ELECTRIC POWER RESEARCH INSTITUTE

Emerging Protective Relay Issues

Settings and Configuration Management for Protection and Control Systems

1020025

Emerging Protective Relay Issues:

Settings and Configuration Management for Protection and Control Systems

1020025

Technical Update, December 2010

EPRI Project Manager

Y. Lu

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

THE FOLLOWING ORGANIZATION, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

Quanta Technology, LLC

This is an EPRI technical update report. A technical update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organization, under contract to the Electric Power Research Institute (EPRI), prepared this report:

Quanta Technology, LLC
4020 Westchase Blvd., Suite 300
Raleigh, NC 27607

Principal Investigators
J. Holbach
E. Udren
S. Ward

This report describes research sponsored by EPRI.

This publication is a corporate document that should be cited in the literature in the following manner:

Emerging Protective Relay Issues: Settings and Configuration Management for Protection and Control Systems. EPRI, Palo Alto, CA: 2010. 1020025.

ABSTRACT

One of the major concerns from experts in the current state investigation of protection and control (P&C) systems is with the complexity of configuring today's microprocessor relays and managing the settings and firmware versions of a large protection fleet. Errors in setting or configuration are a serious risk for protection misoperation and threaten power system reliability.

The roadmap report forecasts that as protection equipment and systems continuously evolve in the more feature-rich and sophisticated direction, management of the configuration and setting is becoming more critical in future. Without a proper management and process in place, operation personnel can easily make mistakes by accidentally changing relay parameters in service. Meanwhile, the scope of P&C devices has been expanded beyond traditional protective relays. New substation intelligent electronic devices and network equipment, such as Ethernet switches, routers, PMUs, PDCs, and data communications infrastructures, are being used for P&C nowadays and should be included in the configuration and setting management as well.

Many utilities are still using paper records or setting sheets to maintain P&C configuration data, which heavily relies on human intervention and therefore tends to be error-prone. Some utilities recognize that even to deal with the complexity of today's P&C systems, a tightly managed system is required to develop, maintain, and control all settings and configuration data in a consistent and reliable way. In future, a standardized configuration and setting management system will become an essential part of a complete P&C system. The power utility industry need to take initiatives to stay ahead in dealing with this emerging critical system reliability issue.

This report describes how configuration management (CM) can be applied to the setting data and configuration files used in the P&C systems. CM is a more holistic approach that manages and controls the consistency of all relevant P&C data through their entire lifecycle.

Keywords

Configuration management
Intelligent electronic device
Relays
Settings management

ACRONYMS

CM	configuration management
GOOSE	generic object oriented substation event (IEC 61850)
HMI	human machine interface
I/O	inputs/outputs
IEC 61850	IEC standard for communication networks and systems in substations
IED	intelligent electronic device
IOS	Innovative Organizational Systems (a company name)
IPS	Intelligent Process Solutions (a company name)
IT	information technology
LED	light-emitting diode
NERC	North American Electric Reliability Council
P&C	protection and control
PDC	phasor data concentrator
PMU	phasor measurement unit
RTDS	real-time digital simulator
SCADA	supervisory control and data acquisition
SCD	system configuration description (an IEC 61850 configuration file)
XML	extensible markup language

CONTENTS

LIST OF FIGURES

1
REPORT CONTENTS

High Level Problem Description

In 2009, EPRI carried out an investigation of utility industry issues with current generations of protective relaying and of industry needs for the future. The EPRI report *Current State Assessment: Next Generation Relays* (1017773) addresses the current state for the industry, and the EPRI report *Roadmap for the Next Generation Protective Devices* (1017774) presents a roadmap based on the current state. Both reports convey concerns gathered from meetings of industry experts.

One of the major concerns expressed by many experts in the current situation investigation is with the complexity of setting today's microprocessor relays and managing the settings and firmware versions of a large protection fleet. Setting or configuration errors pose a serious risk for protection misoperation and threaten the overall reliability of power systems.

The roadmap report forecasts that as protection equipment and systems continuously evolve in the more feature-rich and sophisticated direction, management of the configuration and setting is becoming more critical in future. Without a proper management and process in place, operation personnel can easily make mistakes by accidentally changing relay parameters in service. Meanwhile, the scope of P&C devices has been expanded beyond traditional protective relays. New substation intelligent electronic devices and network equipment, such as Ethernet switches, routers, PMUs, PDCs, and data communications infrastructures, are being used for P&C nowadays and should be included in the configuration and setting management as well.

Many utilities are still using paper records or setting sheets to maintain P&C configuration data, which heavily relies on human intervention and therefore tends to be error-prone. Some utilities recognize that even to deal with the complexity of today's P&C systems, a tightly managed system is required to develop, maintain, and control all settings and configuration data in a consistent and reliable way. In future, a standardized configuration and setting management system will become an essential part of a complete P&C system. The power utility industry need to take initiatives to stay ahead in dealing with this emerging critical system reliability issue.

This report describes how configuration management (CM) can be applied to the setting data and configuration files used in the P&C systems. CM is a more holistic approach that manages and controls the consistency of all relevant P&C data through their entire lifecycle.

Next Generation Relaying 2009 Report

In the EPRI report *Current State Assessment: Next Generation Relays* (1017773), the section "Development and Standardization of User Tools" was one of the requirements that the development of tools for management and control of protection system settings mentioned.

The report addressed the critical issue of microprocessor relays and Ethernet communications devices having thousands of settings, any one of which could cause misoperation. The normal maintenance technique for equipment failure is to replace an entire unit, so a management system must support rapid setting of the replacement device, as well as closed loop verification of setting correctness. New protection system maintenance standards require that in condition-monitored relays not subject to routine time-based testing, the settings are verified as correct by some means other than testing—this must be a tightly managed and documented settings control system. In addition, the settings storage and management tool needs to be tied to protection setting tools, notably coordination study programs, as well as to unified system modeling proposed in the next section.

High Level Requirements

In the review of existing tools, it was found that there is a major focus on the change management and database functionality of setting and configuration files. These elements will remain as core elements, even in future CM, and will need to be accompanied by the following:

- **Managing the configuration information used for the generation of a setting file**. If any of the information considered for the generation of a setting file changes, it may trigger a change request of the existing file. This is partially handled by processes inside of the utilities but needs to be supported by a CM tool.
- **Configuration status accounting**. Configuration status accounting is the tool to keep track of all changes and give an accurate, timely information base of the setting and configuration file throughout the product's lifecycle. It will report the actual configuration information as well as allow historical traceability of this information.
- **Standardize data formats**. Currently, many of the data used for the generation of setting files, the setting files themselves, and reports are in proprietary formats or in nonstandardized formats. To optimize the settings management process, it is desirable that the industry develops standard data representation. Many activities in different standard bodies are currently addressing this, and IEC61850 and IEEE-PSRC are working together to develop standard data representations for setting and configuration data (IEEE-PSRC H5, "Common Format for IED Configuration Data") and event data (IEEE-PSRC H6, "Standard Common Format for Event Data Exchange [COMFEDE] for Power System").
- **Standardize programming tools**. At this time, in most cases, the industry has to use proprietary tools to program IEDs. The definition of common data representation will allow the development of common tools to program IEDs. This will eliminate unnecessary translation of data files and simplify the setting file generation process.

These listed requirements will enhance the CM and provide the functionality required by new regulations and that is needed by the more complex and faster moving technology in the P&C environment.

Tool Vendor Discussions Summaries

In general, it was found that the tools available in the P&C industry can be classified in three groups. Note that this list may not be complete.

1. **Change management process support**. The tools from the manufacturers IOS and IPS are supporting the change management process. Both tools will allow programming a workflow, assigning roles, and following the work progress (see Figures 1-1 and 1-2). All changes will be recorded and can be used for the accounting functionality inside of the CM process. The database functionality is inherent in both tools.

