MTTR). The availability of a device is an indication of the operational time of the scheme. In order for a protection scheme to have a high degree of availability, it must have a low Mean Time To Repair (MTTR) or else a high Mean Time Between Failure (MTBF). Both the reliability of the protection scheme and the time it takes to repair a protection scheme factor into determining the overall availability of the protection. Redundancy plays an important role in increasing the overall availability.

3 Differences Depending on Application Area

3.1 Bulk power system

The Bulk Power System, also referred to as the Bulk Electric System includes critical transmission system elements that could have a significant adverse impact on system reliability. Faults on Bulk Power System (BPS) equipment may cause widespread instability, system separation, or cascading failure sequences.

Recently, there has been increased regulatory effort to create uniform mandatory reliability standards for all Bulk Power System equipment to prevent widespread disturbances. Some active reliability standards in force for portions of the Bulk Power System include fully redundant and separate protection systems intended to ensure no single failure could prevent high speed fault clearing thus causing a widespread system disturbance.

3.2 Industry practices

Practices of redundant relaying protection vary widely from utility to utility and are influenced by many factors including but not limited to the size of the utility and its economic and technical resources, internal and external utility regulations of the reliability and security requirements, and the availability and change of technology. The benefits of single protection systems are easily quantifiable when they are considered against the cost of failed main grid equipment coupled with the cost of the extended outage time. The benefits of a redundant protection system are not as easily realized when the anticipated failure of the protection system simultaneous to a system disturbance is unlikely to occur.

Because protective relaying provides no profit and is only required for infrequent and random abnormal operation of the power system, it can be described as insurance that prevents damage to the main grid equipment while minimizing outage time. Like all insurances the economics of the risks versus benefits are analyzed by utility managers and engineers. Larger utilities with abundant financial and technical resources research different protection schemes to determine the optimal balance between robustness and performance. However, there are different types of economic justification other than insurance that drive the application of a second protection scheme. As the power system is operated closer to its limits, less time is available for controlled outages for maintenance and uncontrolled outages due to equipment failure. The scenario of a stressed power system enforces the need for redundant protection systems that allow for relay maintenance without a line outage or for continued operation when the primary relay system fails.

Companies with EHV (Extra High Voltage; 345 kV and above) transmission systems, special protection schemes, large generation plants, and large distribution loads share similar redundant relaying protection practices because of external guidelines from regional reliability organizations as well as the threat to the overall stability to the system from an extreme disturbance.

In lower voltage systems common compromises of a fully redundant protection schemes include single trip coils to the circuit breaker, single CT and PT connection input to both sets of relays, and installations where only one battery is used.

Companies accept compromises in accordance with their own internal reliability standards. An example of an internal reliability standard would require the single-mode failure of any protection scheme to not prevent the detection of a fault. One possible common mode failure is the loss of a power supply of a multi-function microprocessor relay. This requirement allows redundant relay sets to receive a single PT input through separate fused protected sources for their distance functions which are backed up by overcurrent functions from redundant CT inputs. Another factor that contributes to the compromises of implementing a fully redundant protection scheme is the interconnection to existing equipment. An example of a limited redundant protection system results from connecting to existing circuit breakers that were originally built with single trip coils. In this case the cost of replacing the breaker to complete a fully redundant protection scheme would likely outweigh the other before mentioned benefits. Other advances from the manufacturing industry such as the conversion from electromechanical, to the solid state, and then to digital microprocessor technology have influenced company practices of protective relaying redundancy. In the beginning implementations of micro-processor based relaying, utilities sometimes utilized the proven reliability of the existing electro-mechanical relay systems with the new micro-processors relays that had limited industry experience. The result was a redundant hybrid protection system consisting of micro-processor and electromechanical technology.

An external influence affecting redundant practices occurs when one utility requests interconnection to another utility's transmission system. Utilities request these new interconnections for more transmission capacity, new generation, or to secure reliability of large distribution loads. In these instances they are

subject to the interconnection requirements of the transmission utility which may include redundant protection practices. Redundant relaying practices can also be transferred between companies when one utility acquires system facilities such as substations or generation plants from another utility. In this case the new owner of the existing equipment is not always likely to change the protection schemes to match their own thus inheriting the redundant relaying practices of the former owner. Reasons not to make the change over may include a lack of economic feasibility or technical resources or both.

3.3 Degree of redundancy required

There are several types of protection. One type refers to a main (individual) protection of each primary element the electrical system consists of such as a transformer, bus, line, etc. Examples of the main protection include bus or transformer differential, transformer overcurrent, and line distance protection. This type of protection is ascribed to each element of the system to protect only this element from its own failures or faults, and it does not operate for a fault or failure occurring on another element of the system, i.e. outside its zone of protection.

Another type refers to an individual protection, which protects the element of the system it is ascribed to from its own failures and faults and, additionally, may serve as a backup for a fault or failure occurring in the neighboring zone of protection. An example of this type of protection is the line distance protection, which protects a designated line in its primary zone and serves as a remote backup for a downstream neighboring line in its backup zone should the protection assigned to the neighboring line malfunction or fail to clear a fault on that line. Thus, the line distance protection can be a combination of two protection types: main (individual) and backup.

The third type, local backup, such as breaker failure scheme protects the neighboring elements from faults in either primary or neighboring/adjacent zones whenever the breaker fails to operate when called upon.

Finally, the fourth type refers to a system wide area protection, which protects one element or a group of elements of the system from failures and faults that occur in the neighboring or remote zones of protection. System integrity protection schemes or remedial action schemes represent this type of protection.

Utilizing the classification offered above, it can be seen that the main protection of each primary element of the system should have the highest degree of redundancy because, should it fail or malfunction, the respective system element it is assigned to protect will be left without protection. Therefore, in addition to the main protective device, each primary element of the system should have a local backup protective device, which operates concurrently with the main protective device or in lieu of it when it is unavailable. For critical system elements which are required to be tripped for faults within a specific critical clearing time or high- and extra-high voltage elements, two fully redundant protection systems (packages) which operate simultaneously (if both are available) but independently from each other become necessary.

Part of the nature of backup protection is that it provides a form of redundancy to the primary or main protection for a power system element. Two separate devices to provide protection is the most common form of redundancy. Therefore backup is already a form of redundant protection, making additional equipment to provide redundancy unnecessary.

Wide area system protection schemes are usually installed due to the lack of transmission or generating capacity during single or double contingencies. Such schemes are normally critical to system operation and may result in extreme contingencies for a failure to operate or loss of significant load or generation for a scheme operation that was not intended. Therefore wide area system protection schemes (SIPS, SPS or RAS) are often built fully or, at least partially redundant.

3.4 Transmission protection

Transmission lines linking generating stations and distribution substations of the electrical system form a network where power flows in different directions in accordance with economic dispatch and power demand. If a certain transmission line is out of service, the power usually pushed through this line is redirected to flow through another line or group of lines in a parallel or other alternative path. This makes

the transmission system very flexible and dependable. A single mode of failure in the transmission system typically would not disrupt operation of the whole system. However, because there may not be enough parallel or alternative routes due to a lack of infrastructure, or other scheduled or forced outages, a danger of cascading outages, which can disrupt the system operations and cause power outages, is always present and has to be accounted for.

Transmission lines of high voltage (100 kV up to 230 kV) and extra high voltage (345 kV and above) are usually a part of a critical path in the transmission system since they carry the bulk of the load and may not be adequately backed by parallel paths and may not have reliable alternative routes. These lines may need to be tripped in the shortest possible (critical) clearing time so as to not cause power flow swings or disturbances in the system. Otherwise, if longer clearing times occur, they may cause instability and lead to the system's collapse.

Transmission line protection has to be very dependable since it is relied upon to isolate the line from the rest of the system when it fails. At the same time, the protection has to be secure as to not falsely operate and cause another healthy line in the system to trip.

To assure high dependability of the line protection, the high- and extra-high voltage transmission lines are typically protected with two fully redundant protective relaying systems so that, should an element in one protection system fail and prevent clearing a line fault, the other protection system, being completely independent from the failed one, will clear the fault. Additionally, there can be a third protection system, installed either as another primary system or to back up the operation of the primary redundant protection systems.

To increase security of the line protection, the three protection systems may not be allowed to operate independently from each other. At least two of the three must sense a fault on a line and initiate trip signals to trip the line out of service. This type of scheme is called a voting scheme.

Transmission lines of lower voltages (115, 138, and 161 kV) are typically protected with two protective relaying systems. However, since they are not as critical to the power grid as the high- and extra-high voltage transmission lines and there are usually more parallel and alternative routes in the lower voltage transmission networks, the second protection system is designed to provide a local backup to the primary system. In this case, the second system does not possess all the components to be fully redundant to the primary system. However, should the primary system fail, the second protection system will respond to the fault on the line in a backup, usually time delayed tripping action. The choice of such a primary/backup scheme may be based on historical practice, but is more often acceptable if studies confirm that power system performance will meet appropriate requirements, even for operation of the backup protection scheme. Optionally, the protection of such lines may still be designed to be fully redundant and independent.

Subtransmission lines of voltages 69 kV and below and radial distribution lines are usually of local importance only and not critical to the power grid. They may have adequate parallel or alternative routes or ability to be bridged on the distribution buses. Therefore, a single protection system is utilized to protect such a line and, should it fail during a fault on the line, remote backup protection will clear the fault in an appropriate time-delayed tripping action. Although, in this case, more customers may be affected, the overall power grid's integrity will not be jeopardized. Optionally, a local backup protection system may be added to protect such a line to avoid the situation of losing more load than necessary during a fault on the line and simultaneous line protection failure.

A failure of a single piece of equipment such as a generator, transformer, capacitor, or reactor may have more significant consequences than a loss of a single transmission or distribution line. The generator is an important and expensive machine and may be severely damaged or even destroyed if its protection fails to isolate it for an internal fault or fault in the system. The transformer or reactor may catch fire for its internal fault, and its isolation from the system is very critical so as not to cause damage to other equipment in a substation.

Therefore, to assure high dependability of the equipment protection, two fully redundant protection systems are typically utilized to protect critical pieces of equipment. If this is a distributed or local generator or transformer, two protection systems may still be utilized with the second system being a local backup to the primary protection system.

3.5 Special Protection Schemes

Special Protection Schemes (SPS) are protective relay schemes designed to detect predefined abnormal system conditions and initiate automatic corrective action that will result in acceptable system performance. SPS are designed to be highly reliable and secure relaying schemes. They are used to help maintain system stability, acceptable voltages and equipment loading, often by initiating one or more of the following actions: reducing generation, modifying system configurations, and or inserting equipment that serves to correct an unacceptable system condition. For example, SPS are often used to allow generators to operate at full output even under single contingency outages that would otherwise result in curtailment of generation in preparation of the next contingency event. Under-voltage and under-frequency load shedding (and out of step) schemes are not included in the NERC definition of an SPS.

SPS, RAS (Remedial Action Scheme) and SIPS (System Integrity Protection Schemes) are equivalent alternative nomenclatures.

Redundancy designs of special protection schemes are common practice among utilities. A 1992 joint survey performed by CIGRE and IEEE investigating special protection schemes, reported that many North American Utilities cited “reliability criteria that are prescribed by regional councils and that redundancy in the design was considered important.” Both the present NERC standards governing SPS and the related procedures of the various North American Regional Reliability Councils require a substantial level of redundancy in Special Protection Schemes.

3.6 Control function in protective relays

Even though relay protection of power system assets have proven to be a vitally important aspect of any electrical system requirement, a review and evaluation of the control system, including redundancy, must be completed. By invoking redundancy techniques, the substation system performance and reliability of the power system can be measured and improved.

Redundancy as it relates to the control system can enhance the overall performance of the power system. Modern protection relaying devices have continued to add more protection elements and features to a single box. These would include but not limited to programmable inputs/outputs, dual polarizing, dual breaker failure elements, multi-breaker reclose schemes, multiple zones and levels of various protections, capability to create special logic and alarms, loss of potential schemes, switch-onto-fault schemes, displaying of various metering information, capturing and displaying event data in various formats, etc. Following that trend, they have also included logic capability for the building/developing simple virtual circuits up to very complex configurations. With such flexibility provided by the microprocessor relays, redundancy can really be considered as a plausible contribution since costs of all the required hardwire is virtually included in the software of the relay.

Developing a philosophy of where and how substation control via protection relays is deployed will enable the user to define a protection methodology just as it is done today with external switches, meters, lockout relays and other auxiliary relays.

4 Application Redundancy

4.1 Hardware for fully redundant systems

For the protection of Interconnected Power Systems, the requirement for redundant protection systems is not only necessary to avoid major system disturbance, but also may be compulsory as part of regulatory obligations. For the protection of systems of lesser importance, the redundancy can be optional provided that the power system elements are adequately and reasonably protected. Therefore, in determining whether the protection redundancy should be made compulsory or optional, one should consider the following questions:

- The cost of providing redundant protection systems is justifiable
- The loss of the power system, due to a single contingency failure of the protection system, is deemed an acceptable risk
- Regulatory organizations may require redundancy for Interconnected Power System
- Protection system without redundancy could adversely impact maintenance frequency and interval criteria
- Protection system without redundancy could adversely impact safety of equipment, facilities, and the public
- Redundant communications scheme may be necessary if a protection system uses communications, i.e. for transfer tripping upon a breaker failure condition, can the backup relays provide remote backup protection for a loss-of-communications or out-of-service communications condition and/or can a local breaker failure isolate the infeed so that remote relays sense all faults in adjacent lines?

When required, a fully redundant protection system can be realized using separate and independent sensing devices, trip modules, protective relays, and batteries. The following system and design requirements may then be considered:

- Separate current transformers for each protection group
- Separate voltage transformers or at least dual voltage supply (one voltage transformer with separate secondary windings) for each protection group
- Each independent protection system may be mounted on separate panels or segregated on a single panel
- Independent and separate battery systems (A and B)
- Maintain routing of cables from instrument transformers as separate as possible
- Dual trip coils for circuit breakers
- Provide separate communication channels for teleprotection and transfer trips

4.1.1 Protection Systems ‘A’ and ‘B’

Redundant protection systems are usually designated ‘A’ group and ‘B’ group. For full redundancy, both groups, each of which is composed of the measuring and auxiliary logic modules, should be self-contained and independent of each other, capable of detecting and isolating all types of faults in the highest possible speed with dependability and security. Neither group is considered secondary to the other. A physical separation of ‘A’ and ‘B’ systems should be maintained to reduce any chance of the complete failure of both systems, by such catastrophic incident as fire, if they are mounted on the same panel. Some North American regional electricity organizations require physical separation between protection systems as part of the bulk power system protection criteria.

The reliability of the relay measuring/logic module is of paramount importance. However, the redundancy or duplication alone would not automatically bring the maximum reliability to protection systems unless the very components used in relays are equally reliable. The components, especially those used in modern microprocessor relays, must be of, collectively, proven quality as either demonstrated by practical operational experience or approved by reputable testing authorities. Some utility companies have a stated internal policy against the use of the identical relays in both A’ and ‘B’ groups for fear of common mode failure. It is deemed that a malfunction or a design defect that may be inherent in a component could lead to simultaneous failure of both protection systems. Other utility companies may use identical relays to reduce cost.

The dedicated auxiliary logic module if it exists (or trip logic module) must also be provided in association with the measuring logic module to achieve true redundancy – i.e. ‘A’ group measuring module be tied to ‘A’ auxiliary module and ‘B’ group to measuring relay ‘B’ auxiliary module. Some utilities, however, avoid the use of auxiliary trip modules utilizing discrete relays, since the microprocessor based measuring relays can provide the complete auxiliary trip module functionalities such as trip seal-in features, multiple inputs and outputs, self-contained alarm monitoring. This approach may be advantageous in saving costs as well as in simplifying the protection modules by reducing a number of relays and wirings in the design.

4.1.2 Instrument transformers

Fully redundant protection systems need to have redundant instrument transformers. Following are some items to consider and examples:

Dual secondary CCVT or VT, as shown in Figure 4, is the most common arrangement for most HV and EHV systems. In this arrangement Relay Set A and Relay Set B are shown as multifunction relays (or two groups of electromechanical relays) consisting of impedance-distance and over current based protection functions.

Two sets of VTs or CCVTs, as shown in Figure 5, is an ideal arrangement, but it is hard to justify because of economic reasons and physical space requirements for the regular switching stations. When this type of arrangement is applied, it is often in critical switching stations in critical paths.

The economics and physical constraints of installing two VTs need to be considered. The loss of a VT is not as crucial as losing a CT since the transmission line and substation bus can most likely remain in service and some backup protection can still function with the loss of a VT. Upon loss of potential there will be an increase in the risk of an overtrip but if the main concern is dependability then this may be an acceptable risk until the VT is repaired. Modern microprocessor relays can quickly alarm remotely for a loss of potential (LOP). These relays then have selections to either permit certain non-directional over current trips or to block trip. A repairman can be sent to repair the LOP problem, hopefully before an over trip occurs.

Another important factor to consider is physical space in the yard. In many urban locations space is a big issue and it is not possible to install two separate VTs due to space constraints. In fact there are many remote locations where due to environmental restrictions the footprint of the substation has to be as small as possible.

Two protection groups can be supplied from separate secondary windings on one voltage transformer or potential device. Consideration should be given so that a complete loss of one or more phase voltages does not prevent all tripping of the protected element and each secondary winding has sufficient capacity to permit its use for protection of the circuit.

CTs are installed around the bushing of the Power Circuit Breaker (PCB) and are usually not a problem for redundancy issues.

