Anomaly Checks for Relay Settings

Report to the Main Committee from PSRC

WG I18

Final Report

Date:- January 2011

P.G. McLaren (chairman), M. Nagpal (vice-chairman), H. Ashrafi, R. Barone, S. Brahma, D. Fontana, R. Garcia, A. Girgis, D. Goodrich, Y. Liao, D. Loudermilk, M. Meisinger, S. Musunuri, M. Sachdev, R. Turner, S. Turner.

Table of Contents

1.0 Introduction

"Anomaly Checks for Relay Settings" met twice as a Task Force before becoming WG I18 of the Relay Practices sub-committee. The Task Force decided not to concern itself with security measures within the relay software itself but rather to concentrate on how the relay engineer could best be sure that correct settings were established and maintained on a relay. The WG assignment was as follows:

The WG will produce a report on relay software features and setting practices which minimize the possibility of wrong settings being downloaded to a relay. The WG will commence its task by conducting a survey of relay manufacturers and utilities to get information on present practice. ***It should be noted that the survey was completed before the NERC/FERC guidelines (Reliability Standards for the Bulk Electric Systems of North America, CIP-002-1 to CIP-009-1) were put in place.***

In addition to the above mentioned Survey the WG took note of the fact that CIGRE sub-committee B5.31 entitled "Life–time Management of Relay Settings" was working on a report likely to contain information of interest to the WG and resolved to include this information with appropriate acknowledgements. During subsequent deliberations the report of WG C3 of the IEEE PSRC entitled "Processes, Issues, Trends and Quality Control of Relay Settings." was mentioned as another document to be consulted. Once the results of the survey were known and the relevant information had been extracted from CIGRE B5.31 and C3 the WG resolved to finish its work by compiling a "Best Practices" section in the final report.

2.0 Results of the Surveys sent to Manufacturers and Utilities

The objective of the survey was to identify sources of unintended setting errors and currently used deterrent mechanisms by the utility industry to guard against deliberate tampering with the relay settings. Separate questionnaires were prepared for relay manufacturers and utilities and sent out at the end of 2008. 15 relay manufacturers and 53 utilities were targetted using PSRC members as the initial recipients. 9 manufacturers and 19 utilities responded.
The questionnaires covered two main fields of interest, relay settings and relay security with an additional category on software for the manufacturers. The questions and detailed responses are given in the appendix (6.0). A brief summary of the responses follows.

2.1 Relay Settings/Software

2.1.1 Manufacturers

All respondents' relays log that a setting change has been made but only 2 log the actual change. All provide multiple groups of settings but are evenly split on whether or not they allow setting changes to be simultaneously applied to multiple groups.
In terms of interfaces, all respondents' relays have RS 232, RS 485 and Ethernet and a couple also have Serial Fiber Optic interfaces offered as options. Not all relays come with all the interfaces as standard fare.
Most have a "Compare" function which allows settings on the relay to be compared to calculated values residing on a connected PC. This function may also cover configuration and logic. The way in which the comparison results are presented varies. The connected PC needs to be running software available from the manufacturer, usually provided on a CD but in a few cases, publically available on the web (with or without a password). Most relays allow simple standard software upgrades.

2.1.2 Utilities

The majority of respondents rely upon a peer review process to catch setting calculation errors. About half as many rely on applying sanity checks (eg: verifying Z2>Z1). A handful use software tools and other processes. The majority of the utilities deploy settings via local file downloads. Only two respondents use remote file downloads. A small number of utilities still apply settings manually from hard copies. While there is slightly more acceptance of remotely applying non-critical settings, the majority of utilities apply setting changes, critical or non-critical, using local access. The vast majority of respondents use commissioning tests to ensure that the downloaded settings are as intended. Setting comparisons were slightly less popular. It should be noted that the number of responses exceeded the number of surveys received because many utilities use a combination of methods.

Approximately two thirds of the utilities polled experienced cases where actual relay settings differed from those intended mainly due to human errors, except two attributed to computer glitches. Most utilities verify settings during routine maintainenance testing – though testing cycles vary from 2 to 14 years. Besides routine maintenance testing, relay mal-operation was reported as the major factor that prompted relay setting checks. However, one utility also responded that they checked settings when tampering was suspected. Most respondents indicated that they performed settings or coordination reviews in response to network changes. However, several also indicated they perform routine coordination studies with intervals varying from 3 to 10 years.

2.2 Security

2.2.1 Manufacturers

The majority of respondents do not have configurable ports but those that do, offer “read/write”, “read only” or “disable” options.
Password levels range from 2 to 8 with 1 to 16 characters, including numbers or letters. The majority allow an indefinite number of attempts at a password but those that do not will lock out for a specific period and may alarm. No manufacturer requires the default password to be changed but one requires periodic changes in the password. When attempting to insert the password most will time out after a user selectable timespan. The procedure for resetting the password differs widely, e.g. “on the CD or website”, “in instruction manual”, “tech support”, “return to factory”. In 3 cases no knowledge of the previous password is required. Not all relays log the reset or change of password.