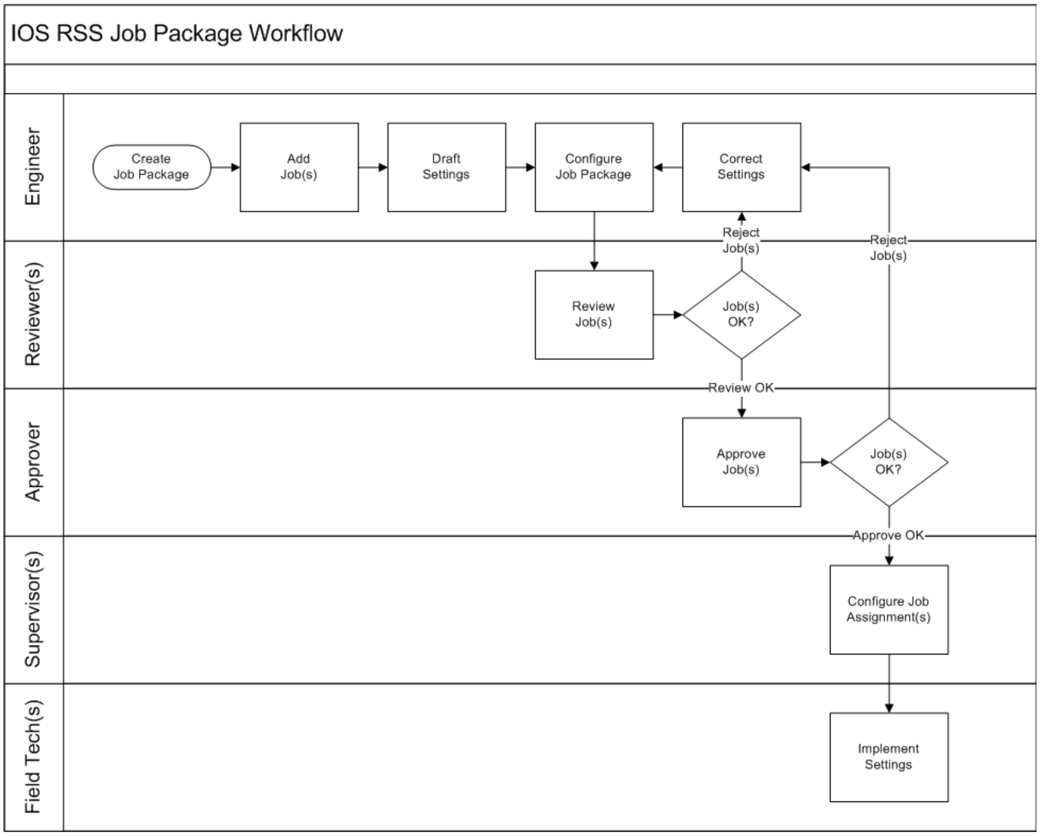


Figure 1-1
IOS RSS® workflow (IOS RSS® is a web-based equipment configuration management system)

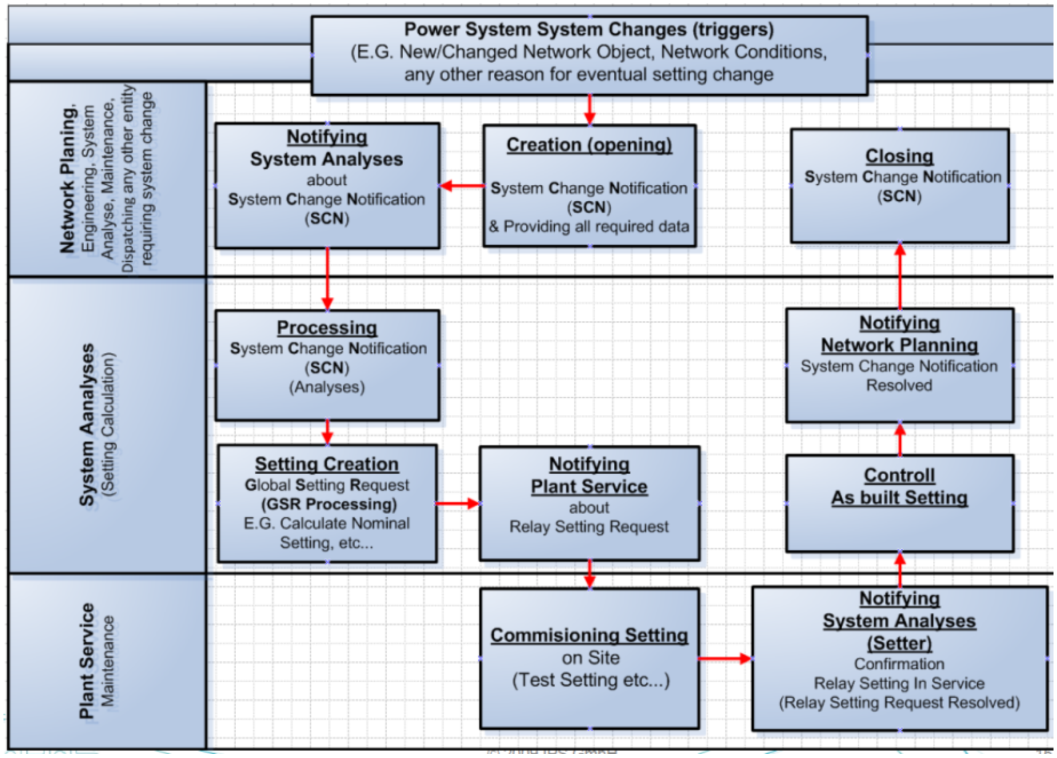

Power System System Changes (triggers)
(E.G. New/Changed Network Object, Network Conditions, any other reason for eventual setting change
Network Planing, Engineering, System Analyse, Maintenance, Dispatching any other entity requiring system change
Notifying
System Analyses
about
System Change Notification
(SCN)
Creation (opening)
System Change Notification
(SCN)
& Providing all required data
Closing
System Change Notification
(SCN)
System Aanalyses
(Setting Calculation)
Processing
System Change Notification
(SCN)
(Analyses)
Notifying
Network Planning
System Change Notification
Resolved
Setting Creation
Global Setting Request
(GSR Processing)
E.G. Calculate Nominal Setting, etc...
Notifying
Plant Service
about
Relay Setting Request
Controll
As built Setting
Plant Service
Maintenance
Commisioning Setting
on Site
(Test Setting etc...)
Notifying
System Analyses
(Setter)
Confirmation
Relay Setting In Service
(Relay Setting Request Resolved)

Figure 1-2
IPS-RELEX™ workflow

2. **Database tools**. There are two groups of applications that are supplying the functionality of a setting file database:

- **Coordination program** databases like CAPE and ASPEN will have common models of the relay setting files and offer the database functionality. The export and import of data files between manufacturer tools and the database are only partly supported because of a missing standard representation. In addition, the actual setting will also be based on the main functionality of this tool, as well as the information to be stored, which was used to generate the setting (system model). Test report or event data are normally not stored in this database.
- **Test equipment manufacturers** like Doble, Omicron, and Megger store settings mostly in their proprietary format. Omicron developed a so-called XRIO format that is an extensible markup language (XML)-based language to represent setting data in a common format. At this time, only one manufacturer (Siemens) is able to import and export this format. In addition, the database will also be able to store test reports generated during the commissioning and maintenance test.

All tools function as a data repository and offer no advanced functionality like tracking changes or comparing settings between relay and database. None of the tools support the change process.

3. **Proprietary manufacture database tools**. Each relay manufacturer supports its product with a proprietary programming tool that functions also as a database and supports normally one manufacturer data format only. The setting and configuration data, in some cases, can be exported in common formats like text, Excel, or XML. The import of common formats was observed by one manufacturer (Siemens, XML format) only. Most of these tools support and compare functionality to verify the consistency of the settings applied to the relay in relation to data in the database. Fault event data and fault recording data are also stored in the database. None of the tools supports the change process or helps track changes.

