IEEE PSRC Working Group Report
Final Report 7.3 – March 10, 2007

Processes, Issues, Trends and Quality Control of Relay Settings

Chairperson: Steven A. Kunsman

Vice Chairperson: Gary L. Kobet

This report has been prepared by the IEEE PSRC System Protection Subcommittee Working Group C3. The following persons have made contributions to this report:

Alex Apostolov, Ken Birt, Ron Beazer, Oscar Bolado, Art Buanno, Patrick Carroll, Rick Cornelison, Arif Cubukcu, Hyder DoCarmo, Kevin Donahoe, Dale Fredrickson, Ashok Gopalakrishnan, George Gresko, Bryan Gywn, Mike Jensen, Steven Kell, Gary Kobet, Steven Kunsman, Federico Lopez, Don Lukach, Tony Napikoski, Jim O'Brien, Frank Plumptre, Russell Patterson, Greg Sessler, Bill Strang, Jon Sykes, Eric Udren and Solveig Ward.

Table Of Contents

1. Purpose

The purpose of this report is to address present-day issues utilities have with developing, checking, applying, and maintaining quality relay settings. Issues discussed include the complexity of relay settings; multiple setting groups; documentation handling; database consistency; and the archival of relay setting calculations, setting sheets, and test records. Also addressed are triggers for periodic review of issued protection device settings.

These issues are addressed relative to present industry practices by utilities as prescribed by their own internal processes (documented or undocumented), as well as practices (if any) dictated by national and regional reliability councils.

2. Introduction

The evolution of a system often includes an increase in the complexity of that system. This holds true for the evolution of the protection and control system of the modern utility substation. A large part of this increased complexity can be found in the application and continuing operation of modern protection devices. Issues raised by these devices include the increased number of integrated functions, the interoperability of devices in multi-vendor installations, tracking different firmware versions and the use of different device configurations all applied to the numerous substation configurations. Upcoming standards (e.g., IEC 61850) begin to address the compatibility and interoperability issues, but the utility-installed base of different protection technologies makes the task of managing the system infrastructure extremely difficult. The overall network reliability can be adversely affected by protective device misoperation due to incorrect or misapplied relay settings. As the regulatory bodies continue to focus on system reliability improvements, developing best practices and quality assurance procedures addressing relay settings becomes an integral part of system reliability.

A relay setting can be thought of as a command to a protective device. It calls for the device to take a specific action based on the system conditions input to the device. The command is based on a prediction of the system conditions during a class of events, such as equipment failures, that require specific actions to take place. The format of the command is based on how the device operates. In recent years, the requirements of the device have been expanded to include routine actions such as equipment operation. Therefore, the commands to control these operations are also a part of the relay setting.

The quality of the relay settings are affected by the following:

- Prediction of the system condition during actionable events. The prediction of system conditions is often provided directly from fault studies performed on power system models or from real events.
- The creation of the setting. The process by which system conditions are translated into commands for a device.
- The application of the setting to the device. The delivery of the setting and the physical process of applying the setting to the device.
- Maintenance of the settings. Changes in the operating system, relay setting philosophy, or device technology may require the assessment of the relay settings.

Relay settings include different parameters depending on the device and most importantly, the intended protection application. A relay setting can be the type of protection characteristic to the actual set point for the protection element. Modern protective devices contain hundreds or even thousands if user settable parameters to allow protection and control applications to be tailored for the specific line, transformer or other protection applications. The relay setting parameters are used by the microprocessor protective relay to perform the devices intended application use according to the relay engineer’s design. For an electromechancal relay, the relay setting can be the selectable physical arrangement of tapped windings and tension coils that determine when the relay will operate.

3. Definitions

IED - Intelligent Electronic Device - Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers).

IPP - Independent Power Producer - Any entity that owns or operates an electricity generating facility that is not included in an electric utility's rate base. This term includes, but is not limited to, co-generators and small power producers and all other non utility electricity producers, such as exempt wholesale generators, who sell electricity.

NERC - North American Electric Reliability Council - A nonprofit corporation whose mission is to ensure that the bulk electric system in North America is reliable, adequate and secure.

Pareto analysis – A quality assurance procedure to evaluate, categorize and prioritize in rank order issues and/or defects.

RTO - Regional Transmission Organization - Independent entities, established by FERC Order 2000 issued in December 1999, that will control and operate regional electric transmission grids free of any discriminatory practices.

4. Quality Control and Quality Management System

4.1. Need for a System to Manage Settings and Firmware Versions

Prior to microprocessor-based products, each protective relay had a limited number of settings. These settings were calculated by relay engineers and typically logged in record books. The need for setting changes was infrequent, and the relays had a long design life. Much of the functional behavior of a relay system was defined by the wired interconnections among the individual relays or modules in the system, which seldom if ever changed after commissioning.

Multifunctional microprocessor relays may have thousands of settings. A particular array of settings may be linked to a particular hardware design variation among many identical-looking relay types from the same manufacturer. Furthermore, the settings may be linked to a relay firmware version that is routinely updated by the manufacturer for error correction or feature addition, sometimes frequently. It is difficult enough to set each relay correctly in the substation design and commissioning stages, it is nearly impossible to identify or control subsequent setting errors in a large relay population without a new system of quality assurance and procedural control.

In modern relays, the settings contain not only numerous protective functions but also the operation, interconnection, and configuration of these functions. Many of these settings capture design choices that were traditionally implemented as specific wiring connections on a panel with discrete, single-function relays. Configuration errors in modern multi-function relays have the same effect as wiring errors of the traditional electro-mechanical systems. Accordingly, if the settings are not controlled and undocumented changes occur, it would be analogous to physical wires moving around on the relay panels; a problem not faced in prior generations. The design control that has been inherent in properly implemented panel and wiring drawing control systems now needs to be applied to settings and firmware versions as well. Failure to do so can lead to misoperations and faulty data reporting.

In addition, more regulation from FERC and NERC will drive the need for better configuration control.

4.2. Considerations for Relay Population Management

A system for managing protective relays on a utility system has to address the following attributes:

1. Product tracking through design, purchase, warehousing, installation, commissioning, removal, shipment for repair, restocking, reuse, and disposal.
2. Standards for relay selection, versions in use, and settings.
3. Development and recording process for the relay settings.
4. Loading the settings into the device prior to the commissioning process. Confirmation that the settings are correctly loaded.
5. Maintaining an audit trail of the relay settings from creation through delivery to application and on into maintenance cycles.
6. Setting changes for functions or measurements and the triggers for those changes.
7. Failure and replacement of relays.
8. Tracking and trending repair history of a particular relay for the population of a particular product.
9. Processing of vendor firmware upgrades and determining applicability.
10. Regulatory requirements including information required by RTOs or NERC and identifying which rules apply to a particular setting change (e.g. overreaching zones versus line load ability).

The user also deals with the related tasks of managing event data produced by relays, maintenance activities, test results, and product literature.

4.3. Management of Relay Data Records

To properly address relay population management, different groups such as the relay and substation control engineering, maintenance, operations, purchasing, IT, and executive management must create a management system with specific policies, processes, procedures, tools, and databases.

Policies establish the framework in which the processes and procedures are managed. An example of a policy is how departments work together on a quality process. Processes are systems defined for handling the information flow such as life cycle events of the relays. Procedures are written specific instructions for implementing elements of the process, recognizing the organizational structure and both the policy and tools that are available. Procedures include steps to secure, protect, and back up critical information needed to manage the installed protective relay population. Tools and databases are the programs and storage facilities for handling the relay information to be managed. These are cited in the policies, processes, and procedures.

Configuration Management (CM) is a business process that enables organizations to identify, document, manage and control operational information related to assets (both physical and knowledge) and systems with consistency through out their life cycles.

The primary objective of CM is to assure that assets and systems perform as intended within requirements and that the physical configuration is adequately identified and documented to meet anticipated needs for design, operation, and maintenance.

Some of the information that is managed by CM includes identification of the assets and systems; requirement, design and operational information; physical attributes; documentation; configuration, change control, and equipment history.

CM planning is the foundation for the CM process. Effective planning coordinates CM activities in a specific context over the product life cycle. The output of CM planning is the CM plan.

In CM configuration identification the product/service and its related configuration documentation is identified and defined. Attributes include the documented physical and functional characteristics of the code, specifications, design, and data elements.

CM controls the changes to a product/service and its related configuration documentation. The activity involves requesting, evaluating, approval, and implementation of changes.

CM provides status and information about a product/service and its configuration documentation. Sub activities are the recording and reporting of the status of project configuration items such as the initial approved version, status of requested changes, and implementation status of approved changes.

CM auditing verifies consistency of configuration documentation against the product/service to determine to what extent the actual configuration item reflects the required physical and functional characteristics.