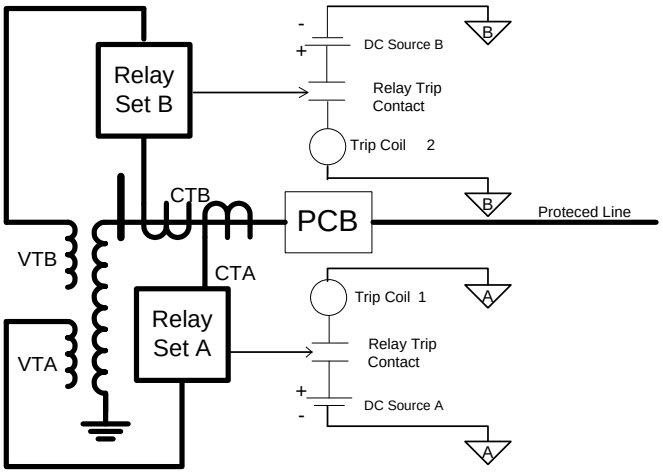


Figure 4. Dual Secondary VT and Separated CTs for Redundant Line Protections

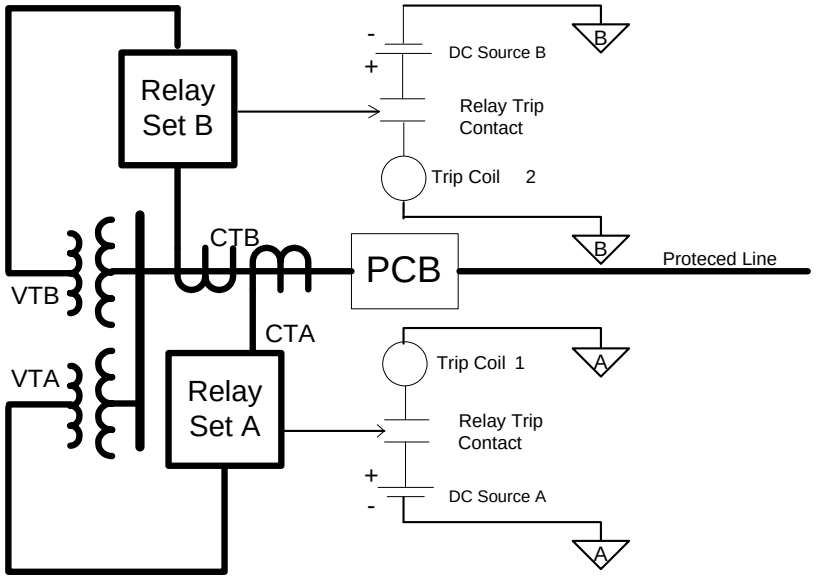


Figure 5. Two Sets of VTs and Separate CTs for Redundant Line Protections

4.1.3 Batteries

A redundant DC battery system may be hard to justify economically and physically (second battery room, etc.), therefore, two DC circuit methods are suggested as a means to achieve acceptable redundancy when only one battery system exists.

- One main circuit with coordinated sub-circuits, as shown in Figure 6. In order to meet redundancy requirements, a non-redundant battery system must be monitored and alarmed such that a failure will be recognized and mitigated.
- Two main circuits and coordinated sub-circuits, as shown in Figure 7. This style control circuit is one way to meet DC redundancy control circuit requirements. However, this method is still a single battery system. It must be monitored and alarmed to be certain that a battery failure will be detected. A single breaker failure system can be connected to one of the coordinated sub-circuits from either of the two the main circuits.

Another method some utility companies implement, when a one battery system exists, is to use an eliminator type battery charger, with fusing and switching devices and appropriate alarms as noted above. This battery charger is over-sized, such that the charger can stand-alone to provide the required DC control voltage and current. When battery testing and maintenance is occurring and the batteries are out of service, the charger must satisfy the continuous load and permit tripping of the largest set of breakers used in a protection scheme, which is generally a bus differential or breaker failure type scheme.

However, in some regions, especially for EHV substations and power plants, it is believed that the reliability of the interconnected power system is so crucial that no single failure of a protection scheme, including the DC and AC power sources can be tolerated and two batteries, chargers and AC sources are used. If space is available in the control room, the incremental cost of a second battery need not be excessive compared to the total cost of the substation or even the rest of the protection systems.

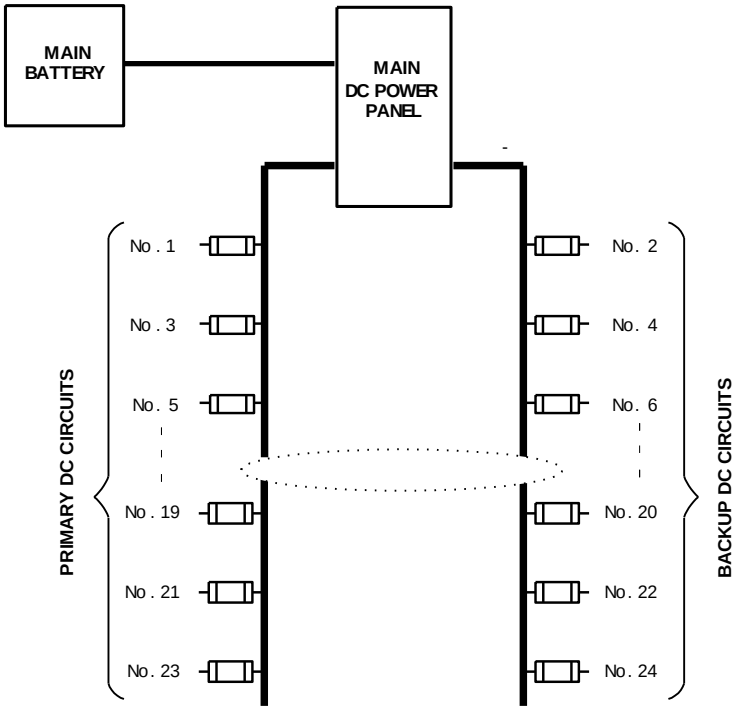


Figure 6. Two DC Circuit Methods

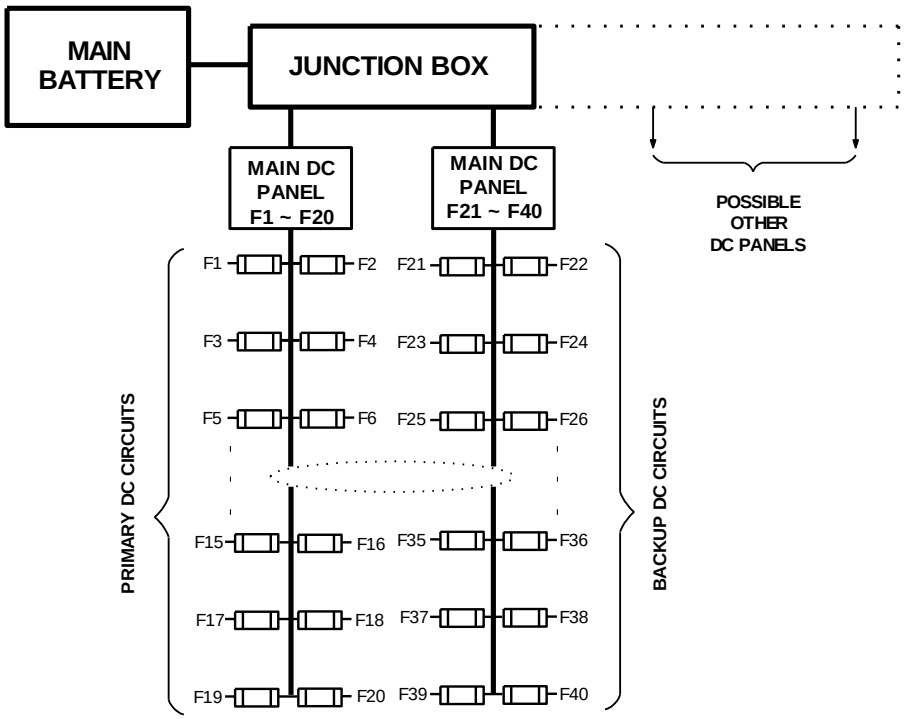


Figure 7. Alternative Two DC Circuit Methods

4.1.4 Physical separation

One facet of hardware redundancy is the consideration of the physical location of each piece of equipment with the goal of minimizing the effects of any single physical event. Some limitations to this are obvious. All of the equipment under consideration is most likely to be located within the same substation. All of the CTs may have to be on the same breaker and maybe even be around the same bushings. Even with this in mind, some physical separation may be achieved. "A" relay schemes can be placed on different panels than the "B" schemes. AC or DC sources can be routed from different breakers and possibly different distribution panels. Cables from the switchyard to the relay panels can be routed by different paths. Multiple cables will be used to provide the separation of AC and DC circuits, allow for additional separation of redundant relays schemes, and provide spare cable to allow for additions or more rapid repairs if future problems arise.
Working separation into a new design is less costly and easier than in an existing scheme. It should be noted that even partial measures to achieve physical separation when revising an existing scheme may be beneficial.
An example of how one utility (National Grid) is specifying physical separation is given in Appendix B.

4.1.4.1 Single point of failure

The goal of providing physical separation is to eliminate, as much as is practical, any single point of failure that could cause the simultaneous failure of two or more complementary relay systems. A few examples may serve to illustrate this concept. If redundant relay schemes are placed on separate panels, one scheme may survive damage from a leaking roof, mice chewing on wiring, or a worker lifting the wrong wire that disables a system. Routing cable on different paths in the switchyard may help provide continuity of service if digging in the yard results in damage to cabling. An animal in a cable channel may also result in damage.

4.1.5 Redundancy applications in protection systems

Following are some examples of typical protection systems used in North America and its redundancy or lack thereof will be analyzed.

4.1.5.1 Line protection

Based on protective relay philosophy / practices as well as regulatory requirements, some utilities use redundant protections with two sets of relays with different designs and / or different components with independent CTs and one set of VT with the separated secondary VTs on EHV lines.

An example of a fully redundant line protection is given in Figure 8.

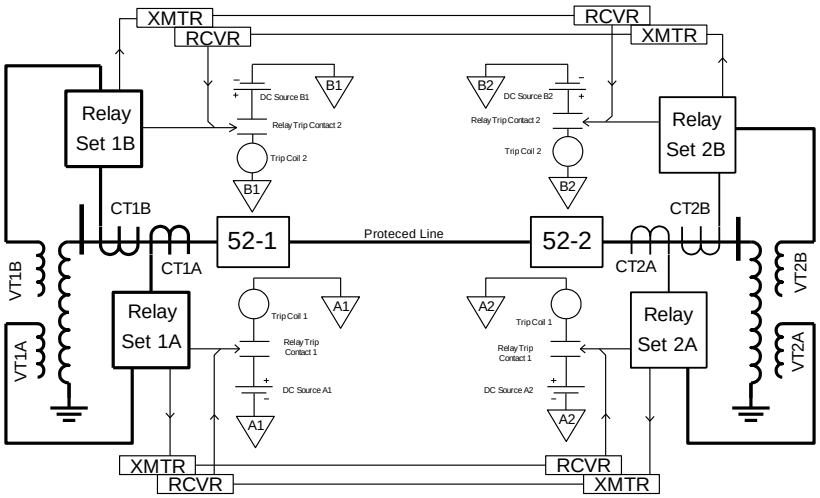


Figure 8. Fully Redundant Line Protection

For lines on lower voltage levels, partial redundancy is shown in Figure 9. This scheme includes two identical relays with two independent CTs and with one VT having two separated secondary windings. The single communication methods can be a fiber optic cable, microwave channels, metallic wire, etc.

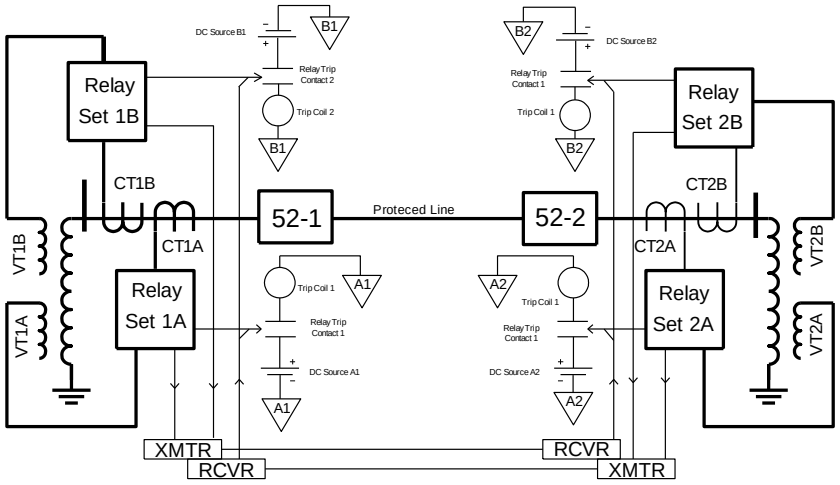


Figure 9. A Partial Redundancy with Single Communication Method

Full redundancy, also taking into account the pilot communication channels, may be accomplished with the application of two identical relays with two different schemes such as Permissive Overreach Transfer Trip (POTT) with microwave communication and Current Differential scheme with Fiber Optic cables. This is illustrated in Figure 10.

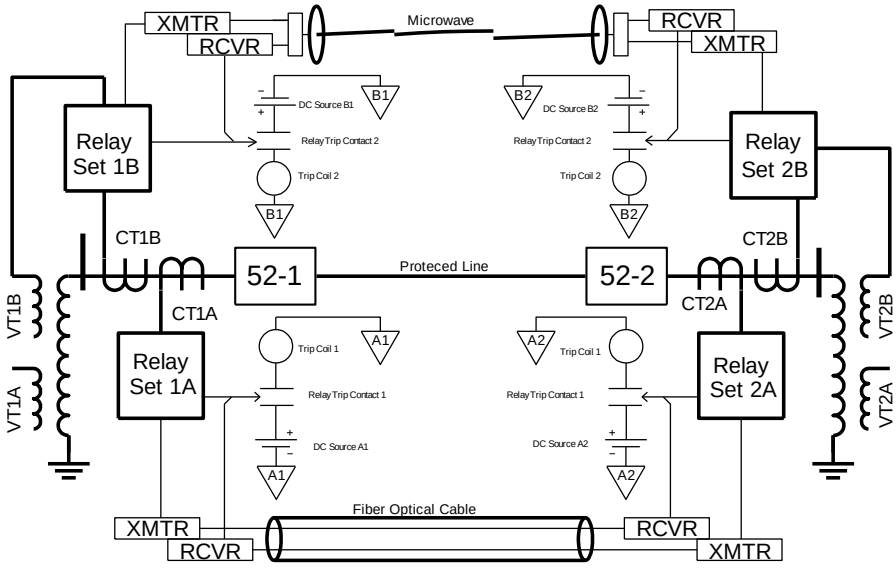


Figure 10. Full Redundancy with Microwave & Current Differential Communication Methods

4.1.5.2 Transformer protection

For redundant protection of generator step up unit (GSU) transformers, some utilities apply a set of dedicated transformer differential relays and a differential element of a generator protective relay as shown in Figure 11.

Although not shown in Figure 10, the GSU transformer neutral normally has a CT used for backup over current protection and the same CT may also be used for a dual polarizing (current portion) source to a directional ground relay used on a transmission line. Thus additional transformer protection redundancy and directional line ground over current relay polarizing redundancy is achieved.

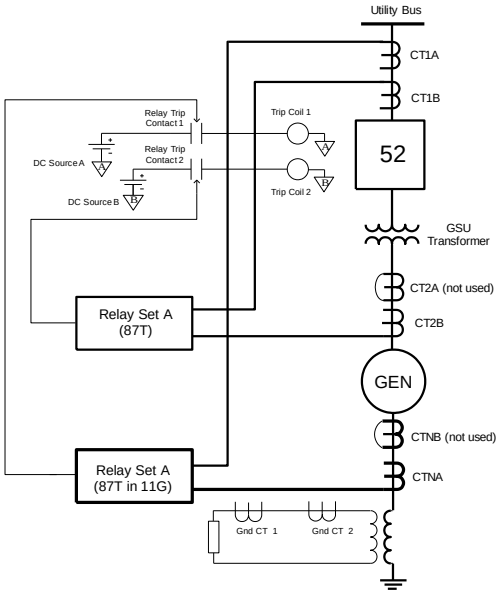


Figure 11. Dedicated Transformer Differential Relay and Redundant differential in the Generator Protection

Redundancy of transformer protection can also be achieved by dedicated transformer differential relay and sets of distance relays which look through the transformer windings from both side of LV and HV, as shown in Figure 12. Both distance relays communicate to each other via a channel.

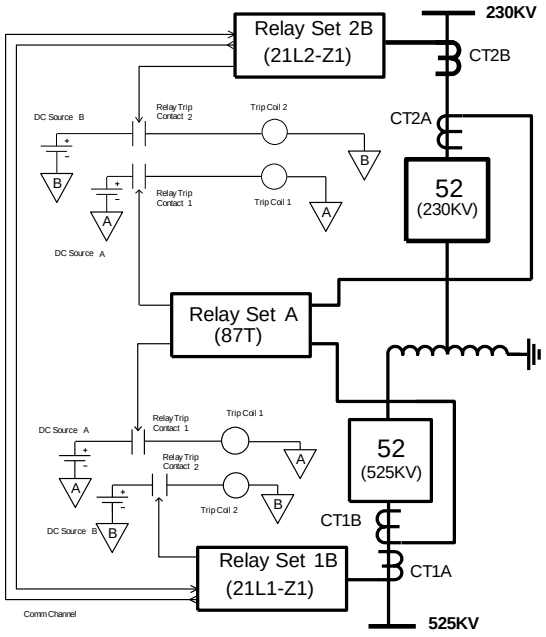


Figure 12. Dedicated Transformer Differential and Distance Relays

4.1.5.3 Bus protection

For EHV buses, redundant bus protections in the form of one set of High Impedance relays (87Z) and one set of Low impedance relays (87B) are commonly applied as shown in Figure 13.

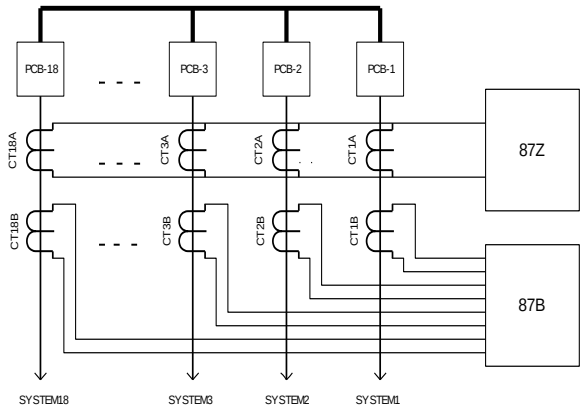


Figure 13. Redundancy with High Impedance (87Z) and Low impedance (87B) Bus Differential Relays

For a Low Voltage (LV) bus which feeds loads or motor circuits, a combination of a transformer differential relay covering LV bus sections and instantaneous/time overcurrent relay is often considered sufficient redundancy. This is illustrated in Figure 14.