Conclusions and Next Steps

This report proposed a CM process similar to the process already used in other industries. After discussing the challenges of creating and managing setting files for intelligent, multifunctional IEDs, the common CM process was mapped to the protection and control industry. The following five basic modules of a CM process will address the challenges mentioned:

- CM planning
- Configuration identification
- Configuration change management
- Configuration status accounting
- Configuration audits

However, the P&C industry has some unique constraints that will need to be addressed individually. For example, is the programming of a complex IED in most cases not possible without a proprietary tool supported by the manufacturer of the particular IED? For the data to program an IED there is no common format defined at this time. Therefore, any CM tool needs to interface and cooperate with proprietary tools from all manufacturers.

The following are two ways this inhomogeneous situation is managed with respect to CM today:

- **Setting files are treated as objects**. In this case, the CM will manage the setting file object without detailed knowledge of the information inside of the object. However, with management functions like version control, change management can be realized without the detailed information inside of the object. With other functionality like verification, template management would have to be realized in cooperation with the proprietary manufacturer tools.
- **Setting files information is represented in a common format**. Settings and configuration information is represented in a common format in a database. This will allow using all CM functionality without any dependability on manufacturer tools. However, if the setting file needs to be applied to the IED, a manual conversion needs to be done, which has always been a source of errors.

Currently, many activities in our industry are addressing this issue, and IEC61850 introduced one solution on how settings and configuration data can be expressed in a common data format and described in an XML format. Unfortunately, at this time, IEC61850 has realized this for the communication configuration only.

Even if there were no common format, it would, from the CM point of view, be sufficient to have an export and import functionality available on the proprietary manufacturer tool. At this time, most manufacturers support the export of data, but only one allows the import.

In this report, a comprehensive and holistic CM specification was created. Some of the most common tools used in our industry were inspected and classified where they fit into the holistic view.

2
INTRODUCTION TO SPECIFICATIONS

Problem Description

The development, installation, and maintenance of settings have always been and will always be a critical task of P&C systems. With the first installation of P&C systems, engineers started to develop processes to ensure the quality and correctness of settings and configurations through the entire lifecycle of the system. Most of these processes are still in place. They are based on an environment where a dedicated protection department was responsible for the setting of electromechanical relays with a limited number of settings and managed the settings on paper records in a record book.

The following developments have changed this environment:

- **Deregulation**: the deregulation of the energy market led to a more competitive environment where economical evaluations required increased efficiency and caused organizational reorganizations with the goal to optimize resources.
- **New technology**: the introduction of numerical technique advanced the functionality for P&C systems and consequently also introduced new challenges like large number of settings and firmware control.
- **New infrastructure**: P&C systems are a part of Smart Grid technology and increasingly rely on communication of P&C data between system components located inside or outside of the substations. The ability to remotely change settings and configuration adds a new dimension to the settings management process.
- **Regulatory requirements**: regulatory bodies such as Federal Energy Regulatory Commission and North American Electric Reliability Council (NERC) require Protection System maintenance and testing programs with the appropriate documentation.

Although the processes in many cases have been adapted to address these changes, it seems necessary to evaluate today’s P&C system environments and future trends to develop a specification for a setting and CM system that is tailored to the needs of the P&C system.

The term *configuration management* is not clearly defined and is sometimes used in the industry with different meanings. For this report, the definition given by the EIA 649 National Consensus Standard for Configuration Management will be used.

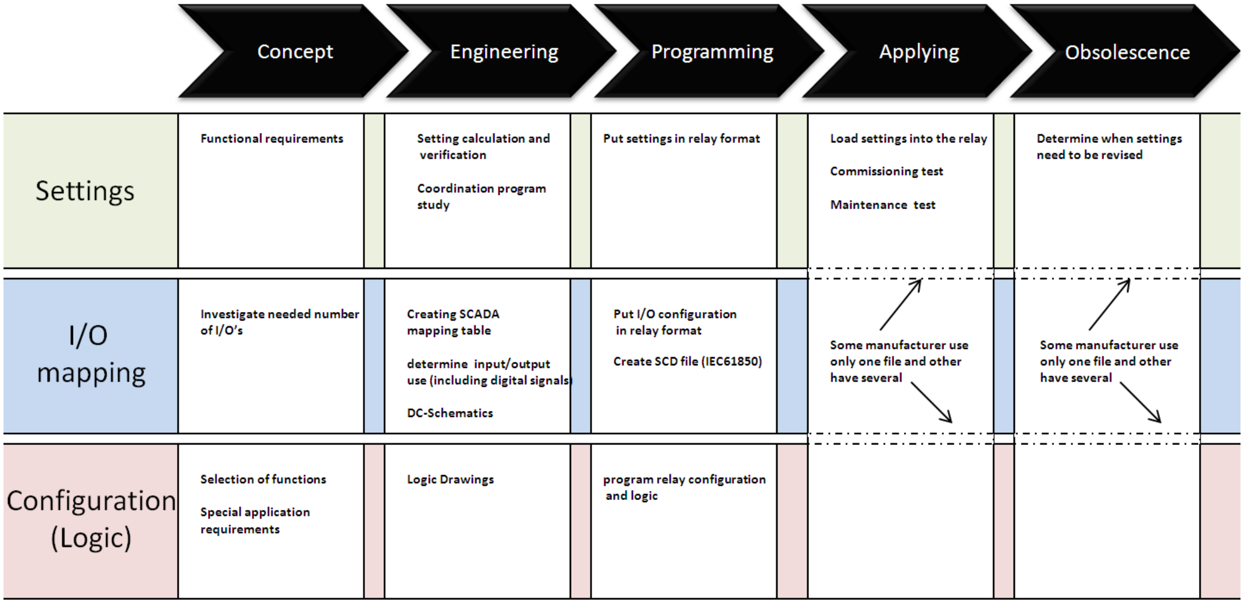
Configuration Management

A general definition is given in the EIA 649 Standard, as follows:

“Configuration Management (CM) applies appropriate processes and tools to establish and maintain consistency between the product and the product requirements and attributes defined in product configuration information. A disciplined CM process ensures that products conform to their requirements and are identified and documented in sufficient detail to support the product lifecycle. CM assures accurate product configuration information and enables product interchangeability and safe product operation and maintenance to be achieved.”

CM is used in different industries, and the terminology is quite different between the different applications. It seems necessary to define the different cycles of the entire lifecycle of a setting and configuration file used in the protection and automation world.

Setting and configuration files of multifunctional numerical relays can consist of three different parts: Settings, inputs/outputs (I/O) mapping, and the data to describe the device configuration. In Figure 2-1, each of these parts focuses on different objectives in setting a device and should be discussed differently. How the data are stored and managed is handled by different manufacturers in different ways.



	Concept	Engineering	Programming	Applying	Obsolescence
Settings	Functional requirements	Setting calculation and verification Coordination program study	Put settings in relay format	Load settings into the relay Commissioning test Maintenance test	Determine when settings need to be revised
I/O mapping	Investigate needed number of I/O's	Creating SCADA mapping table determine input/output use (including digital signals) DC-Schematics	Put I/O configuration in relay format Create SCD file (IEC61850)	Some manufacturer use only one file and other have several	Some manufacturer use only one file and other have several
Configuration (Logic)	Selection of functions Special application requirements	Logic Drawings	program relay configuration and logic		

Figure 2-1
Lifecycle of a setting and configuration file

Settings

This is the actual information needed to customize the selected functions to the requirements of an application. Depending on the relay type and the supported functionality, there can be different classes of settings in a multifunctional numerical relay:

- Protection
- Metering
- Communication
- Administrative
- Power system
- Global
- Phasor measurement unit (PMU)

The protection settings are the most critical part that cannot become standardized and must always be calculated in respect to the actual application. Most of the other settings can be standardized and stored in a template.