4.4. Features of General Quality Systems

The utility should adopt principles applied in the manufacturing and business sectors that measure and improve the performance of control processes. Some of these principles include:

- The control process is documented, controlled, and is readily available to all who must implement it.
- The procedures are formally revised and updated as the processes are improved.
- No actions or observations are handled outside the control process.
- Specific, quantitative, objective, and user-independent performance measurements are part of the process.
- The performance measurements are periodically recorded and tracked.
- Reasons for less than perfect performance are recorded and subjected to analysis such as Pareto which analyzes a distribution of causes for the errors and failures observed.
- The analysis serves as the basis for action plans to solve problems and improve performance.
- The action plans are specific and assigned to responsible personnel with realistic schedules.
- The progress on improvement actions are managed and tracked, with problem solving as needed.
- The measurement and analysis of performance is periodically repeated.
- Users of the quality system are audited by an independent authority for conformance to procedures and for actual performance improvement from adherence to the procedures.
- Successful audits are recognized and documented. Audit findings are also documented for corrective action, and rechecked at the next audit.
- Audits that show significant process problems or failures require increased management action.
- The auditing process is professional and systematic, with trained auditors and is a main feedback mechanism for management.
- A documented corrective action program is effectively used to prevent reoccurrences.

NERC Planning Standard III.A.S3 requires that “all protection system trip misoperations shall be analyzed for cause and corrective action.” A quality system will provide a clear documentation of proactive compliance with these important industry standards, as well as information required by NERC or regional reliability councils for important events.

For example, in a hypothetical management of a relay population, process measurements for a three month interval includes the various data:

1. Number of relay misoperations attributable to incorrect settings.
2. Number of relay misoperations attributable to incorrect firmware versions.
3. Standard outage statistics (CAIDI, SAIFI, etc.) attributable to incorrect settings or firmware versions.
4. Number of firmware upgrades implemented.
5. Backlog of firmware upgrades required.
6. Number of setting changes implemented.
7. Backlog of setting changes required.

8. Number of errors discovered in field version of settings, firmware, or hardware versions as compared to database records.

The IEEE Power System Relaying Committee (PSRC) Working Group (WG), Trends in Relay Performance, developed practical techniques for measuring and tracking performance of relays in service (see also the PSRC WG report "Transmission Protective Relay System Performance Measuring Methodology"). Several utilities implemented this measurement method.

The user must have a process of managing and handling the relay population that produces the required measurements. For example, the process management of the number of discovered errors might have the following results:

- 10 total errors discovered.
- 5 cases – a technician replaced the relay with one having a different firmware version, and then reloaded the inappropriate settings from the old unit.
- 2 cases – the setting engineer misidentified the relay when updating the central settings database.
- 1 case – the firmware version was incorrectly recorded at commissioning, and was not previously discovered.
- 1 case – the firmware version was identified as incorrect during a check, but subsequent investigation showed that the version was correct.
- 1 case – unknown cause for an incorrect setting as compared to the archive.

Each of these cases could generate an action plan, with the priority attention focusing on the most critical problem(s).

Over time performance statistics should improve. In practice, new problems will arise and the analysis process should reveal these issues quickly so that the root cause can be identified.

4.5. Recognized Quality Systems

The international standard ISO 9001 - 2000 defines a quality system approach that can be audited and certified by individuals outside the accredited organization. To summarize, ISO 9001 requires that all the activities of a business process have documented and maintained procedures for the activities required for successful and complete operation, and that the organization actually follows its own procedures reliably. For a concise overview of the ISO 9001 – 2000 standard, there are many references available on the Internet [9].

Far beyond ISO 9001 is the Malcolm Baldridge National Quality Award (MBNQA) auditing process, which calls for proactive and meticulous business process analysis, objective measurement and analysis, full and active participation by management and all members of the organization, and documented continuous improvement of performance. While many of the MBNQA criteria in http://www.quality.nist.gov/Business_Criteria.htm go way beyond specific technical operations to issues for a complete business enterprise, the concepts of performance measurement and continuous improvement are universal and applicable for managing relays.

5. Relay Setting Process

The relay setting process starts with the creation of the setting and the needed resources. The process includes the verification and validation of the settings, addresses when a setting is needed, and has the requirements of setting archival. The relay setting can be identified as having two roles that address separate general operations, the protective setting and the configuration setting. The protective setting determines when to act based on power system conditions including current, voltage, frequency, and status of power apparatus. This operation is common to most protection devices and includes the important task of detecting faults. The configuration setting directs what is to occur once the decision is made to act. This operation is more prevalent in the modern protection device and may be routine operations such as operating equipment.

5.1. System Models

Since the protective device bases its decision to act on measurements of the power system, including current and voltage, it is important to be able to predict what the system conditions are when the device needs to respond. In the past, the computational power was not readily available to calculate the interaction of the numerous elements in a large power system. Therefore, assumptions would be made based on knowledge of the system and a detailed model would be made considering only the closest power system elements. Subsequent calculations based on these limited system models would be known to have a significant range of possible error. To address this, relays needed to be set with sufficient margin to emphasize reliability, security, or speed depending on what was most needed for the situation. As the access to computational power grew so did the accuracy of these models and the ability of different entities to use the models.

Current models for various power system components are created and used in computer simulations by power system operators, planning engineers, and relay engineers. Each of these groups of engineers has a different objective. Therefore, while the various groups are modeling the same system, individual components in the model may be modeled to different levels of complexity, depending on the objective.

For example, system planners are interested in knowing how well the system performs, and what are its operational limits. They might use the results of power flow and transient stability simulations for this purpose and to plan system requirements for the future [1]. Power flow simulations require an accurate modeling of the load in the network in addition to modeling of other components. Stability simulations require accurate modeling of the dynamic characteristics of generators and loads.

In numerous cases, relay engineers are only interested in the fundamental frequency behavior of the system. Some components need not be modeled to the same level of detail as might be required by other types of simulations. Generators are an example of this – they are typically modeled as ideal voltage sources behind an impedance, usually the sub-transient since this impedance is the most accurate representation during intended relay operating times. Transmission lines are typically modeled as lumped parameter components, with or without line charging. Transformers use the pi-model or matrix representations. Fault studies are performed on the network model to determine the settings for the relays that protect the network equipment.

A number of utilities have started performing transient testing of relays. This involves performing electromagnetic transient simulations on a portion of the network, and using the simulation data to test the relay performance. The network model requirements for electromagnetic transient simulations are different from those of fundamental frequency simulations [2]. Transmission lines are modeled as distributed parameter components as opposed to lumped parameter components. Generators can be modeled as ideal sources, or with detailed transient models. Due to the computationally intensive nature of the calculations, transient simulations are performed on small portions of the network, with the rest of the system modeled as a network equivalent.

Irrespective of the objective, the simulations are of little value if their results do not accurately reflect what really occurs in the system. That is, there needs to be some way of comparing the simulation output with the actual system behavior. Differences between the two can be used to modify and enhance the model, i.e., system validation. Figure 5.1 illustrates this concept [1].

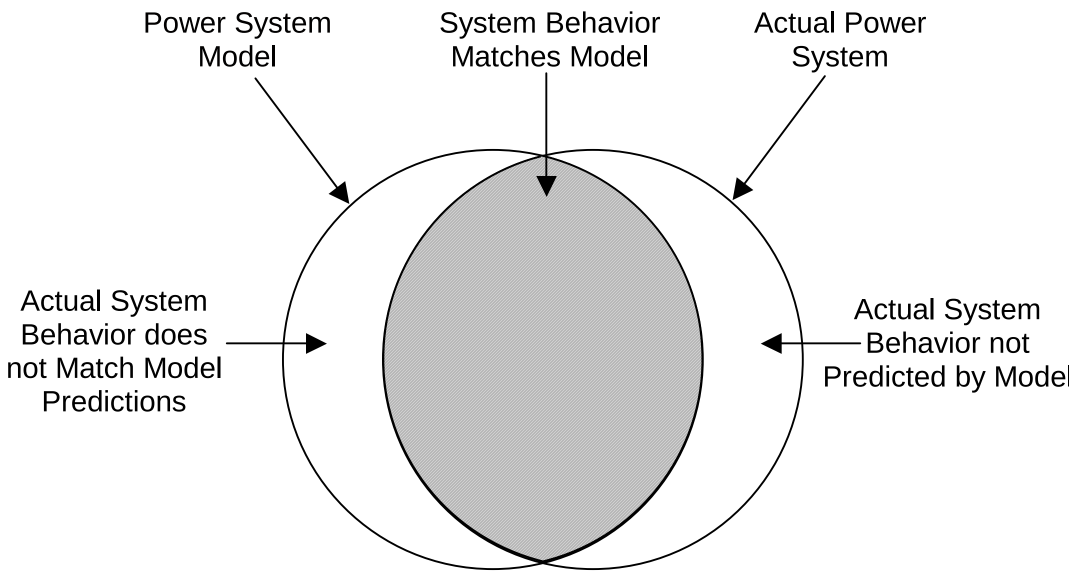


Figure 5.1: System Validation.

The circle labeled "Power System Model" represents the behavior of the mathematical model of the power system. The circle labeled "Actual Power System" describes the behavior of the real system. The shaded area includes those parts of the system model that very closely match the real system behavior. Ideally, the two circles overlap entirely, so that the model is an exact representation of the actual system.

This section concentrates on the verification of the system model from a relay engineer's perspective. That is, verification of the network model, followed by the validation of the predicted relay operation with the actual relay operation.