2.2.2 Utilities

Almost all respondents have remote access to numerical relays via dial-up or intranet with dial-up access still being the majority. *(Survey preceded new NERC/FERC guidelines covering relays with routable protocol and tripping.)* A few respondents also have Supervisory Control and Data Acquisition/Remote Terminal Unit (SCADA/RTU) access. Passwords are still the most commonly used guard against unwanted access to the relays. A few utilities also use a Virtual Private Network (VPN) for secure access. The majority of utilities use password protected intermediate communication interfaces to provide remote access to the relays. Multiple passwords with different authorization levels are used. More than half of the respondents do not use hardened passwords; do not periodically change passwords; or have access to relays from multiple locations. There is almost an even split between those who do and do not alarm on relay access. These alarms are typically generated on higher level access or on multiple password access failure. All respondents use some form of physical deterrent such as gates or doors to prevent unwanted access to the relays. The majority indicated that they deploy video surveillance of their assets.

2.2.3 Additional Features not covered in Questionnaire

Respondents were asked to mention any features they offered or used which were not in the questionnaire. Amongst others (see appendix 28) were mentioned “pickup and range setting checks” and the use of a user name as well as a password.

2.3 Conclusions

There are widely different approaches to checking relay settings and guarding the security of the setting process.
Very few utilities allow remote changes to settings.
Two thirds of the Utilties polled reported cases of settings being different to those intended and attributed those to human error.

3.0 Other Working Groups activities relevant to WG I18

There are at least two other recent or contemporary WG's that have considered the issues of checking relay settings. They are

- WG C3 of the IEEE PSRC entitled "Processes, Issues, Trends and Quality Control of Relay Settings." Dated March 2007.
- CIGRE WG B5.31 entitled "Life-time Management of Relay Settings." Draft Report, 2009.

Both groups have wider ranging mandates than WG I18, as suggested by their respective titles, and the following sub-sections give a brief abstract of material relevant to WG I18.

3.1 WG C3 of the IEEE PSRC

The following abstracts from the report summarize the relevance to WG I18.

"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."

"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, multivendor 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."

3.2 CIGRE WG B5.31 Draft Report

Here are a list of relevant points made throughout the report:

1. A recurring feature is the mention of the need to complete the setting loop by returning the "as left" settings file from the field engineers to the protection engineer who issued the settings in the first instance. Modern relays will generate an "as left" file but older electromechanical and analogue electronic (static) relays will rely on the field engineer to produce this file.
2. The peer review process could include "Challenge" sessions where experienced protection engineers comment and *challenge* the proposed settings. This process should also include junior engineers as part of their education process.
3. Make sure the primary network model is kept up to date and that all groups involved in the settings calculation process are using the same version.
4. Make sure all groups are using the same version of the manufacturers setting software.
5. Make sure unused features are disabled.
6. If using a "Template" make sure it is the right one for the relay and application.
7. Use software which automatically transfers settings from a computer setting calculation into the manufacturers setting software or into the setting sheet to avoid typing errors.
8. If it is necessary to change a setting during commissioning do not leave the changed setting in the relay. If groups of settings are available in the relay keep the original settings in one of the groups.
9. Disable relay outputs during firmware upgrades.
10. Different manufacturers use different names for phase voltages and currents. IEC 61850 will improve this.
11. A "Compare" function should compare the new settings to the old settings.
12. All protection engineers and technicians should be well acquainted with company and external standards, methods and practices, e.g., North American Electric Reliability Corporation (NERC) loadability rules.
13. The setting output document should contain the names of those involved in deriving the settings.
14. Manufacturers should be well informed on utility setting practices and design their setting software accordingly.

4.0 Best Utility Practices

4.1 Introduction

Errors in relay settings can arise from many different sources, some technical, some procedural, some administrative, some inadvertent and some possibly deliberate (hacker). As an example of an error based on several of these factors , the settings for the distance relays on a long ehv line were determined based on a Π-line model in which the charging capacitance was to be fully compensated at both line ends by shunt reactors. When shunt compensation was installed, the shunt reactors used did not fully compensate the line charging currents and furthermore the two reactors were not of the same value. The result of this difference from the planned design was that the zone 2 setting at one end did not quite reach the remote busbar and a fault just in front of the remote busbar would not be picked up in Zone 2. The intertrip signal from the relay trip at the remote end was monitored by the Zone 2 operation of the local relay and therefore would not have allowed the local relay to trip until the zone 3 timer timed out. Fortunately there had not been such a fault location on the line before the "Anomaly" came to light during an upgrade in settings to allow the insertion of series compensation. This example highlights the need to make sure the settings are based on an up-to-date model.
Based on the survey results, the Cigre B5.31 points of interest, and the comments from WG members there follows a compilation of "Best" utility practices to prevent wrong settings being loaded into a relay.

4.2 Sources of Error

4.2.1 Errors occurring during the process of calculating settings

4.2.1.1 Errors of omission or technical errors

- Incorrect method for calculating settings: for example, zero-sequence current is not appropriately considered in calculating setting for ground distance element.
- Over simplification of method for calculating settings: for example, short line model is used for very long lines.
- Settings do not adequately consider transient state: steady state short circuit analysis is typically utilized; high frequency transients may also need to be considered for certain applications such as CVT transients.
- Negligence in calculating settings: for example, using wrong line impedance value, using wrong Current Transformer (CT) value.