I/O Mapping

The I/O mapping determines how the relay interconnects to the environment through different interfaces. In the sense of this report, the following interfaces are considered:

Outputs

- Output contacts
- Analog outputs
- Display light-emitting diodes (LEDs)
- Text or graphical display
- Communication channel(s)

Inputs

- Binary inputs
- Analog inputs
- Push buttons
- Built-in human machine interface (HMI)
- Communication channel(s)

Also, the I/O mapping in many cases can be standardized and stored in a template.

Device Configuration

The device configuration will customize the functionality of a multifunctional relay to a given application. In this step, the selection of which protection functions should be used in the relay will be done. Also, any kind of customized logic programming will be part of the device configuration.

The three listed subclasses in a setting and configuration file are not given by definition. Depending on the philosophy and the design of particular relays, there may be more or less subclasses than defined here. However, for the following discussion, the proposed classification seems sufficient.

During the lifecycle, the setting and configuration information will go through several stages. The whole process starts typically with a new construction, requiring new P&C equipment. The case in which we have an existing file that needs to be revised is special but can be assumed in the same sense.

Concept Phase

The lifecycle starts with the concept phase. This phase is initiated by a request for new settings. The protection application needs to be investigated and based on best practice; regulatory requirements or standards for the appropriate protection functions are selected. A protection system gets designed on a high level, and the interface requirements between the system components will be defined. Information about the protection object is investigated.

Engineering Phase

The engineering phase will calculate the actual settings for the protection functions selected for the application. Depending on the complexity of the application, different tools are used. The tools can range from simple calculator, Excel spreadsheets, or coordination programs up to real-time digital simulator (RTDS) testing. The I/O assignments will be decided in this phase, and the DC drawings will be generated. In the best case, the drawings should show all previously mentioned interfaces and their use. Besides the settings and the interfaces, logic needed in the relay must be designed and documented.

Programming

The programming phase is the step in which all of the information for the settings, I/O mapping, and configuration become translated into a format that is readable by the IED that it is supposed to be applied to. Today, most IEDs are using proprietary formats, and the user is required to manually enter the information into a proprietary tool supplied by the manufacturer. The programming phase can be considered as the actual “manufacturing process” of a setting and configuration file.

Applying

The setting and configuration data become effective inside of the relay when they are downloaded to it. Only after the commissioning test has verified that the setting and configuration inside of the relay let the relay perform in a way described in a test plan will the relay be connected to the system and start its service. Regular maintenance test will reconfirm the correct functionality of the relay and its applied setting and configuration over its lifetime.

Obsolescence

The applied settings and configuration inside of an IED stay unchanged until the need for a change is determined by the following:

- New regulatory requirements
- Change of the primary or secondary energy system
- Change of best practice experience
- Enterprise rules or policies
- Response of misoperation

The obsolete setting and configuration file and the information causing the obsolescence declaration should be archived for configuration status accounting.

CM functions will be applied throughout the entire lifecycle of a setting and configuration file. The CM must therefore be supported by processes and tools that need to accommodate each other. Each utility already has processes and tools in place to develop setting and configuration files; however, recent changes in the industry make it necessary to take a more holistic view of the process in developing, documenting, and managing these files.

3
CONFIGURATION MANAGEMENT

This report proposes a CM approach that is outlined in the EIA 649 Standard and describes how it can be applied to the P&C systems. The CM based in the EIA 649 Standard consists of the following five components:

- CM planning
- Configuration identification
- Configuration change management
- Configuration status accounting
- Configuration audits

It needs to be emphasized that in many utilities processes and tools are already in place that are part of a CM process. The purpose of this section is to create a common terminology and take a more holistic view of the process in developing, documenting, and managing setting and configuration files.

CM Planning

The basis for any implemented CM system builds the CM planning. The configuration planning defines the lifecycle phases of the product (see Figure 3-1). The tools and procedures used during the lifecycle assign responsibilities to various organizational elements and will document all of these.

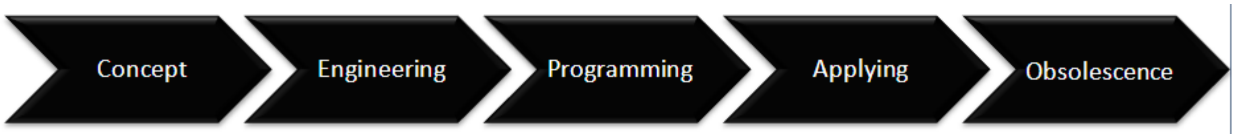


Figure 3-1
Lifecycle for setting and configuration files

The planning needs to address each phase of the lifecycle and be able to answer the following questions:

- Who is responsible for the organization for this phase?
- What are the activities in this phase?
- What is the input for this phase, and what is the output?
- What tools/resources are to be used?
- What metrics can be used to measure the performance of this phase?

An example of planning is the concept phase for the protection setting, shown in Figure 3-2.

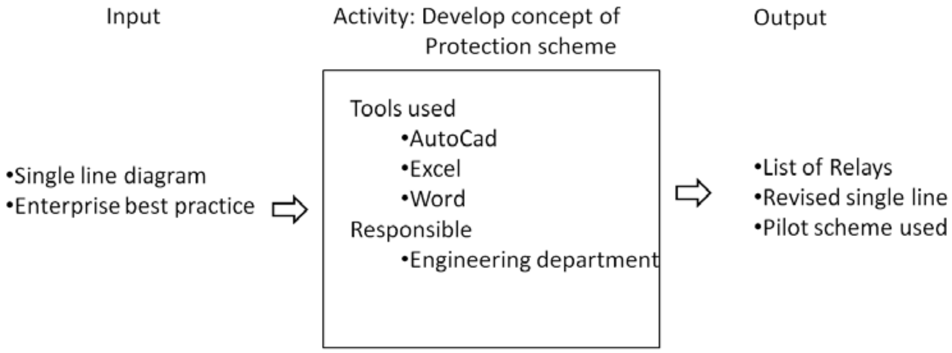


Figure 3-2
Planning description of concept phase for the protection setting

The selection and coordination of tools used in different phases of the lifecycle will help transfer the design information, which is particularly important if the information will become transferred between different departments.

The planning also has to plan for the long-term data by addressing the data management technologies. This has become an issue in the P&C environment where many DOS-based tools were used in the past that are no longer fully supported in the new Windows environment.

Configuration Identification

Configuration identification is the basis from which the configuration of items is defined and verified, items are labeled, changes are managed, and accountability is maintained throughout the product lifecycle.

Tools used today in the P&C environment focus mostly on the setting and configuration file itself. A holistic CM goes further and also includes the management of all information used to generate and maintain the developed setting and configuration file.

The information used for the generation of the file is called *product definition information.* For setting and configuration files, the information includes the following:

- Regulation
- Primary system data
- Best practice guides
- Rules/policies
- Experience
- Power system model
- System design information
- Single-line drawings
- Three-line drawings
- DC schematics
- Templates
- Manuals

- Firmware version
- Software version
- Service letter

All of this information must be identified and monitored. A change in any of this information could potentially trigger a change of the setting and configuration file. Unfortunately, not all of this information can be monitored. Experience, for example, may be existent in the mind of an expert only. To model or describe this knowledge is not simple and sometimes not possible.

Product operational information is information that documents the correctness of the setting and configuration file, which includes the following:

- Maintenance test results
- Commissioning test results
- Test plans
- Fault records
- Event record

Each of these items should have one unique identification and needs to be monitored by a revision number. For any setting and configuration file version it will then be possible to track back the source for the information included in the file. Any fault record can clearly be matched with the setting and configuration file that was active at the time of the recording.

