# Alberta Reliability Standards

**Updated: July 17, 2023**



Calgary Place, 2500, 330-5th Avenue SW Calgary, AB T2P 0L4
Phone: 403-539-2450 | Fax: 403-539-2949

# Alberta Reliability Standards Contents

## ADM – Administrative



## BAL – Resource and Demand Balancing



## CIP – Critical Infrastructure Protection



## COM – Communications

# Alberta Reliability Standards Contents

## PER – Personnel Performance, Training, and Qualifications



## PRC – Protection and Control



## TPL – Transmission Planning



## VAR – Voltage and Reactive

## Purpose

**1** The purpose of this **reliability standard** is to provide a mechanism for a **market participant** to request, and for the **ISO** to approve, appropriate waivers and variances to specific requirements of a **reliability standard**.

## Applicability

**2** This **reliability standard** applies to:

(a) a **market participant**, including:

(i) a **legal owner**; and

(ii) an **operator**; and

(b) the **ISO**.

## Requirements

### Applicable reliability standards

**3(1)** The **ISO** must consider a request for either one or both of a waiver and variance to any requirement in the **reliability standards**, provided that the requirement does not have its own separate mechanism for requesting and approving a waiver or variance.

**(2)** The **ISO** may either grant, in whole or in part, or deny a request for a waiver or variance submitted in accordance with this **reliability standard**.

### Grounds for requesting a waiver or variance

**4(1)** A **market participant** may request either one or both of a waiver and variance to any of the requirements set out in the **reliability standards**.

**(2)** A **market participant** must provide grounds for requesting a waiver or variance which must include one or more of the following circumstances where compliance with the requirements of the **reliability standard**:

(a) is not technically possible or is precluded by technical limitations;

(b) is operationally infeasible;

(c) is operationally unnecessary to achieve the intended purpose or outcome of the **reliability standard**;

(d) cannot be achieved by the required compliance date regardless of good faith efforts by the **market participant** which does not include a failure to appropriately plan;

(e) would pose a safety risk or safety issue;

(f) would conflict with a separate statutory or regulatory requirement that is applicable and cannot be waived or exempted;

(g) would require the incurrence of costs that significantly outweigh the benefits achieved or would result in severe economic hardship;

(h) could be achieved in an alternate timeframe that is reasonable to consider in light of other relevant factors, including upcoming scheduled maintenance, and anticipated facility upgrades;

(i) would have suboptimal results compared with the use of alternate technology that would meet or exceed the objectives of the subject **reliability standards**; and

(j) does not allow for testing the application of technology that was not considered during the development of the requirements.

### Criteria for evaluating a request

**5** The **ISO** must be satisfied that the grounds provided are sufficient and use one or more of the following criteria to evaluate any request for a waiver or variance:

(a) technical feasibility;

(b) operational feasibility and burden;

(c) safety;

(d) economic impacts;

(e) material impacts on a fair, efficient, and openly competitive market;

(f) whether appropriate mitigation measures, mitigation plans, or remediation plans can be or are put in place; and

(g) the **reliability** of the **interconnected electric system**.

### Submission of Information

**6** A **market participant** must:

(a) make a request for a waiver or variance to the **ISO** in writing;

(b) respond to requests from the **ISO** for additional information or for the submission of a revised request; and

(c) advise the **ISO** as soon as practicable upon becoming aware of a material change in the facts or circumstances underlying a request.

### Evaluation Process

**7** The **ISO** must:

(a) acknowledge receipt of a request for a waiver or variance;

(b) request any additional information it requires to complete the evaluation of the request;

(c) provide updates on progress;

(d) provide a written decision to the **market participant**; and

(e) if it denies the request, give reasons.

### Content of a waiver or variance

**8** The **ISO** must include the effective date in an approved waiver or variance and any of the following as applicable:

(a) expiry date;

(b) mitigation or remediation plans, including milestones;

(c) reporting requirements; and

(d) any other terms and conditions the **ISO** considers necessary.

### Ongoing management of a waiver or variance

**9(1)** A **market participant** must, as soon as reasonably practicable, notify the **ISO** of any material change to the facts or circumstances underlying the approval of a waiver or variance.

**(2)** A **market participant** may transfer a waiver or variance with the **ISO**'s written consent which consent will not be unreasonably withheld.

**(3)** The **ISO** may amend or revoke a waiver or variance upon reasonable notice if:

(a) there is a material change to the facts or circumstances underlying the approval of the waiver or variance; or

(b) the **market participant** does not fulfill the terms or conditions of the approval.

### Revision History

| Date | Description |
|---|---|
| 2021-04-22 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to control **Interconnection** frequency within defined limits.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO** except when:

(i) the **ISO** is receiving overlap regulation service;

(ii) the **ISO** is a member of a regulation reserve sharing group and remains in active status under the applicable agreement or the governing rules for the regulation reserve sharing group; or

(iii) the **interconnected electric system** is not synchronously connected to the **Interconnection**.

## 3. Requirements

**R1** The **ISO** must operate such that the **control performance standard** 1, calculated in accordance with Appendix 1, is greater than or equal to 100% for each preceding 12 consecutive **month** period, evaluated monthly.

**R2** The **ISO** must operate such that its clock-minute average of **reporting area control error** does not exceed the clock-minute **area control error** limit of the **balancing authority** for more than 30 consecutive clock-minutes, calculated in accordance with Appendix 2.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of operating such that the **control performance standard** 1 is greater than or equal to 100% as required in requirement R1 exists. Evidence may include dated calculation output from spreadsheets, system logs, or other equivalent evidence.

**MR2** Evidence of operating such that the clock-minute average of **reporting area control error** does not exceed the clock-minute **area control error** limit of the **balancing authority** for more than 30 consecutive clock-minutes as required in requirement R2 exists. Evidence may include dated calculation output from spreadsheets, system logs, or other equivalent evidence.

## 5. Appendices

Appendix 1 - *Equations Supporting Requirement R1 and Measure M1*

Appendix 2 - *Equations Supporting Requirement R2 and Measure M2*

### Revision History

| Date | Description |
|---|---|
| 2019-07-01 | Initial release. |

## Appendix 1 – Equations Supporting Requirement R1 and Measure M1

The **control performance standard** 1 (CPS1) is calculated as follows:

$$\mathrm{CPS1} = (2 - CF) \times 100\%$$

The frequency-related compliance factor ($\mathrm{CF}$), is a ratio of the accumulating clock-minute compliance parameters for the most recent preceding 12 consecutive **months**, divided by the square of the target frequency bound:

$$CF = \frac{CF_{12-\mathrm{month}}}{(\varepsilon 1_{\mathrm{I}})^2}$$

where $\varepsilon 1_{\mathrm{I}}$ is the constant derived from a targeted frequency bound for the **western interconnection** or as revised by the **NERC**.

The rating index $\mathrm{CF}_{12-\mathrm{month}}$ is derived from the most recent preceding 12 consecutive **months** of data. The accumulating clock-minute compliance parameters are derived from the one-minute averages of **reporting area control error**, **frequency error**, and **frequency bias settings**. A clock-minute average is the average of the reporting **balancing authority**'s valid measured variable (i.e., for **reporting area control error** ($RACE$) and for **frequency error**) for each sampling cycle during a given clock-minute.

$$\left(\frac{RACE}{-10B}\right)_{\mathrm{clock-minute}} = \frac{\left(\frac{\sum RACE_{\mathrm{sampling\ cycles\ in\ clock-minute}}}{n_{\mathrm{sampling\ cycles\ in\ clock-minute}}}\right)}{-10\mathrm{B}}$$

And,

$$\Delta F_{\mathrm{clock-minute}} = \frac{\sum \Delta F_{\mathrm{sampling\ cycles\ in\ clock-minute}}}{n_{\mathrm{sampling\ cycles\ in\ clock-minute}}}$$

The **balancing authority**'s clock-minute compliance factor ($CF_{\mathrm{clock-minute}}$) calculation is:

$$CF_{\mathrm{clock-minute}} = \left[\left(\frac{RACE}{-10B}\right)_{\mathrm{clock-minute}} \times \Delta F_{\mathrm{clock-minute}}\right]$$

Normally, 60 clock-minute averages of the **reporting area control error** and **frequency error** will be used to compute the hourly average compliance factor ($CF_{\mathrm{clock-hour}}$).

$$CF_{\mathrm{clock-hour}} = \frac{\sum CF_{\mathrm{clock-minute}}}{n_{\mathrm{clock-minute\ samples\ in\ hour}}}$$

The reporting **balancing authority** must be able to recalculate and store each of the respective clock-hour averages ($\text{CF}_{\text{clock-hour average-month}}$) and the data samples for each 24-hour period (one for each clock-hour; i.e., hour ending (HE) 0100, HE 0200, ..., HE 2400). To calculate the monthly compliance factor ($\text{CF}_{\text{month}}$):

$$\text{CF}_{\text{clock-hour average-month}} = \frac{\sum_{\text{days-in-month}}\left[\left(\text{CF}_{\text{clock-hour}}\right)\left(n_{\text{one-minute samples in clock-hour}}\right)\right]}{\sum_{\text{days-in-month}}\left[n_{\text{one-minute samples in clock-hour}}\right]}$$

$$\text{CF}_{\text{month}} = \frac{\sum_{\text{hours-in-day}}\left[\left(\text{CF}_{\text{clock-hour average-month}}\right)\left(n_{\text{one-minute samples in clock-hour averages}}\right)\right]}{\sum_{\text{hours-in day}}\left[n_{\text{one-minute samples in clock-hour averages}}\right]}$$

To calculate the 12-**month** compliance factor ($\text{CF}_{12\text{-month}}$):

$$\text{CF}_{12\text{-month}} = \frac{\sum_{i=1}^{12}\left[\left(CF_{\text{month-i}}\right)\left(n_{(\text{one-minute samples in month})-i}\right)\right]}{\sum_{i=1}^{12}\left[n_{(\text{one-minute samples in month})-i}\right]}$$

To ensure that the average **reporting area control error** and **frequency error** calculated for any one-minute interval is representative of that time interval, it is necessary that at least 50% of both the **reporting area control error** and **frequency error** sample data during the one-minute interval is valid. If the recording of **reporting area control error** or **frequency error** is interrupted such that less than 50% of the one-minute sample period data is available or valid, then that one-minute interval is excluded from the CPS1 calculation.

A **balancing authority** providing overlap regulation service to another **balancing authority** calculates its CPS1 performance after combining its **reporting area control error** and **frequency bias settings** with the **reporting area control error** and **frequency bias settings** of the **balancing authority** receiving the regulation service.

### Appendix 2 - Equations Supporting Requirement R2 and Measure M2

When actual frequency is equal to scheduled frequency, $BAAL_{High}$ and $BAAL_{Low}$ do not apply.

When actual frequency is less than scheduled frequency, $BAAL_{High}$ does not apply, and $BAAL_{Low}$ is calculated as:

$$BAAL_{Low} = \left(-10B_i \times (FTL_{Low} - F_S)\right) \times \frac{(FTL_{Low} - F_S)}{(F_A - F_S)}$$

When actual frequency is greater than scheduled frequency, $BAAL_{Low}$ does not apply and the $BAAL_{High}$ is calculated as:

$$BAAL_{High} = \left(-10B_i \times \left(FTL_{High} - F_S\right)\right) \times \frac{\left(FTL_{High} - F_S\right)}{(F_A - F_S)}$$

Where:

$BAAL_{Low}$ is the low **area control error** limit of the **balancing authority** (MW)

$BAAL_{High}$ is the high **area control error** limit of the **balancing authority** (MW)

$10$ is a constant to convert the **frequency bias setting** from MW/0.1 Hz to MW/Hz

$B_i$ is the **frequency bias setting** for a **balancing authority** (expressed as MW/0.1 Hz)

$F_A$ is the measured frequency in Hz.

$F_S$ is the **scheduled frequency** in Hz.

$FTL_{Low}$ is the low frequency trigger limit (calculated as $F_S - 3\varepsilon 1_I\ Hz$)

$FTL_{High}$ is the high frequency trigger limit (calculated as $F_S + 3\varepsilon 1_I\ Hz$)

Where $\varepsilon 1_I$ is the constant derived from a targeted frequency bound for the **western interconnection** or as revised by the **NERC**.

To ensure that the average actual frequency calculated for any one-minute interval is representative of that time interval, it is necessary that at least 50% of the actual frequency sample data during that one-minute interval is valid. If the recording of actual frequency is interrupted such that less than 50% of the one-minute sample period data is available or valid, then that one-minute interval is excluded from the **area control error** limit of the **balancing authority** calculation and the 30-minute clock would be reset to zero.

A **balancing authority** providing overlap regulation service to another **balancing authority** calculates its **area control error** limit of the **balancing authority** performance after combining its **frequency bias setting** with the **frequency bias setting** of the **balancing authority** receiving overlap regulation service.

# Alberta Reliability Standard
# Contingency Reserve for Recovery from a Balancing Contingency Event
# BAL-002-AB-3

## 1. Purpose

The purpose of this **reliability standard** is to ensure the **ISO** balances resources and **demand** and returns the **area control error** to defined values, subject to applicable limits, following a reportable **balancing contingency event**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**, only in periods during which the **ISO** is not in active status under a **reserve sharing group** agreement or governing rules for a **reserve sharing group.**

## 3. Requirements

**R1** The **ISO**, when it is experiencing a reportable **balancing contingency event** must:

**R1.1** within the **contingency** event recovery period, demonstrate recovery by returning its **reporting area control error** to at least the recovery value of:

(a) zero (if its pre-reporting **contingency** event **area control error** value was positive or equal to zero); or

(b) its pre-reporting **contingency** event **area control error** value (if its pre-reporting **contingency** event **area control error** value was negative);

however, any **balancing contingency event** that occurs during the **contingency** event recovery period must reduce the required recovery: (i) beginning at the time of, and (ii) by the magnitude of, such individual **balancing contingency event**;

**R1.2**. document all reportable **balancing contingency events** using the form the **NERC** designates; and

**R1.3**. deploy **contingency reserve**, within system constraints, to respond to all reportable **balancing contingency events**; however, the **ISO** is not subject to compliance with requirement R1.1 if the **ISO**:

**R1.3.1** (a) is experiencing an **ISO** declared energy emergency alert level;

(b) is using its **contingency reserve** to mitigate an operating emergency in accordance with its emergency operating plan;

(c) has depleted its **contingency reserve** to a level below its most severe single **contingency**; and

(d) intentionally left blank; or

**R1.3.2** (a) experiences multiple **contingencies** where the combined MW loss exceeds its most severe single **contingency** and that are defined as a single **balancing contingency event**; or

(b) experiences multiple **balancing contingency events** within the sum of the time periods defined by the **contingency** event recovery period and **contingency** reserve restoration period whose combined magnitude exceeds the **ISO**'s most severe single **contingency**.

**R2** The **ISO** must develop, review, and maintain annually, and implement an operating process as part of its operating plan to determine its most severe single **contingency** and make preparations to have **contingency reserve** equal to, or greater than the **ISO**'s most severe single **contingency** available for maintaining system **reliability**.

**R3** The **ISO**, following a reportable **balancing contingency event**, must restore its **contingency reserve** to at least its most severe single **contingency**, before the end of the **contingency reserve** restoration period, but any **balancing contingency event** that occurs before the end of a **contingency reserve** restoration period resets the beginning of the **contingency** event recovery period.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1.1** Evidence of demonstrating the recovery of the **reporting area control error** as required in requirement R1.1 exists. Evidence may include documented reportable **balancing contingency events** using the designated form, or other equivalent evidence.

**MR1.2** Evidence of documenting all reportable **balancing contingency events** as required by requirement R1.2 exists. Evidence may include documented reportable **balancing contingency events** using the designated **NERC** form, or other equivalent evidence.

**MR1.3** Evidence of deploying **contingency** reserve, within system constraints, to respond to all reportable **balancing contingency events**, as required in requirement R1.3 exists. Evidence may include **directive** logs, phone calls, designated forms, or other equivalent evidence.

**MR2** Evidence of developing, reviewing, maintaining and implementing an operating process to determine the most severe single **contingency** and to have **contingency** reserves as required in requirement R2 exists. Evidence may include a dated operating process with a revision history, or other equivalent evidence.

**MR3** Evidence of restoring **contingency reserve** as required in requirement R3 exists. Evidence may include historical data, computer logs, operator logs, or other equivalent evidence.

