CIP-014-2 – Physical Security

Requirement R2 Risk Assessment Review and Verification Methodology

Version 1.4

Regional Transmission

April 13, 2020

Table of Contents

1 Background

The purpose of CIP-014-2 is to identify and 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.[1]

Requirement R1 of the standard requires each Transmission Owner to perform periodic risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in the Applicability Section 4.1.1 of the standard. The risk assessments are to consist of transmission analyses designed to identify the Transmission stations and Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. Requirement R2 of the standard further requires each Transmission Owner to have an unaffiliated third party, such as a registered Planning Coordinator, verify the risk assessment performed under Requirement R1.

The California Independent System Operator Corporation ("CAISO") has been requested by interested Transmission Owners to be their unaffiliated third party verifying entity under Requirement R2[2]. This document outlines the scope, verification methodology and the type of documentation the ISO will be requiring from Transmission Owners to complete a definitive review of their R1 risk assessment. This framework was developed on the basis that the Transmission Owners' facilities are within the ISO's Planning Coordinator area, although the methodology may also be expanded and applied to other Transmission Owners' facilities as well.

2 Scope of Work

The CAISO's Requirement R2 verification of the Transmission Owner's R1 risk assessment transmission analysis will consist of review and verification of the following:

1. The application of Applicability Section 4.1.1 in identifying Transmission stations and substations in scope for the R1 risk assessment.
2. The risk assessment methodology and models used to conduct the risk assessment

[1] Capitalized terms are those from the Glossary of Terms Used in the NERC Reliability Standards.

[2] Requirement R6 of CIP-014-2 requires each applicable Transmission Owner and Operator to have an unaffiliated third party review the security plans developed under Requirement R5. CAISO has not been requested or agreed to be the third party reviewer under R6. The scope of work outlined in this document is solely limited to the review of the transmission analysis related risk assessments under Requirement R2.

3. The risk assessment results
4. The identification of the primary control center that operationally controls each critical station or substation identified in the risk assessment (i.e, the control center that can cause direct physical actions, such as opening a breaker, at the critical station or substation).

3 Risk Assessment Methodology Employed by Transmission Owners

The objective of the risk assessment is to identify the stations and substations that could result in instability, uncontrolled separation, or Cascading in the event of a physical attack. The risk assessment methodology should consider the applicable requirements provided in Reliability Standard TPL-001-4 including Requirements R3, R4 and R6. The CAISO has established a methodology for identifying transmission facilities that could lead to instability, uncontrolled separation, or Cascading in the event of contingencies and has applied the methodology to several previous NERC Standard FAC-014-2 related IROL studies. The CAISO recommends Transmission Owners consider using the applicable elements of the IROL methodology described below in the CIP-014-2 risk assessment, as doing so would provide consistency of methodology across ISO/TOs and NERC Standards.

Power flow or preferably post transient governor power flow and transient stability analyses should be performed to the extent needed to ascertain and demonstrate that contingencies associated with the station or substation under study do not result in instability, uncontrolled separation, or Cascading. For instance, if a station or substation is identified as meeting Requirement R1 using power flow or post transient analysis, performing stability analysis may not be necessary.

3.1 Potential Cascading Due to Excessive Overloading

Excessive overloading can cause Cascading or uncontrolled separation if the excessively overloaded facility is removed from service due to relay action, equipment failure, faults caused by excessive sagging or forced immediate manual disconnection (for example, due to public safety concerns). Given some of these factors cannot be modeled in simulations, a facility should be removed from service due to excessive overloading if the facility loading exceeds the lower of:

a) The facility’s trip setting, and
b) 125 percent of the facility’s highest rating defined for a duration of 30 minutes or more.

If the excessively overloaded facility is a series capacitor on a transmission line, the series capacitor should be short-circuited (bypassed) rather than open-circuited unless specific information is available.

The threshold for excessive overloading is based on the threshold established in the SOL Methodology for the Planning Horizon.[3]

Simulations should be repeated with excessively overloaded facilities successively removed from service until the potential for Cascading, instability or uncontrolled separation is established, the load impact threshold is exceeded or no facility is excessively overloaded.

3.2 Load Impact Threshold

There may be cases where the impact of instability, uncontrolled separation or cascading outages associated with loss of a station or substation is confined to a single facility or a local area. In such cases, the station or substation may not meet Requirement R1 provided the loss of load is demonstrated to be less than 1000 MW. The loss of load threshold is based on the threshold established in the SOL Methodology for the Planning Horizon.

The load impact threshold represents an upper bound for load loss regardless of demonstrated containment, and should include the loss of firm load due to Cascading or the action of UFLS and UVLS schemes. The threshold is intended to restrict the applicability to large-area impacts rather than small-load areas. However, this requirement is not intended to limit the ability of Transmission Owners to identify, or the CAISO to recommend, critical stations or substations under Requirement R1 when doing so is considered prudent.

3.3 Models

Base cases approved by the Western Electricity Coordinating Council (WECC) or preferably base cases that were reviewed or used by the CAISO or the Transmission Owner in the latest annual reliability assessment process should be used as a starting point, since these cases will have the most up-to-date models and system representation within the entire Western Interconnection. The cases should be modified to represent Transmission stations or Transmission substations that are both existing and planned to be in service within 24 calendar months. The base cases should reflect system peak and off-peak scenarios representing stressed system conditions with respect to load, generation, and/or transfers within the system. The ISO may recommend changes to the scenarios used for one or more stations or substations, if it considers the change could result in a more adverse system impact.