5.1.1. Sources of Data

Data collection occurs from various points in the network and includes the fundamental frequency, voltages and currents. A number of devices are used for collecting data:

- Phasor Measurement Unit (PMU): This unit samples the voltage and current waveforms and computes the three voltage and current phasors (magnitude and phase angle). The phasors are time-tagged with an accuracy of around 1microsecond. The measurements can be synchronized to a timing signal from a global position satellite (GPS) or unsynchronized. PMUs are deployed at various locations in the network. If synchronized using GPS they provide a very accurate picture of the current state of the network. A number of applications have been proposed and implemented [1, 3] – state estimation, adaptive out-of-step relaying, system frequency measurement, etc.

- Digital Fault Recorder (DFR): DFRs have long been used to monitor the power system. When triggered, they sample and record the voltage and current information, and also the discrete switching events that they monitor. DFRs are special purpose devices, and are generally found at limited locations in the network, where there are important equipment to monitor. Also, DFRs typically supply time-domain data. DFRs record time sampled data that can be converted to phasors for fundamental frequency analyses. Sample rates of 16,000 to 32,000 samples per second are common for DFRs.

- Digital/Microprocessor Relays: Relay event reports and fundamental frequency information are available from almost all digital relays. The sampling rate of digital relays is significantly less than DFRs, typically 240 to 960 samples per second. While this sampling rate is adequate for the protection functions that the relay is required to perform, it may not be sufficient for monitoring high-frequency events like capacitor switching, lightning strikes etc. Given the low sampling rate, the relays produce good fundamental frequency representations of the recorded signals. Since the relay settings themselves are based on fundamental frequency simulations of the network model, relay records are quite useful in the verification of that model. With advancement in technology, some newer relays capture data at 64 to 96 samples per cycle, and further advancement in technologies will continue to improve the sampling rate capability of digital relays, allowing these to record power system transients more accurately.

5.1.2. Verification of the System Model

The measured data is compared with the simulation data to assess the accuracy of the model. Validating the system model typically involves verifying the system impedances being used for transmission lines, transformers and generators. The process can also be thought of as adjusting the system impedances so that the simulated data matches the recorded data.

For transmission lines, the line impedances are usually computed using a line constants program. The line constants program uses the tower geometry, conductor arrangement, earth conductivity, sag etc. to determine the positive- and zero-sequence impedance of the line. Such programs can handle complex right-of-way situations and arbitrary mutual couplings. Since the network model is a fundamental frequency model and is balanced, decoupling the phase impedances into sequence impedances is assumed to yield a perfectly diagonal sequence impedance matrix. This ignores the non-zero off-diagonal terms of the sequence impedance matrix.

For transformers, the source of impedance data is usually the test report. In some cases, the test report may not be available, or may be incomplete, listing only the positive-sequence impedance. Assumptions are then made regarding the zero-sequence impedance used in the network model, thus leading to discrepancies between the measured data and the simulated data.

During system transients, the generator impedance varies with time. For fundamental frequency network models, generator manufacturers typically supply several impedances as part of the generator data. For steady state studies, the synchronous reactance is normally all that is required. Modeling for protection studies typically use the sub-transient or transient reactance. These models do not normally account for changes in excitation by control action.

One method, applicable to transmission lines, uses the recorded data to compute the line impedance, which is then compared against the numbers computed using the line constants program. Adjustments can be made to the impedance data used in the network model.

Another convenient way to validate the system model is to compute the equivalent source impedance behind the data collection point [4], which can be any one of the sources described earlier. Depending on the location of the data collection equipment, it becomes possible to validate generator impedances and step-up transformer impedances. Elsewhere in the network, the calculation of the source impedance yields a general means of validating the system model.

Both the impedance comparison and source impedance methods are described in Appendix A.

5.1.3. Implications for Relay Setting – Verifying Expected Relay Operation

Relay and DFR records of relay operations can be obtained and compared to the predicted relay operations from the relay simulation that used the network model, assuming that the fault condition can be recreated in the simulation. Any discrepancies between the expected and actual relay operations is an indication that either the system model is in error, and /or the relay model used in the simulation contains errors.

The first step is to try and fix the system model. As explained before, the source impedance technique can be effectively used where the source impedance consists of one or two pieces of equipment. In other cases, it may not be possible to narrow down the source of the error. The relay settings might need margins larger than usual to account for the model errors.

Fixing the relay models used in the simulation is usually a straightforward matter if detailed information about the relay is available from the relay vendor. It is also advantageous to be able to disconnect the relay model from the network model and inject the recorded data from the system into it. This will immediately indicate if the relay model contains errors.

5.2. Relay Setting Calculation and Development

Fault studies of the system model provide a range of expected system conditions during the set of system events that requires relay action. For electromechanical relays, setting up the relay to operate when desired required the inputting of system conditions that satisfied the torque equation. Calculations were needed to determine the tap setting and time dial required for proper operation.

With the advent of microprocessor relays, the calculation of the torque needed to cause motion is no longer necessary. However, determining the settings for the modern relay is no longer a matter of just setting pickup, reach, and time values. The interaction of various elements, which were formerly accomplished through wiring, is now processed through the logic within the microprocessor-based relay.

In order to maintain consistency and follow established practices, written guidelines for calculating relay settings should be available. These guidelines are developed over years of operating experience and through consulting industry standards and guides. These guidelines are subject to change as philosophies, regulatory requirements, and improvements to protective devices change. In addition, all of the logic and configuration settings required for each protective device model and application need to be included in the settings guidelines. A review of these company setting policies, standards and guidelines should be conducted with employees or contractors new to performing setting calculations.

Software is available which assists protection engineers in determining relay settings. The company guidelines can be incorporated in these setting algorithms. Manufacturer or third party software allows for saving “template” settings so that it is not necessary to enter every one of the hundreds of settings for every application of a relay. The standard logic for the various models and schemes are saved in different “template” relays.

The process, or rules, of developing protective settings involves the systematic application of the policies and procedures that have been developed over a number of years. An example is a rule of making the Zone 1 phase distance setting 80% of the positive sequence impedance for a transmission line.

Tools, which are usually available within the framework of a short circuit or relay database programs, can be made to incorporate policies and procedures specific to the fault calculation. Once the accuracy of the setting tool is verified, the tool can be repeatedly applied to the network, thus, saving time, eliminating human error, and performing more thorough fault studies than what was possible using manual methods.

These setting tools can also convert the raw settings determined via the fault study into settings specific to individual relays. However, relay vendors usually provide proprietary software for transferring settings into the relay.

5.3. Multiple Setting Groups

Many microprocessor relays have the capability to store multiple setting groups. This capability allows the user to preprogram different settings for different conditions such as seasonal variations, time based considerations, or different system configurations. Multiple setting groups may also be used to contain specific test settings. Typically, relays that have multiple setting group capability contain between four and eight groups.

These multiple setting groups require special documentation of calculations, setting records, event analysis, and scheme logic. The user may choose to repeat all the calculations or only those that are different from the initial case depending upon the number of differences and the practices of that user.

The active setting group in the relay may be selected either locally or remotely by means of the communications commands to the relay or external control of the relay's digital contact inputs. The digital input state changes may be made manually using a selector switch or may be automatic using a relay or auxiliary contact.

The specific conditions for which each setting group is intended to apply may be described within the setting file providing a clear unique description for each group. The description should be specific as possible. For instance, instead of "summer" versus "winter" ratings, the dates for the two seasons may be specified.

The documentation should also state the means by which the setting group is changed, such as manually through the communications port or automatically by change of a digital input state. If a selector switch is used then the switch contact is included in the design drawings to document the scheme logic.

In many cases only a few of the many settings required by the relay might change from one setting group to another. In such cases, the description specifically identifies those settings that focus on the differences.

In the setting records a complete copy of each setting group should be maintained. This may present a challenge for the user as traditional means of keeping relay setting records may not have included multiple settings for a single relay. A computer database may require additional dimensioning or the relay may need to be listed separately for each setting group.

The change from one setting group to another may not only change the quantitative values of settings, it may change the scheme logic. For instance, one setting group may use Permissive Overreaching Transfer Trip (POTT) logic while another setting group may use Step Distance logic, requiring that multiple logic diagrams be included in the logic design documents.

In event analysis it is imperative that the active setting group be known in order to properly determine the correctness of the relay's performance. Relays that track the changes to the setting groups in a log file that the user can access provide a means of identifying the active group. The event records usually also include the identification of the active setting group at the time of the event. Ideally the event record will include not just the setting group name or number but a listing of all the settings so the actual settings may be verified against those on record.

Most relays are shipped with manufacturer default settings which are identical in each setting group. One common practice, if only one setting group is used, is to change all setting groups to be identical with the desired settings. This prevents accidentally activating the wrong setting group with the default settings. Of course this method will not work if multiple setting groups are used. However, if only some of the setting groups are used, the user may consider setting the unused groups to the group which best protects all conditions, or the one that is expected to be in service the majority of the time.