4.2.1.2 Incorrect short circuit model data

- System model is outdated, and does not reflect prevailing conditions.
- Unbalanced system is not adequately modeled: untransposed line is treated as transposed line.
- Mutual coupling between the two circuits of a parallel line is not adequately represented.
- Transformer and generator grounding scheme is wrongly modeled.
- Choosing wrong generator impedance: subtransient, transient, synchronous impedance.

4.2.1.3 Relay setting software errors

- Errors caused by relay setting software bugs
- Errors caused by improper use of relay setting software

4.2.2 Errors during the process of entering settings to relays

4.2.2.1 Transcription type errors

- Errors occurring when copying calculated relay settings onto the relay setting sheet
- Typo when entering settings to the relay
- Entering relay settings to a different relay
- Enter relay settings to a wrong setting group

4.2.2.2 Errors during the process of checking settings

- Inadvertently change relay settings

4.2.2.3 (Errors caused by hackers due to inadequate security measures)

4.2.2.4 (Errors caused by discontented employees)

4.2.3 Methods of minimizing/eliminating sources of error

4.2.3.1 Peer reviews

Peer review of settings is a process by which errors in relay settings, logical and numerical settings, can be reduced. The extent to which the error can be reduced depends upon effort or level of peer review.

There are various levels of peer review from independent development of settings to a high level review. Independent development requires the maximum effort and is likely to yield settings with minimal errors. While high level peer review may not require as much effort, errors in non-core settings will slip through.

Independent Development of settings requires that two application engineers each prepare a complete set of protection settings independently of each other. Settings are then compared and differences reconciled before releasing for implementation. Independent development nearly eliminates human or calculation errors. It can also catch errors arising when incorrect assumptions or data are applied by one application engineer. Since the settings are developed by two engineers independently and then compared to each other, setting development can require twice as much resource.

Independent Thorough Review requires that one engineer develops the settings, and another engineer performs an independent review of all settings, numerical and logical. This type of review is likely to catch the majority of human or calculation errors. It can potentially also pick up errors from incorrect assumptions or data depending upon the reviewer's expertise and familiarity with the system where the settings are being applied. It is thus recommended that the reviewer be expert with in-depth familiarity with the systems.

Independent High Level Review involves only review of the core settings by peer. Since the review is limited, there is a potential for human or calculation errors in non-core and logic settings to not be detected.

4.2.3.2 Training for young and older engineers/test personnel

It is in the company's interest to make sure its engineers are kept up to date with new technology, new protection techniques and company procedures. All protection engineers and test personnel must be conversant with company and external standards, company methods and processes in determining settings, applying settings and checking settings. This requires ongoing presentations from internal and external experts to keep personnel up to date with rapidly changing technology. Younger engineers will be more comfortable with the new communication and computer technologies but lacking in protection application knowledge while the converse is true for older engineers. As part of their education process, younger inexperienced engineers should be involved in the peer review process for checking new relay settings. Wherever possible training should include hands on experience in setting and testing relays using test sets or real time simulators. The latter are more likely to be encountered in courses offered by manufacturers.

4.2.3.3 Field Testing

4.2.3.3.1 Bench testing

As a relay arrives from the factory, some companies desire to run a bench test to prove the relay functions as designed. The process of this test can range quite extensively.

1. For electro-mechanical and electronic relays, three basic bench testing philosophies exist, if it is to be performed.

(a) Perform a test procedure that verifies each available tap, adjust the relay to prove the lowest available settings and high available settings, and perform other various tests to prove that the relay will operate within any applicable range that is available on this relay.

(b) Perform a test procedure using a pre-determined setting value to verify acceptable relay behavior.

(c) Apply field settings on the relay and test as if the relay were in service. This would be considered the element test, only proven on the test bench rather than in the field.

(2) For microprocessor relays, two basic bench testing philosophies exist, if it is to be performed.

(a) Load a pre-determined group of settings into the relay and perform a test to verify the relay operates as expected.

(b) Apply field settings on the relay and test as if the relay were in service. This would be considered the element test, only proven on the test bench rather than in the field.

(c) Three things should always be proven if bench testing a relay, and that is the A/D converter by performing a Meter Test, verification of all Output contacts and verification of all Inputs.

4.2.3.3.2 Macro-based testing (element testing using automated software)

(1) Element testing is initially performed during relay installation, then repeated on a rotational basis to prove a relay operates as expected with its in-service settings.

(2) With electro-mechanical and electronic relays, it is important that testing be performed to verify any component, mechanical or electronic in nature, has not failed and the relay will operate at expected trip levels.

(3) With micro-processor relays, two main theories exist

(a) Testing methods utilized on electro-mechanical relays are carried over to the micro-processor relay by proving operation of each element that is programmed within this relay. Included in this test should be a meter test to prove proper performance of the Voltage transformers, Current transformers, and the A/D converter, operations to verify relay outputs, and operations to verify relay inputs.

(b) The second theory is that element testing in not required, since the relay is digital in nature, thus is not performed. Instead, you need to simply verify proper operation of items that cannot be monitored digitally; perform a meter test to prove proper performance of the Voltage transformers, Current transformers, and the A/D converter, verify relay output, and verify relay inputs. However, it has been recommended by the manufacturer to incorporate validation of proper operation through monitoring or events reports in lieu of element tests.

(c) Some of the reasoning utilized to continue traditional element testing methods is simply for documentation of actual relay operation and give confidence that the relay will operate as expected.

