Protection security assessment

Solution for protection system performance assessment and improvement

At a glance

A well-designed protection system must be both dependable (operate when it must, as quickly as possible) and secure (not operate when it needn't). These two requirements, referred together as reliability, often conflict with each other and a protection system that is fully secure and dependable is very difficult to achieve.

To a large extent, the reliability of a protection system depends on the settings that are applied on the protective relays that make up the system. Relay settings determine thresholds of operation such as minimum current pickup, inverse-time characteristics, time-delays, impedance reaches, etc. If not set correctly, the resulting protection system could have compromised reliability with serious consequences for both human and equipment safety. Additionally, improperly set relays can cause large scale power outages, resulting in blackouts.

A comprehensive assessment of protection system behavior is essential in ensuring that the settings calculated for the relays result in a system with very high levels of reliability.

The challenge

When calculating protection system settings, relay engineers typically perform a few manual studies to determine the most effective set points and thresholds. While somewhat effective, a manual approach by its nature is unable to comprehensively challenge the protection system and uncover vulnerabilities in it that can compromise protection reliability. A detailed assessment method is required to systematically challenge the protection system and determine its weak points, which can then be mitigated by the relay engineer.

In distribution systems with high penetration of renewable resources and variable network configuration due to use of distribution automation technology, conventional protection systems can suffer from a reduction in reliability. An adaptive protection scheme combined with a detailed assessment of reliability is a potential answer to this problem.

Our solution

Protection security assessment (PSA) enables protection engineers to automatically simulate, assess and improve selectivity, sensitivity and speed of the protection system performance for different network and operation conditions. For this purpose, PSA is offered as both a software solution and consulting service.

Siemens PTI's PSA consulting offering supports the complete workflow from data collection, network and protection simulation and assessment, to settings improvement. The underlying state of the art method is practice-proven and was deployed successfully for protection system reviews in transmission and distribution systems worldwide.

The workflow of the assessment process is shown in Figure 1.

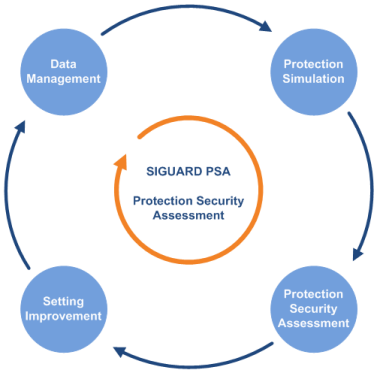

Figure 1: PSA workflow

Data collection

Electronically available network and protection data can be directly imported into PSS®CAPE or PSS®SINCAL simulation software for use during the PSA. Alternatively, there are easy-to-fill data collection spreadsheets facilitating the data collection process.

The data collection process is complemented with a multi-level data plausibility check tool. The strict elimination of data errors results in high quality network and protection data and thus provides the basis for meaningful protection simulation results.

PSA helps to optimize both data management and the reliable assessment of network and protection simulation models.

Simulation & performance assessment

Classical protection coordination methods mainly rely on the graphical depiction of setting values, short-circuit currents and network impedances for a few operating states and contingencies.

By contrast, PSA uses the combined power and protection system simulation and assesses the performance of the protection system by visualizing selectivity. This comprehensive consideration of the complete protection system, consisting of main protection and back-up protection, allows the detection of hidden errors for all possible network and fault scenarios.

The level of detail shown depends on the type of stakeholder who is viewing the results. The results can be represented in an aggregated manner for complete network areas (e.g. for the system operator) or detailed for each protection object or equipment (e.g. for the protection engineer).

The usage of color-coding, as shown in Table 1 below, facilitates identification of incorrect settings, weaknesses and limitations of protection system. If necessary, each step of fault clearing sequence can be analyzed in detail. All currents, voltages and impedances measured by protection devices are reported and explain the protection system behavior.

During a PSA, a large number of fault scenarios are assessed systematically and efficiently. The clear result visualization allows the precise identification of vulnerabilities in the protection system.

Table 1 Level of risk - PSA

Selective Operation	Circuit breakers controlled by relays with primary responsibility for clearing a fault
Over-function	In addition to primary circuit breakers, one or more backup circuit breakers tripped
Under-function	The fault is cleared; however, not all primary circuit breakers tripped.
Not Cleared	Protection system failed to clear a fault.

As a result of a PSA study, customers receive a detailed report as well as recommendations for optimizing their protection system performance based on verified measures.

Adaptive protection

An adaptive protection system is one in which the protective relay settings are continually adjusted in response to changing network conditions. An adaptive protection system will typically include the following activities:

- Capture present network topology
- Capture present protection settings
- Update the model
- Perform a comprehensive Protection Security Assessment (PSA)
- Adapt protection settings to meet sensitivity and selectivity targets
- Evaluate the compromises made
- Deploy new settings to field devices

A pilot implementation of the adaptive protection system has been deployed by Siemens in Germany. The process workflow of this system is shown in Figure 2. The scheme has been set up to evaluate the protection system at 15-minute intervals, unless an immediate evaluation is requested by the operator.

The reference network model containing information about the primary network and the protection system is first updated. Then, a detailed protection security assessment is initiated to determine if the settings as deployed provide adequate protection for the system. In Figure 2, a detailed view for protection engineers is reflected in the graphic shown to the left of the figure. An overall view, such as needed by the operator, is reflected in the graphic shown to the right of the figure.

The protection analysis is triggered by the operator taking a line out of service. The results of the initial security assessment are used to determine new settings, which are then deployed to the field and to the protection system database for use by subsequent analyses.

In Siemens' pilot implementation, the entire process consisting of network and protection snapshot, protection assessment, settings adaptation and deployment runs in an automated manner.

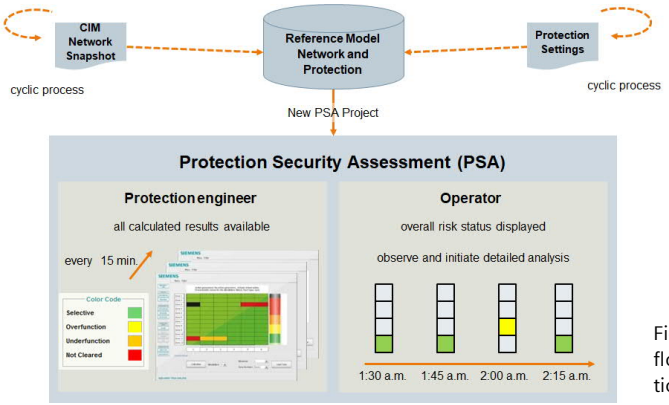

Figure 2 Process workflow - adaptive protection system.

Published by
Siemens AG
Smart Infrastructure
Digital Grid
Humboldtstrasse 59
90459 Nuremberg, Germany

For the U.S. published by
Siemens Industry Inc.
100 Technology Drive
Alpharetta, GA 30005, United States

AL=N, ECCN=EAR99