[3] https://www.caiso.com/Documents/SystemOperatingLimitsMethodology-PlanningHorizon.pdf

3.4 Contingencies to be Simulated

Unless other types of outages at a station or substation such as loss of individual voltage levels have been identified in previous planning studies to be more severe, outages will model loss of each in-scope station and substation along with all associated transformation, protection including SPS, control and communication equipment, as well as all transmission lines that are connected to the station or substation.

In addition, the Transmission Owner should consider taking out two or more stations or substations that are in close proximity to one another. While the Transmission Owner's considerations in this regard could be further informed by expert assessment regarding the threats and vulnerabilities, as a minimum two or more stations or substations within 100 feet of each other should also be studied as a single station or substation.

For stability analysis, each station or substation contingency should be modeled with the worst-case three-phase fault and Delayed Clearing. Unless specific information is available to the contrary, a fault on the station or substation bus with the highest voltage may be considered the worst case fault.

3.5 Monitored Impacts

For each in-scope station or substation contingency, voltage and transient instability, Cascading and uncontrolled separation or impacts that indicate the potential for such Adverse Reliability Impacts needs to be monitored during simulations and reported. These include:

a) Voltage instability or power flow solution divergence
b) Transient instability
c) Cascading
d) Uncontrolled separation
e) Excessive overloading, i.e. overloading exceeding the lower of a facility's trip setting and 125 percent of the facility's highest rating defined for a duration of at least 30 minutes
f) Amount of load disconnected due to Cascading or the action of UFLS and UVLS schemes including load that is disconnected manually when evaluating Cascading due to excessive overloading
g) Facilities tripped during stability analysis by relay action
h) Frequency below under-frequency load shed points.

Other less severe loading, voltage, voltage deviation, transient voltage dip and frequency dip impacts that are not expected to lead to instability, Cascading or uncontrolled separation need not be included in the main risk assessment report.

4 Documentation Required For Verification

Transmission Owners must provide all documentation necessary to perform a definitive verification under Requirement R2 of the standard. The necessary documentation includes a risk assessment report and supporting documentation as described below.

4.1 Risk Assessment Report

The risk assessment report should include:

a) For each Transmission station or substation (existing and planned to be in service within 24 months) owned by the Transmission Owner, the number by voltage class of transmission lines connected to the station or substation and the "aggregate weighted value".
b) The list of stations and substations determined to be in-scope for Requirement R1 including the criteria from Applicability Section 4.1.1 for the selection.
c) A description of the risk assessment methodology and any associated criteria applied.
d) Sufficient description of the base cases, including the rationale for any of the assumptions as needed.
e) Sufficient description of the contingencies used for power flow and stability analyses.
f) Critical Transmission facility and tie line overload and frequency trip settings.
g) Sufficient description of the impacts monitored.
h) For each in-scope station and substation contingencies, the results of the system impact study, including as applicable:
    i. Whether voltage instability, transient instability, Cascading, or uncontrolled separation was identified.
    ii. Excessively overloaded facilities, along with the result of successively disconnecting the excessively overloaded facilities.
    iii. The amount of load disconnected manually or by UFLS, UVLS, along with the cause for disconnection.
    iv. Facilities tripped during stability analysis by relay action.
    v. Frequency below under-frequency load shed points.
i) The list of critical stations and substations that are found to meet the criteria under Requirement R1, and
j) The primary control center that operationally controls each critical station or substation identified (i.e., the control center that can cause direct physical actions, such as opening a breaker, at the critical station or substation).

4.2 Supporting documentation

Supporting documentation may include, but may not be limited to,

a) Documentation from the Reliability Coordinator, Planning Coordinator and Transmission Planner identifying Transmission Facilities critical to the derivation of IROLs under Applicability Section 4.1.1.3.
b) Supporting documentation for Facilities identified as essential to meeting Nuclear Plant Interface Requirements under Applicability Section 4.1.1.3.
c) Study base cases, dynamics files, switching decks and, if used, contingency OTG files.
d) For each station or substation contingency, post transient analysis tool output files showing the switching sequence simulated and the simulation results.
e) Power flow output files, if used, in which network convergence and excessive overloading is monitored.
f) As needed, for each station or substation contingency, one or more power flow diagrams and stability plots (such as frequency, voltage, power flow, relative angles).

5 Outcome of Review

At the conclusion of the R2 review of the Transmission Owner’s R1 risk assessment, the CAISO will provide a risk assessment verification report. The report will be primarily based on the risk assessment report and supporting documentation provided by the Transmission Owner. However, the CAISO may perform its own simulations to confirm the results for one or more stations or substations as needed.

The CAISO risk assessment verification report will include a summary of its verification methodology, a description of the Transmission Owner’s risk assessment reports and supporting documentation reviewed, and the findings, including whether the CAISO concurs with the Transmission Owner’s assessment or recommendations for the addition or deletion of one or more Transmission stations or substations.

6 Schedule

The CAISO will complete the verification within 90 calendar days following receipt of the Transmission Owner’s risk assessment documentation. Transmission owners that are not Participating Transmission Owners shall also provide a $50,000 deposit for the assessment and the 90 calendar day schedule will commence following receipt of the deposit.