Using multiple setting groups for test settings may be useful because it may be necessary to turn off certain elements in order to test other less sensitive elements. In this case it is still important to clearly identify which settings are changed from one group to the next, but other documentation may not be as important. For instance if some settings are merely being turned off, no additional calculations need to be documented. Great care must be taken that the relay is left with the correct setting group active when all testing is complete and the relay is placed in service. This is probably the least advisable use of multiple setting groups because it has the greatest likelihood of the relay having the wrong active setting group. The test setting groups may just as easily be stored external to the relay and only used during testing.

5.4. Input to Relay Settings from Multiple Groups

Multifunction relays have control, metering, event, and oscillography functions in addition to the protection function. These relays also have the means of communicating with other devices and responding to input from other devices. Because they provide such diverse functions, areas other than the protection engineering group often need to provide input into some of the settings for these relays.

Depending on how companies are organized and on the availability and number of other devices performing similar functions as the microprocessor based relays, the following areas of a company may need to have input into relay settings:

- Metering – communication settings
- Communications / IT / Cyber Security – communication settings
- Operations – protection, control, and communication settings,
- Substation Design – control settings
- Fault Data – communication settings
- SCADA – communication settings

As shown above, most of the outside consumers of the microprocessor based relay, only need access for monitoring data. Therefore, communications settings to allow access are very important. A coordination of efforts is required in cases where different engineering groups are responsible for the different types of settings to insure the settings issued are complete and accurate.

5.5. Unused Settings on a Multifunction Device

Multifunction relays can contain hundreds of settings of which many may not be used depending on the scheme employed. Relay misoperations have occurred by elements that were not intended to be active but were set such that system conditions caused those elements to operate. A setting of “OFF” would likely be the most secure but that is not always an option. The next most secure setting would be the least sensitive operating point and the longest possible time delay. A thorough knowledge and understanding of the setting will ensure that the proper setting is selected.

5.6. Review of Relay Settings

5.6.1. Peer Review

Misoperations and outages are scrutinized more highly in today’s environment where such events now have to be reported to NERC. Therefore, a peer review of relay settings should be performed to catch possible mistakes before they cause events. When new relays are installed or major changes are made on existing relay schemes, a peer review should be performed by a person that has equal or greater experience than the person that prepared the settings to verify that the relay settings meet the specifications of the relay and control application. The review generally consists of verifying that the relay scheme is wired according to the design drawings, uses the correct potential and current transformer ratios, and checks the input/output connections for used for tripping and control. Once the relay application is reviewed, then the protection setting calculations are checked for correct application and mathematics. With microprocessor relays, many engineers have found it useful to bench test the settings in an identical relay to verify that the settings load and the relay protection and logic settings operate as designed. For communication-based schemes, the review will include the settings for the communication equipment and associated logic.

The peer review is usually performed by a person that may not be as familiar with the method or philosophy of the setting as the original creator. The reviewer should limit the amount of input received from the setting creator so as to avoid repeating errors the setting creator may have made. The method that is used for a peer review can differ from the method used in the original relay calculation. The peer review does not have to be a recalculation of the settings but rather a review of the basis of the calculations and the communication of the settings.

To review the basis of the calculations requires careful documentation of the setting process including design notes of the calculation assumptions made during the process. When standard settings are used the settings calculations should make reference to those standards. Deviations from the standard, including their reasons must be documented. The reviewer may require additional project documents to verify the calculation basis including planning documents and project files.

The peer review verifies that the settings match the relay engineer's intent of that specific protection and control application, eliminating incorrect settings caused by mechanical and mathematical errors, as opposed to conceptual errors. Peer reviews should be documented and follow established review guidelines. For example, estimating rules could be used to quickly verify calculated settings thus avoiding errors due to misplaced decimal points or typographical errors. It is important to assure that the peer review process is an integral part of the utility's design and quality control procedures.

Logic commands need special attention. An AND logic operator in place of an OR logic operator can mean the difference between a normal operation and significant events. Some relays allow for comment of these formulas that can be used to help identify the intent. New logic applications require careful scrutiny for complex equations. The setting creator should document logic for the configuration setting review process. The use of logic flow diagrams can help the reviewer understand the scheme as well as engineers in the future when changes have to be made.

Similarly, most utilities perform a review of an IPP's generator/transformer protection prior to allowing the IPP to connect and generate into the transmission system.

5.6.2. Commissioning Review

Errors in relay settings have been found during commissioning, including dynamic end-to-end relay testing. End-to-end testing can require multiple testing resources, but tests the complete relay system and is advantageous for inter-tie lines between neighboring utilities. Based on the test results, each utility can review the other utility's relay settings regardless of the line ownership.

5.6.3. System Review

Many utilities perform system wide coordination studies on a rotating time basis and as system configuration or load dynamics change. Settings are created when new stations are built or when new lines or transformers are installed. The overall effects of these system changes can have an impact on other stations than the stations directly involved. Fault duties change at outlying stations, which can affect the operation of the relays. A system change might not seem like much of an issue. However, over time, each small change can add up and become a significant contributor to a significant event. The policy and procedure should assure periodic review of relay settings. These procedures can identify potential settings problems that might otherwise be overlooked.

Modern relays and digital fault recorders collect the actual fault values that can be useful in the validation of the fault study models. If an error is identified in the fault study, then a review needs to be performed with the revised study to avoid potential relay misoperations. The potential deviation between fault studies and the actual system configuration may be remedied by performing periodic comprehensive coordination studies. This review ensures that the relays in the study area are set according to established guidelines and verify system modeling and equipment data.

Some triggers for initiating a review of relay settings are as follow:

- National/regional reliability council requirements
- Review settings just before scheduled field calibration tests
- Whenever a new tap is connected to a line

- Whenever a misoperation has occurred, it should be noted that it is very helpful when the same relay engineer who was responsible for the settings also perform the analysis of relay operations. This is an invaluable part of the feedback loop, which some utilities do not consider.
- Line and/or static/shield wire replacement or reconfiguration – It is critical that the system model used for protection related studies be updated with the latest positive and zero-sequence line impedances and mutual coupling data
- Increased line loading
- New relay firmware being installed

It should be noted that it is not normally necessary to review generator protection, unless the generator system itself has been changed like a stator/turbine upgrade and excitation control changes.

5.7. Relay Setting Archival

Relay settings must be documented and archived in an easily retrievable manner for all personnel that require access. Because of the large number of settings for microprocessor based relays, entering settings for these relays is usually done with the use of software provided by the relay manufacturer in a database format. These databases are often transient, contain only relays of a certain manufacturer, and are difficult for maintaining an inventory of relays. Most computer programs require that data reside in a local database, so it is not uncommon for relay settings to reside in different databases, thus causing access problems.

Asset or configuration management programs can manage relays and their settings along with other corporate assets. Asset management databases are typically designed for enterprise usage and access is generally available to more individuals.

Some reasons to store relays in an asset management database include:

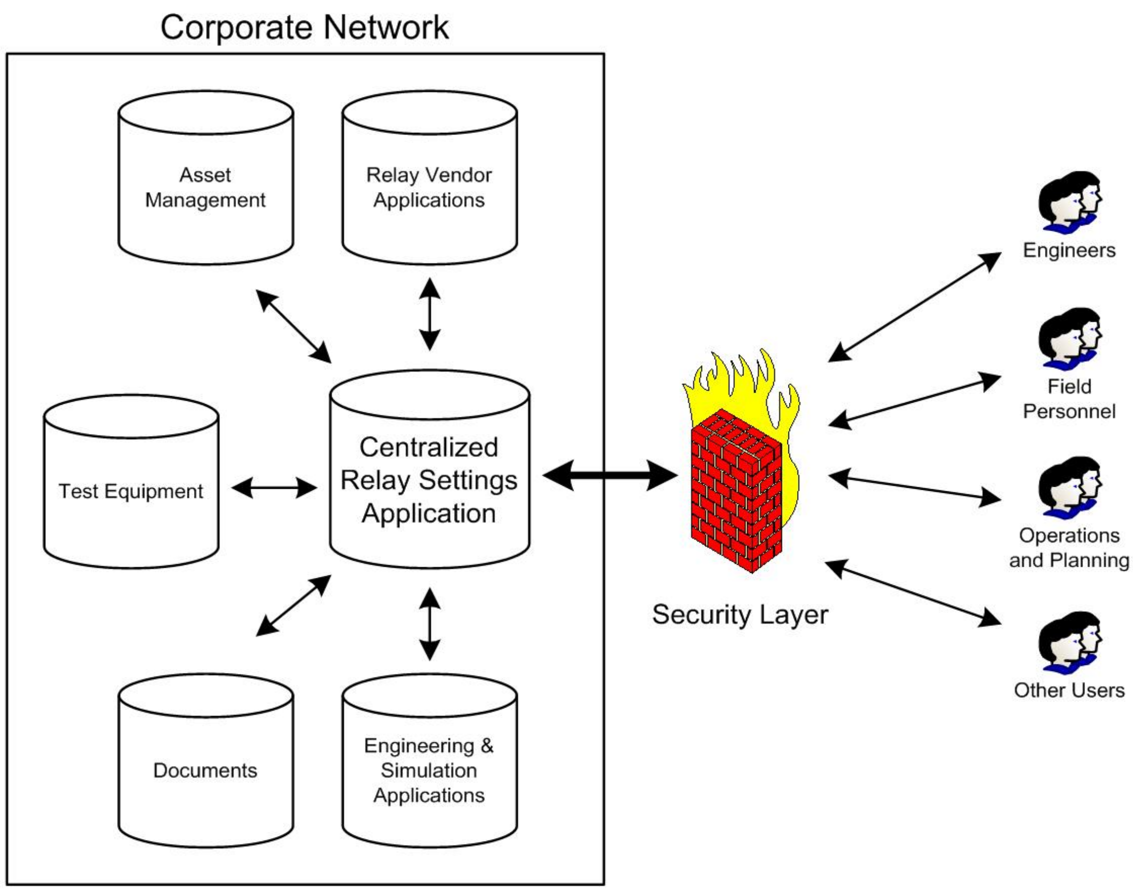
- Short circuit programs provide analysis tools. In order to perform the analysis, data on all relays must be in the database.
- Relay data in short circuit programs tend to be more detailed but are a sub-set of central databases.
- Relays in an asset management system database are typically available to a broader audience.
- Management of asset management databases is often handled by a true database administrator
- Asset management systems do a better job of archiving and managing work processes.
- Relay settings are normally copied to asset management databases only after they have gone through the approval process. Thus, access to preliminary settings is limited.