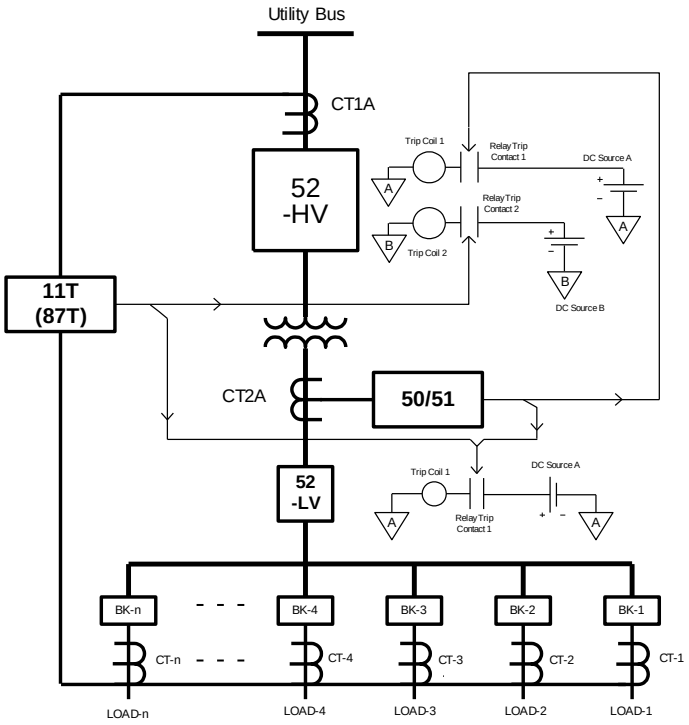


Figure 14. Redundancy for Bus Protection with a Transformer Differential and Phase Overcurrent Relays

4.1.5.4 Generator protection

For providing redundancy for generator protection and making it easier for test/maintenance, some utilities use two identical relays. System A relay uses a generator differential (87G) logic, and System B relay uses a combination of generator stator windings and transformer differential (87U) logic as shown in Figure 15. Redundancy for ground schemes is illustrated in Figure 16.

Other utilities may apply two different manufacturers' generator protective relays to avoid common mode failure. For example, System A uses a 3rd harmonic differential scheme, and System B uses sub-harmonic injection scheme.

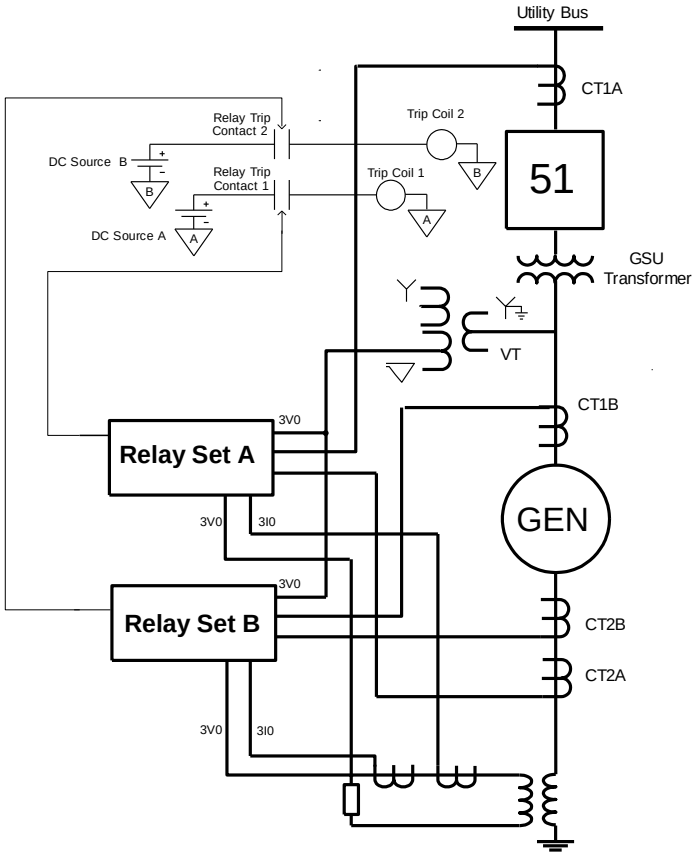


Figure 15. Redundancy with two Relays and two Schemes (87U & 87G)

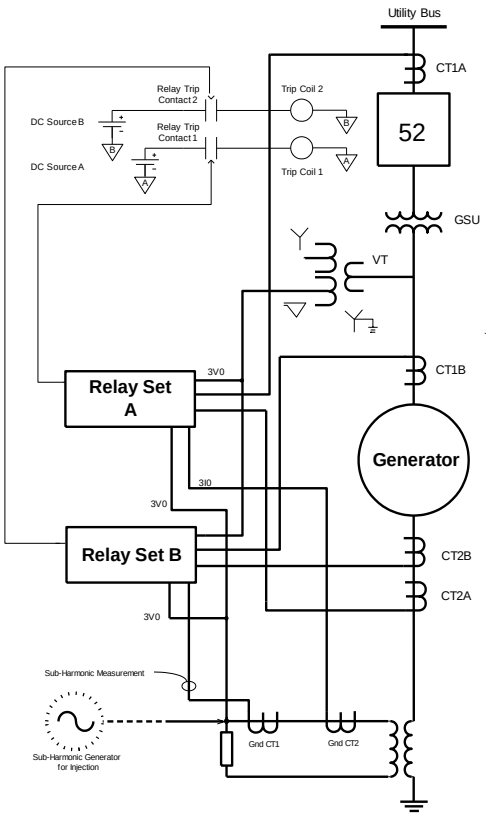


Figure 16. Redundancy with two Ground Schemes (87N & Sub-Harmonic Injection)

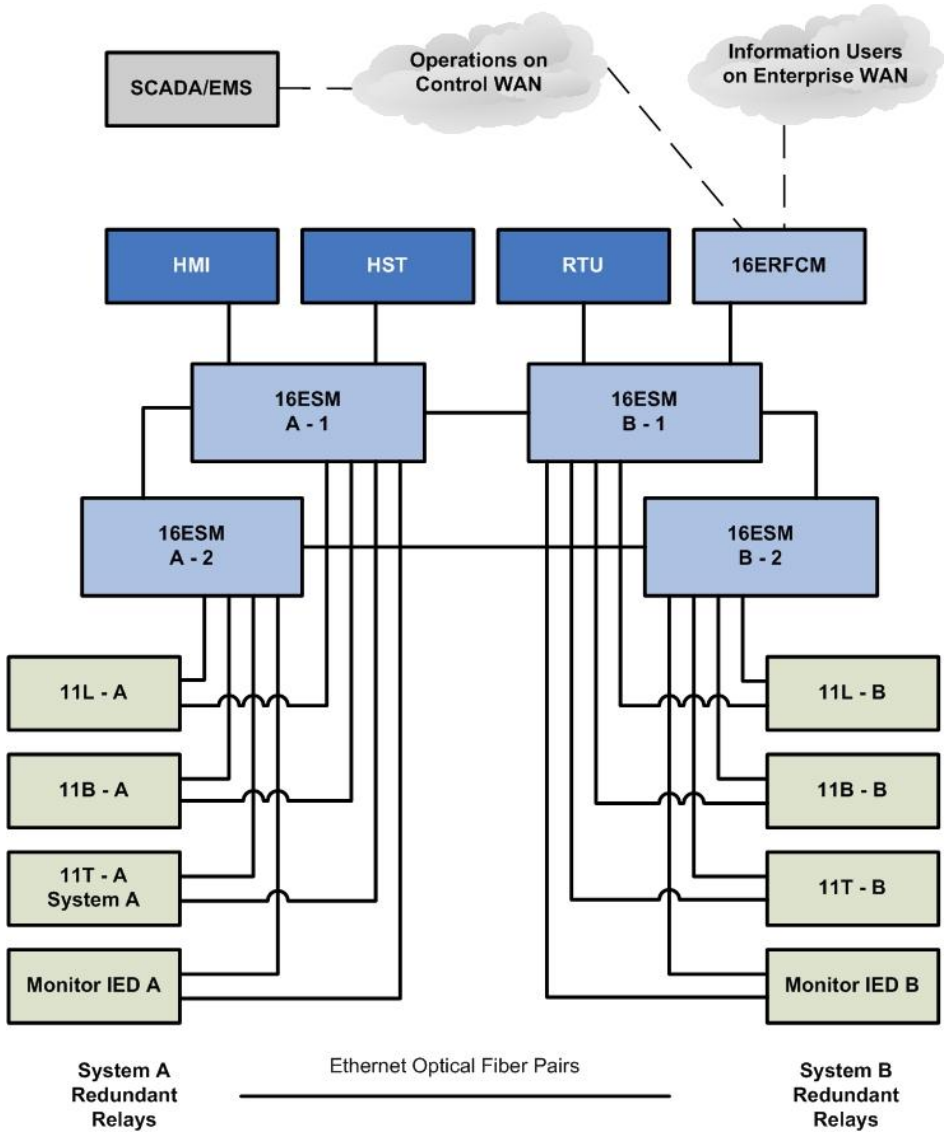
4.1.6 Ethernet LANs with IEC 61850 GOOSE messaging

The standard IEC 61850, “Communication networks and systems for power utility automation”, includes a standard language or protocol that provides a variety of communications services for integrating substation protection and control equipment on an Ethernet local area network (LAN). Of special interest here is the service known as GOOSE messaging. Through a publisher and subscriber mechanism, relays can share status points, control bits, and analog values that are sent or updated in milliseconds for high speed protection. Using GOOSE, high-speed trip and other critical signals are passed between relays over a substation LAN instead of by dedicated wires. See [17] for an overview of GOOSE messaging operation.

Because GOOSE message packets are used for critical tripping commands and other protection exchanges, the design of the LAN that carries messages must incorporate redundancy. Edition 1 of IEC 61850 does not deal with physical networking issues – the network designer must insure that redundancy requirements are met. Figure 17 shows one example of an Ethernet LAN with multiple layers of redundancy. Note that each connecting line in the figure represents a pair of optical fibers – one for each direction. Similarly, the ports on all the devices have two optical connectors. The relays are shown with two fiber pairs – a primary pair and a failover pair. For a start, consider only the primary pair – the failover pair is explained further below.

Note that there are System A and System B redundant relays as described elsewhere in this document. In general, the System A relays send critical GOOSE trip messages to other System A relays. Similarly, System B relays exchange critical messages with other System B relays for redundancy. The overall substation network, however, also connects station level devices including a data concentrator that performs the RTU function, an HMI, a substation historian, and an Ethernet router that connects the substation protection and control to the utility operational wide area network (WAN) for SCADA, EMS, and

enterprise integration. These station level devices and functions need to access metered values, status reports, and control points of both the System A and System B relays using services other than GOOSE, such as IEC 61850 server-client objects or Ethernet DNP3. Therefore, the LANs interconnecting all these devices are not isolated into System A and System B sections. Figure 17 shows one example of how the A and B devices can be integrated on one LAN while still meeting the fundamental requirement for redundancy – that a single credible hardware failure anywhere in the connection cannot disable both the System A and System B protection functions.



Legend (see IEEE C37.2-2008):
11L – multifunction microprocessor line relay (redundant units A and B)
11B – multifunction microprocessor bus relays (redundant units A and B)
11T - multifunction microprocessor transformer relays (redundant units A and B)
16ESM – Managed Ethernet switch
16ERFCM – Managed Ethernet secure VPN router with firewall
RTU – Substation data concentrator (Remote Terminal Unit)
HMI – Operator interface
HST – Substation historian

Figure 17. Redundancy in an Ethernet LAN with IEC 61850 GOOSE

All the System A relays can exchange GOOSE messages through the switch 16ESM A-1, and all the B relays can exchange GOOSE messages through switch 16ESM B-1. These two switches are connected to each other by a fiber pair (usually a Gigabit, or 1GB/s connection), and station level devices can be connected to either switch. The RTU, historian, HMI, has a path through one or two switches to any relay, A or B. Because the A and B switches are electrically isolated and connect only via processed data streams managed by the switches, the A and B switches keep their respective relays suitably isolated to meet redundancy requirements.

However, note that a failure of switch 16ESM A-1 impacts more than one zone relay within the redundant Set A. While we still have not violated the redundancy principle, losing functions in multiple zones of protection in one redundant set is an uncomfortable change from the behavior of older wired designs. To limit the effect of a switch or fiber failure to a single zone relay at worst, LAN designs can include redundancy within the Set A or Set B networks. With the arrangement of Figure 17, a single LAN failure has no functional impact on protection (the user can still get an alarm), or impacts one relay at worst. The strategies for getting this extra communications redundancy within a redundant relay set are:

1. Connect multiple switches in a ring, so that there are at least two paths from any switch port used by a relay to any other such switch port. Ethernet switches include the failover service called rapid spanning tree protocol (RSTP) by which the switches discover and use a normal or default message path without circulating messages forever in a loop – one link in the loop is blocked to achieve this. If the ring suffers a break or if one switch fails, the switches can detect the path loss and immediately set up new routing of messages by unblocking the spare path to maintain communications.

2. Many GOOSE-capable relays have primary and failover communications ports, as shown in Figure 17. Provide two switches or switch groups within the redundant Set A, and also in Set B – in Figure 17, switches 16ESM A-2 and B-2. Connect the relay's primary port to one switch or switch group, and connect the relay's failover port to the other switch group.

If there is a failure of the incoming primary port, its optical fiber link, or the associated switch port at the other end of the link, the relay electronics detect the loss of incoming data or signal carrier and transfer communications operations to the failover port (both sending and receiving operations). With the network connection of Figure 17, this failover port engages different fibers that connect to a different switch in the ring, covering failure of any of these components.

If it is the outgoing path from the relay that fails, the relay electronics cannot detect this. However, some Ethernet switches have a service that does detect the loss of incoming signal to the switch port. If the switch sees the failure of signal from the relay, it stops sending any signal to the relay in return. The relay then senses this action as an incoming signal failure and forces the desired failover to the backup ports and fibers.

The net result of all this is that there are always two or more paths from any relay to any other within each redundant set. So a single communications failure does not impair either the System A or System B relays.

The System A and System B switch groups have dual cross-connections so that substation level IEDs – the data concentrator RTU, HMI, historian HST, WAN connection from router 16ERFCM, and others - can access data from relays in either redundant set even if one of those cross fiber pairs fails. The loop traffic is managed by RSTP. Also, GOOSE messages can pass between redundant relay groups – this can be useful for monitoring of A relays by their B counterparts to alarm failures, and vice versa. Line relays can agree on reclosing control by only one relay at a time.

4.2 Diversity

Diversity in a relaying system can be considered an intentional application of differences in order to prevent common-mode failures between redundant schemes. A number of measures may be applied to provide diversity.

4.2.1 Different operating principles

Electric utilities use different operating principles to provide more extensive coverage during system faults. This philosophy helps to ensure that a disturbance is quickly cleared. It is important to select different operating principles that complement each other well when using more than one main protection scheme. As an example a utility can use both line current differential protection and distance based communications assisted tripping (for example, permissive overreaching transfer trip) to protect their high voltage transmission lines. Line current differential protection is voltage independent and can quickly clear a line fault if a potential transformer has failed at one end of the line while the impedance based line protection can trip via a step distance scheme if the communication channel fails.
Different principles can be utilized via two separate main protection schemes or using the same relay system now that numerical technology is well proven and accepted. Referring to the example above there is a good number of numerical line relays available from various manufacturers that provide both line current differential protection and impedance based protection.

4.2.2 Different manufacturers

One of the main advantages of using different manufacturers is that if a component specific or firmware related malfunction occurs in one relay system it does not prevent the other manufacturer's relay system from operating to clear a fault. Typically different manufacturers use different operating principles for their protection algorithms so if a system fault occurs that one manufacturer's relay system cannot detect then it is still possible that the other manufacturer's relay system can clear the disturbance.

Some utilities' internal guidelines require diversity between set A and set B relay packages thus increasing the security in the event that a single manufacture's product suffers from a common failure in a specific relay model. However, the use of the same manufacture with different operating principles is becoming more popular.

4.2.2.1 Single source

It is an advantage to use a single manufacturer for simplicity, reduction in training and engineering. However, the risk that the supplier will not be able to deliver the required device needs to be considered. For a project already underway, the switch to an alternative supplier may cause delays and costs due to re-engineering and training.

4.2.3 Different communication channels

Different communication channels can be classified as two independent channels, each one running along a separate route, and also as utilizing different communication media such as microwave and optical fiber. Some relay systems such as line protection can operate over two independent communication channels so that should one fail the scheme can still quickly trip during a fault. For EHV installations, most utilities use two main protection schemes for line protection and each has its own independent communication channel. This practice helps ensure that if one scheme fails or is removed from service the other is able to quickly operate during a fault within the zone of protection.

4.3 Coupling redundancy for Power Line Carrier (PLC)

PSRC WG H15 is presently (as of January 2010) writing a report for PLC coupling redundancy. Please refer to this report for a more detailed discussion. A short summary follows.

The goal in protective relaying system power line carrier (PLC) communications channel design is to design a channel that will reliably communicate a protective system function over the power line to the remote end. Channel design is greatly dependant on the type of protective relay scheme used. There are many pieces of equipment involved in a PLC channel. All the different individual components have losses associated with them. Figure 18 below shows a typical PLC channel. The configuration of the equipment will affect the overall attenuation of the channel.