(i) Automated element testing is designed to test an element at the setting provided, which generally will not catch actual settings errors, rather verify the setting that is on the relay. Although, if the elements are tested at settings values, documentation exists as to how that relay will react in service with applied settings.

(ii) Element testing can give one confidence that the relay will operate when a fault occurs. Without performing any element tests at all, one is relying on the device to protect the community and property based simply on the fact it is a digital relay.

(d) Regardless of the method selected, one thing should be understood; if the relay has programmable logic, *element testing will NOT prove the relay will operate correctly when placed in service.* The element test simply proves the internal element bit will come high, but does nothing to verify the element bit is mapped properly through the trip logic to close the desired output. This must be proven in logic testing.

4.2.3.3.3 Logic testing (incorporated into the Functional Test or Trip Test)

(1) Logic testing in its purest sense is specific to microprocessor relays. It is proving that the programmable logic (organization of element bits, inputs, and outputs) created by the protection engineer will function as designed. In a basic sense, this has been performed for years in a much simpler fashion, rather given alternate names such as a trip test or functional test. When a relay of any kind is placed in service, there should be no question that the relay device should be proven to physically operate its intended target. Some companies perform some type of trip verification only at the time of installation, where others continue this practice on a repetitive cycle.

(2) With electro-mechanicals, the trip test is generally performed by closing individual relay output contacts manually to verify proper equipment operation. Since element testing has proven the electrical/mechanical operations of the relay, manually closing the trip contact is acceptable.

(3) With electronic relays, the trip test should be performed by current/voltage injection to prove outputs properly operate the intended target.

(4) For micro-processor relays where logic is handled internally, (output contacts are internally mapped), the trip test (logic test) should be performed by current/voltage injection to prove outputs properly operate the intended target.

(5) For micro-processor relays that utilize programmable logic, it is imperative that the logical operations are proven to be valid. This process can become extremely complex, based on the logic created by the protection engineer. As logic equations by nature can be diverse, applied logic tests will become specific per relay. The more consistent logic equations are applied to the relay, the more consistency will be available to the logic test itself. In the end, the logic testing is performed to verify the logical sequences incorporated into the relay by the protection engineer are valid and will operate desired relay outputs contacts as designed.

(a) *Note: Testing of the logic equations should be proven at the time of relay installation. A written functional description of the logic should be used for testing of the logic equations. Testing to a functional description is necessary to prove the logic operates as intended. If the logic equations are not tampered with, there is no known reason to re-prove logic in subsequent testing. If the logic equations are modified, logic testing should be performed on the modified equations. Even though the logic equations themselves do not require re-verification, repetitive testing cycles should include operations of the outputs contacts. In this case, the trip test should still be performed by current/voltage injection to prove outputs properly operate the intended target.*

4.2.3.3.4 End to End testing (satellite tests for communication assisted relaying schemes)

The end to end test is primarily used to verify the communication channels between two relays, whether this be a carrier scheme, direct transfer trip, mirrored bits, line differential, etc. Synchronised fault voltage and current waveforms derived from off-line simulations are applied simultaneously to the relay at each end of the line. Faults are applied at various points on the line (in the off-line simulations) to prove zone coordination and detection of a forward/reverse fault. The end-to-end tests typically are not written to prove the accuracy of the relay or any elements beyond the scope of what is required to prove the communications scheme. Macro-based testing (steady state testing) is the typical preferred method of proving element accuracy.

4.2.3.3.5 Comtrade file playback

(1) Another method of testing is replaying recorded faults through the relay to monitor expected operation. The recorded faults are acquired by external fault recorders, internal fault recordings captured by the relay, or created by software fault simulation programs. The general format of the file will be a Comtrade file.

(2) The general reason for replaying a Comtrade file is to repeat a specific fault sequence when mis-operations occur during a fault. When troubleshooting a mis-operation, it can be difficult at times to locate the cause with standard element testing, trip testing, or other general troubleshooting skills. Replaying the fault condition can be a useful tool in determining the cause.

(3) Comtrade file playback can be incorporated as a one step verification of the relaying system as a whole. This operation will not prove the accuracy of the relay, but will prove the relay will function properly, that the output contact will operate, and the DC circuitry is still present to the connected device.

4.2.3.4 Design basis documents-issue to field along with relay settings document

Field maintenance and commissioning personnel can also perform an independent review function to ensure that errors in settings do not make it into service. However, they can only provide this function effectively if they actually understand the intent and performance requirements of the relaying system. To this end, it may be useful to provide supplementary information (along with the settings) to field personnel describing the intended functionality of the settings, with information on the logic and basic reaches of relay elements (ideally in functional terms such as "underreach remote bus" rather than "27 primary ohms"). Armed with this information, the field personnel will be better prepared to determine whether the actual relay settings and hardware perform according to the intentions of the protection engineer.

4.2.3.4.1 Generating "as found" and "as left" files in field during testing

As a part of relay testing, technologists can record the settings loaded within the relay both before work proceeds, and after it is completed. With modern numerical relays, relay software can poll the relay for settings and generate these files. These files by themselves do not enforce setting quality, but can be used as part of corporately defined quality assurance and audit processes. Comparison of these files can show:

1. that the settings on the relay have not been changed since the last maintenance.
2. that only the settings which were meant to be changed during maintenance efforts have actually been changed.