## Revision History

| Date | Description |
|---|---|
| 2019-07-01 | Initial release. |

# Alberta Reliability Standard
# Contingency Reserve
# BAL-002-WECC-AB1-2

## 1. Purpose

The purpose of this **reliability standard** is to specify the quantity and types of **contingency reserve** required to ensure reliability under normal and abnormal conditions.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**, which may meet the requirements of this reliability standard through participation in a **reserve sharing group** that the **ISO** has designated as its agent.

This **reliability standard** does not apply in the case of contingencies that result in the **interconnected electric system** losing synchronism with the **western interconnection.**

## 3. Requirements

**R1** The **ISO** must have held, at a minimum, an average amount of **contingency reserve** that is:

**R1.1** the greater of either:

(a) an amount equal to the loss of the most severe single **contingency**; or

(b) an amount equal to the sum of:

three percent (3%) of the hourly integrated amount of load, being the hourly integrated amount of net generation the **ISO** determines is delivered to the grid minus **net actual interchange**;

plus

three percent (3%) of the hourly integrated amount of net generation the **ISO** determines is delivered to the grid;

where “net generation the **ISO** determines is delivered to the grid” is equal to the sum of:

(i) generation from a **generating unit** or **aggregated generating facility** but not including unit service and station service loads;

plus

(ii) generation from an industrial complex or facility that has on-site generation but not including generation serving on-site load;

plus

(iii) generation delivered to the grid by the City of Medicine Hat;

**R1.2** comprised of any combination of the **operating reserve** types specified below:

(a) **spinning reserve**;

(b) **supplemental reserve**;

(c) **interchange transactions** sourced within Alberta that the **ISO** designates as **supplemental reserve**;

(d) **interchange transactions** sourced external to Alberta that the **ISO** designates as **spinning reserve** or **supplemental reserve** and that, by agreement, is deliverable to Alberta on firm transmission service;

(e) a resource, other than a **generating unit**, an **aggregated generating facility** or load, that can provide energy or reduce energy consumption;

(f) load, including demand response resources, demand-side management resources, direct control load management, interruptible load or **interruptible demand**, or any other load made available for curtailment by the **ISO** via contract or agreement; and

(g) during capacity and energy emergencies, load that can be interrupted; and

**R1.3** an amount of capacity from a resource that is capable of fully responding within ten (10) minutes;

except within the first sixty (60) minutes following a **disturbance** resulting from a loss of supply and requiring the activation of **contingency reserve** or except following the deployment of **contingency reserve** during implementation of the **ISO**'s capacity and energy emergency plan.

**R2** The **ISO** must maintain at least fifty percent (50%) of its minimum amount of **contingency reserve** required in requirement R1 as **spinning reserve** that is immediately and automatically responsive to frequency deviations through the action of a **governor** or other control system.

**R3** The **ISO** must, when operating as a sink **balancing authority**, maintain an amount of **operating reserve**, in addition to the minimum **contingency reserve** required in requirement R1, equal to the amount of **supplemental reserve** for any **interchange transaction** designated as part of the **supplemental reserve** of the source **balancing authority** or source **reserve sharing group**, except within the first sixty (60) minutes following an event requiring the activation of **contingency reserve** or except following the deployment of **contingency reserve** during implementation of the **ISO**'s capacity and energy emergency plan.

**R4** The **ISO** must, when operating as a source **balancing authority**, maintain an amount of **operating reserve**, in addition to the minimum **contingency reserve** amounts required in requirement R1, equal to the amount and type of **operating reserve** for any **operating reserve** transactions for which it is the source **balancing authority**.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this reliability standard. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of having held **contingency reserve** as required in requirement R1 exists. Evidence may include:

(a) a **reserve sharing group** agreement including an agent appointment agreement, documentation of the methodology of the **contingency reserve** calculation, or **ancillary services** contracts; or

(b) records of **disturbances** or implementation of the **ISO**'s capacity and emergency plan as required in requirement R1.

**MR1.1** Evidence of calculating the amount of **contingency reserve** as required in requirement R1.1 exists. Evidence may include records of the required and available **contingency reserve**.

**MR1.2** Evidence of having **contingency reserve** that is comprised of the **operating reserve** types as required in requirement R1.2 exists. Evidence may include a **reserve sharing group** agreement including an agent appointment agreement or **ancillary services** contracts.

**MR1.3** Evidence of having access to **contingency reserve** that is capable of fully responding in ten (10) minutes as required in requirement R1.3 exists. Evidence may include a **reserve sharing group** agreement including an agent appointment agreement or technical requirements for **contingency reserve**.

**MR2** Evidence of maintaining at least fifty percent (50%) of the ISO's minimum amount of **contingency reserve** as **spinning reserve** that is immediately responsive to frequency deviations as required in requirement R2 exists. Evidence may include a **reserve sharing group** agreement including an agent appointment agreement or records of **dispatches** of **ancillary services**.

**MR3** Evidence of maintaining an amount of **operating reserve** as required in requirement R3 exists. Evidence may include a sworn affidavit from an appropriate **ISO** representative, authoritative documents that restrict or permit the transactions set out in requirement R3, documents that demonstrate the **ISO** was in a capacity and energy emergency, or a **reserve sharing group** agreement including an agent appointment agreement.

**MR4** Evidence of maintaining an amount of **operating reserve** as required in requirement R4 exists. Evidence may include a sworn affidavit from an appropriate **ISO** representative or a **reserve sharing group** agreement including an agent appointment agreement.

## Revision History

| Effective Date | Description |
|---|---|
| 2015-07-26 | Revised Applicability section to include exclusion for contingencies that result in the **interconnected electric system** losing synchronism with the **western interconnection** |
| 2014-10-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to:

(a) require sufficient **frequency response** from the **ISO** to maintain **Interconnection** frequency within predefined bounds by arresting frequency deviations and supporting frequency until the frequency is restored to its scheduled value; and

(b) provide consistent methods for measuring **frequency response** and determining the **frequency bias setting**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**, unless the **interconnected electric system** is not synchronously connected to the **Interconnection**.

## 3. Requirements

**R1** The **ISO** must:

(a) achieve an annual **frequency response** measure (as calculated in accordance with Appendix A) that is equal to or more negative than its **frequency response** obligation; and

(b) report, in accordance with Appendix A, the annual **frequency response** measure calculated pursuant to requirement R1(a),

which obligations the **ISO** may meet through participation in a **frequencyresponse** sharing group which the **ISO** has designated as its agent.

**R2** The **ISO** must, if it is not receiving overlap regulation service and uses a fixed **frequency bias setting**:

**R2.1** implement the **frequency bias setting** determined in accordance with Appendix A, as validated by the Electric Reliability Organization, into its **area control error** calculation during the implementation period specified by the Electric Reliability Organization; and

**R2.2** use this **frequency bias setting** until directed to change by the Electric Reliability Organization.

**R3** The **ISO** must, if it is not receiving overlap regulation service and is utilizing a variable **frequency bias setting**, maintain a **frequency bias setting** that is:

**R3.1** less than zero at all times; and

**R3.2** equal to or more negative than its **frequency response** obligation when frequency varies from 60 Hz by more than +/- 0.036 Hz.

**R4** The **ISO** must, if it is performing overlap regulation service, modify its **frequency bias setting** in its **area control error** calculation, in order to represent the **frequency bias setting** for the combined **balancing authority area**, to be equivalent to either:

**R4.1** the sum of the **frequency bias settings**, as shown on the **NERC** *FRS Form 1* and *FRS Form 2* for the participating **balancing authorities** and as validated by the Electric Reliability Organization, or

**R4.2** the **frequency bias setting** shown on the **NERC** *FRS Form 1* and *FRS Form 2* for the entirety of the participating **balancing authority areas**.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of achieving an annual **frequency response** measure as required in requirement R1, and of reporting the annual **frequency response** measure as required in requirement R1 exists. Evidence may include dated data plus documented formula in either hardcopy or electronic format that shows an annual **frequency response** measure was achieved that is equal to or more negative than the **frequency response** obligation, a dated document in hard copy or electronic format showing submission of a completed report, or other equivalent evidence.

**MR2** Evidence of implementing the **frequency bias setting** as validated by the Electric Reliability Organization into the **area control error** calculation as required in requirement R2 exists. Evidence may include a dated document in hard copy or electronic format showing the **frequency bias setting** as validated by the Electric Reliability Organization was implemented into the **area control error** calculation within the implementation period specified, or other equivalent evidence.

**MR3** Evidence of maintaining a **frequency bias setting** as required in requirement R3 exists. Evidence may include a dated report in hard copy or electronic format showing the average clock-minute average **frequency bias setting** was less than zero and, during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz, was equal to or more negative than the **frequency response** obligation, or other equivalent evidence.

**MR4** Evidence of modifying the **frequency bias setting** in the **area control error** calculation as required in requirement R4 exists. Evidence may include a dated operating log, database or list, in hard copy or electronic format, showing that when overlap regulation service was performed the **frequency bias setting** was modified in the **area control error** calculation, or other equivalent evidence.

## 5. Appendices

Appendix A - *BAL-003-AB-1.1 Frequency Response & Frequency Bias Setting Standard Supporting Document*

### Revision History

| Date | Description |
|---|---|
| 2019-08-01 | Amended R1 as follows;<br>replaced “reserve” with “response”, bolded frequency and unbolded ‘sharing group’. |
| 2019-07-01 | Initial release. |

## Appendix A

### BAL-003-AB-1.1 Frequency Response & Frequency Bias Setting Standard Supporting Document

**Interconnection Frequency Response Obligation**

The Electric Reliability Organization, in consultation with regional representatives, has established a target contingency protection criterion for each **frequency response** obligation of the **Interconnection**. The default **frequency response** obligation of the **Interconnection** listed in Table 1 is based on the resource contingency criteria, which is the largest category C (N-2) event identified. A maximum delta frequency is calculated by adjusting a starting frequency for each **Interconnection** by the following:

- Prevailing **underfrequency load shedding** first step;
- $CC_{Adj}$ which is the adjustment for the differences between 1-second and sub-second Point C observations for frequency events. A positive value indicates that the sub-second C data is lower than the 1-second data;
- $CB_R$ which is the statistically determined ratio of the Point C to Value B; and
- $BC'_{Adj}$ which is the statistically determined adjustment for the event nadir being below the Value B (Eastern Interconnection only) during primary **frequency response** withdrawal.

The **frequency response** obligation for each **Interconnection** in Table 1 is then calculated by dividing the resource **contingency** criteria MWs by 10 times the maximum delta frequency. In the Eastern Interconnection there is an additional adjustment ($BC'_{Adj}$) for the event nadir being below the Value B due to primary **frequency response** withdrawal. This **frequency response** obligation for the **Interconnection** includes uncertainty adjustments at a 95% confidence level. Detailed descriptions of the calculations used in Table 1 below are defined in the *Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard*.

Table 1

| Interconnection | Eastern | Western | ERCOT | HQ | Units |
|---|---|---|---|---|---|
| Starting Frequency ($F_{start}$) | **59.974** | **59.976** | **59.963** | **59.972** | Hz |
| Prevailing UFLS First Step | **59.5*** | **59.5** | **59.3** | **58.5** | Hz |
| Base Delta Frequency ($DF_{Base}$) | **0.474** | **0.476** | **0.663** | **1.472** | Hz |
| $CC_{ADJ}$ | **0.007** | **0.004** | **0.012** | **N/A** | Hz |
| Delta Frequency ($DF_{CC}$) | **0.467** | **0.472** | **0.651** | **1.472** | Hz |
| $CB_R$ | **1.000** | **1.625** | **1.377** | **1.550** | |
| Delta Frequency ($DF_{CBR}$) | **0.467** | **0.291** | **0.473** | **0.949** | Hz |
| $BC'_{ADJ}$ | **0.018** | **N/A** | **N/A** | **N/A** | Hz |
| Max. Delta Frequency | **0.449** | **0.291** | **0.473** | **0.949** | |
| Resource Contingency Criteria | **4,500** | **2740** | **2,750** | **1700** | MW |

| Interconnection | Eastern | Western | ERCOT | HQ | Units |
|---|---|---|---|---|---|
| Credit for Load Resources (CLR) | | 300 | 1400** | | MW |
| IFRO | -1002 | -840 | -286 | -179 | MW/0.1 Hz |

*The Eastern Interconnection **underfrequency load setting** set point listed is a compromise value set midway between the stable frequency minimum established in the **NERC** standard PRC-006-1, *Automatic Underfrequency Load Shedding* (59.3 Hz) and the local protection **underfrequency load setting** setting of 59.7 Hz used in Florida and Manitoba.

**In the base obligation measure for ERCOT, 1400 MW (load resources triggered by under frequency relays at 59.70 Hz) was reduced from its resource **contingency** criteria level of 2750 MW to get 239 MW/0.1 Hz. This was reduced to accurately account for designed response from load resources within 30 cycles.

An **Interconnection** may propose alternate **frequency response** obligation protection criteria for that **Interconnection** to the Electric Reliability Organization by submitting a *Standard Authorization Request* with supporting technical documentation.

**Balancing Authority Frequency Response Obligation and Frequency Bias Setting**

The Electric Reliability Organization will manage the administrative procedure for annually assigning a **frequency response** obligation and implementation of the **frequency bias setting** for each **balancing authority**. The annual timeline for all activities described in this section are shown below.

For an **Interconnection** with multiple **balancing authorities**, the **frequency response** obligation shown in Table 1 is allocated based on the **balancing authority** annual load and annual generation. The **frequency response** obligation allocation will be based on the following method:

$$FRO_{BA} = IFRO \times \frac{\text{Annual Gen}_{BA} + \text{Annual Load}_{BA}}{\text{Annual Gen}_{Int} + \text{Annual Load}_{Int}}$$

Where:

- Annual $\text{Gen}_{BA}$ is the total annual "Output of Generating Plants" within the **balancing authority area**, on FERC *Form 714*, column c of Part II - Schedule 3.
- Annual $\text{Load}_{BA}$ is total annual load within the **balancing authority area**, on FERC *Form 714*, column e of Part II - Schedule 3.
- Annual $\text{Gen}_{Int}$ is the sum of all annual $\text{gen}_{BA}$ values reported in that **Interconnection**.
- Annual $\text{Load}_{Int}$ is the sum of all annual $\text{load}_{BA}$ values reported in that **Interconnection**.

The data used for this calculation is from the most recently filed *Form 714*. As an example, a report to the **NERC** in January 2013 would use the *Form 714* data filed in 2012, which utilized data from 2011.

**Balancing authorities** that are not FERC-jurisdictional should use the *Form 714 Instructions* to assemble and submit equivalent data to the Electric Reliability Organization for use in the **frequency response** obligation allocation process.

**Balancing authorities** that elect to form a **frequency response** sharing group will calculate a **frequency response** sharing group **frequency response** obligation by adding together the individual **frequency response** obligations of the **balancing authority**.

**Balancing authorities** that elect to form a **frequency response** sharing group as a means to jointly meet the **frequency response** obligation will calculate their **frequency response** measure performance in one of two ways:

- Calculate a group **net actual interchange** and measure the group response to all events in the reporting year on a single *FRS Form 1*, or
- Jointly submit the individual **balancing authorities**' *FRS Form 1*s, with a summary spreadsheet that contains the sum of each participant's individual event performance.

**Balancing authorities** that merge or that transfer load or generation are encouraged to notify the Electric Reliability Organization of the change in footprint and corresponding changes in allocation such that the net obligation to the **Interconnection** remains the same and so that **control performance standard** limits can be adjusted.

Each **balancing authority** reports its previous year's **frequency response** measure, **frequency bias setting** and **frequency bias** type (fixed or variable) to the Electric Reliability Organization each year to allow the Electric Reliability Organization to validate the revised **frequency bias settings** on *FRS Form 1*. If the Electric Reliability Organization posts the official list of events after the date specified in the timeline below, **balancing authorities** will be given 30 **days** from the date the Electric Reliability Organization posts the official list of events to submit their *FRS Form 1*.

Once the Electric Reliability Organization reviews the data submitted in *FRS Form 1* and *FRS Form 2* for all **balancing authorities**, the Electric Reliability Organization will use *FRS Form 1* data to post the following information for each **balancing authority** for the upcoming year:

- **frequency bias setting**; and
- **frequency response** obligation.

Once the data listed above is fully posted, the Electric Reliability Organization will announce the three-day implementation period for changing the **frequency bias setting** if it differs from that shown in the timeline below.