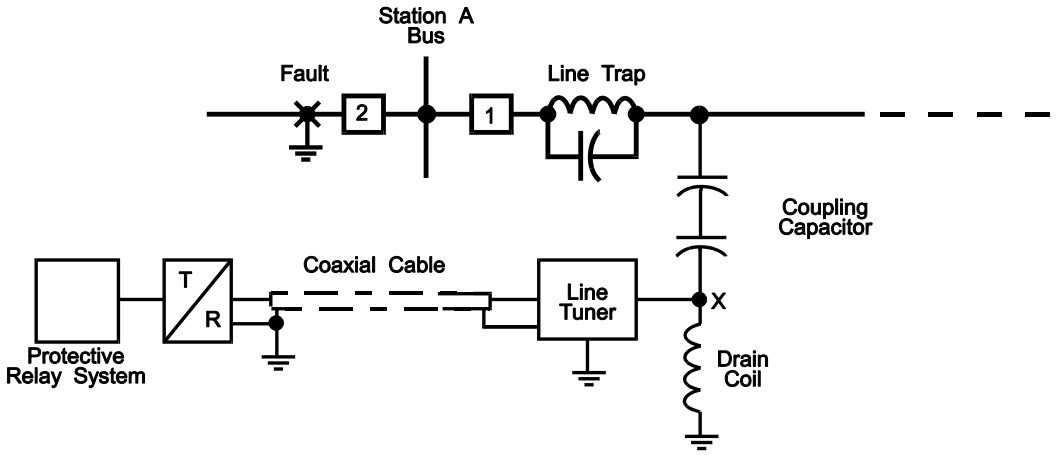


Figure 18. Basic Power Line Carrier System

As with most systems, there is more than one way to couple the carrier to the power-line. The deciding factors may be economic and performance. That is, the best performance may be too expensive to justify for the line being protected so the next best one may be the preference. Most lower voltage lines (below 230 kV) use single-phase-to-ground coupling, requiring only one set of coupling equipment (line tuner, coupling capacitor and line trap). However, for EHV lines (230 kV & higher) dependability and redundancy requirements may dictate multi-phase coupling. Multi-phase coupling will require multi-sets of coupling equipment.

4.3.1 Best coupling systems for redundancy:

One would think that using two totally separate channels (one for each of the pilot relay systems) would result in the most redundancy possible for Power Line Carrier. One system would be coupled on one phase of a three-phase transmission line and the other on another phase. However, this creates two concerns – one being that it is not the best possible coupling for the system on the outside phase and the second one being that there is not enough isolation between transmitters since there is little to no isolation between the two phases and thus the two transmitters are not isolated from each other. Figure 19 illustrates this. This lack of isolation will cause intermodulation distortion. Intermodulation distortion creates new frequencies to interfere with other channels on the same line or adjacent lines. Also from a redundancy point of view, if one line tuner or coax fails, that pilot relay system is completely useless.

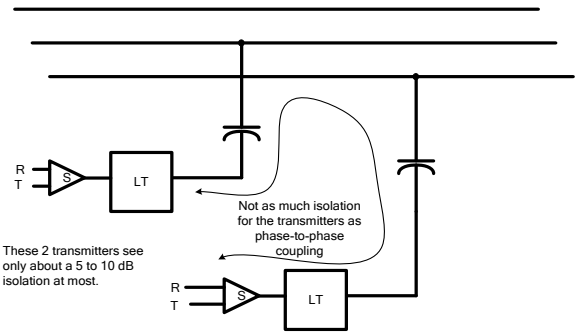


Figure 19. Two Independent PLC Channels, each coupled phase to ground.

A better approach both from an isolation and redundancy point of view is to use phase-to-phase coupling as shown in Figure 20. This coupling scheme provides the second best Mode-1 coupling efficiency. Mode-1 coupling is out on two phases, in on the center phase. Refer to Working Group H15 for details. There are two line tuners/CCVT/Traps used for this method, with the addition of a balancing transformer and various hybrid complements. Even though there are more losses in the transmitter path, there is also much better isolation between the two transmitters. This means no intermodulation distortion to interfere

with other PLC channels. While the hybrids add more components to the overall complement of equipment, as well as a common signal path (in the control house), these devices are passive devices and failures are nearly non-existent. Additionally and more importantly from a redundancy point of view, should one line tuner or coax be lost, both signals are still being coupled to one of the phases and you don't suffer a complete loss of channel of one system, just a reduction in signal strength. Also, since most faults are outside to ground, then having coupled to the center phase, provides some protection against total loss of channel due to lightning strikes. It should be noted that to get full benefit of this coupling scheme the hybrids and common path coaxial cables must be located in the control house and two coaxial cables run to the two line tuners in the switchyard.

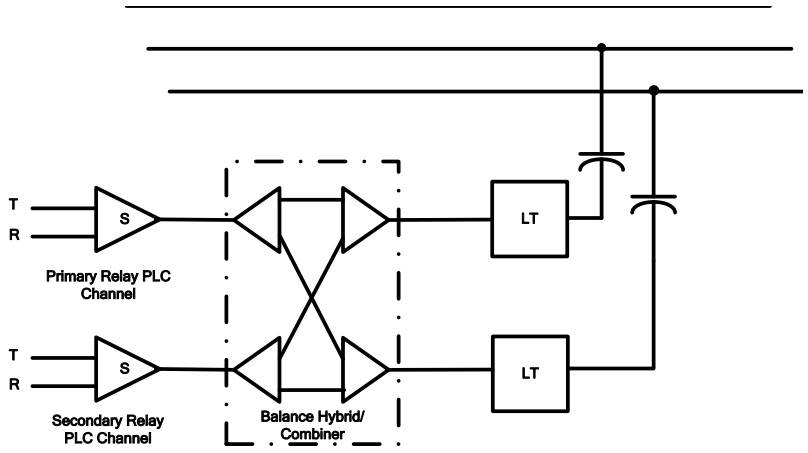


Figure 20. Two PLC Channels, coupled together via phase to phase

Even greater redundancy and Mode-1 coupling efficiency is created when coupling via Mode-1 coupling that uses all three phases and requires three Line Tuners/CCVT's/Traps and additional hybrids and balancing transformers. The balance transformers, hybrids and common path coaxial cables should be in the control house, and therefore, there will be 3 coaxial cable runs from the control house to the switchyard. There is one point of failure - at the coax in the house, but it is not exposed to the elements and should be a short run.

4.4 Switched redundancy

In order to maximize both security and dependability it may be desirable to change the communication output logic configuration depending on channel availability.

Security is increased by use of dual channels connected in an "AND" logic configuration.

Keying noise, channel noise and equipment misoperation due to hardware failure all play a minimized risk when two channels are used rather than one. Additional security is gained if the two channels take different paths, such as separate physical routes, or technologies. However, if one of the channels is out of service the system does not work at all. Out of service is not the same as not producing a command. Namely, out of service means that the equipment is not able to produce a command. Most communication equipment can recognize when it is unable to work and will generate an alarm.

Dependability is increased by use of dual channels connected in an "OR" logic configuration. The gain is realized by way of having two chances to get the command. However, there is a loss of security operating in this configuration because there are two chances of a failure causing a misoperation.

Having the protection system use two "AND" connected channels with automatic switching to "OR" logic upon the failure of a channel provides the most reliable scenario. The alarm circuits of the equipment drive the switching. Therefore, it's very important that the alarm threshold settings are both sensitive and selective. This type of arrangement can be done electronically or via contact logic with appropriate time

delays so that upon an intermittent channel condition the logic is not transitioning. Additionally, having the alarm condition clear for a few seconds to a few minutes before switching back to AND logic reduces the risk of a misoperation.

Systems can be connected to have immediate output via AND logic and time delayed output via OR logic. Voting schemes with time delays can be used with 3 or more channels.

As with schemes that speed up protective relay element timers upon loss of channel, these switched schemes are not dependable if the channel failure occurs simultaneous with a fault. However with a properly designed communication system the likelihood of a channel failure will be a random event setting up the scheme for the highest level of reliably should it be called upon to operate prior to establishing normal channel conditions.

4.5 Voting schemes

A voting scheme requires the simple majority (usually through output contacts in series) of an odd number of primary relays to indicate a system disturbance before the overall protection scheme is energized. Voting schemes typically consist of three primary relays of different manufacturers that receive the same analog and digital inputs from different sources where any two-out-three devices must agree to initiate any tripping action.

Voting schemes are often applied when a high degree of certainty that a protection system will not operate incorrectly is required. They are most commonly utilized in special protection schemes and a few EHV transmission line protection systems where system studies or operational experience have shown that the misoperation of a scheme or inadvertent transmission loss would be detrimental to the overall stability of the system. Figure 21 is a conceptual example of a complete redundant transmission line protection two-out-three voting scheme.

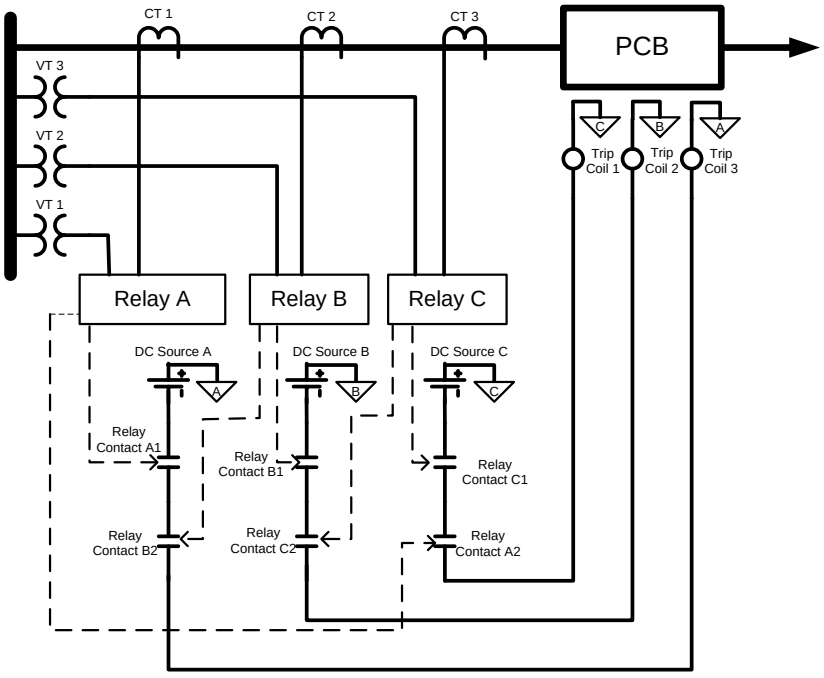


Figure 21. Redundant Voting Scheme

Each relay is connected to its own voltage and current source. The trip circuits consist of separate dc sources connected to the three possible combinations of two separate relay contacts connected in series to each other and to separate trip coils of the PCB. In this scheme if one of the relays misoperates due to a CT failure or PT failure or some other internal logic failure the PCB won't operate without one of the other two relays operating.

4.6 Changes due to microprocessor technology

Most electric utilities have embraced numeric multifunction protection technology as a means of surviving in an industry that has changed dramatically in the last ten years. Led by restructuring and shrinking resources, protection engineers are continuing the move to communicating, multifunction protection technology as a means of reducing cost and maintaining operating performance with fewer personnel. We are at a point in the evolution of the technology where we need to step back and ask some questions about protection reliability. Our application and maintenance philosophies must be reviewed on a regular basis to ensure that they are meeting long-term protection reliability as well today as they did with predecessor technologies such as electromechanical and solid state devices.

The factors influencing reliability are the same for predecessor and numerical multifunction technologies. Reliability factors that influence one technology influence all technologies; the question is to what degree.

Misapplication of protection products will have the same impact on protection reliability regardless of the technology. Assuming, however, that the protection engineer has a good understanding of the power system and that the correct application decisions are made, the following observations can be made:

- Predecessor technologies are time tested, require no new standards, and are understood by all personnel in the engineering, operations, and maintenance loop.
- Obsolescence and cost are slowly but surely eliminating products from the predecessor technology group.
- Manufacturer support for the earlier products is being reduced or eliminated.
- With expanded range and multiple protection elements, multifunction protection systems provide for more flexibility and precision of setting than predecessor technologies, thus reducing “incorrect” operations resulting from borderline or limited range.
- Lower cost/function, smaller size, and feature/function flexibility of multifunction systems allow the protection engineer more freedom to improve protection reliability with little or no additional hardware cost.
- Detailed even reports are usually available from microprocessor relays, while such information required separate recording devices (if available at all) when predecessor technologies are used.

Protection philosophy consists of global guidelines designed to maintain a high level of protection reliability throughout the range of applications on a given power system. Comparisons of predecessor technologies versus numerical multifunction technology reveal some interesting differences related to protection reliability. The following observations can be made:

- Predecessor technologies, if fully operational, provide a high level of dependability resulting from multiple (individual) phase or zone relays and ground relays. When a given protection philosophy is replicated with a three phase device that includes all phases, zones, and ground elements, careful consideration must be given to protection reliability issues such as single contingency failure and common mode failure.
- With self-testing and monitoring, internal sequential events and oscillography, and remote communications, numerical multifunction protection systems are capable of identifying problems, removing themselves from service, and notifying a remote location of the situation. Most situations can be identified and corrected before becoming an “incorrect” operation, thus improving overall protection reliability.
- Protection engineers must guard against inadvertent violation of their company’s philosophical guidelines. For example, the use of a single multifunction device to provide primary and backup protection of a given zone could result in a single contingency failure that disables all protection of that zone.
- The reliability impact of a common mode failure on multifunction protection systems of a single manufacturer should be considered. Predecessor technologies by a single manufacturer take advantage of multiple (individual) phases, zones, and ground relays to offset common mode failure. With all protection elements and phases in one multifunction device, use of a single manufacturer’s equipment for primary and backup protection of a given zone creates the possibility of a common mode failure that could disable all protection.

4.7 Electromechanical schemes

Consider a typical 161kV electromechanical line protection scheme, as shown in Figure 22, with carrier blocking, with Zone 1 (forward), Zone 2 (forward) Carrier Phase and Time-delayed trip, Zone 3 (reverse) Carrier Start and Time Delayed trip, Carrier Ground trip/start, Backup ground Instantaneous/Time Overcurrent. Does this scheme provide inherent relay backup for all fault types?

The scheme provides inherent backup for phase-ground and phase-phase-ground faults as long as carrier is turned on (backup ground backs up carrier ground). If carrier is turned off backup ground becomes primary protection for ground faults, with no other backup within the relay terminal. For phase-phase and three-phase faults, the answer is no, with the following qualifiers:

- If carrier is on, zone 2 backs up zone 1 for all faults
- For faults beyond zone 1, zone 2 is the only relay that will operate.
- If carrier is off, zone 2 backs up zone 1 except for close-in three-phase faults, due to memory voltage expiration
    - For a typical electromechanical relay, the memory action is only effective for a few cycles after the inception of a fault and will not provide time-delay protection for any fault that results in zero voltage at the terminals of the relay."
- Zone 3 with offset will back up zone 1 for close-in three-phase faults, but with a longer time delay (typically 90 cycles)

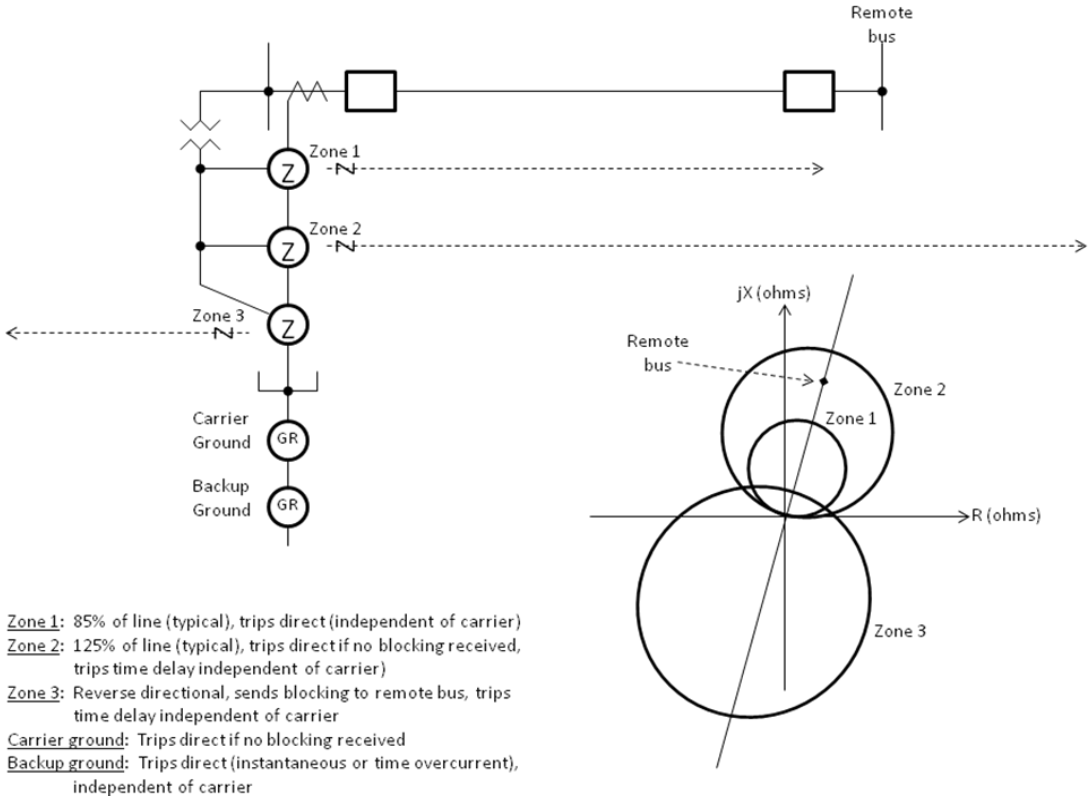


Figure 22. Typical Electromechanical Line Relay Terminal (DCB Scheme)

Some transformer differential schemes using delta-connected CTs using three individual relays can provide redundancy since at least two relays may see any internal fault, as shown in Figure 23. Even single-phase-to-ground faults can produce operating current in two of the relays due to the delta-connection of the CTs.

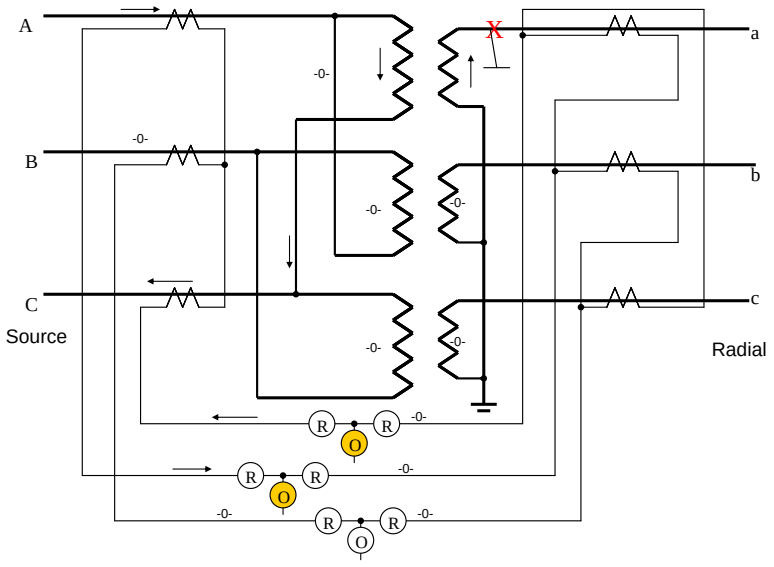


Figure 23. Transformer Differential Scheme

The same is true for bus differential relays with delta-connected CTs. But if the CTs are wye-connected to one relay per-phase, no redundancy exists for single-phase-to-ground faults.