4.2.3.4.2 Using compare functions after uploading settings file into relay.

In most situations involving numerical relays, a complete setting file is generated for upload to the relay regardless of how many settings are actually being modified. However, in cases where setting changes are being issued in a non-native relay setting file format (ie: paper copies, or a simple e-mail), there is the possibility of field staff accidentally changing settings which were not intended to be changed.
By reading the relay settings before and after settings are updated, the comparison function in numerical relay configuration software can verify that only the intended setting(s) were changed.

4.2.3.5 Using compare functions in home office after receiving the "as Found" and "as left" setting files.

It is good engineering practice to have closed loop control over settings. By using the setting retrieval feature of numerical relay configuration software, the "as found" and "as left" settings can be recorded and sent back to the engineer who issued the settings. These files provide the following information:

1. Verification that the previous revision of settings were correctly applied to the relay and that no unauthorized changes were made prior to the application of the new settings.
2. Proof that the new settings were loaded correctly onto the relay
3. A time stamp indicating when these settings were put into service

In addition, by sending **all** relay settings back to the issuing engineer, "Field set" settings (such as communication port settings, event recording settings) can be stored in a centralized location.

4.2.3.6 Software "auto checking" features (range checking, syntax checking etc)

Auto checking features enable the relay to block entry of settings which are either outside of the range of the relay, or "wrong" in some way. These "wrong" settings could be due to an unintentional mistake of the user, or due to the malicious intentions of wrong doers.

The relay must be able to signal when some settings are set out of the range. Therefore the relay setting parameters should be defined with a minimum and a maximum value.
When some invalid characters are attempted to be input, the syntax values need to be checked by the software.
When obviously erroneous values are attempted to be entered, the software should not allow any such inputs.
Also when some settings are modified then a password should be required to accept the changes.
With such basic auto checking features the possibility for an erroneous value to be set to a parameter can be reduced.

4.3 Management of Relay Settings

4.3.1 Methods for Filing Settings

A common method for storing settings from relays is databases. You can customize the database for any relay type, including, but not limited to, overcurrent relays, distance relays, differential relays, and voltage relays. The database is capable of handling electromechanical relays with just a few setting parameters to modern microprocessor relays with hundreds of parameters. You can store one or more sets of setting parameters. Some of these can be historical while others can be emergency or pending settings. You can also store test results. The database is the best method for filing settings if you have a large fleet of numerical relays, such as for a large electric utility.

4.3.2 Security

Numerical relays provide password protection for the communication ports to discourage unauthorized remote access. There are typically several levels of password-enabled security:

1st Level - Establish local/remote communication sessions. Typically allows only verification that contact has been made.

2nd Level - Read-Only Access (ROA), commonly referred to as "look but not touch." The local/remote user can typically view and download events (e.g., oscillography, sequence of events, fault records, etc.), check the results of relay self-test, view metering and breaker status, and possibly view protection settings. ROA prevents anyone without the higher level passwords from making any changes, and thus is an important defense for cyber security.

3rd Level - Full control. This level typically allows full control over the relay. The local/remote user can change relay settings, change passwords, close output contacts, and even disable the relay.

4.3.3 Methods of issuing to field (email, remote retrieval, etc.)

Electronic relay setting files are typically sent out via email or stored on a server that is only accessible by a restricted group of personnel.

4.3.4 Relay testing and setting checks (NERC requirements)

A common commissioning practice is to test all the numerical relay settings to verify they were properly entered. Automated testing using computer software to run the test set or real time simulator has made this possible since the overall commissioning for a numerical relay could consist of several hundred tests. While this is a good check it is still important to ensure that the apparatus is thoroughly protected for the particular application.

All IP addresses should be removed from relays when they are being taken from the station for return back to the manufacturer for service unless special security agreements are in place with the repair facility.

5.0 Conclusions

The results of the surveys indicate that many Utilities have had instances of wrong settings getting on to a relay. The surveys also indicate a wide variety of practices followed by different Utilities in order to minimize such errors. At the time of the survey (early 2009) only one Utility reported a case of suspected tampering. The majority of errors were attributed to "Human error". Cyber security was not (as then) a significant issue since only a few Utilities allowed remote access to settings.

Based on the survey results and information taken from the report of CIGRE subcommittee B5.31, "Life-time Management of Relay Settings" the WG compiled an extensive list of "Best Practices" to be followed by Utilities in order to minimize setting errors. The CIGRE subcommittee also included one recommendation that Manufacturers should be mindful of Utility setting practices when designing their products.

It is clear that the modern multifunction digital relay challenges conventional practice for applying, setting and testing of its functions and that education has a role to play in helping to minimize errors in relay settings.