A **balancing authority** using a fixed **frequency bias setting** sets its **frequency bias setting** to the greater of (in absolute value):

- Any number the **balancing authority** chooses between 100% and 125% of its **frequency response** measure as calculated on *FRS Form 1*; or
- The **Interconnection** minimum as determined by the Electric Reliability Organization.

For purposes of calculating the minimum **frequency bias setting**, a **balancing authority** participating in a **frequency response** sharing group will need to calculate its stand-alone **frequency response** measure using *FRS Form 1* and *FRS Form 2* to determine its minimum **frequency bias setting**.

A **balancing authority** providing overlap regulation will report the historic peak demand and generation of its combined **balancing authority areas** on *FRS Form 1* as described in requirement R4.

There are occasions when changes are needed to **frequency bias settings** outside of the normal schedule. Examples are footprint changes between **balancing authorities** and major changes in load or generation or the formation of new **balancing authorities**. In such cases, the changing **balancing authorities** will work with their regions, the **NERC**, and the Resources Subcommittee to confirm appropriate changes to **frequency bias settings**, **frequency response** obligation, **control performance standard** limits and **inadvertent interchange** balances.

If there is no net change to the **Interconnection** total **frequency bias**, the **balancing authorities** involved will agree on a date to implement their respective change in **frequency bias settings**. The **balancing authorities** and Electric Reliability Organization will also agree to the allocation of **frequency response** obligation such that the sum remains the same.

If there is a net change to the **Interconnection** total **frequency bias**, this will cause a change in CPS2 limits and **frequency response** obligation for other **balancing authorities** in the **Interconnection**. In this case, the Electric Reliability Organization will notify the impacted **balancing authorities** of their respective changes and provide an implementation window for making the **frequency bias setting** changes.

**Frequency Response Measure**

The **balancing authority** will calculate its **frequency response** measure from single event **frequency response** data, defined as: “the data from an individual event from a **balancing authority** that is used to calculate its **frequency response**, expressed in MW/0.1Hz” as calculated on *FRS Form 2* for each event shown on *FRS Form 1*. The events in *FRS Form 1* are selected by the Electric Reliability Organization using the *Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard*. The **frequency response** measure for a typical **balancing authority** in an **Interconnection** with more than one **balancing authority** is basically the change in its **net actual interchange** on its **intertie** with its **adjacent balancing authorities** divided by the change in **Interconnection** frequency. (Some **balancing authorities** may choose to apply corrections to their **net actual interchange** values to account for factors such as nonconforming loads.) *FRS Form 1* and *FRS Form 2* show the types of adjustments that are allowed. Note that with the exception of the contingent **balancing authority** column, any adjustments made must be made for all events in an evaluation year. As an example, if an entity has non-conforming loads and makes an adjustment for one event, all events must show the nonconforming load, even if the non-conforming load does not impact the calculation. This ensures that the reports are not utilizing the adjustments only when they are favorable to the **balancing authority**. The Electric Reliability Organization will use a standardized sampling interval of approximately 16 seconds before the event up to the time of the event for the pre-event **net actual interchange**, and frequency (A values) and approximately 20 to 52 seconds after the event for the post-event **net actual interchange** (B values) in the computation of **frequency response** measure values, dependent on the data scan rate of the **balancing authority**’s Energy Management System.

All events listed on *FRS Form 1* need to be included in the annual submission of *FRS Form 1* and *FRS Form 2*. The only time a **balancing authority** should exclude an event is if its **intertie** data or its frequency data is corrupt or its Energy Management System was unavailable. *FRS Form 2* has instructions on how to correct the **balancing authority**’s data if the given event is internal to the **balancing authority** or if other authorized adjustments are used.

Assuming data entry is correct, *FRS Form 1* will automatically calculate the **frequency response** measure of the **balancing authority** for the past 12 **months** as the median of the **frequency response** measure values. A **balancing authority** electing to report as an **frequency response** sharing group or a provider of overlap regulation service will provide an *FRS Form 1* for the aggregate of its participants.

To allow a **balancing authority** to plan its operations, events with a “Point C” that cause the **Interconnection** frequency to be lower than that shown in Table 1 above or higher than an equal change in frequency going above 60 Hz may be included in the list of events for that **Interconnection**. However, the calculation of the **balancing authority** response to such an event will be adjusted to show a frequency change only to the target minimum frequency shown in Table 1 above or a high frequency amount of an equal quantity. Should such an event happen, the Electric Reliability Organization will provide additional guidance.

# Alberta Reliability Standard
# Automatic Time Error Correction
# BAL-004-WECC-AB-2

## 1. Purpose

The purpose of this **reliability standard** is to maintain the frequency of the **western interconnection** and to ensure that **time error corrections** and **primary inadvertent interchange** payback are effectively conducted in a manner that does not adversely affect the **reliability** of the **western interconnection**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** Following the conclusion of each **month**, the **ISO** must verify that the absolute value of its accumulated **primary inadvertent interchange** for both the monthly **on peak** period and the monthly **off peak** period are each individually less than or equal to 150% of the previous calendar year's peak demand, where peak demand is the highest hourly integrated **net energy for load**.

**R2** The **ISO** must, within ninety (90) days of discovery of an error in the calculation of hourly **primary inadvertent interchange**, recalculate the value of hourly **primary inadvertent interchange** and adjust the accumulated **primary inadvertent interchange** from the time of the error.

**R3** The **ISO** must, while synchronously connected to the **western interconnection**, keep its **automatic time error correction** in service, with an allowable exception period of less than or equal to an accumulated twenty-four (24) hours per calendar quarter for **automatic time error correction** to be out of service.

**R3.1** Notwithstanding requirement R3, the **ISO** may disable automatic **time error correction** if there is a **reliability** concern on the **interconnected electric system** while executing an automatic **time error correction**, and this time will not be included as part of the allowable exception period.

**R4** The **ISO** must compute the following by fifty (50) minutes after each hour:

**R4.1** the hourly **primary inadvertent interchange**;

**R4.2** the accumulated **primary inadvertent interchange**; and

**R4.3** the **automatic time error correction** term.

**R5** The **ISO** must be able to change its **automatic generation control** operating mode between flat frequency, flat tie line, tie line bias, and tie line bias plus **time error** control, to correspond to current operating conditions.

**R6** The **ISO** must recalculate the hourly **primary inadvertent interchange** and accumulated **primary inadvertent interchange** for the **on peak** and **off peak** periods whenever adjustments are made to hourly **inadvertent interchange** or the hourly change in system **time error**, as distributed by the **Interconnection** time monitor.

**R7** The **ISO** must make the same adjustment to the accumulated **primary inadvertent interchange** as it did for any **month**-end meter reading adjustments to **inadvertent interchange**.

**R8** The **ISO** must payback **inadvertent interchange** using **automatic time error correction** rather than bilateral and unilateral payback.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of verifying the absolute value of the **ISO**'s accumulated **primary inadvertent interchange** as required in requirement R1 exists. Evidence may include, but is not limited to, data, screen shots from the **WECC** Interchange Tool, production of data from any other databases, spreadsheets, displays, or other equivalent evidence.

**MR2** Evidence of recalculating the value of hourly **primary inadvertent interchange** and adjusting the accumulated **primary inadvertent interchange** from the time of the error as required in requirement R2 exists. Evidence may include, but is not limited to, data, screen shots from the **WECC** Interchange Tool, production data from any other databases, spreadsheets, displays, or other equivalent evidence.

**MR3** Evidence of keeping the **automatic time error correction** in service as required in requirement R3 exists. Evidence may include, but is not limited to, dated archived files, historical data, or other equivalent evidence.

**MR4** Evidence of computing the hourly **primary inadvertent interchange**, accumulated **primary inadvertent interchange** and **automatic time error correction** as required in requirement R4 exists. Evidence may include, but is not limited to, data, screen shots from the **WECC** Interchange Tool, data from any other databases, spreadsheets, displays, or other equivalent evidence.

**MR5** Evidence of having the ability to change the **automatic generation control** operating mode as required in requirement R5 exists. Evidence may include, but is not limited to, snapshots of the operating interface provided in the energy management system for changing its **automatic generation control** operating mode, or other equivalent evidence.

**MR6** Evidence of recalculating hourly **primary inadvertent interchange** and accumulated **primary inadvertent interchange** as required in requirement R6 exists. Evidence may include, but is not limited to, data, screen shots from the **WECC** Interchange Tool, data from any other databases, spreadsheets, displays, or other equivalent evidence.

**MR7** Evidence of making the adjustments to accumulated **primary inadvertent interchange** as required in requirement R7 exists. Evidence may include, but is not limited to, data, screen shots of the **WECC** Interchange Tool, data from any other databases, spreadsheets, displays, or other equivalent evidence.

**MR8** Evidence of paying back the **inadvertent interchange** as required in requirement R8 exists. Evidence may include, but is not limited to, historical **inadvertent interchange** data, data from the **WECC** Interchange Tool, or other equivalent evidence.

## Revision History

| Date | Description |
|---|---|
| 2016-12-19 | Initial release. |

# Alberta Reliability Standard
# Balancing Authority Control
# BAL-005-AB-1

## 1. Purpose

The purpose of this **reliability standard** is to establish requirements for acquiring data necessary to calculate **reporting area control error** and specify a minimum periodicity, accuracy, and availability requirement for acquisition of the data.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must use a design scan rate of no more than 9 seconds in acquiring data necessary to calculate **reporting area control error**.

**R2** Intentionally left blank.

**R3** The **ISO** must use frequency metering equipment for the calculation of **reporting area control error**:

**R3.1** that is available a minimum of 99.95% for each calendar year; and

**R3.2** with a minimum accuracy of 0.001 Hz.

**R4** The **ISO** must make available to its operating personnel information associated with **reporting area control error** including quality flags indicating missing or invalid data.

**R5** The **ISO** must ensure the system it uses to calculate **reporting area control error** is available a minimum of 99.5% of each calendar year.

**R6** The **ISO** must implement an operating process to identify and mitigate errors affecting the accuracy of scan rate data used in the calculation of **reporting area control error** for its **balancing authority area**.

**R7** The **ISO** must ensure that each **interconnection**, pseudo-tie, and dynamic schedule with an **adjacent balancing authority** is equipped with:

**R7.1** a common source to provide information to both the **ISO** and the **adjacent balancing authority** for the scan rate values used in the calculation of **reporting area control error**; and,

**R7.2** a time synchronized common source to determine hourly MWh values agreed-upon to aid in the identification and mitigation of errors.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of using a design scan rate as required in requirement R1 exists. Evidence may include data files, database, spreadsheets, system logs, display information, other data, or other equivalent evidence.

**MR2** Intentionally left blank.

**MR3** Evidence of using frequency metering equipment for the calculation of **reporting area control error** as required in requirement R3 exists. Evidence may include dated documents, data files, database, system logs, other data, or other equivalent evidence.

**MR4** Evidence of making available information associated with **reporting area control error** as required in requirement R4 exists. Evidence may include graphical display or dated alarm log that provides indication of data validity for the real-time **reporting area control error** based on both the calculated result and all of the associated inputs, or other equivalent evidence.

**MR5** Evidence of ensuring the system used to calculate **reporting area control error** was available as required in requirement R5 exists. Evidence may include data files, database, system logs, other data, or other equivalent evidence.

**MR6** Evidence of implementing an operating process as required in requirement R6 exists. Evidence may include evidence that shows the operating process was implemented, such as dated communications, incorporation in operator task verification, or other equivalent evidence.

**MR7** Evidence of ensuring that each **interconnection**, pseudo-tie and dynamic schedule with an adjacent **balancing authority** is equipped with a common source as required in requirement R7 exists. Evidence may include technical documentation, electronic communications, or other equivalent evidence.

### Revision History

| Date | Description |
|---|---|
| 2019-07-01 | Initial release. |

# Alberta Reliability Standard
# Cyber Security – Supplemental CIP Alberta Reliability Standard
# CIP-SUPP-001-AB1

## A. Introduction

1. Title: Cyber Security – Supplemental CIP Alberta Reliability Standard
2. Number: CIP-SUPP-001-AB1
3. Purpose: The purpose of this **reliability standard** is to allow the **ISO** to approve variances to the requirements of a CIP Cyber Security **reliability standard**, other than **technical feasibility exceptions**.
4. Applicability:

   This **reliability standard** applies to those Responsible Entities listed in CIP-002-AB-5.1, *Cyber Security – BES Cyber System Categorization*, section 4, Applicability.

## B. Requirements and Measures

**R1** A Responsible Entity, other than the **ISO**, must, where it seeks a variance to the requirements of a CIP Cyber Security **reliability standard**, make a request in writing to the **ISO** outlining (i) the requirements of the particular CIP Cyber Security **reliability standard** in respect of which the variance is sought; (ii) the grounds in support of the requested variance, which grounds must not be frivolous or of little merit; and (iii) the requested effective dates of the variance.

**M1** Evidence of a request for a variance being made in writing as required in requirement R1 exists. Evidence may include, but is not limited to, a hard copy or electronic copy of the request.

**R2** The **ISO** and the Responsible Entity must treat a request for a variance under requirement R1, all records related to such a request, and a variance approved under requirement R3, as confidential in accordance with the provisions of section 103.1 of the ISO rules, *Confidentiality*, provided however that where the request for a variance is made by a Responsible Entity whose rights and obligations are the subject of a power purchase arrangement that Responsible Entity may disclose to its counterparties such information in respect of the variance as and if required under the terms of the power purchase arrangement.

**R2.1** Where the **ISO** determines that the disclosure of a request for a variance under requirement R1, all records related to such a request, or a variance approved under requirement R3:

(a) would have no material impact on the **reliability** of the interconnected electric system; and

(b) does not contain information which, in the opinion of the **ISO**, is commercially sensitive,

requirement R2 of this standard does not apply and the **ISO** may publicly disclose the request and all records related to the request in accordance with subsection 2(6)(b)(i) of section 103.1 of the **ISO rules**.

**M2** Evidence of treating the request as confidential as described in requirement R2 exists, unless requirement R2.1 applies.

**R3** The **ISO** must, where it approves a variance requested under requirement R1:

(a) indicate the effective dates of the variance;

(b) identify the Responsible Entity to which the variance applies;

(c) maintain a copy of the variance, in writing; and

(d) provide a copy of the variance, in writing, to the Responsible Entity that has requested the variance.

**M3** Evidence of taking the steps required in requirement R3 exists. Evidence may include, but is not limited to, a written copy of the variance including its effective dates, correspondence to the Responsible Entity enclosing a copy of the variance or other equivalent evidence.

**R4** The **ISO** must not, in any event, approve a variance requested under requirement R1 unless the **ISO** determines, by its own assessment, that the variance has merit and will not have a material impact on the **reliability** of the **interconnected electric system**.

**M4** Evidence of performing an assessment in accordance with requirement R4 exists. Evidence may include, but is not limited to, a copy of the **ISO**’s business practices relating to variances of a CIP Cyber Security **reliability standard**.

**R5** The **ISO** must, where it does not approve a variance requested under requirement R1, provide a copy of its decision, including reasons, in writing, to the Responsible Entity that has requested the variance.

**M5** Evidence of issuing a decision denying the variance requested exists. Evidence may include, but is not limited to, a hard copy or electronic copy of a letter from the **ISO** denying the variance requested.

**R6** Notwithstanding any of the requirements of this **reliability standard**, a Responsible Entity must make a request for a **technical feasibility exception** in accordance with the provisions of CIP-SUPP-002-AB, *Technical Feasibility Exceptions*.

**M6** Evidence of requesting a **technical feasibility exception** as required in requirement R6 exists. Evidence may include, but is not limited to, a hard copy or electronic copy of the request, or other equivalent evidence.

## Revision History

| Date | Description |
|---|---|
| 2017-03-21 | Addition of requirement R6 and associated measure.<br>Revision to purpose statement. |
| 2015-06-05 | Initial release. |

# Alberta Reliability Standard
# Cyber Security – Supplemental CIP Alberta Reliability Standard Technical Feasibility Exceptions
# CIP-SUPP-002-AB

## A. Introduction

1. Title: Cyber Security – Supplemental CIP Alberta Reliability Standard Technical Feasibility Exceptions
2. Number: CIP-SUPP-002-AB
3. Purpose: The purpose of this **reliability standard** is to allow the **ISO** to approve **technical feasibility exceptions** to the requirements of a CIP Cyber Security **reliability standard**.
4. Applicability:

   This **reliability standard** applies to those Responsible Entities listed in CIP-002-AB-5.1, *Cyber Security – BES Cyber System Categorization,* section 4, Applicability.