5 Examples (real life events)

5.1 Example of events that have had an effect on the operability of protection schemes

- Fire in the control house
- Water damage due to control room roof leaking
- Large vehicles crushing and severing control cables
- Objects dropped from cranes
- Ice damage to control cables
- Rodents chewing through cables
- Deterioration of cable insulation causing flashovers to other cables in the same duct
- Snow plows taking items of plant out
- Excavation in the yard damaging control cables
- Loss of communication circuits
- Undetected failures of relays and auxiliary relays
- Inclement and stormy weather, such as hurricanes, tornados, lightning, ice conditions, extreme heat or cold (that results in operating temperatures outside the design limits of relays and communications equipment), etc.
- Vandalism & other acts of intentional damage to the power system
- System faults including momentary system voltage collapse and associated ground rise potentials and noise or power quality impacted to the power system and protection or control schemes.

As can be seen from the above list, some of these issues can easily be addressed by properly implemented redundancy while others may be cost prohibitive. The likelihood of an adverse event, combined with the system impact of such event will dictate degree of redundancy.

However, redundant and separated protection schemes provide the dependability needed to ensure faults are cleared to avoid instability and other system performance violations. If avoidance of instability of an interconnected system is paramount, then the degree of redundancy will be higher.

5.2 Redundancy with common mode failure

A blackout event in 2003 was partly caused by improper redundancy implementation. A microwave SCADA RTU was provided with redundant power supplies that both failed due to ground potential rise. The equipment was not substation hardened. While not the direct cause of the blackout, the lack of an updated reading from the RTU resulted in an Operator action that aggravated the blackout situation.

5.3 Lack of redundant auxiliary relays

A major disturbance in 2004 in the WECC system resulted following a line-to-ground fault on a 230 kV line. The faulted line's electromechanical redundant relays operated a single auxiliary relay, which provided both breaker tripping and breaker failure initiation. Not all of the auxiliary relay contacts operated for the line fault. The fault required nearly 40 seconds to clear and resulted in tripping twenty-one 230 kV, 345 kV, and 500 kV lines, more than 4600 MW of generation and nearly 1000 MW of load.

5.4 Lack of redundancy during construction

A utility was upgrading the bus at a major station. When the new facilities were ready to energize, the bus differential and backup protection schemes were intentionally disabled. Ground cables were inadvertently left on the bus, resulting in blacking out a major part of a large city.

6 NERC Reliability Requirements

At present NERC is developing the scope for a Protection System Reliability Standard. To support this effort the System Protection and Control Subcommittee (SPCS) of the NERC Planning Committee has written a Technical Paper entitled Protection System Reliability - Redundancy of Protection System Elements [15].Before the System Protection and Control Subcommittee was formed in early 2009, it was a Task Force and so it is referred to as the System Protection and Control Task Force (SPCTF) in the Technical Paper.
This Technical Paper can be found on the NERC System Protection and Control Subcommittee web page at:-

http://www.nerc.com/filez/spctf.html - click on 01/14/2009 Redundancy of Protection System Elements

For reference the Introduction to the Technical Paper is reproduced here.

> Introduction: Protection System Reliability - Redundancy of Protection System Elements
>
> The 1997 NERC Planning Standards[1] contained tenets on Protection System redundancy that were not included in the Version 0 translation of those standards. Consequently, the NERC Planning Committee charged the System Protection and Controls Task Force (SPCTF) in late 2005 with preparing a Standard Authorization Request (SAR), with associated justifying technical background material, to reintroduce Protection System redundancy. This technical paper provides the background and support for the development of that Protection System Reliability SAR.
>
> The reliability of the Bulk Electric System (BES) is normally measured by determining the performance of all the various power system elements and their ancillary systems. Protection Systems, being ancillary systems, are critical to establishing and maintaining an adequate level of BES reliability. The NERC reliability standards define the level of reliability to which each owner must design the BES and this in turn, can be used to determine the performance requirements of electric system elements such as breakers, and Protection Systems.
>
> This paper, developed by the NERC System Protection and Control Task Force (SPCTF), proposes Protection System reliability requirements and discusses the reasoning behind the requirements, provides examples and explanations concerning each requirement, and describes how to determine the level of Protection System reliability necessary to meet each requirement. This paper also describes a collaborative and interactive process between the protection and planning engineers to determine the required level of Protection System performance. It should be noted that in parallel to this effort is an IEEE PES/PSRC work group[2] that is developing a special report addressing redundancy considerations for relaying. SPCTF has a liaison

relationship with that working group. The IEEE effort concentrates on the Protection System elements while this paper concentrates on the BES performance implications of Protection System redundancy.

This paper evaluates Protection System clearing times for a normal electric system configuration (planned peak load conditions with all lines in service, typical generation dispatch, typical interchange, and typical switching configuration) for a fault on one electric system element with a Protection System component failure. For a component failure of the Protection System, redundant local backup, and remote backup Protection Systems are evaluated to determine the clearing time for the faulted electric system element under review. Due to the additional complexities involved, the performance requirements of backup Protection Systems for other electric system contingencies are not addressed in this paper.

7 Conclusions

There are many correct methods to accomplish protection system redundancy. Protection system reliability encompasses adequately and redundantly protecting all facilities required in a power system, including but not limited to power plant equipment, substation equipment and bus, transmission lines and distribution lines. Each utility, along with the utility's protection engineers and technicians, consulting engineers, manufacturer's products and service offerings, and industry practices, will have preferred method or methods of protection. Electric system voltage level and element being protected, technical expertise, economics, technology changes, available products from manufacturers, utility management and/or personnel changes, utility/industry protection procedures and changes thereto, industry standards and practices, regulatory requirements and changes thereto, design practice and other changes over time all contribute to the various methods used to achieve an acceptable level of redundancy, reliability, dependability, and security. The electric system should not be prone to have cascading failures. The electric system should successfully operate as close to 100% of the time as is possible. The protection system redundancy goal should always be to promote a reliable electric system that is practical, robust, flexible, and safe to operate.

8 References

[1] IEEE 100-2000 seventh edition International Electrotechnical Vocabulary (IEC 60050)
[2] Transmission and Distribution Electrical Reference Book
[3] PC37.113-1999, IEEE Guide for Protective Relay Applications to Transmission Lines
[4] IEC 60834-1 (1999) 'Teleprotection equipment of power systems – Performance and testing'
[5] P.M. Anderson, B.K. LeReverend, "Industry Experience with Special Protection Schemes" IEEE/CIGRE Committee Report
[6] David Costello, "Fly Safe and Level: Customer Examples in Implementing Dual Primary Protection Systems" SEL White Paper 2007
[7] American Association of Highway and Transportation Officials Stephan Kellogg - http://www.cdm.com/knowledge_center/interview/integrated_asset_management.htm
[8] NPCC Document A-5 Bulk Power System Protection Criteria May 21, 2007
[9] The Authoritative Dictionary of IEEE Standards Terms (IEEE 100-2000 seventh edition)
[10] Analysis and Mitigation of Transmission and Generation System Misoperations ,WECC [Draft] Standard PRC-004-WECC-1, http://www.wecc.biz/index.php?module=pnForum&func=viewtopic&topic=776
[11] ERCOT Operating Guide section 7
[12] C37.119-2005 Guide for Breaker Failure Protection
[13] IEEE Committee Report, "Local Backup Relaying Protection", IEEE Transactions on Power Apparatus and Systems, Vol. PAS-89, No. 6, July/August 1970, pp, 1061-1068.
[14] L.F. Kennedy and A.J. McConnell, "An Appraisal of Remote and Local Back-up Relaying", AIEE Transactions, Vol. 76, pp. 735-741, October 1957
[15] PSRC WG Report "Justifying Pilot Protection on Transmission Lines"
[16] NERC System Protection and Control Subcommittee of the NERC Planning Committee Technical Paper "Protection System Reliability - Redundancy of Protection System Elements"
[17] Udren, E.A., "IEEE (ANSI) Device Number 16 – Ethernet Switches and Routers," Texas A&M Conference for Protective Relay Engineers, College Station, TX, April 2008, Pages 19-22.

Appendix A - Review of present practices

This Appendix lists some existing requirements by regional organizations, as of September 2009. The standards referenced are subject to change and the most current version for the region in question should always be consulted. The information given in this Appendix is for informational purpose only.

1 Regional Reliability Organizations

Regional organizations are specifying redundancy requirements as part of their reliability standards or other applicable standards.

1.1 NPCC (Northeast Power Coordinating Council)

1.1.1 NPCC Background

The NPCC is the voluntary, non-profit international electric Regional Reliability Council formed in January, 1966 shortly after the November 9, 1965 Northeast Blackout that establishes the processes which assure the reliable and efficient operation of the interconnected power systems within its geographic area. That area includes New York, the six New England states, Ontario, Quebec, and the Maritime Provinces in Canada. The total population served is approximately 54 million. The area covered is approximately 1 million square miles.

NPCC initially was comprised of most of the entities that had previously participated in CANUSE (Canada-United States Eastern Interconnection), a much looser and less formal operating/planning organization. Its formation responded in part to Recommendation #4 of the (US) Federal Power Commission NORTHEAST POWER FAILURE November 9 and 10, 1965: A Report to the President.

NPCC Criteria have always focused on the reliability of the northeast interconnected bulk power system, not the underlying transmission network. This concept is exemplified by its performance-based definition of the bulk power system, not by voltage class, but defined in NPCC Criteria A10 which is a set of Planning Criteria that determine if a power system element is 'Bulk Power". In short the definition of a Bulk Power element is if a fault is sustained on that element and it causes instability outside the local area. This is not to be confused with the Bulk Electric System defied by NERC as any element above 100kV.

The northeast interconnected bulk power system is defined as the interconnected electrical systems within Northeastern North America, comprising generation and transmission facilities, on which faults or disturbances can have a significant adverse impact outside of the local area. Local areas are determined by the Council members.

In this context redundancy does not really have much to do with protection systems themselves; the main focus is preserving the integrity of the North East interconnection (NPCC). In order to preserve the Interconnection, instability must be avoided and so to avoid instability we must have reliable and fast protection with breaker failure schemes i.e. a high degree of dependability.

Redundant and separated protection schemes provide the dependability needed to ensure faults are cleared to avoid instability.

Redundant protection schemes are employed to maintain the Interconnection of the Bulk Power system as defined by NPCC.

NPCC Criteria development is a "bottom-up" process; Criteria are developed by the Task Forces, reviewed by the Coordinating Committees, and approved by the members.
The original Criteria that were put in place included the following:

- Basic Criteria for Design & Operation of Interconnected Power Systems–September 20, 1967;
- Bulk Power System Protection Maintenance Criteria–April 22, 1969;
- Bulk Power System Protection Criteria–August 31, 1970.

The Criteria have been reviewed and updated since the original publications, usually every three years. Additional criteria relating to emergency operation, operating reserve and compliance enforcement were also adopted. For additional Criteria and further information please refer to the NPCC web site.

1.1.2 NPCC Bulk Power System Protection Criteria – Found in NPCC Directory

Parts of this section have been taken directly from NPCC Criteria documents. These documents can be found on the NPCC web site at NPCC.org.

The NPCC Bulk Power System Protection Criteria covers aspects relating to dependability and Security. The document states:

"Due consideration shall be given to dependability and security. For those protective relays intended for removal of faults from the bulk power system, dependability is paramount, and the redundancy provisions of the criteria shall apply. For Protective relays installed for reasons other than fault sensing such as overload, etc., security is paramount, and the redundancy provisions of the criteria do not apply. The relative effect on the bulk power system of a failure of a protection system to operate when desired versus an unintended operation shall be weighed carefully in selecting design parameters."

1.1.3 Issues Affecting Dependability

All elements of the bulk power system shall be protected by two protection groups, each of which is independently capable of performing the specified protective function for that element. This requirement also applies during energization of the element.

The two protection groups shall not share the same component. Means shall be provided to trip all necessary local and remote breakers in the event that a breaker fails to clear a fault. This protection need not be duplicated.

NPCC guidance document B5 recommends that two identical measuring relays should not be used in independent protection groups due to the risk of simultaneous failure of both groups because of design deficiencies or equipment problems. Relays from the same manufacturer have been used but different models with different algorithms.

Areas of common exposure should be kept to a minimum to reduce the possibility of both groups being disabled by a single event such as fire, excavation, water leakage, and other such incidents.

1.1.4 Issues Affecting Security

Protection systems shall be designed to isolate only the faulted element, except in those circumstances where additional elements are tripped intentionally to preserve system integrity, or where isolating additional elements has no impact outside the local area.

For faults external to the protected zone, each protection group should be designed either to not operate, or to operate selectively with other groups and with breaker failure protection.

For planned system conditions, protection systems should not operate to trip for stable power swings.

1.1.5 Issues affecting Dependability and Security

The thermal capability of all protection system components shall be adequate to withstand rated maximum short time and continuous loading of the associated protected elements.

Communication link availability, critical switch positions, and trip circuit integrity, shall be monitored to allow prompt attention by appropriate operating authorities.

Bulk power system protection shall take corrective action within times determined by studies with due regard to security, dependability and selectivity.

Protection systems should be no more complex than required for any given application.

The components and software used in protection systems should be of proven quality, as demonstrated either by actual experience or by stringent tests under simulated operating conditions.

Protection systems should be designed to minimize the possibility of component failure or malfunction due to electrical transients and interference or external effects such as vibration, shock and temperature.

Protection system circuitry and physical arrangements should be designed so as to minimize the possibility of incorrect operations due to personnel error.

Protection system automatic self-checking facilities should be designed so as to not degrade the performance of the protection system.

Consideration should be given to the consequences of loss of instrument transformer voltage inputs to protection systems.

Protection systems, including intelligent electronic devices (IEDs) and communication systems used for protection, should comply with applicable industry standards for utility grade protection service. Utility Grade Protection System Equipment are equipment that are suitable for protecting transmission power system elements, that are required to operate reliably, under harsh environments normally found at substations. Utility grade equipment should meet the applicable sections of all or some of the following types of industry standards, to ensure their suitability for such applications:

- IEEE C37.90.1-2002 (oscillatory surge and fast transient)
- IEEE C37.90.1-2002 (service conditions)
- IEC 60255-22-1, 2005 (1 MHz burst, i.e. oscillatory)
- IEC 61000-4-12, 2001 (oscillatory surge)
- IEC 61000-4-4, 2004 (EFT)
- IEC 60255-22-4, 2002 (EFT)
- IEEE C37.90.2-2004 (narrow-band radiation)
- IEC 60255-22-3, 2000 (narrow-band radiation)
- IEC 61000-4-3, 2002 (narrow-band radiation)
- IEEE 1613 (communications networking devices in Electric power Substations)

1.1.6 Equipment and Design Considerations

1.1.6.1 Current Transformers

For protection groups to be independent, they shall be supplied from separate current transformer secondary windings.

Interconnected current transformer secondary wiring shall be grounded at only one point.

Current transformers shall be connected so that adjacent protection zones overlap.

1.1.6.2 Voltage Transformers and Potential Devices

The two protection groups protecting an element shall be supplied from separate voltage sources.

The two protection groups may be supplied from separate secondary windings on one transformer or potential device, provided all of the following requirements are met:

Complete loss of one or more phase voltages does not prevent all tripping of the protected element;

Each secondary winding has sufficient capacity to permit use for protection of the circuit;

Each secondary winding circuit is adequately fuse protected.

The wiring from each voltage transformer secondary winding shall not be grounded at more than one point.

1.1.6.3 Batteries and Direct Current (dc) Supply

DC supplies associated with protection shall be designed to have a high degree of dependability as follows:

No single battery or dc power supply failure shall prevent both independent protection groups from performing the intended function. Each battery shall be provided with its own charger.

Each station battery shall have sufficient capacity to permit operation of the station, in the event of a loss of its battery charger or the ac supply source, for the period of time necessary to transfer the load to the other station battery or reestablish the supply source. Each station battery and its associated charger shall have sufficient capacity to supply the total dc load of the station.

A transfer arrangement shall be provided to permit connecting the total load to either station battery without creating areas where, prior to failure of either a station battery or a charger, a single event can disable both dc supplies.

The battery chargers and all dc circuits shall be protected against short circuits. All protective devices shall be coordinated to minimize the number of dc circuits interrupted.

DC systems shall be continuously monitored to detect abnormal voltage levels (both high and low), dc grounds, and loss of ac to the battery chargers, in order to allow prompt attention by the appropriate operating authorities.

Protection groups dc sources shall be continuously monitored to detect loss of voltage in order to allow prompt attention by the appropriate operating authorities.

1.1.6.4 Station Service ac Supply

On bulk power system facilities, there shall be two sources of station service ac supply, each capable of carrying at least all the critical loads associated with protection systems.

1.1.6.5 Circuit Breakers

No single trip coil failure shall prevent both independent protection groups from performing the intended function. The design of a breaker with two trip coils shall be such that the breaker will operate if both trip coils are energized simultaneously. The correct operation of this design shall be verified by tests.

It is not necessary to duplicate the breaker failure protection itself.

Auxiliary switches may also be required in instances where the fault currents are not large enough to operate the fault current detectors. In addition, auxiliary switches may be necessary for high-speed detection of a breaker failure condition.

1.1.6.6 Teleprotection

Communication facilities required for teleprotection shall be designed to have a level of performance consistent with that required of the protection system, and shall meet the following:

Where each of the two protection groups protecting the same bulk power system element requires a communication channel, the equipment and channel for each group shall be separated physically and designed to minimize the risk of both protection groups being disabled simultaneously by a single event or condition.