The biggest drawback to having relay data in more than one database is the very real possibility of having conflicting data in the databases. Maintaining the same data in multiple databases requires diligence to ensure the data is always correct and up to date in all storage locations especially that all changes required during commissioning are documented and updated in all settings databases. Settings database management is crucial to maintain the quality of relay settings, and therefore, multiple databases are not recommended.

Referring to Figure 6.1, a centralized relay settings application or repository can control access through role-based security. Specific users are not granted access to modify more data than is required to perform their jobs. Technicians may need to read settings and other information and perform simpler calculations, but not add or remove relays from the system. Relay engineers need the ability to perform all calculations and make changes to data within their area of responsibility. A 'library user' may have the ability to change models and algorithms. System administrators have the ability to control access rights and passwords for all users.

Figure 6.1: Centralized Relay Settings Application

6. Master Settings Database Management



Once settings have been calculated and issued, control and management of a settings database is essential. In addition to relay settings, the database may contain calculations, setting criteria, test and maintenance data, obsolete settings, audit trail of setting changes, and external links to other data sources. The settings database is typically part of a larger software application that enables and controls the access to the settings that allows the settings data to be retrieved or written by other applications.

6.1. Master Database Location

In the past it was common that the settings database resided in a 'master' settings notebook or file cabinet. With the advent of computer networks, all or part of this data now resides on servers. This makes the information accessible to all users and modifications of the data may be limited to selected users.

On the server, settings and related information have typically been stored in a variety of formats. Settings may be in word processor files, spreadsheets, general-purpose databases, or vendor specific formats. The advances in Relational Database Management Systems (RDBMS) and other software tools, such as client/server and web-based applications, make it possible to implement a secure and controlled environment. This allows the creation of a feature rich relay database application that also provides access control, data integrity and consistency, redundancy, and accessibility.

6.2. Retrieval of Settings

The retrieval of protective device settings is perhaps one of the most important features of a relay database whether that database is integrated with other applications or is a stand-alone centralized settings database. In the past, settings were transmitted using paper files. While this is practical for electromechanical relays with a small number of settings it is cumbersome to supply paper settings for digital relays with hundreds of settings. Regardless of the relays' complexity, a paper-based transmission is error-prone and inefficient. An electronic method of settings retrieval is therefore the preferred method.

Comparing retrieved settings with those in the master database is an important step in validating the database as well as verifying that the in-service settings are as intended. It may be determined that requested settings are invalid due to reasons that were not communicated to the issuer. It is also possible that settings were modified in the testing process but were incorrectly restored. With the master database validated, other databases that are supported by it will have access to this data. Validation of in-service settings is required in nuclear plants and the transmission yards that they connect to. Audits by the Institute of Nuclear Power Operations (INPO) have reviewed this validation process.

Referring to Figure 6.2, through the master database settings can be transferred to/from:

1. Vendor-specific relay setting software/hardware: Vendors of test equipment, electronic relays, and engineering/simulation software have their own method of storing relay settings. Vendors may use text files, binary files or a database program to store the settings. The database format will undoubtedly differ from the master settings database format. Setting format conversion and transfer of settings from the master database to the vendor specific software must therefore be implemented on an individual basis.

2. Electronic files in special standard formats: Recently, the Extensible Markup Language (XML) format has been gaining popularity as a means of exchanging data. The master database can export the protective device settings using the XML format. Other software can read these XML files and obtain the settings. The Power System Relaying Committee of the IEEE is currently working to expand the IEC 61850 standard to provide a common format for exchanging configuration (settings) data. Once completed, using this standard, various vendor software and IEDs can integrate directly with the relay settings database.

3. Asset management software: The asset management software usually has its own database, with a specific structure, usually different from the structure of the master database. Thus, mapping is required between the two, so that data can be easily exchanged.

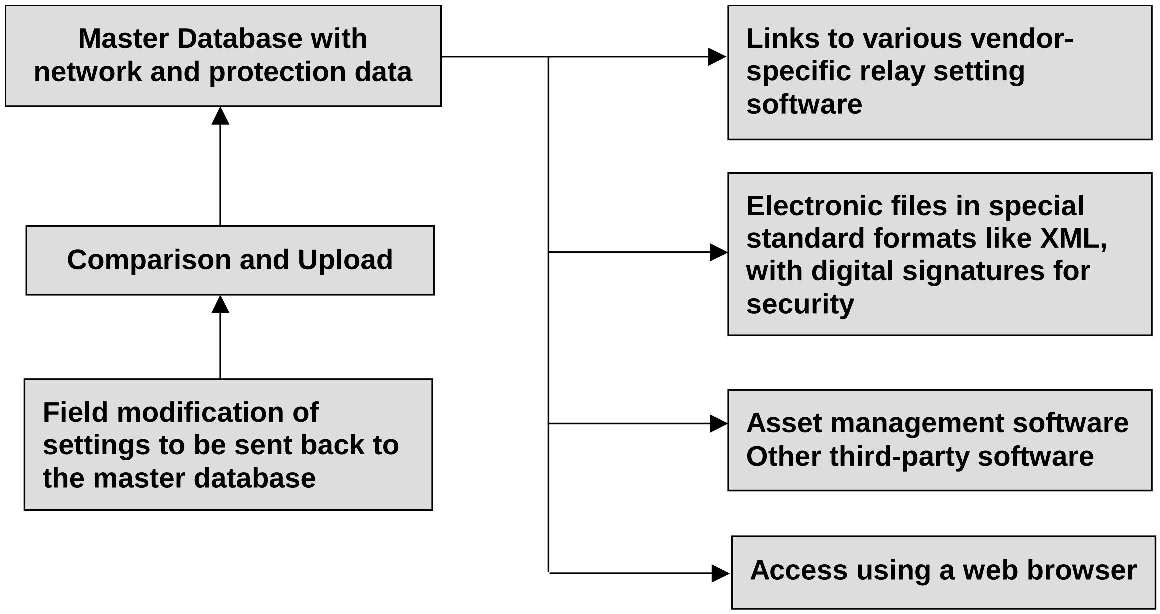


Figure 6.2: Retrieval from and Return of Protective Device Settings.

Another methodology for storing electronic setting files is to treat them as objects. Once created, they can be treated as physical entities that are identified by a naming convention and can be controlled. They can be issued to field technicians using workflow software and stored as objects in the company asset database attached to the relay data. These files can be tracked for quality assurance purposes and accessed when needed for the data they contain. A summary of the settings can be made for day to day operational use but if all the settings are needed for review due to a change, then the relay manufactures software can be used to open the object file as it will be stored in it's original format.

6.3. Archiving Superseded Settings

Some utilities desire to archive superseded settings. In the paper-based system, this was accomplished by putting the old setting sheet in an archive file. For a server file based system, this requires a certain amount of discipline to save the old version. The centralized relay settings database can generate and enforce audit trails that perform the functions of tracking all changes: logging what, when, and by whom. The archived settings can later be retrieved for analysis and audit purposes. Archiving of both superseded and current relay settings will affect the database's management strategy as well as its capacity and capabilities to handle large volumes of data.

6.4. Documentation

Relay documentation includes type specific information such as the model number, style, manual number, and schematics; as well as specific relay information such as firmware revision code, serial number, location, circuit, and relay settings, and test results.

Settings criteria and calculations are normally saved. These can assist in analysis of operations and make future settings changes easier. 'Standard' procedures may be documented as company practices and/or as setting rules in calculation programs.

Unique considerations, assumptions, and the rationale for variations from the normal rules need to be documented for each location. This may be documented in text fields of a database or as stand-alone documents. It is important that this information not be buried in other data or otherwise lost. External documents, such as instruction manuals, test and maintenance procedures, and drawings can be associated with a relay using an integrated document management system.

6.5. Integrated Short Circuit/Setting Database Program

Some integrated programs include a short circuit program, a settings database and other relay modeling tools. In such programs, the database stores not only the network data, but also the protective device data in manufacturer-specific named settings. Therefore, when relay settings are generated after short-circuit studies, generic relay settings are converted to actual named settings and stored in the integrated database.