## B. Requirements and Measures

**R1** A Responsible Entity other than the **ISO** must, where:

(a) a requirement in the CIP Cyber Security **reliability standards** uses the phrase "where technically feasible"; and

(b) the Responsible Entity seeks a variance from the requirement referenced in sub-requirement R1(a) on the grounds of technical feasibility,

request that the **ISO** approve a **technical feasibility exception**.

**MR1** Evidence of a request for a **technical feasibility exception** as required in requirement R1 exists. Evidence may include, but is not limited to, a hard copy or electronic copy of the request, or other equivalent evidence.

**R2** A Responsible Entity must make a request under requirement R1 in writing in the form specified by the **ISO**.

**MR2** Evidence of making a request in writing as described in requirement R1 exists. Evidence may include, but is not limited to, a hard copy or electronic copy of the request, or other equivalent evidence.

**R3** At the **ISO**'s request, a Responsible Entity must provide:

(a) any additional information relating to a request for a **technical feasibility exception**; or

(b) the reasons why the additional information will not be provided.

**MR3** Evidence of providing additional information or reasons in accordance with requirement R3 exists. Evidence may include, but is not limited to, a hard copy or electronic copy of the request and the response, or other equivalent evidence.

**R4** The **ISO** and the Responsible Entity must treat a request for a **technical feasibility exception** under requirement R1, and all records related to such a request, as confidential in accordance with the provisions of section 103.1 of the ISO rules, *Confidentiality*, provided however that where the request for a **technical feasibility exception** is made by a Responsible Entity whose rights and obligations are the subject of a power purchase arrangement, that Responsible Entity may disclose to its counterparties such information in respect of the **technical feasibility exception** as and if required under the terms of the power purchase arrangement.

**MR4** Evidence of treating the request as confidential as described in requirement R4 exists.

**R5** The **ISO** must post the criteria that it considers when determining whether to approve or disapprove a request for a **technical feasibility exception** on the AESO website, and must notify Responsible Entities at least thirty (30) **days** in advance of any amendments to the criteria.

**MR5** Evidence of posting the criteria and notifying Responsible Entities as described in requirement R5 exists. Evidence may include, but is not limited to, a dated copy of the AESO website posting and a dated posting in the AESO stakeholder newsletter.

**R6** The **ISO** must, upon reviewing a Responsible Entity's request submitted under requirement R1 and any additional information provided to the **ISO**, approve the request in whole or in part, or disapprove the request.

**R6.1** The **ISO** must, where the request submitted under requirement R1 is approved, provide a copy of its decision, in writing, to the Responsible Entity that has requested the **technical feasibility exception** and set out:

(a) any terms and conditions of the approval; and

(b) the expiration date of the approval.

**R6.2** The **ISO** must, where the request submitted under requirement R1 is disapproved, provide a copy of its decision, including reasons, in writing, to the Responsible Entity that has requested the **technical feasibility exception**.

**MR6** Evidence of an approval or disapproval of the request as described in requirement R6 exists. Evidence may include but is not limited to a dated copy of the approval or disapproval.

**R7** A Responsible Entity must, where there is a material change in the facts underlying the request for or approval of a **technical feasibility exception**, submit a revised request to the **ISO** under requirement R2 within sixty (60) **days** of becoming aware of the material change.

**MR7** Evidence of submitting a revised request to the **ISO** in accordance with requirement R7 exists. Evidence may include, but is not limited to, a dated record of becoming aware of a material change in facts and a dated hard copy or electronic copy of the revised request, or other equivalent evidence.

**R8** The **ISO** may, after providing written notice to the Responsible Entity, amend or terminate a **technical feasibility exception** prior to the expiration date of the **technical feasibility exception** where:

(a) a Responsible Entity does not fulfill the terms and conditions of the approval;

(b) there is a material change in the facts underlying the approval; or

(c) the Responsible Entity advises the **ISO**, in writing, that the **technical feasibility exception** is no longer required.

**MR8** Evidence of amending or terminating a **technical feasibility exception** and providing notice prior to the expiration date of the approval as described in requirement R8 exists. Evidence may include, but is not limited to, a dated hard copy or electronic copy of the amended or terminated **technical feasibility exception** provided to the Responsible Entity.

## Revision History

| Date | Description |
|---|---|
| 2017-03-21 | Initial release. |

# Alberta Reliability Standard
# Cyber Security – BES Cyber System Categorization
# CIP-002-AB-5.1

## A. Introduction

1. Title: Cyber Security – BES Cyber System Categorization
2. Number: CIP-002-AB-5.1
3. Purpose: To identify and categorize **BES cyber systems** and their associated **BES cyber assets** for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those **BES cyber systems** could have on the reliable operation of the **bulk electric system**. Identification and categorization of **BES cyber systems** support appropriate protection against compromises that could lead to misoperation or instability in the **bulk electric system**.
4. Applicability:

4.1. For the purpose of the requirements contained herein, the following list of entities will be collectively referred to as "Responsible Entities". For requirements in this **reliability standard** where a specific entity or subset of entities are the applicable entity or entities, the entity or entities are specified explicitly.

4.1.1. [Intentionally left blank.]

4.1.2. a **legal owner** of an **electric distribution system** that owns one or more of the following facilities, systems, and equipment for the protection or restoration of the **bulk electric system**:

4.1.2.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.1.2.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.1.2.1.2. performs automatic load shedding under a common control system owned by the entity in subsection 4.1.2., without human operator initiation, of 300 MW or more;

4.1.2.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.1.2.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.1.2.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.1.3. the **operator** of a **generating unit** and the **operator** of an **aggregated generating facility**;

4.1.4. the **legal owner** of a **generating unit** and the **legal owner** of an **aggregated generating facility**;

4.1.5. [Intentionally left blank.]

4.1.6. [Intentionally left blank.]

4.1.7. the **operator** of a **transmission facility**;

4.1.8. the **legal owner** of a **transmission facility**; and

4.1.9. the **ISO**.

4.2. For the purpose of the requirements contained herein, the following facilities, systems, and equipment owned by each Responsible Entity in subsection 4.1 above are those to which these requirements are applicable. For requirements in this **reliability standard** where a specific type of facilities, system, or equipment or subset of facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. One or more of the following facilities, systems and equipment that operate at, or control elements that operate at, a nominal voltage of 25 kV or less and are owned by a **legal owner** of an **electric distribution system** or a **legal owner** of a **transmission facility** for the protection or restoration of the **bulk electric system**:

4.2.1.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.2.1.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.2.1.1.2. performs automatic load shedding under a common control system owned by one or more of the entities in subsection 4.2.1, without human operator initiation, of 300 MW or more;

4.2.1.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.2.1.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.2.1.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.2.2. Responsible Entities listed in subsection 4.1 other than a **legal owner** of an **electric distribution system** are responsible for:

4.2.2.1. each **transmission facility** that is part of the **bulk electric system** except each **transmission facility** that:

4.2.2.1.1. is a transformer with fewer than 2 windings at 100 kV or higher and does not connect a contracted **blackstart resource**;

4.2.2.1.2. radially connects only to load;

4.2.2.1.3. radially connects only to one or more **generating units** or **aggregated generating facilities** with a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**; or

4.2.2.1.4. radially connects to load and one or more **generating units** or **aggregated generating facilities** that have a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**;

4.2.2.2. a **reactive power** resource that is dedicated to supplying or absorbing **reactive power** that is connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, except those **reactive power** resources operated by an end-use customer for its own use;

4.2.2.3. a **generating unit** that is:

4.2.2.3.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW unless the **generating unit** is part of an industrial complex;

4.2.2.3.2. within a power plant which:

4.2.2.3.2.1. is not part of an **aggregated generating facility**;

4.2.2.3.2.2. is directly connected to the **bulk electric system**; and

4.2.2.3.2.3. has a combined **maximum authorized real power** rating greater than 67.5 MW unless the power plant is part of an industrial complex;

4.2.2.3.3. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.3.4. a contracted **blackstart resource**;

4.2.2.4. an **aggregated generating facility** that is:

4.2.2.4.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW unless the **aggregated generating facility** is part of an industrial complex;

4.2.2.4.2. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.4.3. a contracted **blackstart resource**;

and

4.2.2.5. **control centres** and backup **control centres**.

4.2.3. The following are exempt from this **reliability standard**:

4.2.3.1. [Intentionally left blank.]

4.2.3.2. **cyber assets** associated with communication networks and data communication links between discrete **electronic security perimeters**.

4.2.3.3. [Intentionally left blank.]

4.2.3.4. for the **legal owner** of an **electric distribution system**, the systems and equipment that are not included in subsection 4.2.1 above.

5. [Intentionally left blank.]

6. [Intentionally left blank.]

## B. Requirements and Measures

**R1.** Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

(i) **control centres** and backup **control centres**;

(ii) transmission stations and substations;

(iii) **generating units** and **aggregated generating facilities**;

(iv) systems and facilities critical to system restoration, including contracted **blackstart resources** and **cranking paths** and initial switching requirements;

(v) **remedial action schemes** that support the reliable operation of the **bulk electric system**; and

(vi) for the **legal owner** of an **electric distribution system** or **legal owner** of a **transmission facility**, **protection systems** specified in Applicability subsection 4.2.1 above.

**1.1.** Identify each of the high impact **BES cyber systems** according to Attachment 1, Section 1, if any, at each asset;

**1.2.** Identify each of the medium impact **BES cyber systems** according to Attachment 1, Section 2, if any, at each asset; and

**1.3.** Identify each asset that contains a low impact **BES cyber system** according to Attachment 1, Section 3, if any (a discrete list of low impact **BES cyber systems** is not required).

**M1.** Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by requirement R1, and Parts 1.1 and 1.2.

**R2.** The Responsible Entity shall:

**2.1.** review the identifications in requirement R1 and its parts (and update them if there are changes identified) at least once every 15 **months**, even if it has no identified items in requirement R1, and

**2.2.** have its **CIP senior manager** or delegate approve the identifications required by requirement R1 at least once every 15 **months**, even if it has no identified items in requirement R1.

**M2.** Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in requirement R1 and its parts, and has had its **CIP senior manager** or delegate approve the identifications required in requirement R1 and its parts at least once every 15 **months**, even if it has none identified in requirement R1 and its parts, as required by requirement R2.

### Attachments

Attachment 1 – *Impact Rating Criteria*

### Revision History

| Date | Description |
|---|---|
| 2017-10-01 | Initial release. |

## CIP-002-AB-5.1 Attachment 1

### Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

### 1. High Impact Rating (H)

Each **BES cyber system** used by and located at any of the following:

1.1. the **ISO**'s **control centre** and backup **control centre**;

1.2. [Intentionally left blank.]

1.3. each **control centre** or backup **control centre** used to perform the functional obligations of an **operator** of a **transmission facility** for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.8, 2.9, or 2.10; and

1.4. each **control centre** or backup **control centre** used to perform the functional obligations of the **operator** of a **generating unit** or the **operator** of an **aggregated generating facility** for one or more of the assets that meet criterion 2.1, 2.3, 2.6, 2.8, or 2.9.

### 2. Medium Impact Rating (M)

Each **BES cyber system**, not included in Section 1 above, associated with any of the following:

2.1. commissioned generation, by each group of **generating units** or **aggregated generating facilities** at a single plant location, with an aggregate **maximum authorized real power** rating of each of the generating units minus the station service load equal to or exceeding 1500 MW in a single **Interconnection**. For each group of **generating units** or **aggregated generating facilities**, the only **BES cyber systems** that meet this criterion are those shared **BES cyber systems** that could, within 15 minutes, adversely impact the reliable operation of any combination of **generating units** and/or **aggregated generating facilities** that in aggregate equal or exceed 1500 MW in a single **Interconnection**;

2.2. each **bulk electric system** reactive resource or group of resources at a single location (excluding **generating units** and **aggregated generating facilities**) with an aggregate maximum **reactive power** nameplate rating of 1000 MVAR or greater(excluding those at generating units or aggregated generating facilities). The only **BES cyber systems** that meet this criterion are those shared **BES cyber systems** that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR;

2.3. each **generating unit** and **aggregated generating facility** that the **ISO** designates, and informs the **legal owner** of the **generating unit** or **legal owner** of the **aggregated generating facility**, as necessary to avoid an **adverse reliability impact** in the planning horizon of more than one year;

2.4. **transmission facilities** operated at 500 kV or higher;

2.5. **transmission facilities** that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing **bulk electric system** transmission line that is connected to another transmission station or substation;

| Voltage Value of a Line | Weight Value per Line |
|---|---|
| Less than 200 kV (not applicable) | (not applicable) |
| 200 kV to 299 kV | 700 |
| 300 kV to 499 kV | 1300 |
| 500 kV and above | 0 |

2.6. **generating units** at a single plant location, **aggregated generating facilities** or **transmission facilities** at a single station or substation location that are identified by the **ISO** as critical to the derivation of **interconnection reliability operating limits** and their associated contingencies;

2.7. [Intentionally left blank.]

2.8. **transmission facilities** and switchyards associated with **generating units** or **aggregated generating facilities** that connect the generator output to the **transmission system** that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of a **generating unit** or an **aggregated generating facility** identified by any **legal owner** of a **generating unit** or any **legal owner** of an **aggregated generating facility** as a result of its application of Attachment 1, criterion 2.1 or 2.3;

2.9. each **remedial action scheme**, or automated switching system that operates **system element(s)** of the **bulk electric system**, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more **interconnection reliability operating limits** (**IROLs**) violations for failure to operate as designed or cause a reduction in one or more **IROLs** if destroyed, degraded, misused, or otherwise rendered unavailable;

2.10. each system or group of element(s) that performs automatic load shedding under a common control system, without human operator initiation, of 300 MW or more implementing **under voltage load shed** or **underfrequency load shedding** under a load shedding program that is subject to one or more requirements in a **reliability standard;**

2.11. each **control centre** or backup **control centre**, not already included in High Impact Rating (H) above, used to perform the functional obligations of the **operator** of a **generating unit** or the **operator** of an **aggregated generating facility** for an aggregate highest rated net **real power** capability of the preceding 12 **months** equal to or exceeding 1500 MW; and

2.12. each **control centre** or backup **control centre** used to perform the functional obligations of the **operator** of a **transmission facility** not included in High Impact Rating (H), above, with the exception of the **operator** of a transmission facility whose only transmission facility is a radial connection from either a **generating unit**, **aggregated generating facility** or industrial complex to either the **transmission system** or to **transmission facilities** within the City of Medicine Hat.

2.13. [Intentionally left blank.]

### 3. Low Impact Rating (L)

**BES cyber systems** not included in sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in subsection 4.2 of this **reliability standard**:

3.1. **control centres** and backup **control centres;**

3.2. transmission stations and substations;

3.3. **generating units** and **aggregated generating facilities**;

3.4. systems and facilities critical to system restoration, including contracted **blackstart resources** and **cranking paths** and initial switching requirements;

3.5 **remedial action schemes** that support the reliable operation of the **bulk electric system**; and

3.6. for a **legal owner** of an **electric distribution system** or **legal owner** of a **transmission facility**, **protection systems** specified in subsection 4.2.1 of this **reliability standard**.

# Alberta Reliability Standard
# Cyber Security – Security Management Controls
# CIP-003-AB-5

## A. Introduction

1. Title: Cyber Security – Security Management Controls
2. Number: CIP-003-AB-5
3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect **BES cyber systems** against compromise that could lead to misoperation or instability in the **bulk electric system**.
4. Applicability:

4.1. For the purpose of the requirements contained herein, the following list of entities will be collectively referred to as “Responsible Entities”. For requirements in this **reliability standard** where a specific entity or subset of entities are the applicable entity or entities, the entity or entities are specified explicitly.

4.1.1. [Intentionally left blank.]

4.1.2. a **legal owner** of an **electric distribution system** that owns one or more of the following facilities, systems, and equipment for the protection or restoration of the **bulk electric system**:

4.1.2.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.1.2.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.1.2.1.2. performs automatic load shedding under a common control system owned by the entity in subsection 4.1.2., without human operator initiation, of 300 MW or more;

4.1.2.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.1.2.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.1.2.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.1.3. the **operator** of a **generating unit** and the **operator** of an **aggregated generating facility**;

4.1.4. the **legal owner** of a **generating unit** and the **legal owner** of an **aggregated generating facility**;

4.1.5. [Intentionally left blank.]

4.1.6. [Intentionally left blank.]