Teleprotection equipment shall be monitored to detect loss of equipment and/or channel to allow prompt attention by the appropriate operating authorities. Teleprotection systems shall be provided with means to test for proper signal adequacy.

Teleprotection equipment shall be powered by the substation batteries or other sources independent from the power system.

Except as identified otherwise in these criteria, the two teleprotection groups shall not share the same component.

The use of a single communication tower for the radio communication systems used by the two groups protecting a single element is permitted.

Teleprotection systems should be designed to prevent unwanted operations such as those caused by equipment or personnel.

Two identical teleprotection equipments should not be used in independent protection groups, due to the risk of simultaneous failure of both groups because of design deficiencies or equipment problems. Areas of common exposure should be kept to a minimum to reduce the possibility of both groups being disabled by a single event such as fire, excavation, water leakage, and other such incidents.

Teleprotection systems should be designed to mitigate the effects of signal interference from other communication sources and to assure adequate signal transmission during bulk power system disturbances.

1.1.6.7 Control Cables and Wiring and Ancillary Control Devices

Control cables and wiring and ancillary control devices should be highly dependable and secure. Due consideration should be given to published codes and standards, fire hazards, current-carrying capacity, voltage drop, insulation level, mechanical strength, routing, shielding, grounding and environment.

1.1.7 Environment

Each separate protection group and Teleprotection protecting the same system element shall be on different non-adjacent vertical mounting assemblies or enclosures.

In the event a common raceway is used, cabling for separate groups protecting the same system element shall be separated by a fire barrier.

Means shall be provided to trip all necessary local and remote breakers in the event that a breaker fails to clear a fault as follows:

Breaker failure protection shall be initiated by each of the protection groups which trip the breaker, with the optional exception of a breaker failure protection in an adjacent zone.

Fault current detectors shall be used to determine if a breaker has failed to interrupt a fault.

1.2 WECC PRC 004-WECC-1

Analysis and Mitigation of Transmission and Generation System Misoperations
WECC [Draft] Standard PRC-004-WECC-1
http://www.wecc.biz/index.php?module=pnForum&func=viewtopic&topic=776

1.2.1 Assuring Functional Redundancy

1.2.1.1 Transmission or Generation Protection Misoperations

The WECC Standard PRC-004-WECC-1, “Analysis and Mitigation of Transmission and Generation System Misoperations,” describes operating and reporting requirements following protection and remedial

action scheme (RAS) misoperations on the most critical facilities within the Western Electricity Coordinating Council. Most of these facilities are part of the BES (> 200 kV), though some (rated below 100 kV) are designated as critical by the appropriate Reliability Coordinator. Requirements for other parts of the BES within WECC are covered directly by the NERC Planning Standard III.A (1998, redundancy) and WECC PRC-STD-001 (misoperations) require that all recent operations are reviewed for correctness.

The PRC-004–WECC-1 Standard does not directly require a specific redundancy level. Instead, it defines timing requirements for removal and repair of misoperating Functionally Equivalent Protection or RAS equipment. The owner's and operator's required actions and allowable repair times are a function of the level of redundancy still available following the misoperation.

The term RAS is in common use within WECC, while other areas more commonly use Special Protection System (SPS). The newer term, System Integrity Protection Scheme (SIPS) is beginning to be used to categorize the same types of schemes.

This Standard applies to the owners and operators of all facilities in the United States listed in the Major WECC Transfer Paths in the Bulk Electric System or Major WECC Remedial Action Schemes (RAS) tables. This Standard does not apply directly to Canadian and Mexican facility owners and operators, but is expected to be incorporated as those regulatory authorities agree to be bound by the NERC standards.

Many of the requirements of this Standard have been in place since the late 1990's as part of the Reliability Management System (RMS). The RMS is now being retired since mandatory NERC standards are in place. This new Standard expands some definitions and requirements with corresponding measures of performance. The Standard uses the following terms and definitions:

1.2.2 Functionally Equivalent Protection System (FEPS)

A Protection System that provides performance as follows:

- Each Protection System can detect the same faults within the zone of protection and provide the clearing times and coordination needed to comply with all Reliability Standards.
- Each Protection System may have different components and operating characteristics.

1.2.3 Functionally Equivalent RAS (FERAS)

A Remedial Action Scheme (RAS) that provides the same performance as follows:

- Each RAS can detect the same conditions and provide mitigation to comply with all Reliability Standards.
- Each RAS may have different components and operating characteristics.

1.2.4 Security-Based Misoperation:

A Misoperation caused by the incorrect operation of a Protection System or RAS. Security is a component of reliability and is the measure of a device's certainty not to operate falsely.

1.2.5 Dependability-Based Misoperation:

The absence of a Protection System or RAS operation when intended. Dependability is a component of reliability and is the measure of a device's certainty to operate when required.

No operating restrictions are required when two functionally equivalent protection systems or RAS remain in service. Conversely, when no functionally equivalent protection scheme or RAS is available, the facility must be removed from service or schedules adjusted so that the RAS is not required.

Misoperations may be recognized by operating personnel (i.e. system operators). The Standard allows one day, though such protection system or RAS misoperations are generally fairly obvious and can be identified within a few minutes, e.g. too many or the wrong breakers trip for the actual system fault. This type of misoperation is usually, but not always security-based.

Misoperations may also be detected by protection personnel subsequent to operations that initially appear to be correct. Event record analysis may show an incorrect operation, e.g. the primary scheme operated

as intended, but the backup scheme did not. The Standard allows 20 business days to perform appropriate reviews. These misoperations may be either security- or dependability-based.

Discovery of the problem by either system operators or protection personnel starts two "misoperation clocks." A protection system or RAS that experiences a security-based misoperation must be removed from service within 22 hours to avoid the possibility of repeating misoperations which may be affected by normal daily load cycles. A a dependability-based misoperation (a failure to operate when intended) does not require the non-operating system to be removed from service. For either type of misoperation, the failed system must be repaired or replaced within 20 business days unless at least two functionally equivalent protection systems or RAS remain available. If repair or replacement cannot be accomplished within 20 business days, the unprotected facility must be taken out of service or schedules adjusted so that the RAS is not required. Figure A-1 illustrates these requirements.

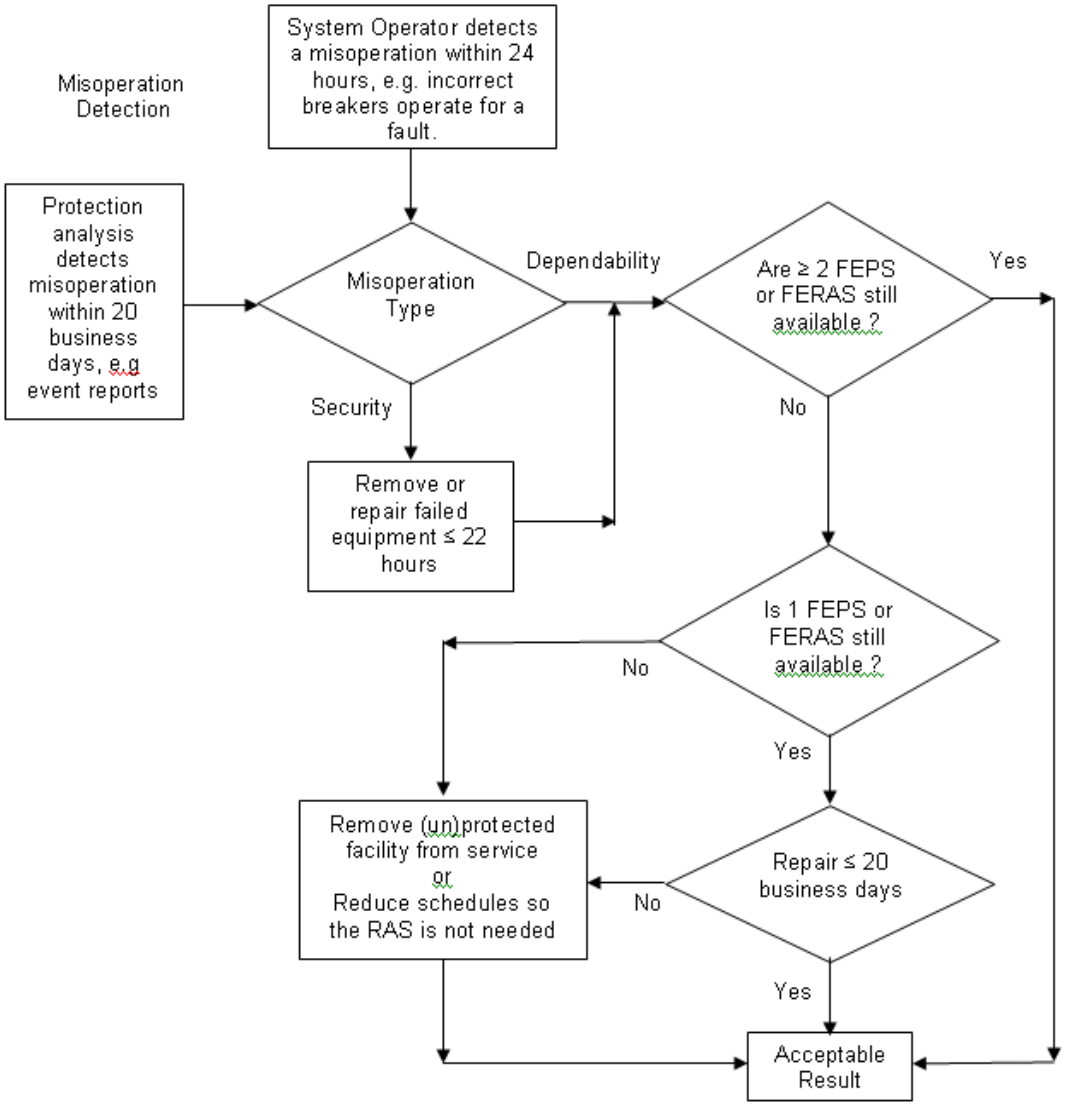


Figure A-1. WECC Major path protection and RAS reliability and redundancy requirements for Functionally Equivalent Protection Systems (FEPS) and Functionally Equivalent Remedial Action Schemes (FERAS).

1.3 WECC Remedial Action Scheme Design Guide

The WECC (Western Electricity Coordinating Council) Guide for RAS (Remedial Action Scheme) design defines redundancy as “to allow removing one scheme following a failure or for maintenance while keeping full scheme capability in service with a separate scheme”. While this definition was written for RAS and SPS (Special Protection Scheme) systems, it was born from long standing protective relay practices. Therefore, many of the concepts addressed in the RAS Design Guide seem applicable to protective relay systems as well. The Guide encourages full redundancy, but focuses on minimum requirements based on consequences, availability of effective backup protection, criticality, and general good practice.

Redundancy requirements cover all aspects of design. These include detection, arming, power supplies, communication, logic controllers, and trip close circuits. While some of these systems are generally not part of a protection scheme, the intent is that any single point of failure will not cause the system to not operate as intended. Protection systems usually excluded from redundancy requirements include station battery, VT and CT devices, and communication antenna towers.

To be an acceptable alternative to full redundancy the scheme design should meet the following criteria:

- Adequate backup should allow overtripping when the communication system is non-redundant.
- All critical alarms should be monitored and annunciated
- The electric system can be adjusted so that the RAS need not be armed.
- Dispatchers are trained to immediately adjust the electric system so that RAS will still meet operational requirements. For a stability limited system within 10 minutes, and for a thermally limited system within 30 minutes.

Typical protection schemes operate at speeds that are too fast for operator intervention, so the last two bullet points would not apply to relay systems used for equipment protection.

Adequate backup protection is a minimum requirement for RAS. If operation of the backup system results in a situation where any one single component failure will not violate the RAS performance requirements, then full redundancy may not be required. Typically, however, logic systems will require full redundancy to assure meeting minimum performance requirements. The designer should consider the power system effects if the redundant “as armed” control actions do not match. RAS controller should at least provide a “mismatch alarm”, or have a two out of three type voting scheme. This type of RAS is mostly used on large, critical schemes.

If one controller or component of an otherwise redundant scheme is not available due to failure or maintenance, some conditions exist under which the system can continue to operate. These conditions generally involve some kind of system de-rating and/or adjustment.

1.4 ERCOT

ERCOT Operating Guide section 7: “Disturbance Monitoring and System Protection” dated October 1, 2007, specifically section 7.2.2 System Protective Relaying Design and Operating Requirements for ERCOT System Facilities states that Facility owners shall periodically review their protective relaying systems including the need for redundancy. Per the guide, “Protective systems must be sufficient to meet the system performance levels as defined in NERC Planning Standard I.A. and the associated Table I.” The guide also states “where redundant protective relaying systems are needed separate ac current inputs and separately fused dc control voltages shall be provided with protective relaying upgrades.” No other section of the guide specifically defines redundancy but the following statements addresses requirements or makes suggestions for the use of redundancy.

Section 7.2.5.1: Requirements and Recommendations for ERCOT System Facilities General Protection Criteria, Dependability, “all elements of the ERCOT System operated at 100 kV or above shall be protected by two protective relay systems. Each protective relay system shall be independently capable of detecting and isolating all faults thereon.”

“The protective relay system design should avoid the use of components common to the two protective relay systems.”

Breaker failure protection need not be duplicated.

Section 7.2.5.2 Equipment and Design Considerations, Batteries and Direct Current Supply states that two batteries with their own charger should be used but allows the use of one battery with two separately protected branches. “For a new facility, two batteries shall be required in locations that remote backup clearing of lines and substation faults is not achieved. Where only one battery is used, remote backup clearing of line and substation faults is required.”

Section 7.2.5.2 Equipment and Design Considerations, AC Auxiliary Power states, that “there should be two sources of station service AC supply, each capable of carrying all the critical loads associated with the protective relay system.”

Section 7.2.5.2 Equipment and Design Considerations, Circuit Breakers states “two trip coils, one associated with each protection system, shall be provided for each operating mechanism.”

Section 7.2.5.3 Equipment and Design Considerations, Transmission line Protection states, “each of the two independent protective relay systems shall detect and initiate action to clear any line fault without undue system disturbance.” The transmission line protection should consist of :

- “Primary phase and ground protection over a communications channel.
- Backup relaying with at least two zones of phase protection.
- Backup relaying with at least two zones of ground protection, or backup relaying with ground directional overcurrent relaying (time delay and instantaneous)”

Section 7.2.5.2 Equipment and Design Considerations, Transmission Station Protection states, “each zone in a station shall be protected by two independent protective relay systems. For Zones not protected by line protection, at least one of the two protective relay systems shall be a different type.”

Section 7.2.5.2 Equipment and Design Considerations, Breaker Failure Protection states that duplicate breaker failure protection is not required.

Section 7.2.5.2 Equipment and Design Considerations, Generator Protection states, “Generator faults shall be protected by more than one protective relay system.”

Section 7.2.5.2 Equipment and Design Considerations, Automatic Under-Frequency and Under-Voltage Load Shedding Protection Systems “need not be duplicated”

1.5 IEEE/PSRC Guides

1.5.1 Breaker Failure Guide

C37.119-2005 addresses redundancy as follows:

1.5.1.1 Backup protection considerations

An ideal backup protection scheme should be completely independent of the primary protection, and based on prior discussion, it can be seen that local backup protection is faster and more effective at limiting damage than remote backup protection schemes. To provide ideal local backup protection it would then be necessary to have physically and electrically independent relays fed by physically separate instrument transformers that use redundant but separate battery systems to operate a system where each circuit breaker had an equivalent backup circuit breaker immediately electrically adjacent. While these features may be included in the design of any given substation, the cost and space requirements of ideal local backup protection can be limiting and the use of backup breakers can be generally prohibitive.

A reasonable level of local backup protection is accomplished by employing fully duplicated tripping systems, independent and galvanically isolated, operating in a one-out-of-two tripping arrangement, with

each tripping system initiating circuit breaker failure protection. Local breaker backup in the form of breaker failure protection can then be depended upon to fulfill the function of the independent breaker by operating adjacent breakers to clear the fault.

In general, where local breaker failure relaying is deemed required, protection systems failure should not be a cause of breaker failure. That is, redundant relaying systems, as independent as practical, should be provided. Each system may operate separate or both breaker trip coils, either directly or indirectly.

1.5.1.2 Summary

Due to its severity, a trip initiated by the breaker failure protection must only be performed if absolutely necessary. Every effort must first be made to successfully trip the circuit breaker. Redundancy in the breaker tripping paths should be employed.

1.5.1.3 Single-phase re-trip logic

When single-phase tripping is applied, some utilities may choose to use one set of trip coils for single-phase tripping and another set for three-phase tripping. Both the primary and secondary line protection sets are connected to trip only one set of trip coils. Breaker manufacturers provide the second set of trip coils as a redundant means to actuate the breaker tripping mechanism. The re-trip feature is then relied upon to provide necessary redundancy for control circuit and trip coil failures. The breaker failure relay must measure a separate initiate for each phase and must provide three individual re-trip outputs. Where individual contacts trip the breaker three-phase, such as a lockout relay, then a fourth initiate input and a three-phase re-trip output may be included in the scheme. On systems where delayed tripping is undesirable, no intentional delay is added to the re-trip function.

1.5.1.4 Multiple schemes within a relay

With the use of programmable relays, several breaker failure schemes can be programmed with the bypass scheme in one relay. One such application is as shown in Figure A-2.

The first scheme [comprised of a control timer, AND gates 1 and 2, and breaker failure timer (62-1)] is similar to conventional schemes. Though this scheme will not delay operation in breaker-and-one-half or ring bus configurations, it is disabled after the control timer times out and the initiating contact fails to reset. The second scheme is comprised of AND gate 4 and breaker failure timer (62-2), and will provide redundancy to the first scheme. Both breaker failure timers are set to the same delay. The third scheme comprised of AND gate 3, will initiate a breaker failure output directly without any additional time.