Configuration Change Management

Configuration change management is a process for managing configuration changes and variances. Change control is the process that involves the following:

- Identifying the need for a change
- Defining the change
- Managing the actual change process
- Documenting the change

This element in the CM is the most critical for protection setting and configuration files, and utilities always pay attention to change management. The result is that processes and tools are developed heavily around this element. More and more change management is required by regulatory bodies like NERC (CIP 3-2):

“Change Control and Configuration Management—The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control, and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.”

The change management has to monitor all product definition information as recorded during the configuration identification and evaluate the consequences of changes on any of these items. The whole change process will become initiated if the need of a change is identified and a request for a change is issued.

Note that a change of one element can cause the change of several product definition information elements. For example, if a transmission line becomes added into the system, it will require a change of the power system model and the single-line and three-line drawing and eventually will also change the setting information.

The change process for protection settings has the following steps:

- Issuing a change request
- New setting calculation
- Generating a new setting file
- Generating a new test plan
- Applying new settings
- Verifying new settings

Each of these steps will include several substeps; however, for the discussion in this report, the previous considerations are sufficient.

Configuration Status Accounting

The configuration identification helps describe which information is used to generate and maintain a certain setting and configuration file. The change management describes the process to update the file, based on a change request. Configuration status accounting is the tool to keep track of all changes and gives an accurate, timely information base of the setting and configuration file throughout the product lifecycle.

It will report the actual configuration information and allow historical traceability of this information.

Configuration status accounting should be able to answer the following questions:

- What is the latest configuration information?
- What was the configuration information for the setting file version X.XX?
- Who made a change?
- What changes were made?
- When were the changes made?
- Why were the changes made?
- Who authorized the changes?

Configuration Audit

Configuration audits establish and document that the performance and functional requirements have been achieved by the design and that the design has been accurately documented in the configuration documentation.

For P&C systems, the following procedures are applied:

- **Commissioning and maintenance test**. This test verifying the actual setting file is applied to the IED. During the setting development, there is also a test plan developed that can be used for this task. A test set will run a number of tests and verify the correct response of the IED.
- **Setting file comparison**. An automatic or manual comparison of setting files stored inside of the database and data applied to the relay is done for the verification.
- **Setting and configuration reviews**. Setting calculation can be reviewed or verified by independent resources. Utilities may decide that settings need to become reviewed in certain time intervals.

All of these activities will be recorded and documented by the configuration audit system.

This section is focused on the CM applied to setting and configuration files of P&C systems. However, the concept can easily be expanded to a whole P&C system. This is particularly necessary if the different configurations of different IEDs in the system depend on each other. A change of the configuration in one IED would cause the change in one or more other IEDs in the system.

The CM would keep track of these dependencies through the product configuration information. As soon as an IED configuration file will be changed, the change management process would determine the dependencies between the files and, if needed, will also issue a change request for the second IED file.

The dependencies of IED settings are the rule in transmission and distribution applications and always require a careful coordination. However, modern protection schemes rely more and more on communication support to enhance the protection performance. This will add an additional complexity because it will require that, in addition to the protection settings, the I/O configuration will need to be synchronized inside of a protection system.

For example, if binary information is sent through a communication channel to a second IED, the second IED needs to have a description of the meaning of the bit. If the meaning becomes changed on the receiving side, the CM needs to ensure that the configuration file of the receiving IED becomes reconfigured to reflect the change.

4
DATABASE ELEMENTS

Depending on the focus of the CM, the database must be able to manage different elements of information. Core elements for P&C systems are the settings and configuration data of all P&C system components.

Figure 4-1 gives an overview of items that the CM for P&C systems can apply to, but it is not all inclusive, and all items are not necessarily required for all types of applications or devices.

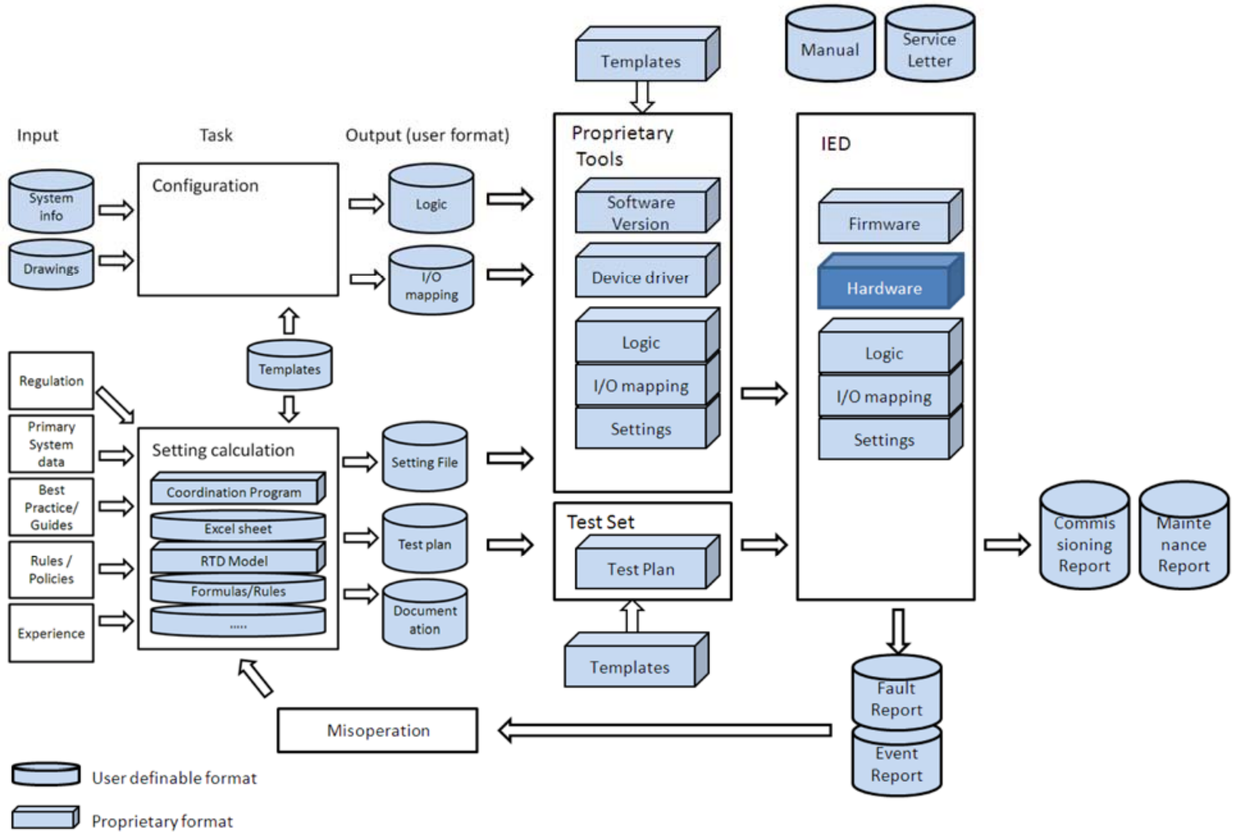


Figure 4-1
CM items

Data of Single Device

P&C systems are built of different devices. The performance of the whole system requires that all devices are working together and that they are properly coordinated with each other. This is not new and was always a requirement. Obvious examples are line differential relaying and distance relaying using teleprotection schemes. Most other types of relays need to consider settings and/or configuration of adjacent devices for selectivity purposes. Modern solutions are increasingly using communication between IEDs rather than wiring between IEDs to exchange status information and enhance protection system functionality. This can be observed with proprietary bit exchange solutions and on standardized solutions in utility communication architecture, distributed network protocol, and IEC61850. Also, in the near future, the exchange of sampled values between IEDs through communication will become a reality.