4.1.7. the **operator** of a **transmission facility**;

4.1.8. the **legal owner** of a **transmission facility**; and

4.1.9. the **ISO**.

4.2. For the purpose of the requirements contained herein, the following facilities, systems, and equipment owned by each Responsible Entity in subsection 4.1 above are those to which these requirements are applicable. For requirements in this **reliability standard** where a specific type of facilities, system, or equipment or subset of facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. One or more of the following facilities, systems and equipment that operate at, or control elements that operate at, a nominal voltage of 25 kV or less and are owned by a **legal owner** of an **electric distribution system** or a **legal owner** of a **transmission facility** for the protection or restoration of the **bulk electric system**:

4.2.1.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.2.1.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.2.1.1.2. performs automatic load shedding under a common control system owned by one or more of the entities in subsection 4.2.1, without human operator initiation, of 300 MW or more;

4.2.1.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.2.1.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.2.1.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.2.2. Responsible Entities listed in subsection 4.1 other than a **legal owner** of an **electric distribution system** are responsible for:

4.2.2.1. each **transmission facility** that is part of the **bulk electric system** except each **transmission facility** that:

4.2.2.1.1. is a transformer with fewer than 2 windings at 100 kV or higher and does not connect a contracted **blackstart resource**;

4.2.2.1.2. radially connects only to load;

4.2.2.1.3. radially connects only to one or more **generating units** or **aggregated generating facilities** with a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**; or

4.2.2.1.4. radially connects to load and one or more **generating units** or **aggregated generating facilities** that have a combined **maximum authorized real power**

of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**;

4.2.2.2. a **reactive power** resource that is dedicated to supplying or absorbing **reactive power** that is connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, except those **reactive power** resources operated by an end-use customer for its own use;

4.2.2.3. a **generating unit** that is:

4.2.2.3.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW unless the **generating unit** is part of an industrial complex;

4.2.2.3.2. within a power plant which:

4.2.2.3.2.1. is not part of an **aggregated generating facility**;

4.2.2.3.2.2. is directly connected to the **bulk electric system**; and

4.2.2.3.2.3. has a combined **maximum authorized real power** rating greater than 67.5 MW unless the power plant is part of an industrial complex;

4.2.2.3.3. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.3.4. a contracted **blackstart resource**;

4.2.2.4. an **aggregated generating facility** that is:

4.2.2.4.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW unless the **aggregated generating facility** is part of an industrial complex;

4.2.2.4.2. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.4.3. a contracted **blackstart resource**;

and

4.2.2.5. **control centres** and backup **control centres**.

4.2.3. The following are exempt from this **reliability standard**:

4.2.3.1. [Intentionally left blank.]

4.2.3.2. **cyber assets** associated with communication networks and data communication links between discrete **electronic security perimeters**.

4.2.3.3. [Intentionally left blank.]

4.2.3.4. for the **legal owner** of an **electric distribution system**, the systems and equipment that are not included in subsection 4.2.1 above.

5. [Intentionally left blank.]

6. [Intentionally left blank.]

## B. Requirements and Measures

**R1.** Each Responsible Entity, for its High Impact and Medium Impact **BES cyber systems**, shall review and obtain **CIP senior manager** approval at least once every 15 **months** for one or more documented cyber security policies that collectively address the following topics:

**1.1** Personnel & training (CIP-004-AB-5.1);

**1.2 Electronic security perimeters** (CIP-005-AB-5) including **interactive remote access**;

**1.3** Physical security of **BES cyber systems** (CIP-006-AB-5);

**1.4** System security management (CIP-007-AB-5);

**1.5** Incident reporting and response planning (CIP-008-AB-5);

**1.6** Recovery plans for **BES cyber systems** (CIP-009-AB-5);

**1.7** Configuration change management and vulnerability assessments (CIP-010-AB-1);

**1.8** Information protection (CIP-011-AB-1); and

**1.9** Declaring and responding to **CIP exceptional circumstances**.

**M1.** Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 **months**; and documented approval by the **CIP senior manager** for each cyber security policy.

**R2.** Each Responsible Entity for its assets identified in CIP-002-AB-5.1, requirement R1, part 1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain **CIP senior manager** approval for those policies at least once every 15 **months**:

**2.1** Cyber security awareness;

**2.2** Physical security controls;

**2.3** Electronic access controls for external routable protocol connections and **dial-up connectivity**; and

**2.4** Incident response to a **cyber security incident**.

An inventory, list, or discrete identification of Low Impact **BES cyber systems** or their **BES cyber assets** is not required.

**M2.** Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 **months**; and documented approval by the **CIP senior manager** for each cyber security policy.

**R3.** Each Responsible Entity shall identify a **CIP senior manager** by name and document any change within 30 **days** of the change.

**M3.** An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the **CIP senior manager**.

**R4.** The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP **reliability standards**, the **CIP senior manager** may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the **CIP senior manager**; and updated within 30 **days** of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.

**M4.** An example of evidence may include, but is not limited to, a dated document, approved by the **CIP senior manager**, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

## Revision History

| Date | Description |
|---|---|
| 2017-10-01 | Initial release. |

# Alberta Reliability Standard
# Cyber Security – Personnel & Training
# CIP-004-AB-5.1

## A. Introduction

1. Title: Cyber Security – Personnel & Training
2. Number: CIP-004-AB-5.1
3. Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the **bulk electric system** from individuals accessing **BES cyber systems** by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting **BES cyber systems.**
4. Applicability:

4.1. For the purpose of the requirements contained herein, the following list of entities will be collectively referred to as "Responsible Entities". For requirements in this **reliability standard** where a specific entity or subset of entities are the applicable entity or entities, the entity or entities are specified explicitly.

4.1.1. [Intentionally left blank.]

4.1.2. a **legal owner** of an **electric distribution system** that owns one or more of the following facilities, systems, and equipment for the protection or restoration of the **bulk electric system**:

4.1.2.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.1.2.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.1.2.1.2. performs automatic load shedding under a common control system owned by the entity in subsection 4.1.2., without human operator initiation, of 300 MW or more;

4.1.2.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.1.2.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.1.2.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.1.3. the **operator** of a **generating unit** and the **operator** of an **aggregated generating facility**;

4.1.4. the **legal owner** of a **generating unit** and the **legal owner** of an **aggregated generating facility**;

4.1.5. [Intentionally left blank.]

4.1.6. [Intentionally left blank.]

4.1.7. the **operator** of a **transmission facility**;

4.1.8. the **legal owner** of a **transmission facility**; and

4.1.9. the **ISO**.

4.2. For the purpose of the requirements contained herein, the following facilities, systems, and equipment owned by each Responsible Entity in subsection 4.1 above are those to which these requirements are applicable. For requirements in this **reliability standard** where a specific type of facilities, system, or equipment or subset of facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. One or more of the following facilities, systems and equipment that operate at, or control elements that operate at, a nominal voltage of 25 kV or less and are owned by a **legal owner** of an **electric distribution system** or a **legal owner** of a **transmission facility** for the protection or restoration of the **bulk electric system**:

4.2.1.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.2.1.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.2.1.1.2. performs automatic load shedding under a common control system owned by one or more of the entities in subsection 4.2.1, without human operator initiation, of 300 MW or more;

4.2.1.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.2.1.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.2.1.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.2.2. Responsible Entities listed in subsection 4.1 other than a **legal owner** of an **electric distribution system** are responsible for:

4.2.2.1. each **transmission facility** that is part of the **bulk electric system** except each **transmission facility** that:

4.2.2.1.1. is a transformer with fewer than 2 windings at 100 kV or higher and does not connect a contracted **blackstart resource**;

4.2.2.1.2. radially connects only to load;

4.2.2.1.3. radially connects only to one or more **generating units** or **aggregated generating facilities** with a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**; or

4.2.2.1.4. radially connects to load and one or more **generating units** or **aggregated**

**generating facilities** that have a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**;

4.2.2.2. a **reactive power** resource that is dedicated to supplying or absorbing **reactive power** that is connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, except those **reactive power** resources operated by an end-use customer for its own use;

4.2.2.3. a **generating unit** that is:

4.2.2.3.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW unless the **generating unit** is part of an industrial complex;

4.2.2.3.2. within a power plant which:

4.2.2.3.2.1. is not part of an **aggregated generating facility**;

4.2.2.3.2.2. is directly connected to the **bulk electric system**; and

4.2.2.3.2.3. has a combined **maximum authorized real power** rating greater than 67.5 MW unless the power plant is part of an industrial complex;

4.2.2.3.3. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.3.4. a contracted **blackstart resource**;

4.2.2.4. an **aggregated generating facility** that is:

4.2.2.4.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW unless the **aggregated generating facility** is part of an industrial complex;

4.2.2.4.2. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.4.3. a contracted **blackstart resource**;

and

4.2.2.5. **control centres** and backup **control centres**.

4.2.3. The following are exempt from this **reliability standard**:

4.2.3.1. [Intentionally left blank.]

4.2.3.2. **cyber assets** associated with communication networks and data communication links between discrete **electronic security perimeters**.

4.2.3.3. [Intentionally left blank.]

4.2.3.4. for the **legal owner** of an **electric distribution system**, the systems and equipment that are not included in subsection 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no **BES cyber systems** categorized as High Impact or Medium Impact according to the CIP-002-AB-5.1 identification and categorization processes.

5. [Intentionally left blank.]

6. [Intentionally left blank.]

## B. Requirements and Measures

**R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R1 – Security Awareness Program.*

**M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-004-AB-5.1 Table R1 – Security Awareness Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.1 | High Impact **BES cyber systems**<br><br>Medium Impact **BES cyber systems** | Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to **BES cyber systems**. | An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as:<br><br>• direct communications (for example, e-mails, memos, computer-based training); or<br><br>• indirect communications (for example, posters, intranet, or brochures); or<br><br>• management support and reinforcement (for example, presentations or meetings). |

**R2.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-AB-*

*5.1 Table R2 – Cyber Security Training Program.*

**M2.** Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-AB-5.1 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

| CIP-004-AB-5.1 Table R2 – Cyber Security Training Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**. | Training content on:<br>2.1.1. cyber security policies;<br>2.1.2. physical access controls;<br>2.1.3. electronic access controls;<br>2.1.4. the visitor control program;<br>2.1.5. handling of **BES cyber system information** and its storage;<br>2.1.6. identification of a **cyber security incident** and initial notifications in accordance with the entity's incident response plan;<br>2.1.7. recovery plans for **BES cyber systems**;<br>2.1.8. response to **cyber security incidents**; and<br>2.1.9. cyber security risks associated with a **BES cyber system**'s electronic interconnectivity and interoperability with other **cyber assets**. | Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials. |
| 2.2 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and | Require completion of the training specified in part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable | Examples of evidence may include, but are not limited to, training records and documentation of when **CIP exceptional circumstances** were invoked. |

| CIP-004-AB-5.1 Table R2 – Cyber Security Training Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**. | **cyber assets**, except during **CIP exceptional circumstances**. | |
| 2.3 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**. | Require completion of the training specified in part 2.1 at least once every 15 **months**. | Examples of evidence may include, but are not limited to, dated individual training records. |

**R3.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to **BES Cyber Systems** that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R3 – Personnel Risk Assessment Program.*

**M3.** Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

| CIP-004-AB-5.1 Table R3 – Personnel Risk Assessment Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**. | Process to confirm identity. | An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity. |
| 3.2 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**. | Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:<br>3.2.1. current residence, regardless of duration; and<br>3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive **months** or more.<br>If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed. | An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check. |

| CIP-004-AB-5.1 Table R3 – Personnel Risk Assessment Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.3 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**. | Criteria or process to evaluate criminal history records checks for authorizing access. | An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks. |
| 3.4 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**. | Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to parts 3.1 through 3.3. | An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments. |
| 3.5 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and | Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk | An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals |

| CIP-004-AB-5.1 Table R3 – Personnel Risk Assessment Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**. | assessment completed according to parts 3.1 to 3.4 within the last seven years. | with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years. |

**R4.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R4 – Access Management Program.*

**M4.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

| CIP-004-AB-5.1 Table R4 – Access Management Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 4.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and | Process to authorize based on need, as determined by the Responsible Entity, except for **CIP exceptional circumstances**:<br>4.1.1. electronic access;<br>4.1.2. unescorted physical access into a **physical security perimeter**; and<br>4.1.3. access to designated storage locations, whether physical or electronic, for **BES cyber system information**. | An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a **physical security perimeter**, and access to designated storage locations, whether physical or electronic, for **BES cyber system information**. |

| CIP-004-AB-5.1 Table R4 – Access Management Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 2. **physical access control systems**. | | |
| 4.2 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**. | Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records. | Examples of evidence may include, but are not limited to:<br>• dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or<br>• dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing). |
| 4.3 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control** | For electronic access, verify at least once every 15 **months** that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary. | An example of evidence may include, but is not limited to, documentation of the review that includes all of the following:<br>1. a dated listing of all accounts/account groups or roles within the system;<br>2. a summary description of privileges associated with each group or role;<br>3. accounts assigned to the group or role; and<br>4. dated evidence showing verification of the privileges for the group are |

| CIP-004-AB-5.1 Table R4 – Access Management Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | **systems**. | | authorized and appropriate to the work function performed by people assigned to each account. |
| 4.4 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**. | Verify at least once every 15 **months** that access to the designated storage locations for **BES cyber system information**, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions. | An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following:<br>1. a dated listing of authorizations for **BES cyber system information**;<br>2. any privileges associated with the authorizations; and<br>3. dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions. |

**R5.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R5 – Access Revocation.*

**M5.** Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-004-AB-5.1 Table R5 – Access Revocation | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 5.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and | A process to initiate removal of an individual's ability for unescorted physical access and **interactive remote access** upon a termination action, and complete the | An example of evidence may include, but is not limited to, documentation of all of the following:<br>1. dated workflow or sign-off |

| CIP-004-AB-5.1 Table R5 – Access Revocation | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**. | removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights). | form verifying access removal associated with the termination action; and<br>2. logs or other demonstration showing such persons no longer have access. |
| 5.2 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**. | For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next **day** following the date that the Responsible Entity determines that the individual no longer requires retention of that access. | An example of evidence may include, but is not limited to, documentation of all of the following:<br>1. dated workflow or sign-off form showing a review of logical and physical access; and<br>2. logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary. |
| 5.3 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**.<br>Medium Impact **BES cyber systems** with **external routable connectivity** and | For termination actions, revoke the individual's access to the designated storage locations for **BES cyber system information**, whether physical or electronic (unless already revoked according to requirement R5.1), by the end of the next **day** following the effective date of the termination action. | An example of evidence may include, but is not limited to, workflow or signoff form verifying access removal to designated physical areas or cyber systems containing **BES cyber system information** associated with the terminations and dated within the next **day** of the termination action. |

| CIP-004-AB-5.1 Table R5 – Access Revocation | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | their associated:<br>1. **electronic access control and monitoring systems**; and<br>2. **physical access control systems**. | | |
| 5.4 | High Impact **BES cyber systems** and their associated:<br>• **electronic access control and monitoring systems**. | For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to parts 5.1 or 5.3) within 30 **days** of the effective date of the termination action. | An example of evidence may include, but is not limited to, workflow or signoff form showing access removal for any individual **BES cyber assets** and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions. |
| 5.5 | High Impact **BES cyber systems** and their associated:<br>• **electronic access control and monitoring systems**. | For termination actions, change passwords for shared account(s) known to the user within 30 **days** of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 **days** following the date that the Responsible Entity determines that the individual no longer requires retention of that access.<br>If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 **days** following the end of the operating circumstances. | Examples of evidence may include, but are not limited to:<br>• workflow or sign-off form showing password reset within 30 **days** of the termination;<br>• workflow or sign-off form showing password reset within 30 **days** of the reassignments or transfers; or<br>• documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 **days** following the end of the operating circumstance. |

## Revision History

| Date | Description |
| --- | --- |
| 2017-10-01 | Initial release. |

# Alberta Reliability Standard
# Cyber Security – Electronic Security Perimeter(s)
# CIP-005-AB-5

## A. Introduction

1. Title: Cyber Security – Electronic Security Perimeter(s)
2. Number: CIP-005-AB-5
3. Purpose: To manage electronic access to **BES cyber systems** by specifying a controlled **electronic security perimeter** in support of protecting **BES cyber systems** against compromise that could lead to misoperation or instability in the **bulk electric system**.
4. Applicability:

4.1. For the purpose of the requirements contained herein, the following list of entities will be collectively referred to as "Responsible Entities". For requirements in this **reliability standard** where a specific entity or subset of entities are the applicable entity or entities, the entity or entities are specified explicitly.