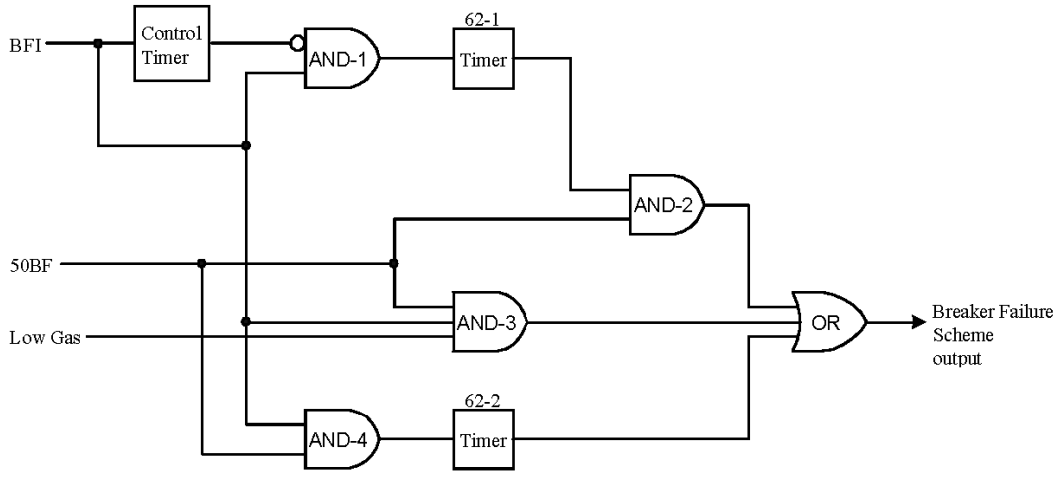


Figure A-2. Multiple scheme breaker failure

1.5.1.5 Dual breaker alternative

In those cases where stability studies show that the critical clearing time is less than the shortest backup clearing time attainable with high-speed breaker failure protection schemes, the only solution may be to install two identical breakers in series, with both breakers being tripped simultaneously by the protection schemes. With this arrangement, and fully redundant protection schemes, instrument transformers, and control power sources, it can be assumed that at least one of the breakers will successfully interrupt the fault. Thus, the total clearing time will be the same as the primary clearing time, and no breaker failure scheme is necessary.

1.5.1.6 Breaker failure actions

Depending on the application and the specific practices of the company or user, a breaker failure operation can initiate the following actions:

- Trip each electrically adjacent breaker in the same substation regardless of voltage level. This should be accomplished through either a single dedicated breaker failure auxiliary relay or through two independent auxiliary relays, one or both of whose primary functions may be associated with another protection scheme (typically a differential scheme). Redundant auxiliary tripping relays allow a single relay scheme to be unavailable without affecting the operation of the breaker failure relaying.
- Trip the failed breaker. This action may be considered redundant, particularly if “re-trip” logic is used in the scheme.

1.5.2 Local backup relaying protection, transaction paper I

IEEE Committee Report, “Local Backup Relaying Protection”, IEEE Transactions on Power Apparatus and Systems, Vol. PAS-89, No. 6, July/August 1970, pp, 1061-1068.

This paper would be more aptly titled “Local Protection System Redundancy”. The paper is a survey of 253 relay engineers (48% response rate) with questions concerning protection system redundancy applied locally. The paper discusses:

- Current and Potential Source Backup
- Relay Backup
- For line protection
- For transformer protection
- For bus protection
- For DC source (battery) protection
- The survey also attempted to cover relay backup for generator protection, but the results were not usable
- Breaker-Failure Backup

The abstract reads: “Results of a survey and symposium on local backup relaying protection is presented. The survey covers the responses of 121 relay engineers to questions pertaining to their present-day [late 1960s] preferences on duplicate relays, dc and ac sources, control power, and breaker failure protection. The symposium offered the opportunity to present detailed philosophy, circuit configuration, and explanations to supplement the statistics compiled in the survey.”

Some results of this late-1960s survey are listed as follows:

Table A-I. Percentage of responders with duplicate (redundant) equipment per voltage level

Equipment		**Voltage level**		
		66-100 kV	100-300 kV	>300 kV
Current sources		18	52	94
Potential sources		2	9	28
Line protection system	Primary and backup	38	73	57
	Redundant	2	9	43
Transformer protection	Primary and backup	40	58	57
	Redundant	8	10	30
Bus protection	Primary and backup	12	18	16
	Redundant	4	5	29
Battery system		6	8	20

1.5.3 Local backup relaying protection, transaction paper II

L.F. Kennedy and A.J. McConnell, "An Appraisal of Remote and Local Back-up Relaying", AIEE Transactions, Vol. 76, pp. 735-741, October 1957

The purpose of this paper was to: "…analyze the performance on modern [sic] systems of both remote and local back-up relays with particular emphasis upon the problem of maintaining good service even in the event of a failure of the primary protective system to operate as planned."

At the time of writing, remote backup was still the most generally used form of backup. But the paper proposed backup protection be abandoned because it could not meet functional requirements as follows: 1) Recognize the existence of all faults; 2) Recognize the failure of primary equipment to clear as planned, and a) initiate tripping of minimum number of breakers to clear the fault; b) operate in minimum time required to avoid loss-of-synchronism.

The following conclusions are presented in the paper:

- Remote Backup: "Back-up protection that can fail to clear a fault, that can drop an entire station unnecessarily, that is slow, and that can drop loads unnecessarily, cannot be considered to be adequate. Remote backup is in all those categories."
- Relay Backup: "Relay back-up, even the equivalent of two first-line systems, is inadequate. Trouble may lie beyond the relays (trip circuit, etc) [or may be in the information supplied to the relays]."
- Breaker Backup, First-Line Relays with Timer: "Back-up protection that can fail cannot be considered to be adequate. Breaker backup, consisting of only the first-line relays and a timer, is inadequate because the failure may be in the relays or in the information supplied to the relays."
- Breaker Backup with Separate Relays: "Breaker backup, with separate back-up relays, provides sound back-up protection. However, its operating time is slower than necessary. Also, although it provides a measure of relay backup, failure of the first-line relaying (or of the information supplied to it) results in unnecessary tripping of back-up breakers. Relay backup trips only the breakers on the faulted circuit."
- A local back-up system as described in this paper, using for backup an entirely separate group of relays from that used for first-line protection, will meet all functional requirements for back-up protection [and only for ~20% more cost]."

The system described in the paper is for transmission lines and advocates dual primary systems fed from [ideally] separate current and potential supplies. The paper assumes separate batteries would not be feasible, but separate fusing would be feasible.

1.5.4 Line protection guide (1999)

The PSRC line protection guide is addressing redundancy in the following sections:

1.5.4.1 "Criticality" of the line

One of the more significant determinants in transmission line protection is the criticality of the line to the system. This determination will define such considerations as the desired level of reliability and the role cost will play in the design. A system's most critical lines may justify redundancy in protection, communication, and perhaps even dc auxiliary supply. Less critical lines may be adequately protected with step distance or overcurrent systems.

The determination of criticality could be based on voltage level, line length, proximity to generation sources, load flows, stability studies, customer service considerations, or other factors.

1.5.4.2 Failure modes

Protective relaying scheme design should minimize the effects of "single-point failures." A single-point failure is any one failure of a relay, breaker, dc auxiliary supply, communication system, or any other component of the overall protective system which results in defeating the intended functionality of the scheme. Redundancy or duplication of protection, local backup protection, remote backup protection, and duplication of other system components are used to minimize the effects of single-point failures.

1.5.4.3 Redundancy

Redundancy for transmission line protection can be provided by a number of methods, each with varying levels of complexity, benefits, and costs. These methods include two or more duplicate protection schemes, local backup, remote backup, and the duplication of dc sources, CTs, VTs, and breaker trip coils.

Different, or perhaps identical, protection systems operating in parallel is a common practice on most transmission lines. Independent operating principles of these different protection systems are often considered important. The degree of duplication in dc sources, CTs, VTs, and the application of interrupting devices is usually determined by the importance of the application and the consequences of single contingency failures.

1.5.4.4 Multiterminal lines

Transmission lines with more than two main terminals offer additional challenges for correctly detecting faults on the line, primarily because of radical changes in fault current levels and apparent impedances as one or more terminals are opened. The system configuration may result in sequential tripping to protect these lines. If sequential tripping results, care should be taken concerning the redundancy of the relay design, because failure of a relay at one terminal may prevent detection of the fault at another terminal. Sequential tripping also delays fault clearing. Pilot schemes may eliminate sequential tripping. .

1.5.4.5 Local backup

The basic form of local backup relaying is the inclusion of redundancy in the protection scheme. This redundancy can range from the use of additional zones of independent relays to full duplication of the protective scheme, including CTs, VTs, battery, and trip circuits. Typically, the higher the voltage level, the greater the redundancy applied. The use of local backup reduces the long delays and the loss of selectivity that occur with the operation of remote backup relaying. The tradeoff occurs in extra cost for the additional equipment.

1.5.5 Justifying pilot protection on transmission lines

The WG D8 report addresses redundancy as follows:

1.5.5.1 Reasons pilot is unavailable

Some relay systems become completely disabled (not reverting to non-pilot stepped distance) when pilot is turned off. For this reason, some designers chose to install two redundant relay systems (with an additional electromechanical backup set) to allow pilot to be switched off one set.

1.5.5.2 Line current differential relays and their built-in or external pilot-aided distance backup

If the distance protection is located in a separate relay and is pilot-aided, it can have its own communication channel if it is necessary for complete redundancy or still share the same communication channel with the line current differential protection. An obvious advantage of this design is eliminating the common hardware failures. A drawback of implementing the primary and backup protection functions in

the separate relays is additional cost of the hardware and the second communication channel when it is required.

1.5.5.3 Criteria to Determine Number of Pilot Systems Required

The need for two or three pilot protective systems will be determined by protection system owners based on their level of confidence in the systems employed and the number of contingency failures taken into account.

Appendix B - National Grid's Requirements for Physical Separation

National Grid has a specific document, Physical Separation of Protection Systems at New England Bulk Power Stations that is used in contracts to guide contractors in designing protection schemes having to meet NPCC Bulk Power System Protection Criteria.

This standard document is provided for reference only and to illustrate how physical separation plays a role for redundancy in the protective relay system. It covers requirements not discussed in detail in the report as the report focuses on redundancy measures for the protective relays in particular and not the specific physical separation requirements provided in National Grid's standard document. However, the standard document is included in the report as an example that protective relaying redundancy is just one part of the overall redundancy considerations for Power System Protection.

This standard documents National Grid's requirements for the physical separation of redundant protection systems for New England bulk power system (BPS) stations.

1.0 INTRODUCTION

1.1 This document provides National Grid's requirements for the physical separation of redundant protection systems for New England bulk power system (BPS) stations. The purpose of physical separation is to increase protection system dependability by eliminating common points of failure between systems, which may include but are not exclusive to fire, contamination, dig-in or mechanical damage. Physical separation of redundant protection systems is also a requirement of the *NPCC Bulk Power System Protection Criteria Document A-5* for BPS facilities. In the event that requirements of the NPCC Document A-5 are deemed to be stricter than the requirements of this standard, the requirements of the NPCC Document A-5 shall prevail.

1.2 The term dependability, as used in this standard, refers to the degree of certainty that protections will operate when required to operate. Whereas security refers to the degree of certainty that protections will not operate when not required to operate.

2.0 GLOSSARY OF TERMS

The following definitions for various terms used through this standard are derived from the *NPCC Glossary of Terms Criteria Document A-7*.

Bulk power system — the interconnected electrical systems within northeastern North America comprising generation and transmission facilities on which faults or disturbances can have a significant adverse impact outside of the local area. In this context, local areas are determined by the Council members.

Component — refers to components of equipment or protection systems rather than elements of a power system. See Element.

Element — any electric device with terminals that may be connected to other electric devices, such as a generator, transformer, circuit, circuit breaker, or bus section.

Energize — to make a piece of equipment or circuit alive.

Fault — an electrical short circuit.

Protected element — the power system element protected by the subject protection system. Examples: Line, bus, transformer, generator.

Protection — the provisions for detecting power system faults or abnormal conditions and taking appropriate automatic corrective action.

Protection group — a fully integrated assembly of protective relays and associated equipment that is designed to perform the specified protective functions for a power system element, independent of other groups.

Notes:
(a) Variously identified as Main Protection, Primary Protection, Breaker Failure Protection, Back-Up Protection, Alternate Protection, Secondary Protection, A Protection, B Protection, Group A, Group B, System 1 or System 2.
(b) Pilot protection is considered to be one protection group.

Protective relay — a relay that detects a power system fault or abnormal condition and initiates appropriate control system action.

Relay — an electrical device designed to respond to input conditions in a prescribed manner and after specified conditions are met to cause contact operation or similar abrupt change in associated electric control circuits. (Also: see protective relay).

Short circuit — an abnormal connection (including an arc) of relatively low impedance, whether made accidentally or intentionally, between two points of different potential. Note: The term fault or short-circuit fault is used to describe a short circuit.

The following definitions for various terms used through this standard are adapted from IEEE Std. 384-1992 *IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits* for applicability to protective relay applications.

Associated circuits — Circuits that are not physically separated or are not electrically isolated from a particular protection group. See protection group.

Barrier — a device or structure interposed between protection groups or between a protection group's equipment or circuits and a potential source of damage to limit damage to the protection group to an acceptable level.

Isolation device — a device in a circuit that prevents malfunctions in one section of a circuit from causing unacceptable influences in other sections of the circuit or other circuits. Examples of isolation devices include fuses, circuit breakers and diodes.

Redundant equipment or system — equipment or system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function regardless of the state of operation or failure of the other.

Separation distance — space that has no interposing structures, equipment, or materials that could aid in the propagation of fire or that could otherwise disable redundant systems or equipment.

3.0 APPLICABILITY

3.1 New Facilities

This standard shall apply to all new BPS facilities.

3.2 Existing Facilities

Systems at existing facilities may not be sufficiently separated to comply with this standard. Following are a number of specific situations involving existing facilities.

3.2.1 Planned Upgrades to Existing Facilities

These situations will most often be encountered by asset replacement strategies like relay replacement programs. An assessment shall be done and accepted by the Manager of Protection Engineering as to whether particular upgrades to existing protection systems in BPS facilities shall comply with this standard or would follow the separation practices that previously existed for that facility provided those practices are not in conflict with the objectives of this standard.

3.2.2 Facility Classification Upgraded to BPS

These situations arise from system configuration changes such generation and transmission infrastructure additions. This standard shall apply to protection systems in facilities whose facility classification is upgraded to BPS. Such a classification change would likely require the development of a mitigation plan to achieve compliance with this standard.

3.2.3 Additions to BPS Facilities

This standard shall apply to protection systems for BPS elements added to an existing BPS facility. It is recognized that separation may not be practical at points that tie with existing protection schemes, such as connecting with existing cable trays or trenches. Circumstances where this standard cannot be met must be brought to the attention of the Manager of Protection Engineering at the scoping phase for evaluation as a possible technical exception.

3.2.4 In-Kind Replacement of BPS Equipment

This standard shall not apply to the replacement of a BPS element or protective relay if it is replaced “in kind” as a result of an in-service failure. Existing practices shall apply. Otherwise, the upgrade is a planned upgrade subject to the provisions of the *Planned Upgrade to Existing Facilities,* section 3.2.1 of this standard.

4.0 SYSTEM DESIGNATIONS

4.1 Designations for independent redundant protection systems shall be System 1 and System 2. Non-independent systems may be designated as Main and Backup.

5.0 OPEN YARD SUBSTATION LAYOUT

5.1 Separate cable trench systems shall be established for System 1 and System 2. The substation layout shall facilitate separate routing of conduit and trench systems for System 1 and System 2 from the control house to all breaker bays, transformers and other equipment. Future bay or transformer additions shall be taken into account if known. System 1 and System 2 cable trenches shall be separated by a horizontal distance of not less than 3ft. Usage of a common trench with a dividing barrier shall be avoided. Figures B-1 and B-2 illustrate cable trench routing for typical breaker-an-a-half substation yards.

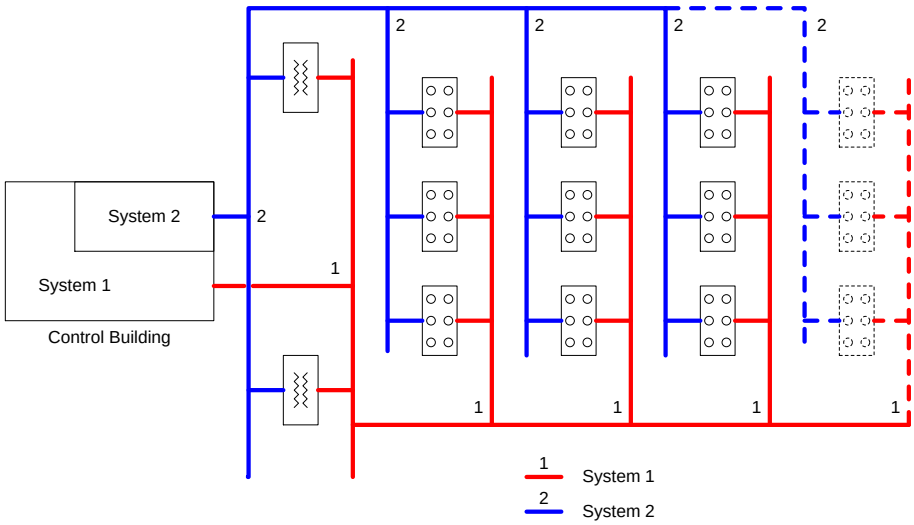


Figure B-1

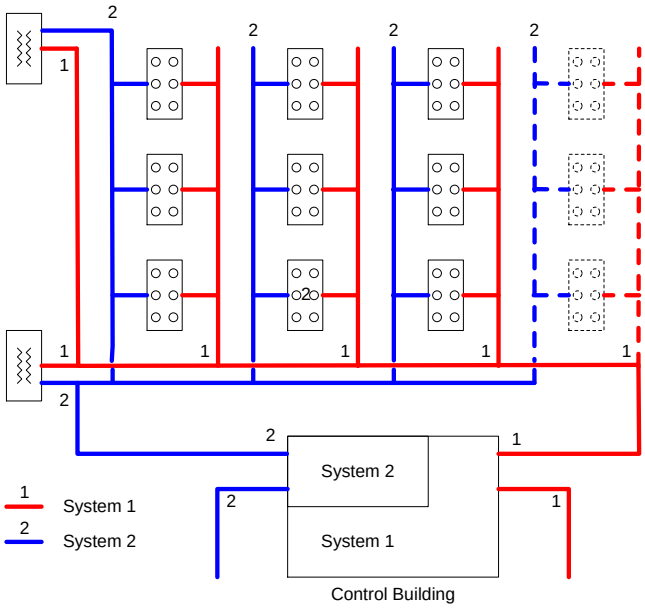


Figure B-2

5.2 System 1 and System 2 cable trenches shall not cross unless access to a power system element is prevented by physical arrangement. Where such trench crossings are unavoidable, they shall do so by one system trench being fully enclosed and passing underneath the second trench with vertical separation not less the distances established in the *Cable Tray and Conduit Systems* section of this standard. Trenches with earth bottoms shall be considered as having an open configuration for the purpose of determining the appropriate separation distances.