6.6. Database Structure

The primary function of the database is to archive analytical data used by various protection functions such as short-circuit analysis, relay settings calculation, coordination checking, and electronic settings transfer to or from digital protective devices. The structure of the data and internal triggers must promote data integrity and self-consistency. A secondary function is to serve as a repository for record-keeping data that may be important to the overall protection operation but are not used by the analytical functions.

One method of organizing the data is to divide it conceptually into “library” and “system” data. Examples of data that belong to the library include models of protective relays, reclosers, fuses, instrument transformers, power transformers, circuit breakers, conductors and transmission line tower designs. Relay models include the various elements like IOC, TOC, DIR, DIST, which make up the relay, and the available settings for those elements. Usually, element settings are self-contained, with each element having its own group of dedicated settings. This was indeed the case with electromechanical relays. In digital relays, which have a large number of settings, many of these settings affect more than one relay element. The relay model must accommodate both types of devices.

System data includes the network data for fault and power flow calculations along with specific instrument transformers and protective devices and their settings at various network locations. The relay engineer works with the system data to perform short-circuit studies, relay setting calculations and protection coordination analyses.

7. Relay Setting Implementation and Maintenance

Once the relay setting has been created and a database put in place to manage the settings there is still the operation of applying the relay setting to the relay. As with all other facets of the relay setting, the increased complexity of the protective device has resulted in new challenges in this process that can affect the quality of the relay setting. The process that takes the created relay setting and applies it to the relay including the steps to verify the successful transmittal of the setting is considered the relay setting implementation. Requirements after initial application to maintain the quality of the setting is considered relay setting maintenance.

7.1. Relay Setting Transmittal and Presentation

The transmittal of relay setting information to testing technicians has changed as relays have evolved from electromechanical to microprocessor-based devices. Electromechanical relays were typically designed for a single, specific function, each requiring few settings and with typical test plans. The setting calculations, coordination analysis, setting documentation and test points were typically completed by hand and summarized on a setting sheet. The setting sheet was either mailed or hand-delivered to the test technician for application and testing. The document was marked with any changes made during testing, signed as set, and returned to the office for archiving.

In contrast, microprocessor-based relays usually contain many protective and logic functions, which result in more settings and detailed documentation requirements. The settings are normally supplied to the test technician in an electronic format for automated download onto the relay and/or test equipment. Fault simulation test files created within a fault analysis program or from a previous event are also sometimes supplied in an electronic format to the test technician. Additional testing required, such as customized relay logic, is also supplied to the test technician.

Following the application of microprocessor-based relay settings and the completion of testing, the installed settings are electronically verified against the supplied settings and downloaded into a master relay setting database and/or fault analysis program for archival. This electronic verification is either done locally by the test technician, or remotely by the system protection engineer. A separate database is typically required for various brands of relays, although there is a trend towards nonspecific databases that can contain settings for numerous relay manufacturers. The developed test plans and testing results are documented electronically within a test equipment database and can be used for future maintenance testing. In addition to test results, specific relay data such as firmware identification is documented and entered into a maintenance management system. A paper copy of the settings and documentation, if supplied, is marked with any changes, signed as set, and returned to the utility relay/system engineering for archiving.

Transmittal of relay setting information may also be required for system operation. For instance, analysis of relay action may be required during an event either on or off site. Under these circumstances some have found interpreting settings files as being time intensive. Previously, the operation of relays could be analyzed by reviewing schematic connections between protective elements that reflected the wiring needed between different devices. Design choices could be easily understood by reviewing these documents. Many of these design choices are now internal to the relay and are determined by the setting. One approach that addresses this is the creation of logic diagrams that are considered equivalent to other construction drawings. They fall under the same quality assurance measures and control procedures as other prints but communicate the configuration and logic settings internal to the relay.

7.2. Test Values

For electromechanical single-function relays, the relay engineer typically calculates test values at the time the settings are developed. While field test personnel may perform factory recommended commissioning tests during initial installation, some tests are based on the specific settings applied to the relay. This test confirms that operation of the relay at the setting chosen matches the model behavior presented by the manufacturer.

For distance relays, the test would include the reach at the maximum torque angle, which involves applying a test voltage, setting the current phase angle lagging the test voltage at a value equal to the maximum torque angle, and ramping up the current until the relay just picks up. The specific test voltage applied is calculated by the relay engineer to be the voltage at the relay terminal for a radial fault at the limit of the relay reach using the source impedance and the relay reach in a voltage divider network. A test for the maximum torque angle (MTA) is also performed based on the setting chosen by the relay engineer and may need to be adjusted depending on relay style. The MTA test may also include test points on either side of MTA to ensure the relay picks up at the appropriate points of the mho circle.

For time overcurrent relays, tests would include a check of the minimum pickup, and a check of the characteristic curves, typically by running several test currents at increasing multiples of pickup and comparing the operate time against the manufacturer's published curve.

With the advent of multifunction microprocessor-based relays, the trend is away from testing each individual function within the relay. Although some utilities still perform these tests, more utilities have their field test personnel simply load the settings on the relay as provided by the relay engineer. Another method is to rely on the manufacturer's factory test document with default factory settings or relay settings provided by the utility. The relays are then field tested using a couple of test points to verify the "as-left" condition of the relay before placing it in service. Testing plans might include tests of the relay with the manufacturer's default settings. Then, after the specific relay settings are applied per the relay setting sheet, field personnel will perform a set of dynamic tests also provided by the relay engineer as produced by the short-circuit program, for faults in different locations within and outside of the zone of protection. Modern testing equipment can be programmed to quickly run multiple tests to more completely record the "as-left" condition. Relay performance, including targets and pilot channel logic, is then compared against the intended design, by field personnel, sometimes with the assistance of the relay engineer. Another form of test for communication aided relaying schemes are end-to-end satellite testing where in-section and out-of-section faults are simulated at various locations for the affected line section to measure and document the performance of the relay application including the relay connections to the communication equipment.

7.3. Applying and Verifying Correct Settings

Early generation of electromechanical and solid state relays have a limited number of relay settings. The set points are applied through the use of physical setting devices (switches, taps, slides, etc.) and are visually verified. Verification of the settings, as well as the relay characteristics, is also accomplished by testing the relay against calculated test points.

In contrast, microprocessor relays usually contain many protective and logic functions, which in turn results in significantly more settings. Settings are usually applied to microprocessor-based relays using one of three methods; use of front panel relay interface, manual entry using a terminal emulation program, or download of settings using vendor-specific software. The two manual methods of setting the relay can be inefficient, tedious, and prone to typographical errors, all of which can be avoided by using the automated download method. Verification of the settings is either done visually by a line-by-line review of the manually entered settings, or via vendor specific software that automates the comparison between settings in the relay and settings file intended for the application. Use of automated settings comparison is highly recommended since it is a very effective mechanism to detect settings discrepancies.

The ability to communicate with microprocessor-based relays allows downloading relay settings from a remote location, such as an office or another substation. This can be an efficient method to modify relay settings but care must be taken when considering this alternative especially when modifying tripping elements or equations as a single typo can prevent proper operation.

7.4. Relay Compatibility to Settings Files

The relay setting files have to be compatible with the firmware version in the relay. Some firmware revisions are extensive enough that they add or revise setting names. When that happens, the setting files for the older firmware is not the same as the files for the new firmware. This can be a problem when replacing a failed relay with a newer one. In that case, the Relay Engineer will usually have to evaluate the differences and develop a new setting file for the newer firmware. Many utilities try to standardize on a specific firmware version to avoid this problem.

Vendor-specific setting program versions also have to be compatible with the relay. Upgrading firmware revisions may require the use of a new relay setting tool version as well as changes to the setting files. Generally, the latest version of a vendor-specific setting program will be compatible with older relays by that vendor.

7.5. Relay Maintenance Records

Various methods for periodic relay testing and maintenance can be utilized. Periodic test reports can be kept on paper records and archived at the maintenance office with copies sent to various interested parties (i.e. engineering and protection) for historical purposes. The reports can be generated electronically with the results stored on a shared network drive for use by various internal groups. Test results can be documented in an asset management database.

Commissioning test reports are perhaps the most important documents since they provided the baseline data for future test reports. These test reports can be archived to a database for access by all authorized and interested groups.

8. Vendor Specific Relay Setting Issues

The modern protective device increased in complexity, thus leading to increased complexity in application that each vendor addresses in their own way. The use of high quality protective devices compounds the overall complexity.

8.1. Differences in Databases

Relay manufacturers presently store relay setting data in several different formats. A common method is to store the setting data in relational database. Security may be implemented for the database or the data file extensions may be renamed to obscure their true format. Another common approach is writing the relay settings into a delimited text file sometimes using a CRC checksum to verify data integrity. A third approach is to use a binary file structure for the data that is vendor specific. Vendors of relay analysis programs normally use relational databases.

A systemic problem is that nearly any relay function can be expressed using different terms. Each parameter of that function may also have several widely used names. In the past, manufacturers were not always consistent in defining common relay functions and parameters. This inconsistency has led to difficulties in exchanging data between applications.

