WECC
Electric Reliability and Security for the West

Controls Guidance and Compliance Failure Points

PRC-024-3

System Protection

August 2023

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 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 controls objectives.

> ***Note:*** *Guidance questions should help an entity understand, develop, 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 and Instructions

Control Objective: Aim or purpose of internal control to address identified risk or operational concern.

Control Activities: Policies, procedures, techniques, and mechanisms to achieve control objectives and mitigate related risks.

Internal Control: The plans, methods, policies, and procedures to fulfill a mission, goals, and objectives. Internal control components include:

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

Quality Assurance/Quality Control (QA/QC): How an entity *verifies* 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 ERO Enterprise for use in the Compliance Oversight Plan (COP). Entities should use risk categories to understand, monitor, and mitigate both existing and potential risks.

Risk Category

System Protection: Bulk Power System (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 Objective(s)

Your entity should perform a risk assessment and identify entity-specific control objectives to mitigate those risks. WECC has identified generic control objectives that may help your entity mitigate the risks associated with the risk categories mentioned above and PRC-024-3. You may want to consider these three objectives:

> **Control Objective 1**: Ensure settings are properly calculated for all applicable frequency and voltage protection.
>
> **Control Objective 2**: Analyze the effects of frequency and voltage excursion on the system protection.
>
> **Control Objective 3:** Set frequency and voltage protection to prevent trips and momentary cessations within the "no trip zone."

Reliability and Security Control Activities

Control activities are how your entity meets your control objectives. As you design controls, your entity should tailor them to entity-specific control 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: Ensure settings are properly calculated for all applicable frequency and voltage protection.

Control Activity A: Identify applicable frequency and voltage protection (Relates to risk associated with R1 and R2)

1. How does your entity ensure you have identified all:
    a. Generator protective relays that trip the generating resource?
    b. Protective functions within control systems that trip the generating resource?
    c. Protective functions that signal the generating resource to cease injecting current?
2. What tool(s) does your entity use to manage frequency and voltage protection data (e.g., spreadsheet, single database, multiple databases, file share)?
    a. Are component settings and inventory maintained in the same repository?
    b. How are protection relaying and inverter-based resource (IBR) protective functions differentiated?
    c. Who has the authority to update the inventory or the settings data?
    d. Is there a backup or secondary authority that ensures continuity?
3. What QA/QC does your entity perform to confirm data was entered correctly?

Control Activity B: Coordinate with the manufacturer to determine appropriate settings.

1. What process does your entity use to coordinate with the inverter manufacturer to ensure that inverter-protection settings are set using the following principles from NERC Industry Recommendations?[1]
    a. Are AC voltage protection settings expanded as widely as possible within the inverter-equipment capability? Is inverter instantaneous AC voltage tripping eliminated or minimized? (e.g., zero or near-zero time delay using instantaneous peak measurements)
    b. Is inverter-frequency protection set based on equipment capability? Does frequency protection operate on a filtered frequency measurement over a time window? Is inverter instantaneous frequency tripping eliminated or minimized?
    c. Is inverter instantaneous AC overcurrent protection set based on maximum inverter capability?
    d. Is inverter phase lock loop (PLL) loss of synchronism and/or phase jump protection set as widely as possible (or eliminated, if possible) to maximize ride-through capability?
    e. Is inverter DC bus protection configured to avoid any unnecessary tripping, particularly in

1 Industry Recommendation Inverter-Based Resource Performance Issues, North American Reliability Corporation, March 14, 2023

response to unbalanced faults?

f. Are all inverter AC and DC protections documented, including technical basis and the inverter capability curves (particularly for items a–e above)?

g. Are inverter-reconnection settings (voltage and frequency levels and time delay) coordinated with inverter-protection settings and the requirements established by the Balancing Authority?

2. What process does your entity use to ensure that all collector system and substation protection settings at the facility are set using the following principles listed in the NERC Industry Recommendations?
    a. Are protection settings based on the equipment ratings of the equipment they are intended to protect?
    b. Is the use of instantaneous voltage tripping eliminated or minimized? (e.g., zero or near-zero time delays)
    c. Is the use of instantaneous frequency tripping eliminated or minimized? Does frequency protection operate on a frequency measurement over a time window?
    d. Are protection settings coordinated with inverter- and plant-level controller protection and controls?
    e. Are plant-level trip settings in the power plant controller disabled?
3. What process does your entity use to coordinate with inverter manufacturer(s) and power plant controller manufacturer(s) to ensure that facility control modes, fault ride-through modes and parameters, and protections are set and coordinated according to the principles listed in the NERC Industry Recommendation?
    a. Are inverter and plant-level fault ride-through controls set and coordinated to ensure maximum ride-through capability and the provision of essential reliability services?
    b. Are fault ride-through parameters set to maximize active current delivery during the fault and post-fault periods unless otherwise limited by its current limit or reactive power priority mode? Are reactive power priority modes set to minimize reductions in active current, while providing and prioritizing a strong and appropriate reactive current response?
    c. Are all protection settings set to maximize ride-through performance, while still preventing damage to the equipment?
    d. Does facility output return to pre-disturbance active power levels as soon as possible without any artificial ramp rate limit or delay imposed by the power plant controller? Do ramp rates established by the Balancing Authority for dispatch impede plant recovery of active power post-fault?
4. What process does your entity use to coordinate with inverter manufacturer(s) and power plant controller manufacturer(s) to not artificially limit reactive power capability delivered to the point of interconnection?
5. If manufacturer settings do not meet NERC Industry Recommendations, what process does your

entity use to mitigate the resulting risk?

