Generator Relay Loadability

System Protection

WECC Intent

The *Controls Guidance and Compliance Failure Points* document guides registered entities in assessing risks associated with their business activities and designing appropriate internal controls in response. WECC's intent is to provide examples supporting the efforts of registered entities to design controls specific to operational risk *and* compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards. The registered entity may use this document as a starting point in assessing risk and designing appropriate internal controls. Each registered entity should perform a risk assessment to identify its entity-specific risks and design appropriate internal controls to mitigate those risks; WECC does not intend for this document to establish a standard or baseline for entity risk assessment or control objectives.

> ***Note:*** *Guidance questions help an entity understand and document controls. Any responses, including lack of affirmative feedback, will have no consequences on an entity's demonstration of compliance during a Compliance Monitoring and Enforcement Program (CMEP) engagement.*
>
> ** Please send feedback to internalcontrols@WECC.org with suggestions on controls guidance and potential failure points questions.*

Definitions

Control Objective: The aim or purpose of specified controls; control objectives address the risks related to achieving an entity's larger objectives.

Control Activities: The policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks.

Internal Control: The processes, practices, policies or procedures, system applications and technology tools, and skilled human capital that an entity employs to address risks associated with the reliable operation of its business. Internal control components include:

- Control Environment;
- Risk Assessment;
- Control Activities;
- Information and Communication; and
- Monitoring.

Quality Assurance / Quality Control (QA/QC): How an entity *verifies* whether it performed an activity or verifies an activity was performed *correctly* (examples include separation of duties, having a supervisor double-check someone's work, etc.).

Risk Category: Type of operational and inherent risks identified by the Electric Reliability Organization (ERO) Enterprise for use in the Compliance Oversight Plan (COP). Entities should use Risk Categories to understand, monitor, and mitigate known and future risks.

Risk Category

The purpose of the PRC-025 standard is to ensure load-responsive protective relays associated with generation Facilities are set at a level to prevent unnecessary tripping of generators during a system disturbance. Unnecessary tripping of generators resulting in the removal of dynamic Reactive Power exacerbates the severity of the voltage disturbance, and as a result changes the character of the system disturbance. In addition, the loss of Real Power could initiate or exacerbate a frequency disturbance. The risks associated with this standard fall into the System Protection risk category as identified by the ERO Enterprise.

System Protection: BPS reliability and security requires adequate generation supplies to meet existing load during steady-state and expected dynamic conditions. When faults or failures occur, the system must isolate the problem but maintain BPS integrity as much as possible. Protection systems must identify the type and location of the problem and isolate the appropriate part of the BPS while minimizing the disturbance to the remainder of the system. This requires Protection Systems associated with the generation, transmission, and load to accurately detect system properties and respond appropriately to unsafe conditions. Protection System settings must allow control systems to provide a full range of control and allow the system to "ride-through" expected transients. Owners of interconnecting BPS devices and systems must coordinate their system settings with neighboring systems to ensure they achieve the desired outcome and prevent unnecessary disconnection of equipment. Protection Systems must also respond to Misoperations of primary protection. Entities must identify and correct the source of operational failures.

Control Objectives

Your entity should perform a risk assessment and identify entity-specific control objectives to mitigate those risks. To help entities get started, WECC has identified generic control objectives to mitigate the risks associated with the risk categories mentioned above and PRC-025-2. You may want to consider these two objectives:

Control Objective 1: Track applicable Protection Systems and settings.

Control Objective 2: Determine Protection System settings.

Reliability and Security Control Activities

Control activities are how your entity meets your control objectives. When designing and implementing controls, they should be tailored to meet the applicable objectives.

Below are examples of control activities based on good practices WECC has observed that are designed to meet the objectives listed above. WECC does not intend for these activities or the associated questions to be prescriptive. Rather, they should help your entity consider how you might meet your objectives in your own unique environment. They also may help your entity identify controls you did not realize you had.

Control Objective 1: Track applicable Protection Systems and settings.

Control Activity A: Identify applicable Generating units and Elements.

