Life-time management of relay settings

The Cigré B5.31 brochure describes a generic setting management process, based on the “best practises” of utilities based around the world. The process requires that all the changes that could affect the settings of a protection relay during its life time are identified, controlled and validated. This is necessary to ensure power system security is maintained, even during constrained operating scenarios.

The report recognises that the methods and techniques used to manage relay settings vary between utilities and are particularly influenced by organisational structures, out-sourcing and the levels of expertise available within the utility or collaborating organisations. However, irrespective of these factors, it is fundamentally important that the settings applied at an actual relay are strictly controlled and are always identical to those stored and maintained at the engineering centre.

The difficulties associated with managing other types of setting parameters, such as primary system topology, scheme logic and the mapping of inputs and outputs, are also described. Traditionally, these were fixed during the design of the relay or protection scheme, but now, digital relays have settings implemented within their logic or application configuration firmware, which need to be managed within an auditable setting control process.

The potential issues that a utility is expected to face in the life time management of their existing and future relay settings are highlighted and then discussed with respect to the tools and techniques needed to adapt and control the settings.

During the life time of a relay, the overall requirement on the utility is to develop a quality assurance process which simplifies the setting management process, minimises the possibility of human error and provides an auditable record of any changes made.

Generic process for managing settings

Many utilities outsource their engineering and setting calculations to an external contractor, while others implement and execute the entire process themselves. The proposed generic process is applicable to both of these scenarios, as well as the more common partial outsourcing of selected tasks. In addition, even though some utilities are organised functionally and others on a process basis, the generic process can be used regardless of company structure and the levels of outsourcing. The process ensures the hand-over of information is clearly defined within the organisation and the roles and responsibilities of individuals or work teams appropriately specified. A typical example is when engineering and field commissioning are performed by separate departments within the organisation or its outsourcing partners. The engineering department needs to pass the settings to the field department and be able to track and confirm that the approved settings were downloaded into the relay. After commissioning, the settings in the actual relay are uploaded and returned to the engineering department, where the settings issued are compared with the settings installed, to ensure they are the same and no changes or errors have occurred.

Organisation and people

Different utility organisational structures can result in setting management procedures that involve:

- Complete in-house designs (using the utilities own dedicated staff)
- Partnership arrangements (that share the activities with third parties)
- Full outsourcing (with in-house management and control)
- Third party delivery of complete turnkey projects.

In-house calculation and management of protection settings requires the utility to have sufficient well trained personnel to meet their current and near future needs.

---

**Fig. 1: Management flow chart.**

energize - September 2013 - Page 42
setting related needs. To ensure this is achievable the utility must be committed to the development and training of the next generation of protection engineers.

Outsourcing is an arrangement in which an external company provides protection setting services for a utility. Many utilities are considering, or have considered, outsourcing as a part of their operational efficiency improvements or as a method of gaining access to specialists unavailable within the utility. Outsourcing can range from specialist support, to the use of external companies who perform most or all of the protection activities required by the utility.

Many utilities provide support for their protection setting activities using a partnership between their own in-house experts and the resources of external organisations. The level of involvement of utility personnel in these activities depends on the type and size of the utility, the internal policies of the utility and its owners, and the regulatory framework applicable in the region where the utility operates.

Implementation of setting management

It has been identified that various triggers may require a review and update of the relay settings, including: asset replacement, new connections, primary plant changes, line reconductoring, temporary system changes, modifications in a neighbouring utility, secondary system changes, failures, maloperations, communication changes, setting reviews, new reliability requirements, manufacture recommendations or alerts, such as externally mandated changes.

An important feature is how the settings are organised within the relay. Generally, this is structured according to the setting policy of the relay manufacturer, but the organisational purpose for the utility is to help facilitate the verification of the settings and to simplify and standardise the processes used for the generation and modification of the settings.

Suitable criteria are:

- Settings that are fixed for a relay type
- Settings that are fixed for a specific application
- Settings that are individually derived.

Version control applied to the settings installed in a relay requires strict management and quality control. This is necessary to ensure the combination of the hardware version, firmware version, scheme logic, settings files and setting program are fully compatible and correct for the chosen protection scheme. It is essential that any modification in the settings can be undertaken in a carefully controlled manner, appropriate for changing protection and network requirements. This generally means that a utility fixes on a particular version of the relay, which is extensively tested and all the necessary support documentation generated.

Cyber security issues

The widespread use of communications for remotely accessing IEDs or digital relays increases the possibility of a malicious attack on a utility’s infrastructure. Historically, electromechanical and static relays did not include a communication interface and consequently could not be accessed and modified remotely. Any changes, including removing relays from service, required staff to be physically present within the station.

Software tools

A wide range of software tools are available to support the management of protection relays. Many tools were not originally designed for setting management purposes and consequently only support some of the process steps. They can be divided into utility specific or commercially available databases, network calculation tools, relay manufacturer tools and test set manufactures tools.

Recommended improvements and emerging developments

It is essential that a utility implements a quality procedure, based on a generic process that uses a structured approach to the management of settings. The setting engineer checks the setting configuration file, and determines if the settings are right for the application. The updating of the settings must be checked, documented and any changes securely stored. An area of concern is the need for firmware updates. It is recommended that the firmware is only changed if the existing firmware might result in a problem for the utility. Setting management is easier if you have fewer settings to change; therefore it is recommended that most of the settings required by a particular utility are fixed in advance by the manufacturer.

Utilities have traditionally managed the settings in an incremental manner; however, settings management procedures will need to be extensively changed to take full advantage of the IEC 61850 standards. To achieve this, new tools will need to be developed to allow seamless transfer and control of new language and database files. Settings management procedures based on IEC 61850 systems are starting to incorporate methods to take full advantage of the standard. Certain facilities are provided within the standard regarding change control and identification, and the use of Substation Communication Language (SCL) files offers opportunities to automate the process. These new facilities enable more reliable processes to maintain “as operating” documentation, rather than “as built” documentation, in a single file. As the SCL files take over the drawing of database records, this will create new opportunities to interrogate the files and include time stamps of changes, identification of devices including vendor serial number and firmware version.

Conclusion

A generic approach to the systems, procedures and guidelines for the life-time management of protection settings is described in the report. The emphasis has been on the need to provide adequate tools and processes to control the type and quantity of information that can be accessed by engineers/technicians with different levels of authorisation and to protect relays from malintentioned or inappropriate access. The report also identified future challenges associated with the lifetime management of relays and outlined how these may be addressed using a set of rules and recommendations. The overall principle of maintaining the setting files, and the associated chronological record of the changes, is vital to maintain the integrity of the protection system and help the utility analyse how the relay responded to future events, especially those that resulted in a protection maloperation.

This implies version management must be a secure process that captures the changes and the reasons for each change. Firmware and setting software versions must equally be controlled to avoid errors using incompatible versions between relays and the software used to set them. The adoption of new data and communication standards, such as IEC 61850, will have a significant impact on the way future settings will be managed. New software tools are needed to control the increasing numbers of settings available in digital relays, and to ensure their management is both more efficient and less susceptible to errors.

Acknowledgement

This article first appeared in Electra June 2013 and is republished here by permission.

Contact Rob Stephen, Eskom, Tel 031 563-0063, rob.stephen@eskom.co.za