Control Activity C: Track changes to frequency and voltage protection (Relates to risk associated with R1 and R2)

1. Does your entity periodically review the list of applicable frequency and voltage protection to ensure accuracy and completeness?
2. How does your entity track changes, emergency or planned, that may affect protection settings and coordination?
    a. Who documents the changes?
    b. How do you know whether a system or equipment change should trigger a new analysis of settings?
    c. Is there a process to verify that appropriate follow-up actions are triggered after a change?

Control Objective 2: Analyze the effects of frequency and voltage excursion on the system protection.

Control Activity A: Analyze the protection system's response to frequency and voltage excursion (Relates to risk associated with R1 and R2).

1. Following a frequency excursion, what method does your entity use to analyze frequency protection operation to determine whether protection operated correctly?
2. Following a voltage excursion, what method does your entity use to determine whether voltage protection operated correctly?
3. Following an excursion, does your entity perform quality control to confirm setting calculations are correct?

Control Activity B: Coordinate with inverter manufacturer to document and mitigate known causes of inadvertent Protection System operation during normally cleared BPS faults.

1. What process does your entity use to identify inadvertent operations of Protection Systems?
2. What process does your entity use to coordinate with the inverter manufacturer to determine appropriate mitigations?
3. What Quality Controls are implemented to ensure inverter hardware or firmware updates are completed for all inverters supplied by manufacturers?

Control Activity C: Identify regulatory and equipment limitations that may permit tripping within the "no trip zone" (Relates to risk associated with R1, R2, and R3).

1. How does your entity identify and document limitations?
    a. What tool(s) does your entity use to track regulatory and equipment limitations? (e.g., spreadsheet, database)
    b. What supporting documentation is maintained?
        i. Study results

ii. Experience from an actual event
iii. Manufacturer's specifications or recommendations

2. How is the cumulative turbine lifetime frequency excursion allowance tracked?
    a. Is any process triggered if or when the cumulative excursion allowance is approached or exceeded?
3. What process does your entity use to coordinate with inverter manufacturer(s) in instances where IBRs fail to ride through normally cleared BPS faults to provide technical justification for the deficiency?
    a. How is the technical justification developed (manufacturer advice, additional studies, documented technical limitations of the IBR)?
    b. What activities, if any, does your entity perform to eliminate or reduce the impact of equipment limitations?
4. How do you track efforts to eliminate or reduce the impact of equipment limitations?
5. By what method does your entity communicate regulatory or equipment limitations to appropriate entities?
6. How does your entity ensure updates regarding limitations are provided to the appropriate entities?
    a. What process(es) does your entity have in place to ensure updates to the regulatory and equipment limitations are provided to appropriate entities in the case of equipment repair, replacement, or adjustment?
    b. Who is responsible to update the documentation?

Control Objective 3: Set frequency and voltage protection to prevent trips and momentary cessations within the "no trip zone."

Control Activity A: Ensure Protection System field personnel are aware of the implications of updating protection settings when repairing or replacing protection equipment.

1. What tools does your entity have in place to support Protection System field personnel regarding setting frequency and voltage protection?
    a. Do you include detailed information in a work order system?
    b. Do you use checklists?
    c. What QA/QC process is used to ensure settings or setting changes have been implemented on a device?

Control Activity B: Review all protection changes before implementation, and address the impacts when found.

1. How does your entity ensure it coordinates proposed changes to protection (internally and with external entities) before implementing the change?
2. How does your entity determine whether a change to a protection setting affects activities required elsewhere in the standards?

a. Do you have any technology tools to automatically cross-reference settings with other standards?
b. Do you use checklists to coordinate settings across requirements?

Control Activity C: Review implemented protection settings.

1. What Quality Control does your entity perform to confirm protection is set as designed?
2. What changes would trigger an additional review of actual settings?
    a. Equipment changes?
    b. Events?
    c. Other?
3. Does your entity have periodic reviews of protection settings?
    a. How frequently do you review protection settings?
    b. Do you have a task management system to notify you when a protection setting is due for review?
    c. What do you compare the settings to?
        i. Do you specifically review them for compliance with specific requirements?
        ii. Do you compare them to the last documented setting?
4. Does your entity have periodic reviews of relay-level one-line diagrams and other design documentation to ensure applicable relays are accounted for within inventory?
5. Does your entity conduct periodic reviews of functions (and their settings/triggers) within associated control systems that respond to electrical signals that may trip or provide signals to trip or cease injecting current?

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 set frequency protection such that the applicable protection does not cause the generating resource to trip or cease injecting current within the "no trip zone" during a frequency excursion.

Potential Failure Point (R2): Failure to set voltage protection such that the applicable protection does not cause the generating resource to trip or cease injecting current within the "no trip zone" during a voltage excursion at the high side of the GSU or MPT (per Attachment 2 or per Transmission Planner's location-specific study).

Potential Failure Point (R3): Failure to document known regulatory or equipment limitations.

Potential Failure Point (R3): Failure to communicate known regulatory or equipment limitations or changes to limitations to Planning Coordinator and Transmission Planner within 30 days.

1. Does your entity have controls to track the timing of the communication?
2. Does your entity verify receipt of the information by interested parties?

Potential Failure Point (R4): Failure to provide applicable protection settings to the Planning Coordinator or Transmission Planner that models the associated generating resource(s) within 60 calendar days of receipt of a written request for the data and within 60 calendar days of any change to those previously requested settings.

1. Does your entity have controls to track the receipt of a request through to response?
2. What person or group is responsible to—
    a. Receive the request?
    b. Track the request?
    c. Respond to the request?
3. Does your entity perform QA/QC to confirm it responded to the request within 60 calendar days?
4. Does your entity verify receipt of the requested information by interested parties?
5. Does your entity have controls to monitor previously requested data for changes?