The modern P&C system will consist of several components communicating to each other rather than being wired together. Figure 4-2 illustrates some components that will be present in a future P&C system:

- IEDs perform P&C functions.
- A switch (Ethernet switch) is used for intrasubstation communications between the IEDs and the merging unit.
- A router is used for intersubstation communications, for example, from the substation controller to the Supervisory Control and Data Acquisition (SCADA) system at the control center.
- PMU is a phasor measurement unit typically used for wide area monitoring and/or protection.
- A phasor data concentrator performs preprocessing of the PMU data before sending it to a control center.
- Sensors and the merging unit provide analog data to the IEDs from the primary equipment.
- The programmable logic controller performs customized logic function for advanced automation.

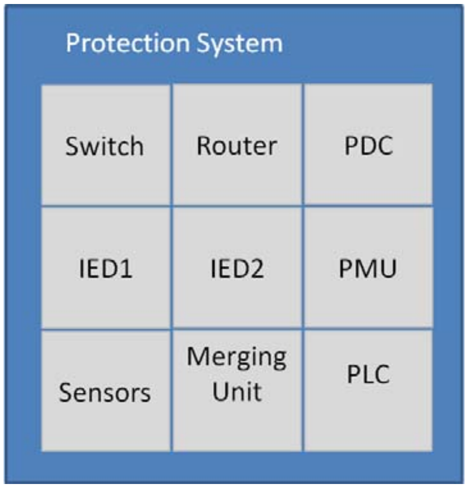


Figure 4-2
Components of a modern protection system

In most cases, IEDs are the core elements of any P&C system; however, the merging units, switches, routers, and PMUs are also essential components used in a modern and/or future protection system. From the CM point of view, all components have at least three major components to monitor: the hardware version, the firmware version, and the version of the setting/configuration file. In many cases, there are constraints that a certain firmware version can be applied to only a certain hardware version or that a setting/configuration file requires a certain firmware. Incompatibility between versions was, is, and will always be a source of problems ranging from wasting time and resources to misoperations. An effective CM targets to eliminate problems related to different versions.

Firmware

The firmware is generated and released by the manufacturer. It is common that modern numerical relays can have different firmware versions for different components of the relay, particularly if it is a multiprocessor-based IED. For example, an IED can have a protection processor with its own firmware on which the protection task runs and a second communication processor handling the communication task with a totally different firmware version. Each released firmware version has a different functionality and can have different requirements for the hardware version and/or setting and configuration file version. Although many utilities consider it good practice to apply the same firmware for all IEDs in the field, this is often impractical. As the firmware evolves over time because of hardware upgrades, bug fixes, and/or functional enhancements by the manufacturer, it is a major task to maintain a certain firmware version for the utility relay population. The firmware typically exists in the form of a file in a proprietary format and can be loaded into the devices with the appropriate hardware by using standard software tools or proprietary tools. Older microprocessor devices typically required replacement of a hardware module (EPROM, EEPROM).

The acceptance and the use of a new firmware should undergo an approval process before it becomes used in the utility. The knowledge of the changes in the firmware version will help identify whether a particular device needs to be included in upgrades recommended by the manufacturer based on their notification (service letter).

Hardware Version

The hardware is normally more static and will not undergo a frequent change like the firmware. However, it is not uncommon that a device consists of several components that can become replaced independently. In many cases, the hardware version of a component is of importance to the firmware or setting and configuration file and needs to be monitored by the CM system. The knowledge of the hardware version may help identify whether a particular device needs to be included in upgrades recommended by the manufacturer based on their service letter.

Settings/Configuration

The setting and configuration file is the third part besides the hardware and the firmware needed for a reliable operation of a device. The utility is responsible for the setting and configuration file, and therefore the CM should not only manage the file itself, but also manage all components and tools used to generate the particular file for the IED and manage all information that documents the correctness of the setting and configuration of the device. Note that, although this document refers to a “setting and configuration file” as one object, there are P&C devices that are using different files for settings and for configuration such as user programmable logic. The considerations and recommendations in this document are also valid for these devices, the difference being that the system management tool needs to ensure that these separate files are combined into one object or stored together with a cross-reference in the database.

IEDs require adjustments of three major parts (see Figure 4-3): I/O mapping, configuration/logic, and settings that may need to be determined by different groups in the utility.

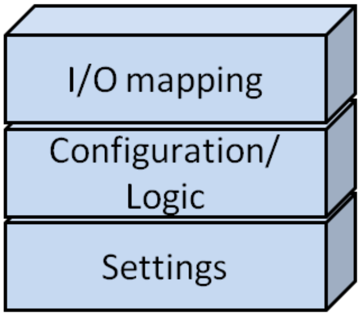


Figure 4-3
Parts of a setting and configuration file

I/O Mapping

The I/O mapping determines how the connections from the internal software elements are made to the external world. For example, if a protection function detects a fault and generates a trip command, this protection trip command needs to be properly configured in a relay to either trip circuit breakers or generate some alarms. The most common use for this protection trip today would be to map it to the output contact that is wired to the circuit breaker. In this example, an output contact was used to connect the software-generated information to the external world. The following is a list of possible output interfaces:

- Output contact
- LED on the IED
- Display on the IED
- GOOSE message output to an Ethernet switch
- SCADA through a communications port

The device software-generated internal logic signals (like the previous example of “Protection Trip”) are typically also programmable (mapped) to functions internal to the device such as the following:

- Sequence of event recording/triggering
- Fault records
- Programmable logic

On the input side, the following interfaces are available:

- Binary input (electrical sensing opto-coupler)
- Push button on IED
- Built-in HMI of IED
- GOOSE message
- SCADA control command

The I/O mapping typically needs input from different groups in the utility. The SCADA group will give the input on which information will be communicated to and from the control center. The operations group will give an input of how to use the LEDs and pushbuttons of the device, and the design group will determine the use of the output relays and the binary inputs. The protection department in charge of analyzing any event will select the information needed to be recorded by the fault record and what information this record should contain.

It is good practice in a utility to have standard arrangements developed that are stored in a template file. Whenever a new setting and configuration file needs to be developed for a new IED, the process would start with the template file that already has the standard I/O mapping included. From the CM point of view, this template file needs to be managed because there may be different versions and/or future changes.

Configuration/Logic

The configuration and user-defined logic in an IED could be listed as different items. However, they are so closely related that they can be treated as one common part. The configuration of an IED is on a global level, and there is no clear definition as to what falls under “configuration” and what falls under “settings.” One commonly used definition is that any setting or selection that does not relate to a single protection function is a configuration item. Examples of configuration are the number of setting groups used and user-defined logic. The setting group selection influences many protection elements, and the user programmable logic normally combines the information of several protection elements to generate an output.

The configuration and user-defined logic is normally standardized in a utility and included in a template file. In particular, the user-defined logic is a critical element that requires resources for the development and verification of correctness, which should not be repeated on each new setting and configuration file. From the CM point of view, this template file needs to be managed because there may be different versions and/or future changes.

Setting

Modern, numerical, multifunctional IEDs have hundreds of settings. It has become quite a challenge to set these devices. However, typically only a limited number of settings needs to be changed for a specific application, and most of the other settings stay the same. For a standard application, I/O configuration and the programmable logic would not need to change. Consequently, most of the settings are fixed and stored in the template. Protection-related settings always need attention and typically cannot be standardized.

Passwords

The management of passwords has become more important and required by NERC for critical cyber assets. Even if the password will not impact the protection performance, it may be useful for commissioning or maintenance work to have the password information stored and accessible in the database. However, this raises the question about different access rights for different users (to be discussed later). A process needs to ensure that the password is updated in the database if it was changed in the device.

Location

The location is important if monitoring of a device over its lifecycle is considered. The location and/or status will change during buying, stocking, testing, applying, repairing, and discharging the device.

Manual

The manual of a device is an important source of information and needs to be consulted over the entire lifetime of a device. The manual is normally different for different firmware versions and/ or hardware versions, and a CM system should include this and a configuration information item.