6.0 Appendix

Survey Questions and Responses for Relay Manufacturers

Please respond to this survey based upon relays that are being offered today. Also, if your company offers different series' of relays please fill out a separate form for each series. *(Comments from respondents are shown bulleted in italics immediately after the item to which they apply)*

RELAY SETTINGS QUESTIONS

1. When a relay setting change is made, does the relay (check all that apply):
   - Close a contact II
   - Log that a change has been made IIIIIII
   - Log the actual change II
   - Other (please specify):
2. Does your relay provide multiple groups of relay settings?
   - Yes IIIIIIIII
   - No
3. If yes does your relay allow setting changes to be simultaneously applied to multiple groups of settings?
   - Yes IIIII
   - No IIII

SOFTWARE RELATED QUESTIONS

4. What communication interfaces does your relay provide (check all that apply)?
   - RS-232 IIIIIIII
   - RS-485 IIIIIIII
   - INCOM I
   - Ethernet IIIIII
   - USB I
   - Serial Fiber Optic IIII
   - WiFi I
   - Radio I
5. Does your relay software have a compare function, so that settings on a relay can be easily compared to the calculated (issued) settings?
   - Yes IIIIIII
   - No II
6. Will the above compare function also work for the logic and configuration settings?
   - Yes IIIII
   - No III

   •*Software will tell you if logic has been changed but not specifically what changed; all setting changes are specifically listed*

7. If the above answer is yes, how is the compare function performed?
   - *Software performs a line-by-line comparison of active relay settings to archived and/or external settings file*
   - *Software compares active settings to those residing on the PC*
   - Changed parameters in (5) are shown in detail; a change in (6) is shown by a general indication; the parameter set has a CRC checksum - changes between device and PC are shown by CRC difference
   - Actual relay settings are read by the "Software" and the user selects the "compare to" relay setting file; a report with the settings differences will be generated by the software
   - Setting violations are flagged then changes are not allowed
8. Does your software allow for simple standard updates? As an example, if one logical AND setting needed to be changed to an OR setting, can that change be made to each relay with a software action, rather than having to manually make the change on each relay?
   - Yes IIIIII
   - No IIII
9. Is your relay software available to the general public?
   - Yes III
   - No IIIII
   - *Not general public, this requires website registration and approval.*
10. Does your relay software require the user to change the factory default password?
    - Yes
    - No IIIIIIIII
11. Does your relay software require the user to change the password periodically?
    - Yes I
    - No IIIIIIII
12. If Yes, how often?
13. For a computer to connect to your relay, does the computer need to have special software installed?
    - Yes IIIIII
    - No I

    - *Can use ASCII terminal*
14. If yes where can such software be obtained (check all that apply)?
    - A CD supplied to the user by you IIIIIII
    - A publically accessible website III
    - A password-protected website II
    - Other (please specify)
15. After a user logs into the relay, will the relay time out after a certain period of inactivity?
    - Yes IIIIII
    - No III
16. If yes what is the time out value?
    - *5 minutes*
    - *user selectable*
17. Without knowing the password, can someone reset the password?
    - Yes III
    - No IIIIII
18. Where can one find out the procedure to reset the password (check all that applies)?
    - A CD supplied to the user by the vendor IIIII

    - *Yes if the active password is known and authorized by security level.*
    - A publically accessible website I
    - A password-protected website II
    - Other (please specify):

    - *Contact factory technical support (3)*
    - *Instruction manual*
    - *Must be returned to the factory*
19. Does your relay make a log when a password is reset?

- Yes IIIII
- No IIII

20. Does your relay make a log when a password is changed?
    - Yes IIIII
    - No IIII

SECURITY RELATED QUESTIONS:

21. Do your relays have configurable ports?
    - Yes IIII
    - No IIIII
22. If yes, what are the configurations available (check all that apply)
    - Read-only III
    - Read/Write III
    - Disable II
23. How many and what type of password levels do your relays have?
    - 8 (2)
    - *7*
    - *5*
    - *4*
    - *3 (2)*
    - *2*
24. Regarding the relay password, what is the minimum number of characters?
    - *1 (2)*
    - *3*
    - *4 (2)*
    - *16*
25. Can both letters and numbers be used in the relay password?
    - Yes IIIIIII
    - No II
26. How many attempts at a password are allowed?
    - 2
    - 3 I
    - Other (please specify)
        - *Unlimited (7)*
27. Once that number of password attempts is exceeded, what happens with the relay (check all that applies)?
    - An alarm contact operates I
    - The relay locks out the user for a period of time II
    - Other (please specify) II
28. Do you offer any additional features, not covered above, which help to avoid anomaly check issues?
    - *Usernames with passwords*
    - *Graphical user interface and programmable logic representation*
    - *Setting range checking*
    - *Pickup checks (will not accept setting if relay is active and will exceed pickup with new settings)*
    - *CRC checks on file transfers*
    - *Settings for one amp rated relay cannot be uploaded to a five amp rated relay and vice versa*

Survey Questions and Responses for Utilities (19 respondents)

(Comments from respondents are shown bulleted in italics immediately after the item to which they apply)

RELAY SETTINGS QUESTIONS

1) What practices do you adopt to ensure that the new settings are correct after relay settings are calculated? Check all those that apply to you.

- ☐ Peer review lllllllllllll
- ☐ Sanity check such as range check (e.g., Z2 > Z1) llllllll
- ☐ Software that automatically checks settings llllll
- *On a limited basis(1)*
- ☐ Other: - llll

- *After setting values have been input into the relay settings file, a "second pass" of the settings file will be made by the engineer to check for accuracy. This is preferably but not always done on a different day than when the settings values were input initially.*
- *Minimal sanity checking internal to relay*
- *End to end testing*
- *Software that uses templates to ensure consistent relay logic and setting summaries which summarize the actual settings that have been used*

2) How are settings downloaded to the relay?