Standard IEC 61850 provides a common data structure, utilizing XML, to describe all substation data including relays and their settings. PSRC working group H5 is working on the use of IEC 61850 in developing a common data format for IEDs and legacy devices. XML is the mark-up language used for representing data in a structured format. In a XML, each relay element can be described using standard parameters. The standard can be extended to legacy devices but a conversion protocol would need to be developed for each device type. Utilizing a standard format, applications and IEDs can exchange data without requiring customized interfaces and translation applications. XML ensures data integrity by using the XML Signature standard. Signatures can be used to help detect external manipulation of the data. Relay model definitions can be stored at a web service that is provided by the original manufacturer or standards body. Users could look up or query these definitions on the Internet so that a consistent relay model is used by various applications. Each company can then extend the relay model definition to meet its particular needs.

8.2. Firmware Version Control

Two practices that have been successfully applied by utilities to control the firmware versions of relays in their system are the following:

1. Use fixed firmware versions in relays used on the system and to be purchased. The company then controls when firmware is updated in its relays and can evaluate whether new firmware versions are of value.

2. Track the firmware version of all relays in use, location of each relay and document differences in each firmware revision.

IEEE Recommended Practice PC37.231, Recommended Practice for Microprocessor-based Protection Equipment Firmware Control, calls for establishment of a Firmware Controller (may be a person or an organizational function), and the means by which this function interfaces with a relay manufacturer to answer questions relating to firmware versions, related settings issues, and documentation. This supports one particular detail of the overall system required by the above two practices.

A method on the manufacturer side to control firmware versions could be to limit firmware revisions to those that fix bugs or glitches. These "fixes" should not alter the IED functionality, its behavior with communication software, or the corresponding literature.

Changes regarding upgrades such as extension of ranges, addition of settings, or modification and addition of functions should be considered as model changes and identified in the catalog/part number. An upgrade of firmware to reflect such changes should imply a change on the IED faceplate data.

By using these manufacturer side guidelines, users should not experience unexpected changes from one vintage to the next when ordering IEDs with the same catalog/part number. In addition, the I3 Working Group of the IEEE PSRC is producing a recommended practice describing methods of assuring quality of relay firmware

9. Access Control

Relays are critical to the power system. The settings in a relay determine the response or non-response of the device. Incorrect settings may have serious effect on the power system operation.

Typically, only the protection personnel are allowed to change relay settings. However, the multi-function nature of microprocessor relays has extended use of protection devices to other groups as well. For example, a modern relay may replace a traditional RTU and provide metering data and control functions for opening and closing breakers and other switches or be connected to a substation computer that performs automation and control functions.

The multi-function nature of the relay may require settings changes by other groups, in addition to protection engineers. This creates an added challenge to track, document and verify relay settings. Modern relay designs recognize the need for increased access to the device and provide some means to help control setting changes:

- Passwords. Most relays have password protection for settings changes.
- A relay log and an alarm when setting changes have been made.
- Multiple levels of access, with different passwords for each level. Typically, there is a read-only level that may be viewed by a larger number of users, and a restricted full-access level for setting changes.
- A relay with multiple settings groups where a switch to another pre-verified group may be allowed by non-relay personnel, while change of individual parameters is not.

While procedures for access restriction to the substation are well established, the increased remote access to microprocessor relays is less regulated. Possible remote access points are:

- Modem (dial-up via phone line)
- Wireless
- Local and Wide Area Network (LAN/WAN)
- Internet

In addition to utility personnel, other groups may have needs to access the relays during certain conditions. These groups may include:

- Contractors
- System Integrators
- Equipment vendors
- Manufacturers

Remote access to change relay settings is one of the concerns for 'Cyber Security Issues for Relays' and is addressed in IEEE PSRC working group C1. Changing settings, from a cyber security point of view, does not differ from other malicious actions that can be performed when accessing a microprocessor relay. However, a setting change might not result in an immediate action by the relay and the attack could go undetected for some time.

A method of implementing a control scheme for remote access is to provide security and prevent any unauthorized access to the substation relays and related equipment via a modem. This scheme assumes that an RTU exists at the substation. The scheme includes the following features:

- RTU control points pulse a latching relay.
- One latching relay state represents "Enable Remote Access" and the other state represents "Disable Remote Access".
- The telephone line to the modem is connected through the latching relay.
- An additional latching relay contact provides feedback to the RTU on the status of the access, whether enabled or disabled.

This scheme provides a very high level of security because the modem connection is normally open, preventing any unauthorized use. Remote access to the modem requires the following:

- Person(s) requiring modem access are required to call the Power System
- Dispatcher to request that remote access to the stations dial-up modem be enabled
- The Dispatcher will issue a command to the RTU to actuate the designated output, which will pulse the designated latching relay coil.
- This will complete the phone line connection to the modem, allowing it to receive a phone call.

Another scheme is to restrict setting changes to a single individual or department. Many utilities use the extended capability of microprocessor relays to provide status, control and metering functions to a station RTU via a serial communication link. This functionality has replaced traditional analog transducer and hard-wired alarm connections to a central station RTU in all new installations and many retrofit locations. Any settings required for these extended functions are communicated to the protection engineer during the schematic and/or relay setting development phase. The automation engineer will also initiate setting changes through the protection engineer if changes associated with automation are required.

One practice is that the protection engineer is the individual responsible for all protective relay settings and documentation. The automation engineer or any other group that needs to change relay settings, works through the protection engineer to implement necessary automation settings. This, however, creates a possible bottleneck if the protection engineer is required to be the gatekeeper for all relay settings changes regardless of the protection functions impacts.

Schemes can also be achieved via password management. Relay access passwords are established that allow read-only access to automation engineers, maintenance personnel, system operator, etc. A more secure full-access level in which setting changes may be made is reserved for relay engineers and test technicians. Non-utility personnel may not be allowed remote access to relays. Testing contractors could utilize temporary passwords to complete necessary setting changes and testing – the settings are changed to secure passwords by company personnel following contract testing and/or commissioning.

10. Conclusions and Recommendations

The increasing complexity and higher demands from the power system place great importance on the availability of the network. Any misoperation can have catastrophic and wide-scale impacts (e.g., recent blackouts). The network protection and control system is an integral component to the overall system stability. The overall network reliability can have an adverse impact by protective device misoperation due to incorrect or wrong device settings. Correct operation of the protective relay system is highly dependent on:

- Validity of the network model
- Fault studies of the network
- Relay setting calculations
- Configuration management of the relay settings
- Policies and procedures to assure field personnel properly install and test relay settings
- Audit and validation of the protection relay settings
- Setting changes based on network modifications or changing system dynamics

Modern protection devices have increased in capability but also complexity, leading to the utility challenges in the ability to maintain system integrity due to the amount of integrated functions, multi-vendor installations, different firmware versions, different device configuration tools, and a number of different substation configurations. The utility-installed base of different protection technologies makes the task of managing the system infrastructure extremely difficult. Regulatory bodies continue to focus on system reliability improvements, the need to develop best practices and quality assurance procedures.

The recommendations that can be drawn from this report to improve the relay setting process are:
- **Implement a Quality Assurance System** including policy and procedures to formalize the relay settings process including maintenance, testing, and verification of the relay settings. The policy and procedures should be established according to a recognized quality system like ISO 9001.
- **Utilize a Configuration Management (CM) System** to manage and archive the relay setting calculations, setting sheets, setting download files and test/verification records, that also provide history and traceability. Establishment of a master settings database as part of the CM System will assure that the subscribers/users of the relay setting always have the correct version.
- **Establish an Audit and Validation Process** to routinely compare installed relay settings to the master database setting and to review the system network model for any changes that could require a change in or have an adverse affect on the relay performance.

11. References

[1] J. Paserba, C. Amicella, R. Adapa, and E. Dehdashti, “Assessment of Applications and Benefits of Phasor Measurement Technology in Power Systems”, in EPRI Wide Area Measurement Systems (WAMS) Workshop, Lakewood, Colorado, April 1997.

[2] Working Group D-6 of the Line Protection Subcommittee of the IEEE Power System Relaying Committee (Chairman K. Mustaphi), “EMTP Reference Models for Transmission Line Relay Testing”, Draft Version.

[3] Working Group H-7 of the Relaying Channels Subcommittee of the IEEE Power System Relaying Committee (Chairman A. G. Phadke), “Synchronized Sampling and Phasor Measurements for Relaying and Control”, IEEE Transactions on Power Delivery, vol. 9, no. 1, pp. 442-452, January 1994.

[4] C. F. Henville, “Digital Relay Reports Verify Power System Models”, IEEE Transactions on Power Delivery, vol. 13, no. 2, pp. 386-393, April 1998.

[5] L. Philippot and J.-C. Maun, “An application of Synchronous Phasor Measurement to the Estimation of the Parameters of an Overhead Transmission Line”, in Proceedings of the Fault and Disturbance Analysis and Precise Measurements Conference, Arlington, Virginia, November 1995.

[6] H.-J. Koglin and M. Schmidt, “Estimation of Transmission Line Parameters by Evaluating Fault Data Records”, in Proceedings of the 12th Power Systems Computation Conference, Dresden, Germany, August 1996.