Service Letter

Service letters sent out by manufacturers are important documents that sometimes trigger a setting or configuration change, a hardware change, or a firmware change of a device. It is critical for the reliable performance of a P&C system that the recommendations given by the manufacturer are followed. A service letter is issued to describe a constraint for a specific firmware version or hardware version of a device.

Device Setting Templates

As shown previously, the development of templates can make the development of new setting and configuration files more efficient. It is good practice in utilities to develop standard applications with standard I/O configurations, standard device configurations, and standard logic inside of the devices. All of these can be included in a template file. Then, the generation of a new device file will need to focus on the application-specific settings only. The use of templates will eliminate double work and reduce the risk for errors. However, because of changes in the standard applications, the template file will also undergo different versions, and a CM system needs to monitor this file and its application.

Test Plan

With the issuing of settings for an IED, the engineering department develops a test plan on how to verify that the correct settings are loaded into the relay. This becomes part of the commissioning test, and the commissioning test report will document that the relay functioned and performed as intended during commissioning. The test plan can be given in several forms but needs to be translated into particular test hardware (test set). The test plan needs to be stored and managed because it represents an important tool to verify the correct relay settings.

Test Plan Templates

The test plan is based on a template that defines all tests necessary for a certain protection function. The actual test plan only needs to adapt to the particular settings that are unique for this application. The definition of which settings are required will change over time, and the template will undergo revisions. If a change in the template is required, it needs to be decided whether and how these changes should be applied to the previous test plans that originated from this template.

Test Results

The test results reported during the commissioning test and the maintenance test are proof of the IED functionality with the applied settings. The test report is a response of the test plan and the setting and the configuration file used inside of the IED.

Fault Event Records

If an IED responds to a fault event, it produces reports that help analyze the IED behavior. The records are important for documentation of the settings and configuration of an IED and need to be stored if the relay response was not as expected. Correct operations could also be of interest to store because these testify that the device operated as intended at that time and provides a certain level of setting/configuration verification. For an unexpected operation, the event report could be part of the documentation for a required setting change.

The major reports available from P&C devices are the sequence of events and a fault record, including sampled analog values. Fault records can be used for retesting the IED after a setting change to verify the improved behavior. Event fault records are also used to verify a firmware upgrade or configuration change, especially if the event was the cause of a design change.

Setting Tools

Setting tools can range from simple Excel spreadsheets to complex simulator (for example, RTDS) testing to find the correct settings for an application. To make the setting calculation process repeatable, all information used to generate the settings should be stored in the database. In particular, this could include the following:

- Short-circuit data for the application
- Coordination program models and cases
- RTDS models and test cases
- Excel spreadsheets

The tools and test case should consider regulation requirements, policies, rules, and best practices.

Systems Information

Figure 4-1 shows the steps and data files typically needed to set and document the configuration of a single device. However, a P&C system consists of several components that work together. The description of the whole system will change over time as the system changes and as it is necessary to update the data.

Drawings

Drawings typically already have a well-established CM process in place because they have been used over decades to document protection systems. However, microprocessor devices are changing traditional schematics. Internal programmable user logic, or fixed logic, replaces external wiring and auxiliary devices that traditionally would be represented on a protection system DC schematic. To fully understand the protection system functionality, access to this logic is required. This poses an additional challenge for the management system because the internal logic is typically stored in a proprietary format in the manufacturer’s proprietary tool. The fixed logic is generally available in the product manual only and in noneditable format.

IEEE PSRC has recognized the need to address this issue, and Working Group I5 is producing a report titled “Schematic Representation of Power System Relaying” to be completed and published in 2011.

System Configuration Description Files

System Configuration Description (SCD) files are files used inside of an IEC61850 substation to describe the device configuration of all devices in the substation in relation to communication.

This file is generated with the system configuration tool. It includes all information that is sent between the IEDs and the client system and the description of the information exchange between IEDs. Although IEC61850 has a mechanism built in to detect whether all IEDs are configured as described in the same SCD file, it should be included as one item in the CM.

Configuration Tools

In most cases, a proprietary-manufacturer-developed tool is needed to load the setting and configuration file into the IED. The complexity of these programs can range from simple hyper terminal application to sophisticated software packages. Most manufacturers store the settings and configuration data in proprietary formats and therefore it is not possible to access and load the settings directly into the relay without this tool. In the future, it is envisioned that all manufacturers will have standard data formats that will allow the use of standard tools to download the data into the IEDs. IEC61850 laid the groundwork, and it seems feasible that XML-based setting files can be loaded directly into a P&C device in the future. At this time, the settings are generally entered manually into the manufacturer's tools and stored in a manufacturer-defined format and database.

Device Driver

It is important that if the data are entered into the proprietary tool for use on a particular IED, the tool needs to support the IED firmware version and the hardware version. The manufacturer may supply a new firmware version that may have different settings, as compared to the previous version. The inconsistency of different versions creates frustration for operational and maintenance personnel in the utility. Proper CM can mitigate these problems.

Software Version

The proprietary manufacturer tool is software packages, which by themselves will undergo a certain evolution. The changes are caused by enhancing functionality and fixing bugs in the software. It is not always given that the latest software version will support all previous device firmware versions, and the user has to monitor this carefully. Often, several tools are needed to support different relays with different firmware versions.

Tools for Obsolete Products

It is not uncommon that for a product that is no longer supported by the manufacturer that the setting and configuration tool will no longer be supported or updated. This is of concern for devices that use a proprietary file format because the tool may not be compatible with a newer operating system. It is therefore important that the management system has the ability to store the settings and configuration in a standard format for archiving.

5
DATABASE FUNCTIONAL REQUIREMENTS

To support the configuration status accounting task, all information on configuration items need to be stored and maintained throughout the item’s lifecycle. Section 3 gave an overview of all information associated with a P&C system that should be stored and monitored over the lifecycle of the system.

The following will focus on setting and configuration files as core configuration items of P&C systems. However, all elements in Section 3 should be included in the database, as applicable.

Setting and Configuration Data

The basic requirement of any database tool is its ability to store the description of a configuration item. Core elements for P&C systems are IEDs, switches, routers, and merging units that are communicating with each other. A key description element of each of these components is given by the settings and the configuration data. As described in Section 3, the representation of the data can be in different formats, and sometimes they even exist in proprietary manufacturer formats only. It would be desirable to store the data inside of the database in a format that can be read, edited, compared, and queried without the need to use any proprietary tools. Text formats or descriptions in XML format are examples of standard formats that the database needs to support. For example, the comparison of two different versions could easily be done by commonly available tools.

However, these standard formats (see Figure 5-1) may not be directly supported by proprietary tools used by different manufacturers.

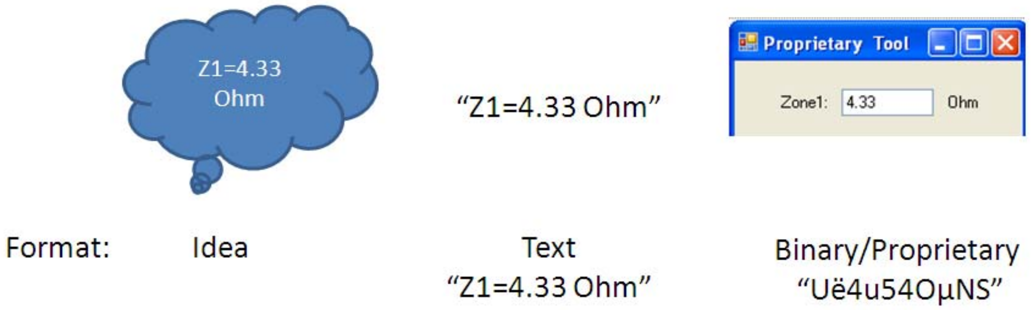


Figure 5-1
Data formats

This would make manual interaction necessary whenever information is exchanged between the devices and the database. For this reason, the database needs to be able to also store the proprietary setting and configuration file format as a description of a device as one object. A comparison of two settings and configuration files would require that the proprietary tool offers this functionality, and this would be handled outside of the central database. Note that even if two binary files are different, the setting and configuration data can be the same. The handling of the data file as an object will limit the ability to manage certain data elements individually. Setting classes or different access levels could not be managed for different settings or configuration data.