- ☐ Electronic file [LOCAL☐/REMOTE☐] L(lllllllllllllllll) R(ll)
- ☐ Manually (e.g., hard copy) llllllll
- ☐ Other: -

3) How do you change relay settings for protection *critical* settings such as zone 2 time delay?

- ☐ Locally lllllllllllllll
- ☐ Remotely llll
- *Response is broken into stations with SCADA or without SCADA*

4) How do you change relay settings for protection *non critical* settings such as fault record length?

- ☐ Locally lllllllllll
- ☐ Remotely llllllll
- *Response is broken into stations with SCADA or without SCADA*
- *Rarely, in emergencies only.*

5) What measures are taken to ensure that the intended settings are saved in the relay after the new relay settings are downloaded to a relay?

- ☐ Setting comparison lllllllllll
- ☐ Testing based on software CAPE, ATP, or ASPEN? lll
- ☐ Functional testing through tests such as secondary injection test lllllllllllllll
- ☐ Other:- ll

- *Where network access is available, setting comparison is performed without human (technician) transmission back to Engineering office.*
- *Setting comparison only for non-critical setting changes. Injection testing for all other changes. Injection testing may be element by element, or system testing based on ASPEN simulation.*
- *A second Relay Technician verifies the settings, and a text dump is uploaded from the relay and verified by a Protection Engineer, after commissioning.*

6) Did your company experience cases in which actual settings saved on the relay differ from the intended settings listed on the relay setting sheet?

- ☐Yes lllllllllll
- ☐No llllll

If YES what reasons caused such disparity?

- ☐ Human errors llllllllll
- ☐ Computer glitches ll
- ☐ Other:- l

- *Setting template did not match relay version*

7A) How often do you check relay settings to make sure that the settings are intended settings and have not been tampered with?

- *During maintenance cycle of the relays and also after questionable operations(*lllllll)
- *We have started to do setting comparison between settings on file in Relay Database and those found on the relay when routine maintenance is done (every 4 years).*
- *None after complete comparison right after implementation.*
- *Settings review about every 5 years.*
- *Only when a project or misoperation would drive setting changes at that particular terminal*
- *Never just to verify relay settings.(2)*
- *3 to 6 years on a preventative maint. cycle. Every correct and in-correct operation tests some of the elements.*
- *Not answered.*(1)
- *During routine testing every 10 years or so, or when other projects occur where those settings need to be reviewed (this happens maybe every 2-3 years on avg). And anytime we download fault events for review (maybe once every 2-5 years)*
- *4-6 years*
- *at reliability test - currently 14 year cycle*
- *per the relay PM cycle*
- *Any time a setting change is needed, or if NERC compliance requires periodic maintenance*.

7B) What prompts you to do so?

- ☐ Relay mal-operation lllllllllllllll
- ☐ Suspected tampering action such as indicated by logs l
- ☐ Other: - llllllll

- *Routine maintenance check. Settings reviews. Part of normal relay preventive maintenance procedure, in service settings are compared with issued settings.*
- *Not answered.(2)*
- *Not specified (1)*
- *Doing coordination work in the area.*
- *Reliability test*
- *NERC compliance*

8A) How often do you verify relay settings to make sure that the settings meet the protection requirements?

- *Coordination studies are performed on as needed basis. Usually new project work, relay replacements, system changes result in the initiation of setting reviews and coordination studies.Roughly every 5 years we will perform a coordination study on a given area and verify relay settings unless the area has recently been studied due to capital projects/reconfiguration where the relays were reset.*
- *Usually after power system changes or misoperations.*
- *Coordination every 3 years*
- *About every 5 years*
- *when a project dictates that work must be done at that terminal*
- *At time of initial commissioning or major setting revision*
- *Not scheduled.*
- *As needed(3)*

- *Anytime a system element changes or new equipment is going into service or other equipment is being replaced. No real time schedule to go out and check ALL settings in a relay. We do have macros in CAPE that run yearly to check ground coordination across the system.*
- *Depending on a case by case basis.*
- *Done during normal maintenance cycles, firmware changes, unexpected relay operation and settings changes(2)*
- *When system improvements/changes are made. Relay miss operation such as instantaneous overreach.*
- *Varies by function*
- *Every 10 years*
- *Every five years or less on the Bulk Electric System Relays or when a possible problem is noted.*
- *Same as Q7*

8B) What prompts you to do so?

☐ Relay mal-operation IIIIIIIIIIIIIII
☐ Power system changes IIIIIIIIIIIIIIII
☐ Relay firmware upgrade IIIIIIII
☐ Other: - IIIII

- *Routine area coordination study(2).*
- *Relay settings review policy*
- *PM cycle(2)*

SECURITY RELATED QUESTIONS:

9) Do you have numerical relays at your substations that can be remotely accessed? If NO go to 10. If YES, check those that apply to you and indicate the percentage of each based upon your total number of numerical relays in-service)

☐ Dial-up (What %? 100(2), 94(1), 75(2), 50 (1), 40(1), 35(1), 20(3), 10(1), <5(1))
☐ Intranet (What %? 70(1), 60 (1), 55(3), 40(1), 15(2), 3(1), 1(1))
☐ Internet (What %? 50 (1))
☐ SCADA/RTU (What %? 99.9(1),80(1), 40(1), 35 (1), <5(2))