[7] “Transmission Protective Relay System Performance Measuring Methodology”, IEEE/PSRC Working Group I3, 9/16/1999, available at www.pes-psrc.org.

[8] IEEE Power System Relaying Committee, “Data and Data Base Structures for Protection Engineering”, TP-129-0, September, 1996.

[9] Praxiom Research Group Limited , “ISO 9001 2000 Translated into Plain English” available at http://praxiom.com/iso-9001-b.htm.

Appendix A: **Verifying Transmission Line Impedances**

Computing the transmission line impedance using data recorded by relays or DFRs is fairly straightforward, if the fault location is known.

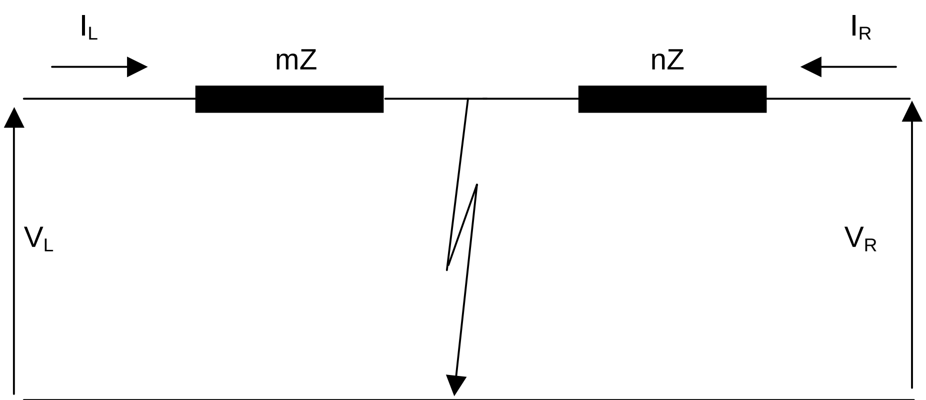


Figure A.1: Line with Fault at Known Location.

In figure A.1, let the transmission line impedance be Z. It needs to be determined from the relay or DFR data recorded at one or both ends. This data is denoted by the voltages VL and VR and the currents IL and IR, as shown.

The fault location is known. That is, m and n are known quantities, m+n = 1.

If the fault is a zero-impedance fault, then knowledge of voltage and current information from one end is sufficient to determine the impedance of the line Z.

However, if the fault impedance is unknown, as is usually the case, knowledge of the voltage and current from both ends of the line can be used to eliminate the fault impedance from the algebraic equations for voltage balance.

Figure 4.2 is for a single-phase circuit. For the three-phase fundamental frequency network, the positive-, negative- and zero-sequence networks have to be suitably connected (depending on the fault type) to obtain the solution.

Researchers have proposed other methods for line impedance estimation that do not depend on knowledge of the fault location [5, 6]. Some of the salient features of these methods are:

1. Data is acquired from either DFRs or digital relays
2. The data can be for disturbances either on the line of interest or on external lines.
3. The data recordings may or may not be synchronized.
4. For unsynchronized data, data from multiple events is required for accurate estimation of the line parameters.

The computed line impedances are compared with the impedances as determined by the line constants program.

This is especially critical for ground distance relays that depend on and are highly sensitive to the zero sequence system model, which includes zero-sequence mutual coupling. Errors in the zero-sequence system model have resulted in over reach/under reach of ground distance (as well as backup ground instantaneous overcurrent) elements.

Using the Equivalent Source Impedance for Model Validation

Figure A.2 shows the positive-, negative- and zero-sequence circuits involving the source impedance, at the location where data is collected.

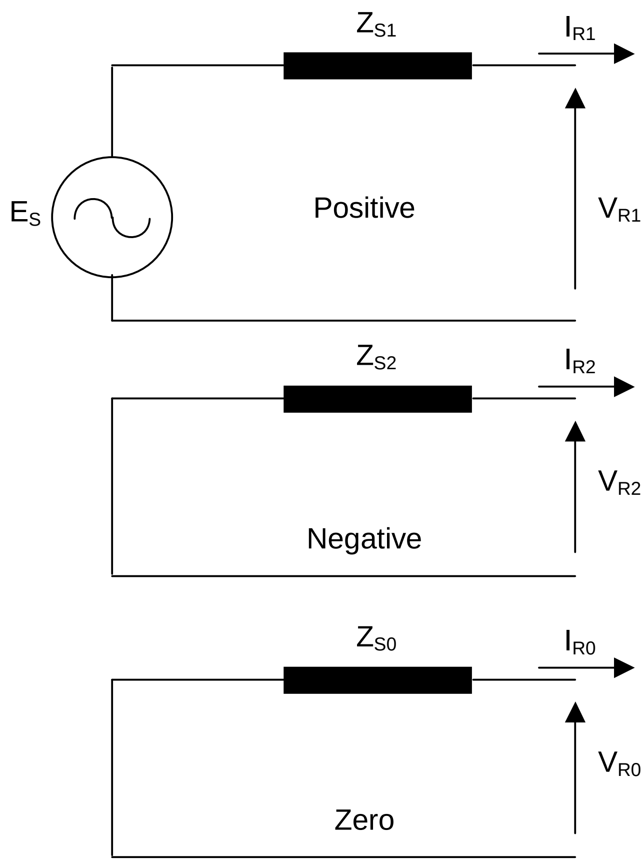


Figure A.2: Source Impedances at Data Collection Point.

The circuit in Figure A.2 shows the equivalent source impedances behind the data collection point in each sequence – ZS1, ZS2 and ZS0. The voltages and currents recorded at the data collection point (to the right of the source impedance) are also shown. These are the post-fault voltages and currents denoted by VR1, IR1, VR2, IR2, VR0 and IR0.

The EMF ES is the internal EMF of an equivalent generator at the data collection bus. Its value depends on the pre-fault current flow, and is not easily known. If the pre-fault load flow is ignored, then ES is equal to the pre-fault voltage at the data collection bus.

The source impedance is then defined as –1 times the ratio of the change in the bus voltage from pre-fault to fault condition to the change in the branch current from pre-fault to fault condition. In other words, the source impedance in each sequence can be written as

$$Z_{S1} = -\frac{V_{R1} - V_{R1,PRE}}{I_{R1} - I_{R1,PRE}}$$

$$Z_{S2} = -\frac{V_{R2}}{I_{R2}}$$

$$Z_{S0} = -\frac{V_{R0}}{I_{R0}} \qquad (1)$$

The subscript "PRE" above denotes pre-fault measurements.

Notice that the pre-fault voltages in the negative- and zero-sequence circuits are assumed to be zero, implying a balanced network. Also, the data collection device must be able to record the pre-fault voltage and current.

It is very important to note that in general, the source impedance computed using Equation (1) depends on the location of the fault along the line. In the general case, not all the current that flows through the source impedance will flow through the data collection point also. There will be paths from the source impedance to the remote terminal through which fault current will flow. As the fault location changes, the fault currents will redistribute themselves and change the source impedance at the data collection point.

If the line is radial or if we have a true two-machine system, the source impedance behind the data collection point is unique.

The source impedance computed from the recorded data is compared with the source impedance computed from the network model at the same location. Of course, the system condition in terms of open breakers, out-of-service equipment, off-line generators etc. has to be included when computing the source impedance from the network model. Not having an exact match with actual system condition when the data was recorded is another source of error in model validation.

The applicability of the source impedance technique to model validation can be understood from the one-line diagram in Figure A.3.

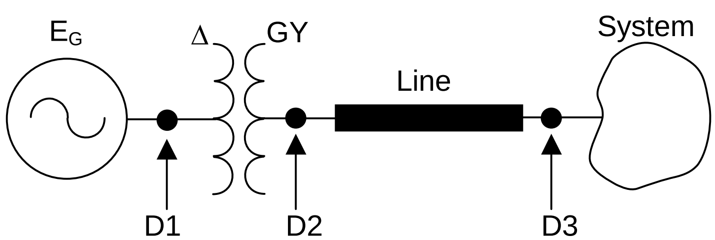


Figure A.3: Example One-Line Diagram.

The system consists of a generating station EG, with a delta-GY transformer, connecting to a line. At the end of the line is the rest of the system; the network is radial, and therefore a good candidate for model validation using the source impedance technique.

Three points D1, D2 and D3 in Figure 4.4 are possible points for data collection.

A fault on the high side of the transformer, with data collection on the low side (D1) will produce data that can be used to validate the positive- and negative-sequence impedance data of the generator.

A ground fault anywhere along the line, or in the system, with data collection on the high side of the transformer (D2) will produce data that can validate the zero-sequence impedance of the transformer. Note that the transformer is connected delta-GY, and therefore, the zero-sequence source impedance at D2 comprises entirely the zero-sequence impedance of the transformer.

Finally, data collection at point D3, with faults anywhere on the line or transformer can help validate the equivalent source impedance of the rest of the system. In this case, discrepancies between the simulated source impedance and the source impedance computed from measured data cannot be attributed to one particular piece of equipment.

Mismatch between the actual system conditions during data recording and during simulations is another factor to be considered.