6.0 GIS SUBSTATION LAYOUT

6.1 Separate cable trench systems shall be established for System 1 and System 2. The substation layout shall facilitate separate routing of conduit and trench systems between breaker bays, transformers and other equipment. If the control room is not attached to the switch house,

separate cable trench systems shall be used from the control room to the switch house. Future bay or transformer additions shall be taken into account if known. Usage of a common trench with a dividing barrier shall be avoided.

6.2 Figure 9-3 illustrates cable trench and tray routing for a portion of a typical GIS breaker-an-a-half switch house layout. Where system 1 and system 2 enter the switch house they shall enter the building via separate entrance ways. System 1 cables run from the control house to breaker local control cabinets (LCCs) via trench and from LCCs to individual breakers via trench. System 2 cables run from the control house to LCCs via overhead cable tray and from LCCs to individual breakers via trench and conduit. In the case where the control room is separate from the switch house, then sections 5.1 and 5.2 shall apply for the portion between control room and switch house. Where trench crossings are unavoidable, they shall do so with formed and sleeved passages having a vertical separation not less the distances established in the *Cable Tray and Conduit Systems* section of this standard.

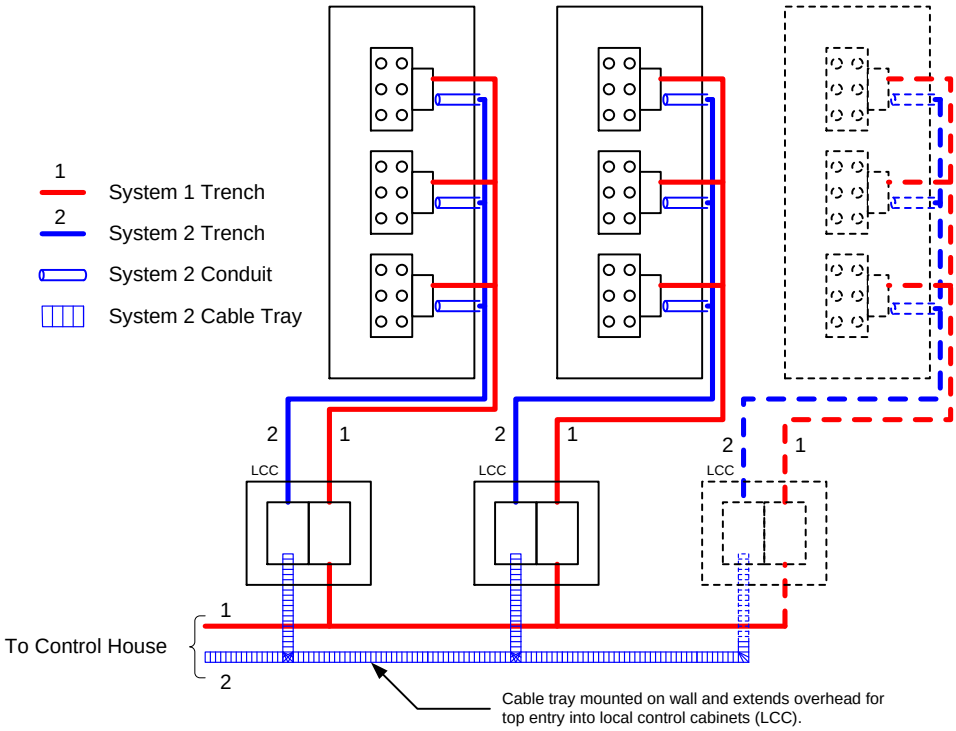


Figure B-3

7.0 CONTROL HOUSE ARRANGEMENT

7.1 System 1 and System 2 protection groups shall be housed in separate control rooms separated by a 2-hour fire rated solid wall with self-closing doors for the passage of personnel and equipment. Each auxiliary supporting feature such as heat, air conditioning and control room ventilation shall be assigned to the same protection group it supports and shall be subject to the same physical separation requirements as the protection systems it supports.

7.2 Each cable tray or conduit penetrating the solid wall barrier for necessary cross-connections shall be assigned to the same protection system it supports and shall be clearly labeled with the supported system on both sides of the solid wall barrier. All System 1 wall penetrations shall be

grouped together and all System 2 wall penetrations shall be grouped together with the two groups being separated. As far as is practical, the groups of System 1 and System 2 wall penetrations shall be placed at opposite ends of the solid barrier wall to maximize physical separation.

7.3 The mounting of DC switchboards back to back on each side of the wall separating the system 1 and system 2 rooms shall be avoided.

7.4 The intent of these separation requirements is to minimize the chance that an event such as fire, storm, chemical contamination, excavation, or other construction activities from becoming a common failure mode between systems.

8.0 CABLE TRAY AND CONDUIT SYSTEMS

8.1 When cable trays and conduits approach an Element such as transformers, breakers, etc., they shall approach on opposite sides or from top and bottom. Where this is not possible or for other conditions where cable trays and conduits must pass in closer proximity, the minimum separation distances in Table B-I shall apply.

Table B-I

Configuration Type	Minimum Separation Distance
Open to open configurations	$D_H \geq 6$ in (Horizontal) $D_V \geq 12$ in (Vertical)
Enclosed to enclosed configurations	$D_H \geq 1$ in (Horizontal) $D_V \geq 1$ in (Vertical)
Enclosed to open configurations	$D_H \geq 6$ in (Horizontal) $D_V \geq 12$ in (Vertical)

8.2 Cable trays with open bottoms and tops shall be considered to be an open configuration. Cable trays with solid bottoms and tops shall be considered to be an enclosed configuration. Conduits shall be considered to be an enclosed configuration. The above distances are derived from distances established in IEEE Std. 384-1992 *IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits* Table 2 for interactions in limited hazard areas involving power circuits with cable sized no larger than 2/0 AWG. Figures B-4 and B-5 are examples of typical cable tray and conduit configuration geometries.

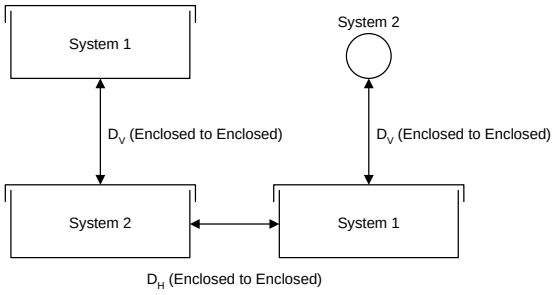


Figure B-4

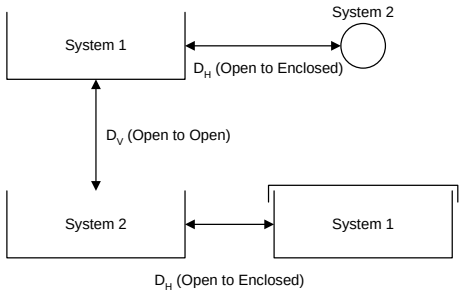


Figure B-5

9.0 CIRCUIT BREAKERS

9.1 Circuit breakers used on the BPS shall be equipped with two independent trip coils. The breaker shall operate if either trip coil is energized or if both trip coils are energized simultaneously.

9.2 System 1 and System 2 relay and control wiring shall use breaker auxiliary contacts from physically separate contact block assemblies. All auxiliary contact blocks shall be labeled as being associated with either System 1 or System 2.

10.0 STATIONARY BATTERIES AND BATTERY CHARGERS

10.1 There shall be two independent stationary battery and charger systems, one for System 1 and one for System 2. Usage of a standalone battery charger without batteries is not acceptable as a second DC system. No single battery or DC power supply failure shall prevent both independent protection groups from performing their intended functions.

10.2 Each of System 1 and System 2 station batteries shall have sufficient capacity to supply the total DC load of the station. That is, each battery capacity sizing shall take into account continuous and momentary ampere loadings of both Systems 1 and 2. For each battery momentary amps, the end of duty cycle requirement for worst case tripping shall include both System 1 and System 2 trip coil currents plus related relays.

10.3 Each of System 1 and System 2 battery chargers shall have sufficient capacity to supply the total DC load of the station. That is, each charger shall be rated to supply both System 1 and System 2 continuous loads plus the charging current for one battery.

10.4 The two battery systems shall be interconnected via a matrix of transfer switches on the DC side of the battery chargers, which shall enable manual transfer of DC load between systems while insuring that the failure of a single switch cannot disable both battery systems. The transfer switch arrangement for a typical pair of redundant battery systems is illustrated in Figure B-6.

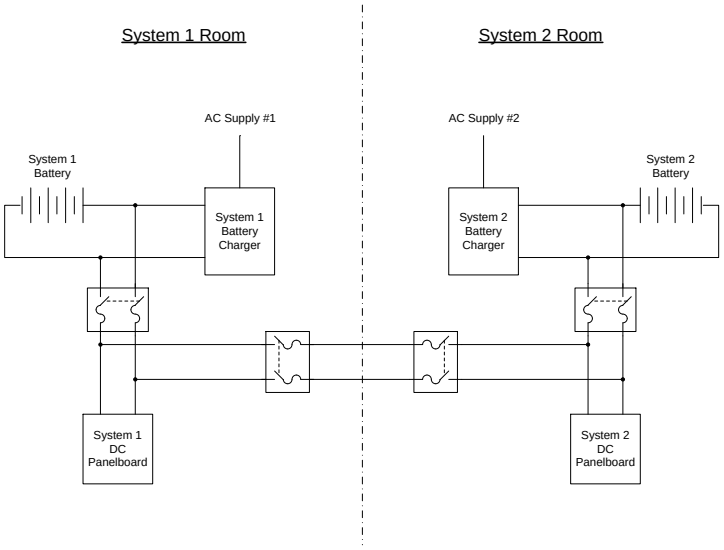


Figure B-6

11.0 RELAY AND CONTROL CABINETS

11.1 Relay and control cabinets located in the System 1 control room shall be associated with System 1 and relay and control cabinets located in the System 2 control room shall be associated with System 2. Devices, wires and cables in a System 1 relay and control cabinet associated with System 2 shall be separated and isolated from all System 1 devices, wires and cables. System 1 devices, wires and cables in a System 2 cabinet shall be similarly separated and isolated.

11.2 Separation distances defined in the *Cable Tray and Conduit Systems* in section 8 of this standard shall apply to devices, cables and wires within and entering relay and control cabinets with the exception of devices, such as relays and switches, on which wires from both systems must land.

11.3 Figure 9-7 illustrates System 1 and System 2 trip circuits for a typical 3-pole breaker. All devices and wires are associated with either System 1 (red) or System 2 (blue). The determination of correct system association is made by determining which system's battery energizes the particular device or wire. This method of analysis makes it easy to determine "crossover" wiring and devices which bridge the two systems and on which wiring from both systems must land.

11.4 In the event there are unavoidable cross connections between Systems 1 and 2, the devices, terminal blocks and wires associated with the other system shall be separately grouped in the cabinet. For example, System 2 devices, terminal blocks and wires in a System 1 relay and control cabinet shall be grouped separately on the right side of the cabinet (as viewed from the rear) and shall be separated from System 1 by at least 6 inches. System 2 wires entering a System 1 cabinet shall be grouped together and shall be separated from System 1 cables by at least 6 inches. The System 2 grouping shall preferably occur at the top of the cabinet right side to minimize the run of System 2 cable conductors in parallel with System 1 cable conductors within the cabinet. Similarly, System 1 devices, terminal blocks and wires in a System 2 cabinet shall be separately grouped and physically separated.

11.5 System 1 switchboard positive and negative buses (SWBD P1 and SWBD N1) shall not energize any wires entering a System 2 cabinet unless they are electrically isolated via fuses or circuit breakers. A fault on System 1 wires and devices inside a System 2 cabinet shall not disable the System 1 switchboard positive and negative supply. Figure B-7 illustrates the usage of a separate set of DC buses (XDC P1 and XDC N1) to achieve isolation of System 1 wires entering

a System 2 cabinet. Similarly, System 2 switchboard positive and negative buses (SWBD P2 and SWBD N2) shall not energize any wires entering a System 1 cabinet unless they are electrically isolated via fuses or circuit breakers. A fault on System 2 wires and devices inside a System 1 cabinet shall not disable the System 2 switchboard positive and negative supply.

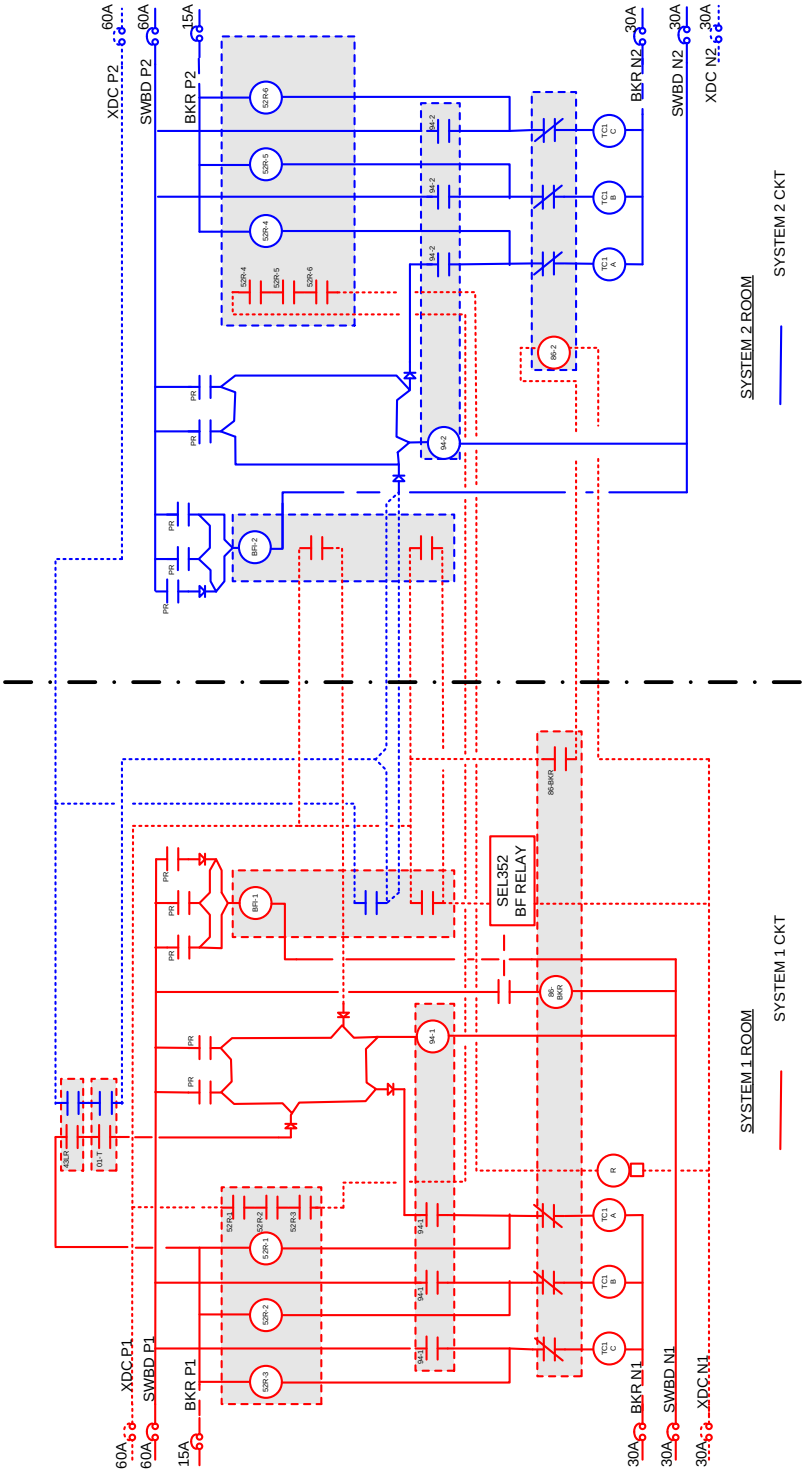


Figure B-7

12.0 INSTRUMENT TRANSFORMERS

12.1 CTs

12.1.1 Physical separation for all CT wiring shall be in accordance with sections 5, 6 and 7 of this standard. There shall be separate junction boxes for System 1 and System 2 CT wires. Physical separation of junction boxes shall be as per the distances established in the *Cable Tray and Conduit Systems,* section 8 of this standard.

12.1.2 System 1 protections shall be connected to the outermost CTs defining any zone of protection. System 2 protections shall be connected to the 2nd outermost CTs. Exceptions to this convention may include a previously existing convention in place at an existing substation. Exceptions are discouraged, if necessary they shall be clearly noted as exceptions on affected Relay and Metering Oneline as well as Current and Voltage drawings.

13.1 VTs

13.1.1 Usage of a single set of VTs at a given measuring point is allowable provided the VTs have two electrically isolated secondary windings. Secondary windings shall be designated at Windings X and Y. Secondary leads from Windings X and Y shall be run in physically separate trench, conduit and cable tray systems as defined sections 5, 6, 7 and 8 on this standard. There shall also be separate junction boxes for System 1 and System 2 VT wires. Physical separation of junction boxes shall be as per the distances established in the *Cable Tray and Conduit Systems* section 8 of this standard.

13.2.1 System 1 protections shall be connected to the winding designated as "Winding X." System 2 protections shall be connected to the winding designated as "Winding Y." Exceptions to this convention may include a previously existing convention in place at an existing substation. Exceptions are discouraged. If necessary, they shall be clearly noted as exceptions on affected Relay & Metering Oneline and Current & Voltage drawings.

13.0 REVISION HISTORY

Version	Date	Description of Revision
1.0	03/06/07	First version of new document