Technical Rationale

Project 2023-06 CIP-014 Risk Assessment Refinement
Reliability Standard CIP-014-4 | September 2024

CIP-014-4 – Physical Security

In performing the risk assessment, the Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Attachment 1. The Standard requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or Cascading within an Interconnection.

The purpose of Reliability Standard CIP-014 is to protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. To properly identify candidates for such Transmission station(s) and Transmission substation(s), the Transmission Owner shall evaluate the criteria listed in Attachment 1.

Rationale for Requirement R1

Performing Risk Assessments

Requirement R1 is developed to ensure that each Transmission Owner establishes a list of applicable Transmission station(s) or Transmission substation(s) in accordance with Attachment 1. Aligning the 36 months look ahead in Requirement R1 with the 36 month risk assessment cycle ensures that system topology of the cases used to assess applicability is consistent with the system topology in the risk assessment models.

Rationale for Requirement R2

Each Transmission Owner shall, at a minimum, consider the specifications in Requirement R2 for general applicability to their systems, and whether specifications and thresholds need to be stipulated for each Parts 2.1 and 2.2 in their documented criteria.

A certain amount of discretion and flexibility is intended to be allowable for each Transmission Owner in their respective proximity criteria to document, establish, and demonstrate from a technical basis that various aspects of proximity for their Transmission station(s) or Transmission substation(s) either are or are not appropriate to consider in their risk assessments.

Rationale for Requirement R3

Per Requirement R3, each Transmission Owner is required to have a risk assessment methodology, but the SDT intends for each TO to have flexibility to define its own methodology, including the criteria by which analytical results will be examined to identify Transmission station(s) or Transmission substation(s) that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. The TO is not required to develop its own methodology and is free to use a methodology developed elsewhere, such as in coordination with neighboring TOs or ISOs.

Rationale for Requirement R3, Part 3.1

TOs should have the flexibility to determine the amount of acceptable load loss, acceptable generation loss, or other measurements of system response when determining the impact of an event to the Transmission system. Criteria for measures such as load loss or generation loss should consider the impact to the Interconnection instead of local impacts.

Large loss of generation or load due to the evaluated disturbance, as well as consequences of isolating faulted equipment, could result in severe System impacts. The documented risk assessment methodology shall include the amount of acceptable load loss, the amount of acceptable generation loss, and post-event response resulting in instability, uncontrolled separation, or Cascading within an Interconnection. Conditions and thresholds used for determining critical Transmission station(s) or Transmission substation(s), i.e., those that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection, should be part of the documented risk assessment methodology.

It is up to the TO to identify post-event measures that can be used to assess the criticality of a Transmission substation or Transmission substation. Suggested measures are listed below. A TO can decide that one or more of the items are not applicable to their location within the interconnection and if any additional items should be included

These thresholds can be treated as proxies for other conditions such as excessive frequency deviation.

- Steady state voltages
- Transient voltage response
- Thermal loading of Facilities
- Relay loadability
- Rotor angle stability
- Frequency exceeding generator limits
- Frequency stability
- Acceptable damping of oscillations
- Cascading line tripping
- Steady-state voltage stability

Rationale for Requirement R3, Part 3.2

The performance of both steady state and dynamics simulations is required for all applicable Transmission station(s) and substation(s). Dynamic simulations are required by the SAR after NERC and FERC determined that steady-state simulations alone are insufficient for determining whether the loss of a Transmission station or Transmission substation could result in instability, uncontrolled separation, or Cascading within an Interconnection.

Transmission Owners shall develop documented criteria for the conditions listed in Requirement R3, Part 3.1.1, which includes branch thermal exceedance thresholds, bus voltage exceedance thresholds, load loss thresholds, generation loss thresholds, etc.

Rationale for Requirement R3, Part 3.3

The DT believes that simulation of a fault is a reasonable assumption for possible events that could impact a single Transmission station or Transmission substation, and for events that could simultaneously impact multiple Transmission stations or Transmission substations.

Rationale for Requirement R3, Part 3.4

The requirement that simulations shall assume the loss of communications and system protection is consistent with the SAR. It is also consistent with the use of “inoperable” in the standard.

Rationale for Requirement R3, Part 3.4.1

The DT believes that the use of delayed or remote clearing times is consistent with the description of a Transmission station or Transmission substation being rendered inoperable by an event that disabled local protection systems.

Rationale for Requirement R3, Part 3.4.2

While there are commonly used generic clearing times for remote clearing that are consistent across the industry, actual clearing times can be shorter or longer depending on conditions and design considerations at an individual TO. The difference of a few cycles can have a significant impact on the transient behavior of generating units, therefore, it is required that the risk analysis use actual clearing times or more conservative values.

Rationale for Requirement R4

Joint ownership of Transmission substations and Transmission stations was discussed in the Guidelines and Technical Basis of previous versions of the CIP-014-3 standard. Because the CIP-014-4 Risk Assessment Refinement SAR calls for clarification regarding Transmission substations and Transmission stations of differing ownership, this section was moved to its own requirement within R4.

Rationale for Requirement R5

Rationale for Requirement R5, Part 5.2

<u>Identification of Primary Control Centers</u>

After completing the risk assessment under Requirement R5 and verified under Requirement R6, it is important to additionally identify the primary control center that operationally controls each Transmission station or Transmission substation, that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. A primary control center “operationally controls” a Transmission station or Transmission substation when the control center’s electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker.

Requirement R6 through Requirement R10 are Requirement R2 through Requirement R6 in CIP-014-3. The Drafting Team did not make any changes to these Requirements. Therefore, the technical rationales are not provided here.