4.1.1. [Intentionally left blank.]

4.1.2. a **legal owner** of an **electric distribution system** that owns one or more of the following facilities, systems, and equipment for the protection or restoration of the **bulk electric system**:

4.1.2.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.1.2.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.1.2.1.2. performs automatic load shedding under a common control system owned by the entity in subsection 4.1.2., without human operator initiation, of 300 MW or more;

4.1.2.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.1.2.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.1.2.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.1.3. the **operator** of a **generating unit** and the **operator** of an **aggregated generating facility**;

4.1.4. the **legal owner** of a **generating unit** and the **legal owner** of an **aggregated generating facility**;

4.1.5. [Intentionally left blank.]

4.1.6. [Intentionally left blank.]

4.1.7. the **operator** of a **transmission facility**;

4.1.8. the **legal owner** of a **transmission facility**; and

4.1.9. the **ISO**.

4.2. For the purpose of the requirements contained herein, the following facilities, systems, and equipment owned by each Responsible Entity in subsection 4.1 above are those to which these requirements are applicable. For requirements in this **reliability standard** where a specific type of facilities, system, or equipment or subset of facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. One or more of the following facilities, systems and equipment that operate at, or control elements that operate at, a nominal voltage of 25 kV or less and are owned by a **legal owner** of an **electric distribution system** or a **legal owner** of a **transmission facility** for the protection or restoration of the **bulk electric system**:

4.2.1.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.2.1.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.2.1.1.2. performs automatic load shedding under a common control system owned by one or more of the entities in subsection 4.2.1, without human operator initiation, of 300 MW or more;

4.2.1.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.2.1.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.2.1.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.2.2. Responsible Entities listed in subsection 4.1 other than a **legal owner** of an **electric distribution system** are responsible for:

4.2.2.1. each **transmission facility** that is part of the **bulk electric system** except each **transmission facility** that:

4.2.2.1.1. is a transformer with fewer than 2 windings at 100 kV or higher and does not connect a contracted **blackstart resource**;

4.2.2.1.2. radially connects only to load;

4.2.2.1.3. radially connects only to one or more **generating units** or **aggregated generating facilities** with a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**; or

4.2.2.1.4. radially connects to load and one or more **generating units** or **aggregated generating facilities** that have a combined **maximum authorized real power**

of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**;

4.2.2.2. a **reactive power** resource that is dedicated to supplying or absorbing **reactive power** that is connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, except those **reactive power** resources operated by an end-use customer for its own use;

4.2.2.3. a **generating unit** that is:

4.2.2.3.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW unless the **generating unit** is part of an industrial complex;

4.2.2.3.2. within a power plant which:

4.2.2.3.2.1. is not part of an **aggregated generating facility**;

4.2.2.3.2.2. is directly connected to the **bulk electric system**; and

4.2.2.3.2.3. has a combined **maximum authorized real power** rating greater than 67.5 MW unless the power plant is part of an industrial complex;

4.2.2.3.3. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.3.4. a contracted **blackstart resource**;

4.2.2.4. an **aggregated generating facility** that is:

4.2.2.4.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW unless the **aggregated generating facility** is part of an industrial complex;

4.2.2.4.2. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.4.3. a contracted **blackstart resource**;

and

4.2.2.5. **control centres** and backup **control centres**.

4.2.3. The following are exempt from this **reliability standard**:

4.2.3.1. [Intentionally left blank.]

4.2.3.2. **cyber assets** associated with communication networks and data communication links between discrete **electronic security perimeters**.

4.2.3.3. [Intentionally left blank.]

4.2.3.4. for the **legal owner** of an **electric distribution system**, the systems and equipment that are not included in subsection 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no **BES cyber systems** categorized as High Impact or Medium Impact according to the CIP-002-AB-5.1 identification and

categorization processes.

5. [Intentionally left blank.]

6. [Intentionally left blank.]

## B. Requirements and Measures

**R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-AB-5 Table R1 – Electronic Security Perimeter.*

**M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-AB-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-005-AB-5 Table R1 – Electronic Security Perimeter | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.1 | High Impact **BES cyber systems** and their associated:<br>• **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>• **protected cyber assets** | All applicable **cyber assets** connected to a network via a routable protocol shall reside within a defined **electronic security perimeter**. | An example of evidence may include, but is not limited to, a list of all **electronic security perimeters** with all uniquely identifiable applicable **cyber assets** connected via a routable protocol within each **electronic security perimeter**. |
| 1.2 | High Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>• **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>• **protected cyber assets** | All **external routable connectivity** must be through an identified **electronic access point**. | An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified **electronic access points**. |
| 1.3 | **Electronic access points** for High Impact **BES cyber systems**<br>**Electronic access points** for Medium Impact **BES cyber** | Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. | An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed |

| CIP-005-AB-5 Table R1 – Electronic Security Perimeter | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | **systems** | | and that each access rule has a documented reason. |
| 1.4 | High Impact **BES cyber systems** with **dial-up connectivity** and their associated:<br>• **protected cyber assets**<br>Medium Impact **BES cyber systems** with **dial-up connectivity** and their associated:<br>• **protected cyber assets** | Where technically feasible, perform authentication when establishing **dial-up connectivity** with applicable **cyber assets**. | An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection. |
| 1.5 | **Electronic access points** for High Impact **BES cyber systems**<br>**Electronic access points** for Medium Impact **BES cyber systems** at **control centres** | Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. | An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented. |

**R2.** Each Responsible Entity allowing Interactive Remote Access to **BES cyber systems** shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-AB -5 Table R2 – Interactive Remote Access Management.*

**M2.** Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-AB -5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-005-AB-5 Table R2 – Interactive Remote Access Management | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.1 | High Impact **BES cyber systems** and their associated:<br>• **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and | Utilize an **intermediate system** such that the **cyber asset** initiating **interactive remote access** does not directly access an applicable **cyber asset**. | Examples of evidence may include, but are not limited to, network diagrams or architecture documents. |

| CIP-005-AB-5 Table R2 – Interactive Remote Access Management | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | their associated:<br>• **protected cyber assets** | | |
| 2.2 | High Impact **BES cyber systems** and their associated:<br>• **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>• **protected cyber assets** | For all **interactive remote access** sessions, utilize encryption that terminates at an **intermediate system**. | An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates. |
| 2.3 | High Impact **BES cyber systems** and their associated:<br>• **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>• **protected cyber assets** | Require multi-factor authentication for all **interactive remote access** sessions. | An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used.<br>Examples of authenticators may include, but are not limited to,<br>• something the individual knows such as passwords or PINs. This does not include User ID;<br>• something the individual has such as tokens, digital certificates, or smart cards; or<br>• something the individual is such as fingerprints, iris scans, or other biometric characteristics. |

## Revision History

| Date | Description |
| --- | --- |
| 2017-10-01 | Initial release. |

# Alberta Reliability Standard
# Cyber Security – Physical Security of BES Cyber Systems
# CIP-006-AB-5

## A. Introduction

1. Title: Cyber Security – Physical Security of BES Cyber Systems
2. Number: CIP-006-AB-5
3. Purpose: To manage physical access to **BES cyber systems** by specifying a physical security plan in support of protecting **BES cyber systems** against compromise that could lead to misoperation or instability in the **bulk electric system**.
4. Applicability:

4.1. For the purpose of the requirements contained herein, the following list of entities will be collectively referred to as "Responsible Entities." For requirements in this **reliability standard** where a specific entity or subset of entities are the applicable entity or entities, the entity or entities are specified explicitly.

4.1.1. [Intentionally left blank.]

4.1.2. a **legal owner** of an **electric distribution system** that owns one or more of the following facilities, systems, and equipment for the protection or restoration of the **bulk electric system**:

4.1.2.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.1.2.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.1.2.1.2. performs automatic load shedding under a common control system owned by the entity in subsection 4.1.2., without human operator initiation, of 300 MW or more;

4.1.2.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.1.2.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.1.2.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.1.3. the **operator** of a **generating unit** and the **operator** of an **aggregated generating facility**;

4.1.4. the **legal owner** of a **generating unit** and the **legal owner** of an **aggregated generating facility**;

4.1.5. [Intentionally left blank.]

4.1.6. [Intentionally left blank.]

4.1.7. the **operator** of a **transmission facility**;

4.1.8. the **legal owner** of a **transmission facility**; and

4.1.9. the **ISO**.

4.2. For the purpose of the requirements contained herein, the following facilities, systems, and equipment owned by each Responsible Entity in subsection 4.1 above are those to which these requirements are applicable. For requirements in this **reliability standard** where a specific type of facilities, system, or equipment or subset of facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. One or more of the following facilities, systems and equipment that operate at, or control elements that operate at, a nominal voltage of 25 kV or less and are owned by a **legal owner** of an **electric distribution system** or a **legal owner** of a **transmission facility** for the protection or restoration of the **bulk electric system**:

4.2.1.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.2.1.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.2.1.1.2. performs automatic load shedding under a common control system owned by one or more of the entities in subsection 4.2.1, without human operator initiation, of 300 MW or more;

4.2.1.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.2.1.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.2.1.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.2.2. Responsible Entities listed in subsection 4.1 other than a **legal owner** of an **electric distribution system** are responsible for:

4.2.2.1. each **transmission facility** that is part of the **bulk electric system** except each **transmission facility** that:

4.2.2.1.1. is a transformer with fewer than 2 windings at 100 kV or higher and does not connect a contracted **blackstart resource**;

4.2.2.1.2. radially connects only to load;

4.2.2.1.3. radially connects only to one or more **generating units** or **aggregated generating facilities** with a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**; or

4.2.2.1.4. radially connects to load and one or more **generating units** or **aggregated generating facilities** that have a combined **maximum authorized real power**

of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**;

4.2.2.2. a **reactive power** resource that is dedicated to supplying or absorbing **reactive power** that is connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, except those **reactive power** resources operated by an end-use customer for its own use;

4.2.2.3. a **generating unit** that is:

4.2.2.3.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW unless the **generating unit** is part of an industrial complex;

4.2.2.3.2. within a power plant which:

4.2.2.3.2.1. is not part of an **aggregated generating facility**;

4.2.2.3.2.2. is directly connected to the **bulk electric system**; and

4.2.2.3.2.3. has a combined **maximum authorized real power** rating greater than 67.5 MW unless the power plant is part of an industrial complex;

4.2.2.3.3. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.3.4. a contracted **blackstart resource**;

4.2.2.4. an **aggregated generating facility** that is:

4.2.2.4.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW unless the **aggregated generating facility** is part of an industrial complex;

4.2.2.4.2. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.4.3. a contracted **blackstart resource**;

and

4.2.2.5. **control centres** and backup **control centres**.

4.2.3. The following are exempt from this **reliability standard**:

4.2.3.1. [Intentionally left blank.]

4.2.3.2. **cyber assets** associated with communication networks and data communication links between discrete **electronic security perimeters**.

4.2.3.3. [Intentionally left blank.]

4.2.3.4. for the **legal owner** of an **electric distribution system**, the systems and equipment that are not included in subsection 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no **BES cyber systems** categorized as High Impact or Medium Impact according to the CIP-002-AB-5.1 identification and

categorization processes.

5. [Intentionally left blank.]

6. [Intentionally left blank.]

## B. Requirements and Measures

**R1.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-AB-5 Table R1 – Physical Security Plan.*

**M1.** Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-AB-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

| CIP-006-AB-5 Table R1 – Physical Security Plan | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.1 | Medium Impact **BES cyber systems** without **external routable connectivity**<br><br>**Physical access control systems** associated with:<br>• High Impact **BES cyber systems**, or<br>• Medium Impact **BES cyber systems** with **external routable connectivity** | Define operational or procedural controls to restrict physical access. | An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist. |
| 1.2 | Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets** | Utilize at least one physical access control to allow unescorted physical access into each applicable **physical security perimeter** to only those individuals who have authorized unescorted physical access. | An example of evidence may include, but is not limited to, language in the physical security plan that describes each **physical security perimeter** and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs. |

| CIP-006-AB-5 Table R1 – Physical Security Plan | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.3 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets** | Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into **physical security perimeters** to only those individuals who have authorized unescorted physical access. | An example of evidence may include, but is not limited to, language in the physical security plan that describes the **physical security perimeters** and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs. |
| 1.4 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets** | Monitor for unauthorized access through a physical access point into a **physical security perimeter**. | An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a **physical security perimeter**. |
| 1.5 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: | Issue an alarm or alert in response to detected unauthorized access through a physical access point into a **physical security perimeter** to the personnel identified in the **bulk electric system cyber security incident** response plan within 15 minutes of detection. | An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a **physical security perimeter** and additional evidence that the alarm or alert was issued and communicated as |

| CIP-006-AB-5 Table R1 – Physical Security Plan | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets** | | identified in the **bulk electric system cyber security incident** response plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated. |
| 1.6 | **Physical access control systems** associated with:<br>• High Impact **BES cyber systems**, or<br>• Medium Impact **BES cyber systems** with **external routable connectivity** | Monitor each **physical access control system** for unauthorized physical access to a **physical access control system**. | An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a **physical access control system**. |
| 1.7 | **Physical access control systems** associated with:<br>• High Impact **BES cyber systems**, or<br>• Medium Impact **BES cyber systems** with **external routable connectivity** | Issue an alarm or alert in response to detected unauthorized physical access to a **physical access control system** to the personnel identified in the **bulk electric system cyber security incident** response plan within 15 minutes of the detection. | An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to **physical access control systems** and additional evidence that the alarm or alerts was issued and communicated as identified in the **bulk electric system cyber security incident** response plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated. |
| 1.8 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and | Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access | An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of |

| CIP-006-AB-5 Table R1 – Physical Security Plan | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 2. **protected cyber assets**<br><br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets** | into each **physical security perimeter**, with information to identify the individual and date and time of entry. | physical entry into each **physical security perimeter** and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into **physical security perimeters** that show the individual and the date and time of entry into **physical security perimeter**. |
| 1.9 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets**<br><br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets** | Retain physical access logs of entry of individuals with authorized unescorted physical access into each **physical security perimeter** for at least ninety **days**. | An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into **physical security perimeters** that show the date and time of entry into **physical security perimeter**. |

**R2.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-AB-5 Table R2 – Visitor Control Program.*

**M2.** Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-AB-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-006-AB-5 Table R2 – Visitor Control Program |
|---|

| Part | Applicable Systems | Requirements | Measures |
|---|---|---|---|
| 2.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets** | Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each **physical security perimeter**, except during **CIP exceptional circumstances**. | An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within **physical security perimeters** and additional evidence to demonstrate that the process was implemented, such as visitor logs. |
| 2.2 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets** | Require manual or automated logging of visitor entry into and exit from the **physical security perimeter** that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during **CIP exceptional circumstances**. | An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within **physical security perimeters** and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information. |
| 2.3 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and | Retain visitor logs for at least ninety **days**. | An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety **days**. |

| CIP-006-AB-5 Table R2 – Visitor Control Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets** | | |

**R3.** Each Responsible Entity shall implement one or more documented **physical access control system** maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-AB-5 Table R3 – Maintenance and Testing Program.*

**M3.** Evidence must include each of the documented **physical access control system** maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-AB-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-006-AB-5 Table R3 – Maintenance and Testing Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.1 | **Physical access control systems** associated with:<br>• High Impact **BES cyber systems**, or<br>• Medium Impact **BES cyber systems** with **external routable connectivity**<br>Locally mounted hardware or devices at the **physical security perimeter** associated with:<br>• High Impact **BES cyber systems**, or<br>• Medium Impact **BES cyber systems** with **external routable connectivity** | Maintenance and testing of each **physical access control system** and locally mounted hardware or devices at the **physical security perimeter** at least once every 24 **months** to ensure they function properly. | An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each **physical access control system** and locally mounted hardware or devices associated with each applicable **physical security perimeter** at least once every 24 **months** and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 **months**. |

## Revision History

| Date | Description |
| --- | --- |
| 2017-10-01 | Initial release. |

# Alberta Reliability Standard
# Cyber Security – System Security Management
# CIP-007-AB-5

## A. Introduction

1. Title: Cyber Security – System Security Management
2. Number: CIP-007-AB-5
3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting **BES cyber systems** against compromise that could lead to misoperation or instability in the **bulk electric system**.
4. Applicability:

4.1. For the purpose of the requirements contained herein, the following list of entities will be collectively referred to as “Responsible Entities”. For requirements in this **reliability standard** where a specific entity or subset of entities are the applicable entity or entities, the entity or entities are specified explicitly.