1. How does your entity ensure an accurate list of applicable generating units and Elements?
    a. Do you have a change management control to recognize possible required changes to Protection Systems when:
        i. New units are added?
        ii. Elements are changed?
        iii. Upgrades occur to applicable Facilities?
    b. Do you periodically review your identification of generating units and other applicable Elements?

Control Activity B: Ensure load-responsive relays are identified.

1. What tools or job aids do you use when identifying relays or conducting a review (e.g., one-line diagrams, relay and control diagrams)?
2. How does your entity monitor for additions, removals, or changes to load-responsive relays?
    a. What process do you follow to manage changes?
    b. Is there an as-built process that includes notifications related to the criteria?
3. How does your entity record "exclusions" per Attachment 1 of PRC-025-2?
4. Does your entity review the list of relays periodically?
    a. If so, how frequently?
5. Does your entity review the list of relays based on some trigger?
    a. If so, what triggers a review?

Control Activity C: Ensure necessary information is tracked and readily available

1. What tool or automated system does your entity use to track applicable equipment and Protection

Systems? (e.g., database, spreadsheet)

   a. Is it integrated with any other automated systems? (e.g., PRC-005 workorder system)
   b. If so, are there any flags or alerts to trigger PRC-025-2 criteria analysis based on changes made to applicable or like equipment?

2. Is your tool capable of tracking applicable equipment from planning through implementation and as-built phases?
3. What attributes does your entity track?
   a. Application
   b. Relay type
   c. Option selected per Table 1
   d. Settings
   e. Calculation summaries
   f. Simulations run and supporting data and assumptions
   g. Date of most recent calculations
   h. Date implemented
   i. Exclusions
3. If Protection Systems are re-evaluated or if new Protection Systems are installed, who has the authority to update your entity's tracking tool?
4. Does your entity use PRC-025 setting criteria for any elements to which PRC-025 is not applicable?
   a. If so, are they tracked together with applicable Protection Systems?

Control Objective 2: Determine Protection System settings.

Control Activity A: Determine which criteria to apply to each relay

1. How does your entity determine which criteria to use for each relay?
   a. How do you ensure it results in a setting that prevents unnecessary tripping of generators during a system disturbance?
   b. How do you ensure it results in a setting that achieves its desired protection goal?
2. Who is responsible for determining the appropriate criteria to apply?
   a. Is the decision made by a team?
3. Does your entity have a process to coordinate the selection of settings criteria with interconnected entities?
4. Do you have a peer review process?

Control Activity B: Run simulations and perform calculations per Attachment 1.

1. How does your entity select data and models for simulations?
2. How does your entity ensure the integrity of the Protection System settings data?
    a. Do you have a peer review process for simulation results?
    b. Do you have a document management system to store results and associated documentation?

Controls Activity C: Update attributes and calculations.

1. Does your entity have processes to address changes to:
    a. Relay settings?
    b. Inputs to simulations or calculations?
    c. Other?
2. Does your entity have an automated tool to alert you to changes?
3. Does your entity verify the settings are applied per Attachment 1 once the change is completed in the field?

Compliance Potential Failure Points

The control activities listed above are specifically targeted at mitigating risk to the reliability and security of the BPS, but also promote compliance with the referenced standard. Your entity should also develop controls specifically to mitigate compliance risk. The following compliance potential failure points relate directly to compliance risk and warrant consideration.

Potential Failure Point (R1): Failure to apply settings that are in accordance with PRC-025-2—Attachment 1 on each load-responsive protective relay.

1. Does your entity have a review process to ensure settings are in accordance with PRC-025-2—Attachment 1?
    a. Do you perform an initial review of calculations? (e.g., peer review, manager approval)
    b. What triggers require a review? (e.g., major system changes)
    c. How frequently do you conduct periodic reviews (e.g., annually)?
4. Does your entity use a technology to track relay settings that includes alerts for PRC-025-2 compliance?
5. Does your entity track and flag exclusions to Protection Systems per Attachment 1?
6. Does your entity use a technology to track updates to documentation as a result of relay setting selection (e.g., relay and control design and as-built one-line documentation) that supports verification of relay settings?