- *We apply integrated P&C concepts using numerical devices and devices can be accessed through SCADA for operational purposes, not for setting validation or setting change purposes*
- *No answer(1)*

10) Do you use any of the following for the purpose of cyber-security to prevent unwanted access to your numerical relays? (Check those that apply and indicate the percentage of each based upon your total number of numerical relays in-service)

☐ Encryption (What %? 90(1), 50(1))
☐ Passwords (What %? 100(9), 90(3), 60(1), 50(3), <5(1), ?(2))

- *With most being controlled via SCADA by a discrete aux relay that interrupts the phone line to the device. We have recently started using the "NOCONN" feature in 2032's.*

☐ Virtual Private Network (What %?100(3) ,55(2), 50(1), 20(1))

- *We also use a custom device which strips unwanted relay commands out of the incoming serial data stream to the communications processor.*
- *We are in the process of installing a dedicated operational data network with secure VLANs and secure remote access with user authorization and authentication.*

11) Do you use an intermediate communications interface at your substations to remotely

access your numerical relays?

☐ Yes lllllllllllllll

☐ No llll

(If YES then what %? 100(4), 90(3), 80(2), 50(1),40(1), 25(1),15(1),<5(2))

(If YES then how many relays are necessary to install an interface? 1(5),2(2), 4(1), 5(1), *all non GE Relays (1)*)

(If YES then indicate the percentage of your substations with numerical relays that have an interface. 100(2), 95(1), 90(2), 70(2), 50(1),25(1), 5(1))

12) Do you password protect the intermediate communications interface and/or numerical relays?

☐ Intermediate communications interface lllllllllllllll

☐ Numerical relays (What %? 100(12) 90(2), 50(1), 40(1), 5(1))

13) Do you use multiple levels of passwords when available (e.g., level 1 = look but not touch for metering and events, level 2 = change settings)?

☐ YES lllllllllllllll

☐ NO llll

14) Do you use hardened passwords (e.g., R0xor)?

☐ YES lllllll

- *Level 2 only(1)*

☐ NO lllllllllll

15) Do you periodically change the passwords? If so, is this manually or automatically performed and what is the typical period between changes?

☐ YES llllll

☐ NO lllllllllllll

If YES then: ☐ MANUAL lllll

☐ AUTOMATIC

☐ BOTH l

What period are they changed? :- *Annually (4), 3 months, 1-2 yrs*

16) Who has remote access to your assets? For example, your assets might only be remotely accessed from one central location such as a lab or they could be accessed remotely from multiple locations such as a central location (e.g., headquarters) and maintenance offices. Briefly describe these locations.

☐ One location, llll

- *Maintenance/Engineering Office. A private fiber network is configured so that remote access is done through a central server. The server has to verify a legitimate user before access to the private network is established. Once inside the private network all substation locations can be accessed.*
- *Only on site.*
- *Fault analysis room.*
- *Choose not to reply.(1)*
- *No relays can be accessed remotely. Only remote access is operator control which can be done at one main location and at a backup only*

☐ Several locations lllllllllll

- *System Protection engineers and field technicians using personal laptop computers and private network.*
- *relay labs*
- *Most relays can be accessed at any location with access to our corporate telephone or computer network. A smaller percentage are connected to the public telephone system*.
- *SOC, regional centers, engineering office*
- *Via remote desktop to any company workstation*
- *Engineering support staff, field staff*
- *Maintenance offices, ESCC. Theoretically from any PC with a modem, but access is controlled via our system control operators who have an access list and they log who*

requests access.

- *Headquarters*
- *Sensitive information*
- *Anywhere there is access to the intranet.*

17) Do you alarm when your numerical relays are accessed?

☐ YES IIIIIIIIII

- *Level 2 access only(3)*
- *Not all relays alarm when accessed*

☐ NO IIIIIIIII

If YES then briefly describe how you alarm and what actions are taken.:-

- *Alarm is activated when password access fails after a set number of attempts. Also, when access to settings level for setting change is made.*
- *Operations are alerted after three unsuccessful attempts to get into a relay and any time level 2 is accessed.*
- *Relay fail alarm comes up for 2 sec when the relay enters level 2 (access level to allow setting changes). This alarm is typically ignored due to its transient nature.*
- *Log.*
- *Alarms through supervisory either via an annunciator or directly to supervisory.*
- *Reported to on-call operations person.*
- *Control center calls Protection and Control Field Services*
- *Alarm received remotely for second level access. If unexpected follow-up may be requested.*
- *We send an alarm to our dispatch if the level two section is accessed; the relay trouble alarms are reviewed periodically to be sure that the access was done by authorized personnel (Modem access). The intranet access logs the person accessing the substation gateway; this log is reviewed periodically to make sure only authorized personnel are accessing the relays. We are working to get all the critical Bulk Electric System Relays on intranet access this year (Intranet Access).*

18) Do you employ physical means to prevent unwanted access of your assets such as locks on the gates to your substations and doors of the control houses?

☐ Gate IIIIIIIIIIIIIIIII

☐ Control room doors IIIIIIIIIIIIIIII

19) Do you use video cameras for surveillance of your assets?

☐ YES IIIIIIIIIIIII

- *For all critical assets only,*
- *Implemented as a pilot project in one substation.*
- *At a small % of sites*
- *A few*

☐ NO IIII