4.1.1. [Intentionally left blank.]

4.1.2. a **legal owner** of an **electric distribution system** that owns one or more of the following facilities, systems, and equipment for the protection or restoration of the **bulk electric system**:

4.1.2.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.1.2.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.1.2.1.2. performs automatic load shedding under a common control system owned by the entity in subsection 4.1.2., without human operator initiation, of 300 MW or more;

4.1.2.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.1.2.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.1.2.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.1.3. the **operator** of a **generating unit** and the **operator** of an **aggregated generating facility**;

4.1.4. the **legal owner** of a **generating unit** and the **legal owner** of an **aggregated generating facility**;

4.1.5. [Intentionally left blank.]

4.1.6. [Intentionally left blank.]

4.1.7. the **operator** of a **transmission facility**;

4.1.8. the **legal owner** of a **transmission facility**; and

4.1.9. the **ISO**.

4.2. For the purpose of the requirements contained herein, the following facilities, systems, and equipment owned by each Responsible Entity in subsection 4.1 above are those to which these requirements are applicable. For requirements in this **reliability standard** where a specific type of facilities, system, or equipment or subset of facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. One or more of the following facilities, systems and equipment that operate at, or control elements that operate at, a nominal voltage of 25 kV or less and are owned by a **legal owner** of an **electric distribution system** or a **legal owner** of a **transmission facility** for the protection or restoration of the **bulk electric system**:

4.2.1.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.2.1.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.2.1.1.2. performs automatic load shedding under a common control system owned by one or more of the entities in subsection 4.2.1, without human operator initiation, of 300 MW or more;

4.2.1.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.2.1.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.2.1.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.2.2. Responsible Entities listed in subsection 4.1 other than a **legal owner** of an **electric distribution system** are responsible for:

4.2.2.1. each **transmission facility** that is part of the **bulk electric system** except each **transmission facility** that:

4.2.2.1.1. is a transformer with fewer than 2 windings at 100 kV or higher and does not connect a contracted **blackstart resource**;

4.2.2.1.2. radially connects only to load;

4.2.2.1.3. radially connects only to one or more **generating units** or **aggregated generating facilities** with a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**; or

4.2.2.1.4. radially connects to load and one or more **generating units** or **aggregated generating facilities** that have a combined **maximum authorized real power**

of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**;

4.2.2.2. a **reactive power** resource that is dedicated to supplying or absorbing **reactive power** that is connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, except those **reactive power** resources operated by an end-use customer for its own use;

4.2.2.3. a **generating unit** that is:

4.2.2.3.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW unless the **generating unit** is part of an industrial complex;

4.2.2.3.2. within a power plant which:

4.2.2.3.2.1. is not part of an **aggregated generating facility**;

4.2.2.3.2.2. is directly connected to the **bulk electric system**; and

4.2.2.3.2.3. has a combined **maximum authorized real power** rating greater than 67.5 MW unless the power plant is part of an industrial complex;

4.2.2.3.3. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.3.4. a contracted **blackstart resource**;

4.2.2.4. an **aggregated generating facility** that is:

4.2.2.4.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW unless the **aggregated generating facility** is part of an industrial complex;

4.2.2.4.2. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.4.3. a contracted **blackstart resource**;

and

4.2.2.5. **control centres** and backup **control centres**.

4.2.3. The following are exempt from this **reliability standard**:

4.2.3.1. [Intentionally left blank.]

4.2.3.2. **cyber assets** associated with communication networks and data communication links between discrete **electronic security perimeters**.

4.2.3.3. [Intentionally left blank.]

4.2.3.4. for the **legal owner** of an **electric distribution system**, the systems and equipment that are not included in subsection 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no **BES cyber systems** categorized as High Impact or Medium Impact according to the CIP-002-AB-5.1 identification and

categorization processes.

5. [Intentionally left blank.]

6. [Intentionally left blank.]

## B. Requirements and Measures

**R1.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R1 – Ports and Services.*

**M1.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| **CIP-007-AB-5 Table R1 – Ports and Services** | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed. | Examples of evidence may include, but are not limited to:<br>• documentation of the need for all enabled ports on all applicable **cyber assets** and **electronic access points**, individually or by group.<br>• listings of the listening ports on the **cyber assets**, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or<br>• configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others. |
| 1.2 | High Impact **BES cyber systems**<br>Medium Impact **BES cyber systems** at **control centres** | Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable | An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either |

| CIP-007-AB-5 Table R1 – Ports and Services | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | | media. | logically through system configuration or physically using a port lock or signage. |

**R2.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R2 – Security Patch Management.*

**M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-007-AB-5 Table R2 – Security Patch Management | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | A patch management process for tracking, evaluating, and installing cyber security patches for applicable **cyber assets**. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable **cyber assets** that are updateable and for which a patching source exists. | An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual **BES cyber system** or **cyber asset** basis. |
| 2.2 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | At least once every 35 **days**, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in part 2.1. | An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 **days**. |

| CIP-007-AB-5 Table R2 – Security Patch Management | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | | |
| 2.3 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | For applicable patches identified in part 2.2, within 35 **days** of the evaluation completion, take one of the following actions:<br>• apply the applicable patches; or<br>• create a dated mitigation plan; or<br>• revise an existing mitigation plan.<br>Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations. | Examples of evidence may include, but are not limited to:<br>• records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of **BES cyber system** component software revision, or registry exports that show software has been installed); or<br>• a dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations. |
| 2.4 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and | For each mitigation plan created or revised in part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in part 2.3 is approved by the **CIP senior** | An example of evidence may include, but is not limited to, records of implementation of mitigations. |

| CIP-007-AB-5 Table R2 – Security Patch Management | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | **manager** or delegate. | |

**R3.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R3 – Malicious Code Prevention.*

**M3.** Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-007-AB-5 Table R3 – Malicious Code Prevention | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | Deploy method(s) to deter, detect, or prevent malicious code. | An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.). |
| 3.2 | High Impact **BES cyber systems** and their associated: | Mitigate the threat of detected malicious code. | Examples of evidence may include, but are not limited to: |

| CIP-007-AB-5 Table R3 – Malicious Code Prevention | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | | • records of response processes for malicious code detection<br>• records of the performance of these processes when malicious code is detected. |
| 3.3 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | For those methods identified in part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns. | An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns. |

**R4.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R4 – Security Event Monitoring.*

**M4.** Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-007-AB-5 Table R4 – Security Event Monitoring | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 4.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | Log events at the **BES cyber system** level (per **BES cyber system** capability) or at the **cyber asset** level (per **cyber asset** capability) for identification of, and after-the-fact investigations of, **cyber security incidents** that includes, as a minimum, each of the following types of events:<br>4.1.1. detected successful login attempts;<br>4.1.2. detected failed access attempts and failed login attempts;<br>4.1.3. detected malicious code. | Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the **BES cyber system** is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events. |
| 4.2 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per **cyber asset** or **BES cyber system** capability):<br>4.2.1. detected malicious code from part 4.1; and<br>4.2.2. detected failure of part 4.1 event logging. | Examples of evidence may include, but are not limited to, paper or system generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured. |
| 4.3 | High Impact **BES cyber systems** and their associated: | Where technically feasible, retain applicable event logs identified in part 4.1 for at least | Examples of evidence may include, but are not limited to, documentation of the event log |

| CIP-007-AB-5 Table R4 – Security Event Monitoring | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** at **control centres** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | the last 90 consecutive **days** except under **CIP exceptional circumstances**. | retention process and paper or system generated reports showing log retention configuration set at 90 **days** or greater. |
| 4.4 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets** | Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 **days** to identify undetected **cyber security incidents**. | Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred. |

**R5.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R5 – System Access Controls.*

**M5.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts *in CIP-007-AB-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-007-AB-5 Table R5 – System Access Controls | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 5.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control** | Have a method(s) to enforce authentication of interactive user access, where technically feasible. | An example of evidence may include, but is not limited to, documentation describing how access is authenticated. |

| CIP-007-AB-5 Table R5 – System Access Controls | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | **systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** at **control centres** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | | |
| 5.2 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). | An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the **BES cyber system**. |

| CIP-007-AB-5 Table R5 – System Access Controls | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 5.3 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | Identify individuals who have authorized access to shared accounts. | An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account. |
| 5.4 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | Change known default passwords, per **cyber asset** capability. | Examples of evidence may include, but are not limited to:<br>• records of a procedure that passwords are changed when new devices are in production; or<br>• documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device. |
| 5.5 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; | For password-only authentication for interactive user access, either technically or procedurally enforce the following password | Examples of evidence may include, but are not limited to:<br>• system-generated reports or screen-shots of the |

| CIP-007-AB-5 Table R5 – System Access Controls | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | parameters:<br>5.5.1. password length that is, at least, the lesser of eight characters or the maximum length supported by the **cyber asset**; and<br>5.5.2. minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, nonalphanumeric) or the maximum complexity supported by the **cyber asset**. | system enforced password parameters, including length and complexity; or<br>• attestations that include a reference to the documented procedures that were followed. |
| 5.6 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 **months**. | Examples of evidence may include, but are not limited to:<br>• system-generated reports or screen-shots of the system enforced periodicity of changing passwords; or<br>• attestations that include a reference to the documented procedures that were followed. |
| 5.7 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control** | Where technically feasible, either:<br>• limit the number of unsuccessful authentication attempts; or | Examples of evidence may include, but are not limited to:<br>• documentation of the account-lockout parameters; or |

| CIP-007-AB-5 Table R5 – System Access Controls | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | **systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** at **control centres** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | • generate alerts after a threshold of unsuccessful authentication attempts. | • rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts. |

## Revision History

| Date | Description |
|---|---|
| 2017-10-01 | Initial release. |

# Alberta Reliability Standard
# Cyber Security – Incident Reporting and Response Planning
# CIP-008-AB-5

## A. Introduction

1. Title: Cyber Security – Incident Reporting and Response Planning
2. Number: CIP-008-AB-5
3. Purpose: To mitigate the risk to the reliable operation of the **bulk electric system** as the result of a **cyber security incident** by specifying incident response requirements.
4. Applicability:

4.1. For the purpose of the requirements contained herein, the following list of entities will be collectively referred to as "Responsible Entities". For requirements in this **reliability standard** where a specific entity or subset of entities are the applicable entity or entities, the entity or entities are specified explicitly.

4.1.1. [Intentionally left blank.]

4.1.2. a **legal owner** of an **electric distribution system** that owns one or more of the following facilities, systems, and equipment for the protection or restoration of the **bulk electric system**:

4.1.2.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.1.2.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.1.2.1.2. performs automatic load shedding under a common control system owned by the entity in subsection 4.1.2., without human operator initiation, of 300 MW or more;

4.1.2.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.1.2.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.1.2.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.1.3. the **operator** of a **generating unit** and the **operator** of an **aggregated generating facility**;

4.1.4. the **legal owner** of a **generating unit** and the **legal owner** of an **aggregated generating facility**;

4.1.5. [Intentionally left blank.]

4.1.6. [Intentionally left blank.]

4.1.7. the **operator** of a **transmission facility**;

4.1.8. the **legal owner** of a **transmission facility**; and

4.1.9. the **ISO**.

4.2. For the purpose of the requirements contained herein, the following facilities, systems, and equipment owned by each Responsible Entity in subsection 4.1 above are those to which these requirements are applicable. For requirements in this **reliability standard** where a specific type of facilities, system, or equipment or subset of facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. One or more of the following facilities, systems and equipment that operate at, or control elements that operate at, a nominal voltage of 25 kV or less and are owned by a **legal owner** of an **electric distribution system** or a **legal owner** of a **transmission facility** for the protection or restoration of the **bulk electric system**:

4.2.1.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.2.1.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.2.1.1.2. performs automatic load shedding under a common control system owned by one or more of the entities in subsection 4.2.1, without human operator initiation, of 300 MW or more;

4.2.1.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.2.1.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.2.1.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.2.2. Responsible Entities listed in subsection 4.1 other than a **legal owner** of an **electric distribution system** are responsible for:

4.2.2.1. each **transmission facility** that is part of the **bulk electric system** except each **transmission facility** that:

4.2.2.1.1. is a transformer with fewer than 2 windings at 100 kV or higher and does not connect a contracted **blackstart resource**;

4.2.2.1.2. radially connects only to load;

4.2.2.1.3. radially connects only to one or more **generating units** or **aggregated generating facilities** with a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**; or

4.2.2.1.4. radially connects to load and one or more **generating units** or **aggregated generating facilities** that have a combined **maximum authorized real power**

of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**;

4.2.2.2. a **reactive power** resource that is dedicated to supplying or absorbing **reactive power** that is connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, except those **reactive power** resources operated by an end-use customer for its own use;

4.2.2.3. a **generating unit** that is:

4.2.2.3.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW unless the **generating unit** is part of an industrial complex;

4.2.2.3.2. within a power plant which:

4.2.2.3.2.1. is not part of an **aggregated generating facility**;

4.2.2.3.2.2. is directly connected to the **bulk electric system**; and

4.2.2.3.2.3. has a combined **maximum authorized real power** rating greater than 67.5 MW unless the power plant is part of an industrial complex;

4.2.2.3.3. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.3.4. a contracted **blackstart resource**;

4.2.2.4. an **aggregated generating facility** that is:

4.2.2.4.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW unless the **aggregated generating facility** is part of an industrial complex;

4.2.2.4.2. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.4.3. a contracted **blackstart resource**;

and

4.2.2.5. **control centres** and backup **control centres**.

4.2.3. The following are exempt from this **reliability standard**:

4.2.3.1. [Intentionally left blank.]

4.2.3.2. **cyber assets** associated with communication networks and data communication links between discrete **electronic security perimeters**.

4.2.3.3. [Intentionally left blank.]

4.2.3.4. for the **legal owner** of an **electric distribution system**, the systems and equipment that are not included in subsection 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no **BES cyber systems** categorized as High Impact or Medium Impact according to the CIP-002-AB-5.1 identification and

categorization processes.

5. [Intentionally left blank.]

6. [Intentionally left blank.]