Rationale for Attachment 1

The purpose of Reliability Standard CIP-014-4 is to protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack, could result in instability, uncontrolled separation, or Cascading within an Interconnection. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP-014-4 primarily applies to Transmission Owners that own Transmission Facilities that meet the specific applicability criteria in Attachment 1. The Facilities described in Attachment 1 mirror those Transmission Facilities that meet bright line criteria for “Medium Impact” Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1a. Each Transmission Owner that owns Transmission Facilities that meet the criteria in Attachment 1 is required to perform a risk assessment to identify its Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.

This standard also applies to Transmission Operators. A Transmission Operator’s obligations under the standard, however, are only triggered if the Transmission Operator is notified by an applicable Transmission Owner under Requirement R7 that the Transmission Operator operates a primary control center that operationally controls a Transmission station(s) or Transmission substation(s) identified in the Requirement R5 risk assessment. A primary control center operationally controls a Transmission station or Transmission substation when the control center’s electronic actions can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker, as opposed to a control center that only has information from the Transmission station or Transmission substation and must coordinate direct action through another entity. Only Transmission Operators who are notified that they have primary control centers under this standard have performance obligations under Requirements R8 through R10. Primary control center, for purposes of this Standard, is the control center that the Transmission Owner or Transmission Operator, respectively, uses as its primary, permanently-manned site to physically operate a Transmission station or Transmission substation that is identified in Requirement R5 and verified in Requirement R6. Control centers that provide back-up capability are not applicable, as they are a form of resiliency and intentionally redundant.

The DT determined that continuing to use criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-002-5.1a would provide a conservative threshold for defining which Transmission stations and Transmission substations that must be included in the risk assessment in Requirement R5 of CIP-014-4. Additionally, the DT concluded that using CIP002-5.1a Medium Impact criteria was appropriate because it has been approved by stakeholders, NERC, and FERC, and its use provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment. As described in CIP-002-5.1a, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs).

Additionally, the DT determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. First, Transmission stations or Transmission substations interconnecting generation facilities are considered when determining applicability. Transmission Owners will consider those Transmission stations and Transmission substations that include a Transmission station on the high side of the Generator Step-up transformer (GSU) using Attachment 1, criteria 1 and 2. As an example, a Transmission station or Transmission substation identified as a Transmission Owner facility that interconnects generation will be subject to the Requirement R5 risk assessment if it operates at 500kV or greater or if it is connected at 200 kV – 499kV to three or more other Transmission stations or Transmission substations and has an "aggregate weighted value" exceeding 3000 according to the table in Attachment 1, criteria 2. Second, the Transmission analysis or analyses conducted under Requirement R5 should take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations. Additionally, the FERC order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities. The diagram below shows an example of a station.

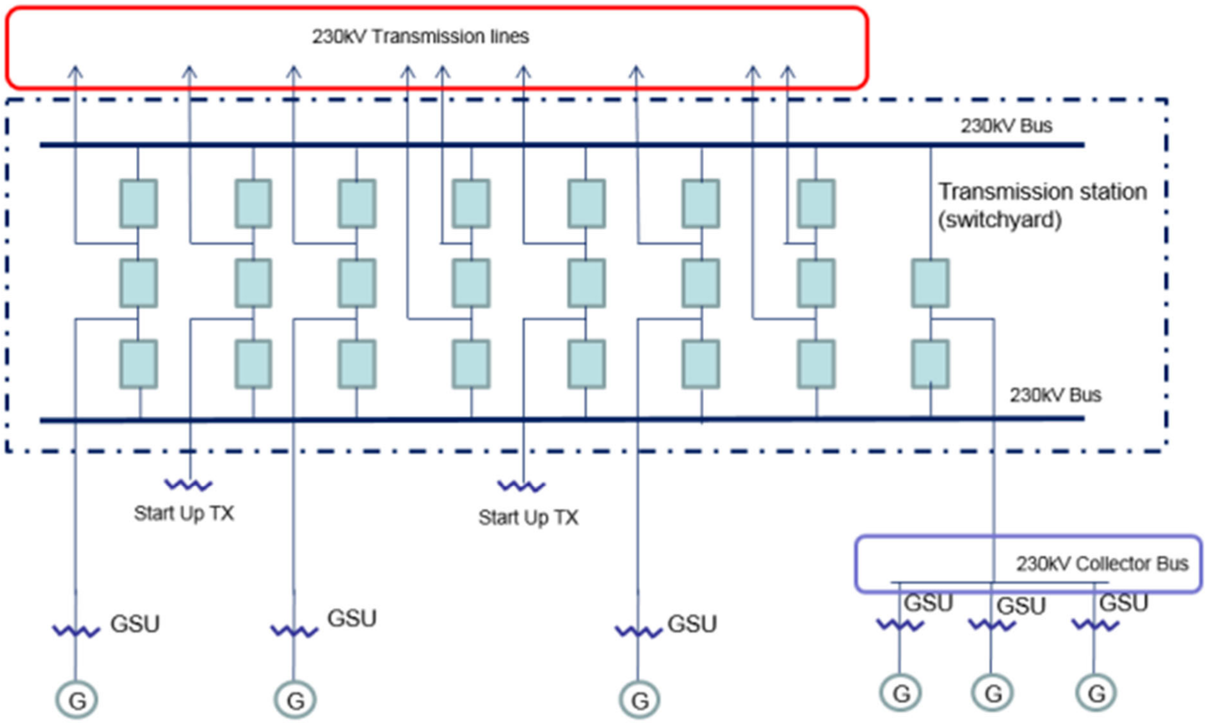

Figure from CIP-014-3 Guidelines and Technical Basis

Also, the DT uses the phrase "Transmission station(s) or Transmission substation(s)" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e., fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (switching stations or switchyards). Therefore, the DT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.