Import and export functionality between standard formats (text, Excel, and XML) and the proprietary manufacturer tool is increasingly supported. Most tools already offer the ability to export the data into standard formats but are limited if the import from a standard format is required. More complex configuration data, like user programmed logic and graphical displays programming (HMIs), are problematic.

To eliminate the problem with different file formats, the industry is focusing on the development of a common format to describe IED settings and configuration data. At this time, a working group, “Common format for IED configuration data,” in IEEE PSRC is evaluating the feasibility of such a common format. The report is expected by mid-2011.

Setting Comparison/Verification

Setting comparison and verification is an important functionality required for effective CM. Comparison can be applied to setting files with different versions and documenting the change from one version to another. This is important for tracking the changes following a change request. The comparison helps verify that only the setting and configuration changes requested were changed.

A second application is for the verification that the setting and configuration of a device are actually described by the stored data inside the database. The IED data should always be verified after the commissioning and maintenance test. The verification can be done through comparing the data file inside of the database against the data file that was retrieved from the relay.

Where possible, the comparison functionality should be performed directly by the database functionality. However, based on the proprietary file format, the comparison may be possible with the proprietary manufacturer tool only.

Another way to verify the correctness of the setting inside of an IED is by applying a test through a test set to the IED and monitoring the response to the test. This will be further discussed later.

Link Between Relays and Database

As described previously, it is important to verify the stored configuration and setting data against the actual data used by the devices and stored inside of the devices. For cyber security purposes, it may become required that the settings of all devices in a protection system considered as critical cyber assets be verified on a regular basis.

It is common that the P&C systems are connected to the enterprise communication system. In these cases, the process to verify the device information against the information stored in the database could be automated. The data from the devices will then be retrieved through the enterprise communication network and compared with the stored data in the database. Different file formats and the access to the relays data through proprietary manufacturer tools can only make this process complex and require customized solutions; however, new standards evolve that make it seem feasible that in the future all manufacturers will support a standardized service to retrieve and/or compare setting and configuration data.

Change Management

Any change request will trigger a sequence of events until the requested change of the settings or configuration is implemented. Processes in the utility make sure that all necessary steps are followed to perform the change, as shown in Figure 5-2.

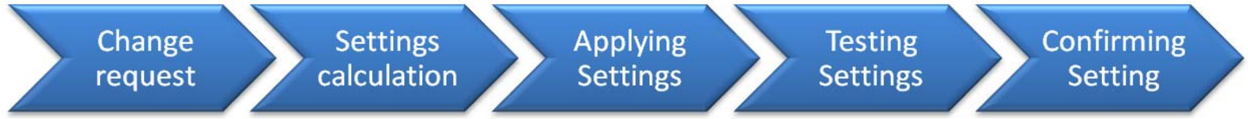


Figure 5-2
Example of a setting change process

A CM toll needs to support or at least efficiently interact with an existing process and monitor the progress of a change. A tool needs to be able to track a change and answer the following questions:

- Who made a change to the P&C system?
- What changes were made to the P&C system?
- When were the changes made?
- Why were the changes made?
- Who authorized the changes?

Status of Change

If a setting and configuration file is in the change process, the status of the change needs to be monitored and documented. The last valid data file version will remain in the system until the change process is finished. To set the file in progress to a new status, the process should trigger the notification of resources involved in the next process step. After the change process is finished, the latest released and confirmed version will replace the previous one. However, based on the change documentation, it should be possible to re-create the previous file using the “undo” button.

Managing Constraints Between Different Files in the Protection System

Very often some of the device settings depend on settings and configuration in other devices in the P&C system. A simple example is the line differential relay system. Both differential relays can communicate only to each other if they are using the same communication parameters. The relation can be more complex, and a CM tool needs to be able to manage these constraints. The support can range from simply documenting this constraint to automatically monitoring and alerting for any violations.

Different Classes of Settings

It is useful to have the ability to classify settings. In a modern numerical IED, there are hundreds of settings related to different functionality in the device. The classification can be related to the functionality inside of the device, for example, protection setting, metering setting, and fault recording settings, or by importance levels. The classification will support the change management to select different processes for different classes of settings.

Setting Templates

As important as the setting files are the templates for setting files. Templates are used to predefine a base structure of settings and configurations that may be standardized in the utility. The database tool needs to be able to track which actual setting file is based on which version of the setting template. If the template gets changed and the change needs to get applied to all IEDs, it should be possible to report all setting files that need to be updated. An example could be that the user-defined logic in the template needs to be changed.

Reporting Tools

Reports are required for a number of reasons, regulatory and/or internal to the utility, and the report content will vary. For example, a regulatory report prompted by a device misoperation may need to contain all data used for determining settings and configuration: the setting and configuration data, test records, verification of setting and configuration of the field device, any relevant fault reports, firmware upgrade, manufacturer service letter, and so on.

This is generally a challenge for the utility engineer because the data typically do not exist in one common format, especially if proprietary manufacturer tools are used. Export functionality from these proprietary tools is generally limited, resulting in time-consuming, manual manipulation to combine all data into one report.

An efficient database reporting tool should provide configuration options so that a number of report formats can be automatically generated by pulling data from the required files. Of course, this also requires that the setting and configuration file is stored (and kept updated) in a format that can be read and used by the reporting tool.

Access Management

The access to the database needs to be controlled, and the data needs to be protected against any unauthorized access. This becomes particularly important in relation to the requirements of cyber security. Although a data file is not directly listed as a critical cyber asset, tampering with a data file can have serious consequences. If settings are changed with bad intentions, they could eventually end up being loaded into the IED and causing a misoperation. The risk of an unintentional change of settings should be minimized by an access control mechanism.

IEEE PSRC is recognizing the cyber security concerns for P&C data files and is addressing this in a Working Group producing a report titled “Cyber Security for Protection Related Data Files.” Completion of the report is expected in 2012.

Access Level

The database tool should be able to assign different access levels and different access roles. Some users need access to read information only but should not have the right to change any of the information. This can even be applied differently to different groups of settings or configuration data. For example, a person responsible for the settings in relation to the metering functionality may not have access to the protection settings.

Access Roles

Role-based access control is based on the assignment of roles for the various job functions in an organization, and users are assigned roles based on their responsibilities and qualifications. A role is always associated with a certain access level and with certain rights.

Account Management

Each person granted access to the database should become an account that manages the access level, the role, and the password of the user. The user should always identify himself or herself by logging in with his or her password to access the database. Any change in the database can then be automatically recorded and associated with the person.

6
REFERENCES

ANSI/EAI-649A, “National Consensus Standard for Configuration Management,” October 2004.

CIGRE Committee B5 Colloquium, “Lifetime Management of Relay Settings,” 2009, Korea.

Configuration Management, http://en.wikipedia.org/wiki/Configuration_management (October 2010).

Current State Assessment: Next Generation Relays. EPRI, Palo Alto, CA: 2009. 1017773.

IEEE-PSRC Report C3, “Processes, Issues, Trends and Quality Control of Relay Settings,” March 2007.

IPS-presentation, NERC-CIPC—Compliant Settings Workflow Management for CAPE User, Dublin 2010.

Export Control Restrictions

The Electric Power Research Institute Inc., (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent more than 90 percent of the electricity generated and delivered in the United States, and international participation extends to 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

1020025

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com