## B. Requirements and Measures

**R1.** Each Responsible Entity shall document one or more **cyber security incident** response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-AB-5 Table R1 – Cyber Security Incident Response Plan Specifications.*

**M1.** Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-AB-5 Table R1 – Cyber Security Incident Response Plan Specifications.*

**CIP-008-AB-5 Table R1 – Cyber Security Incident Response Plan Specifications**

| Part | Applicable Systems | Requirements | Measures |
|---|---|---|---|
| 1.1 | High Impact **BES cyber systems**<br>Medium Impact **BES cyber systems** | One or more processes to identify, classify, and respond to **cyber security incidents**. | An example of evidence may include, but is not limited to, dated documentation of **cyber security incidents** response plan(s) that include the process to identify, classify, and respond to **cyber security incidents**. |
| 1.2 | High Impact **BES cyber systems**<br>Medium Impact **BES cyber systems** | One or more processes to determine if an identified **cyber security incident** is a **reportable cyber security incident** and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a **reportable cyber security incident**. | Examples of evidence may include, but are not limited to, dated documentation of **cyber security incident** response plan(s) that provide guidance or thresholds for determining which **cyber security incidents** are also **reportable cyber security incidents** and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). |
| 1.3 | High Impact **BES cyber systems**<br>Medium Impact **BES cyber systems** | The roles and responsibilities of **cyber security incident** response groups or individuals. | An example of evidence may include, but is not limited to, dated **cyber security incident** response process(es) or procedure(s) that define roles and responsibilities (e.g., |

| CIP-008-AB-5 Table R1 – Cyber Security Incident Response Plan Specifications | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | | | monitoring, reporting, initiating, documenting, etc.) of **cyber security incident** response groups or individuals. |
| 1.4 | High Impact **BES cyber systems**<br><br>Medium Impact **BES cyber systems** | Incident handling procedures for **cyber security incidents**. | An example of evidence may include, but is not limited to, dated for **cyber security incident** response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution). |

**R2.** Each Responsible Entity shall implement each of its documented **cyber security incident** response plans to collectively include each of the applicable requirement parts in *CIP-008-AB-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.*

**M2.** Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-AB-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.*

| CIP-008-AB-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.1 | High Impact **BES cyber systems**<br><br>Medium Impact **BES cyber systems** | Test each **cyber security incident** response plan(s) at least once every 15 **months**:<br>• by responding to an actual **reportable cyber security incident**;<br>• with a paper drill or tabletop exercise of a **reportable cyber security incident**; or<br>• with an operational exercise of a **reportable cyber security incident**. | Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises. |
| 2.2 | High Impact **BES cyber systems**<br><br>Medium Impact **BES cyber** | Use the **cyber security incident** response plan(s) under Requirement R1 when responding to a **reportable** | Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the |

| CIP-008-AB-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | **systems** | **cyber security incident** or performing an exercise of a **reportable cyber security incident**. Document deviations from the plan(s) taken during the response to the incident or exercise. | incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise. |
| 2.3 | High Impact **BES cyber systems**<br><br>Medium Impact **BES cyber systems** | Retain records related to **reportable cyber security incident**. | An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to **reportable cyber security incidents**. |

**R3.** Each Responsible Entity shall maintain each of its **cyber security incident** response plans according to each of the applicable requirement parts in *CIP-008-AB-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

**M3.** Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each **cyber security incident** response plan according to the applicable requirement parts in *CIP-008-AB-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

| CIP-008-AB-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.1 | High Impact **BES cyber systems**<br><br>Medium Impact **BES cyber systems** | No later than 90 **days** after completion of a **cyber security incident** response plan(s) test or actual **reportable cyber security incident** response:<br><br>3.1.1. document any lessons learned or document the absence of any lessons learned;<br><br>3.1.2. update the **cyber** | An example of evidence may include, but is not limited to, all of the following:<br><br>1. dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the **cyber security incident** response plan(s) test or actual **reportable cyber security incident** |

| CIP-008-AB-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | | **security incident** response plan based on any documented lessons learned associated with the plan; and<br>3.1.3. notify each person or group with a defined role in the **cyber security incident** response plan of the updates to the **cyber security incident** response plan based on any documented lessons learned. | response or dated documentation stating there were no lessons learned;<br>2. dated and revised **cyber security incident** response plan showing any changes based on the lessons learned; and<br>3. evidence of plan update distribution including, but not limited to:<br>• emails;<br>• USPS or other mail service;<br>• electronic distribution system; or<br>• training sign-in sheets. |
| 3.2 | High Impact **BES cyber systems**<br>Medium Impact **BES cyber systems** | No later than 60 **days** after a change to the roles or responsibilities, **cyber security incident** response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan:<br>3.2.1. update the **cyber security incident** response plan(s); and<br>3.2.2. notify each person or group with a defined role in the **cyber security incident** response plan of the updates. | An example of evidence may include, but is not limited to:<br>1. dated and revised **cyber security incident** response plan with changes to the roles or responsibilities, responders or technology; and<br>2. evidence of plan update distribution including, but not limited to:<br>• emails;<br>• USPS or other mail service;<br>• electronic distribution system; or<br>• training sign-in sheets. |

## Revision History

| Date | Description |
|---|---|
| 2017-10-01 | Initial release. |

# Alberta Reliability Standard
# Cyber Security – Recovery Plans for BES Cyber Systems
# CIP-009-AB-5

## A. Introduction

1. Title: Cyber Security – Recovery Plans for BES Cyber Systems
2. Number: CIP-009-AB-5
3. Purpose: To recover reliability functions performed by **BES cyber systems** by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the **bulk electric system**.
4. Applicability:

4.1. For the purpose of the requirements contained herein, the following list of entities will be collectively referred to as “Responsible Entities”. For requirements in this **reliability standard** where a specific entity or subset of entities are the applicable entity or entities, the entity or entities are specified explicitly.

4.1.1. [Intentionally left blank.]

4.1.2. a **legal owner** of an **electric distribution system** that owns one or more of the following facilities, systems, and equipment for the protection or restoration of the **bulk electric system**:

4.1.2.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.1.2.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.1.2.1.2. performs automatic load shedding under a common control system owned by the entity in subsection 4.1.2., without human operator initiation, of 300 MW or more;

4.1.2.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.1.2.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.1.2.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.1.3. the **operator** of a **generating unit** and the **operator** of an **aggregated generating facility**;

4.1.4. the **legal owner** of a **generating unit** and the **legal owner** of an **aggregated generating facility**;

4.1.5. [Intentionally left blank.]

4.1.6. [Intentionally left blank.]

4.1.7. the **operator** of a **transmission facility**;

4.1.8. the **legal owner** of a **transmission facility**; and

4.1.9. the **ISO**.

4.2. For the purpose of the requirements contained herein, the following facilities, systems, and equipment owned by each Responsible Entity in subsection 4.1 above are those to which these requirements are applicable. For requirements in this **reliability standard** where a specific type of facilities, system, or equipment or subset of facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. One or more of the following facilities, systems and equipment that operate at, or control elements that operate at, a nominal voltage of 25 kV or less and are owned by a **legal owner** of an **electric distribution system** or a **legal owner** of a **transmission facility** for the protection or restoration of the **bulk electric system**:

4.2.1.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.2.1.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.2.1.1.2. performs automatic load shedding under a common control system owned by one or more of the entities in subsection 4.2.1, without human operator initiation, of 300 MW or more;

4.2.1.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.2.1.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**;

4.2.1.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.2.2. Responsible Entities listed in subsection 4.1 other than a **legal owner** of an **electric distribution system** are responsible for:

4.2.2.1. each **transmission facility** that is part of the **bulk electric system** except each **transmission facility** that:

4.2.2.1.1. is a transformer with fewer than 2 windings at 100 kV or higher and does not connect a contracted **blackstart resource**;

4.2.2.1.2. radially connects only to load;

4.2.2.1.3. radially connects only to one or more **generating units** or **aggregated generating facilities** with a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**; or

4.2.2.1.4. radially connects to load and one or more **generating units** or **aggregated generating facilities** that have a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart**

**resource**;

4.2.2.2. a **reactive power** resource that is dedicated to supplying or absorbing **reactive power** that is connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, except those **reactive power** resources operated by an end-use customer for its own use;

4.2.2.3. a **generating unit** that is:

4.2.2.3.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW unless the **generating unit** is part of an industrial complex;

4.2.2.3.2. within a power plant which:

4.2.2.3.2.1. is not part of an **aggregated generating facility**;

4.2.2.3.2.2. is directly connected to the **bulk electric system**; and

4.2.2.3.2.3. has a combined **maximum authorized real power** rating greater than 67.5 MW unless the power plant is part of an industrial complex;

4.2.2.3.3. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.3.4. a contracted **blackstart resource**;

4.2.2.4. an **aggregated generating facility** that is:

4.2.2.4.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW unless the **aggregated generating facility** is part of an industrial complex;

4.2.2.4.2. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.4.3. a contracted **blackstart resource**;

and

4.2.2.5. **control centres** and backup **control centres**.

4.2.3. The following are exempt from this **reliability standard**:

4.2.3.1. [Intentionally left blank.]

4.2.3.2. **cyber assets** associated with communication networks and data communication links between discrete **electronic security perimeters**.

4.2.3.3. [Intentionally left blank.]

4.2.3.4. for the **legal owner** of an **electric distribution system**, the systems and equipment that are not included in subsection 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no **BES cyber systems** categorized as High Impact or Medium Impact according to the CIP-002-AB-5.1 identification and categorization processes.

5. [Intentionally left blank.]
6. [Intentionally left blank.]

## B. Requirements and Measures

**R1.** Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-AB-5 Table R1 – Recovery Plan Specifications.*

**M1.** Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-AB-5 Table R1 – Recovery Plan Specifications.*

| **CIP-009-AB-5 Table R1 – Recovery Plan Specifications** | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems** | Conditions for activation of the recovery plan(s). | An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s). |
| 1.2 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control** | Roles and responsibilities of responders. | An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders. |

| CIP-009-AB-5 Table R1 – Recovery Plan Specifications | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | **systems** | | |
| 1.3 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems** | One or more processes for the backup and storage of information required to recover **BES cyber system** functionality. | An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover **BES cyber system** functionality. |
| 1.4 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems**<br>Medium Impact **BES cyber systems** at **control centres** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems** | One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures. | An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed. |
| 1.5 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems** | One or more processes to preserve data, per **cyber asset** capability, for determining the cause of a **cyber security incident** that triggers activation of the recovery plan(s). Data preservation should not | An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery. |

| CIP-009-AB-5 Table R1 – Recovery Plan Specifications | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems** | impede or restrict recovery. | |

**R2.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-AB-5 Table R2 – Recovery Plan Implementation and Testing.*

**M2.** Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-AB-5 Table R2 – Recovery Plan Implementation and Testing.*

| CIP-009-AB-5 Table R2 – Recovery Plan Implementation and Testing | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems**<br>Medium Impact **BES cyber systems** at **control centres** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems** | Test each of the recovery plans referenced in requirement R1 at least once every 15 **months**:<br>• by recovering from an actual incident;<br>• with a paper drill or tabletop exercise; or<br>• with an operational exercise. | An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 **months**. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. |
| 2.2 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and | Test a representative sample of information used to recover **BES cyber system** functionality at least once every 15 **months** to ensure that the information is useable | An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) |

| CIP-009-AB-5 Table R2 – Recovery Plan Implementation and Testing | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 2. **physical access control systems**<br>Medium Impact **BES cyber systems** at **control centres** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems** | and is compatible with current configurations.<br>An actual recovery that incorporates the information used to recover **BES cyber system** functionality substitutes for this test. | and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration). |
| 2.3 | High Impact **BES cyber systems** | Test each of the recovery plans referenced in requirement R1 at least once every 36 **months** through an operational exercise of the recovery plans in an environment representative of the production environment.<br>An actual recovery response may substitute for an operational exercise. | Examples of evidence may include, but are not limited to, dated documentation of:<br>• an operational exercise at least once every 36 **months** between exercises, that demonstrates recovery in a representative environment; or<br>• an actual recovery response that occurred within the 36 **month** timeframe that exercised the recovery plans. |

**R3.** Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-AB-5 Table R3 – Recovery Plan Review, Update and Communication.*

**M3.** Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-AB-5 Table R3 – Recovery Plan Review, Update and Communication.*

| CIP-009-AB-5 Table R3 – Recovery Plan Review, Update and Communication | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring** | No later than 90 **days** after completion of a recovery plan test or actual recovery:<br>3.1.1. document any lessons | An example of evidence may include, but is not limited to, all of the following:<br>1. dated documentation of |

| CIP-009-AB-5 Table R3 – Recovery Plan Review, Update and Communication | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | **systems**; and<br>2. **physical access control systems**<br>Medium Impact **BES cyber systems** at **control centres** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems** | learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned;<br>3.1.2. update the recovery plan based on any documented lessons learned associated with the plan; and<br>3.1.3. notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned. | identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned;<br>2. dated and revised recovery plan showing any changes based on the lessons learned; and<br>3. evidence of plan update distribution including, but not limited to:<br>• emails;<br>• USPS or other mail service;<br>• electronic distribution system; or<br>• training sign-in sheets. |
| 3.2 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems**<br>Medium Impact **BES cyber systems** at **control centres** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems** | No later than 60 **days** after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan:<br>3.2.1. update the recovery plan; and<br>3.2.2. notify each person or group with a defined role in the recovery plan of the updates. | An example of evidence may include, but is not limited to, all of the following:<br>1. dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and<br>2. evidence of plan update distribution including, but not limited to:<br>• emails;<br>• USPS or other mail service;<br>• electronic distribution system; or |

| CIP-009-AB-5 Table R3 – Recovery Plan Review, Update and Communication | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | | | • training sign-in sheets. |

## Revision History

| Date | Description |
|---|---|
| 2017-10-01 | Initial release. |

# Alberta Reliability Standard
# Cyber Security – Configuration Change Management and Vulnerability Assessments
# CIP-010-AB-1

## A. Introduction

1. Title: Cyber Security – Configuration Change Management and Vulnerability Assessments
2. Number: CIP-010-AB-1
3. Purpose: To prevent and detect unauthorized changes to **BES cyber systems** by specifying configuration change management and vulnerability assessment requirements in support of protecting **BES cyber systems** from compromise that could lead to misoperation or instability in the **bulk electric system**.
4. Applicability:

4.1. For the purpose of the requirements contained herein, the following list of entities will be collectively referred to as “Responsible Entities”. For requirements in this **reliability standard** where a specific entity or subset of entities are the applicable entity or entities, the entity or entities are specified explicitly.

4.1.1. [Intentionally left blank.]

4.1.2. a **legal owner** of an **electric distribution system** that owns one or more of the following facilities, systems, and equipment for the protection or restoration of the **bulk electric system**:

4.1.2.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.1.2.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.1.2.1.2. performs automatic load shedding under a common control system owned by the entity in subsection 4.1.2., without human operator initiation, of 300 MW or more;

4.1.2.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.1.2.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.1.2.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.1.3. the **operator** of a **generating unit** and the **operator** of an **aggregated generating facility**;

4.1.4. the **legal owner** of a **generating unit** and the **legal owner** of an **aggregated generating facility**;

4.1.5. [Intentionally left blank.]

4.1.6. [Intentionally left blank.]

4.1.7. the **operator** of a **transmission facility**;

4.1.8. the **legal owner** of a **transmission facility**; and

4.1.9. the **ISO**.

4.2. For the purpose of the requirements contained herein, the following facilities, systems, and equipment owned by each Responsible Entity in subsection 4.1 above are those to which these requirements are applicable. For requirements in this **reliability standard** where a specific type of facilities, system, or equipment or subset of facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. One or more of the following facilities, systems and equipment that operate at, or control elements that operate at, a nominal voltage of 25 kV or less and are owned by a **legal owner** of an **electric distribution system** or a **legal owner** of a **transmission facility** for the protection or restoration of the **bulk electric system**:

4.2.1.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.2.1.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.2.1.1.2. performs automatic load shedding under a common control system owned by one or more of the entities in subsection 4.2.1, without human operator initiation, of 300 MW or more;

4.2.1.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.2.1.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.2.1.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.2.2. Responsible Entities listed in subsection 4.1 other than a **legal owner** of an **electric distribution system** are responsible for:

4.2.2.1. each **transmission facility** that is part of the **bulk electric system** except each **transmission facility** that:

4.2.2.1.1. is a transformer with fewer than 2 windings at 100 kV or higher and does not connect a contracted **blackstart resource**;

4.2.2.1.2. radially connects only to load;

4.2.2.1.3. radially connects only to one or more **generating units** or **aggregated generating facilities** with a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**; or

4.2.2.1.4. radially connects to load and one or more **generating units** or **aggregated generating facilities** that have a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart**

**resource**;

4.2.2.2. a **reactive power** resource that is dedicated to supplying or absorbing **reactive power** that is connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, except those **reactive power** resources operated by an end-use customer for its own use;

4.2.2.3. a **generating unit** that is:

4.2.2.3.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW unless the **generating unit** is part of an industrial complex;

4.2.2.3.2. within a power plant which:

4.2.2.3.2.1. is not part of an **aggregated generating facility**;

4.2.2.3.2.2. is directly connected to the **bulk electric system**; and

4.2.2.3.2.3. has a combined **maximum authorized real power** rating greater than 67.5 MW unless the power plant is part of an industrial complex;

4.2.2.3.3. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.3.4. a contracted **blackstart resource**;

4.2.2.4. an **aggregated generating facility** that is:

4.2.2.4.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW unless the **aggregated generating facility** is part of an industrial complex;

4.2.2.4.2. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.4.3. a contracted **blackstart resource**;

and

4.2.2.5. **control centres** and backup **control centres**.

4.2.3. The following are exempt from this **reliability standard**:

4.2.3.1. [Intentionally left blank.]

4.2.3.2. **cyber assets** associated with communication networks and data communication links between discrete **electronic security perimeters**.

4.2.3.3. [Intentionally left blank.]

4.2.3.4. for the **legal owner** of an **electric distribution system**, the systems and equipment that are not included in subsection 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no **BES cyber systems** categorized as High Impact or Medium Impact according to the CIP-002-AB-5.1 identification and categorization processes.

5. [Intentionally left blank.]
6. [Intentionally left blank.]

## B. Requirements and Measures

**R1.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R1 – Configuration Change Management*.

**M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| **CIP-010-AB-1 Table R1 – Configuration Change Management** | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | Develop a baseline configuration, individually or by group, which shall include the following items:<br>1.1.1. operating system(s) (including version) or firmware where no independent operating system exists;<br>1.1.2. any commercially available or open-source application software (including version) intentionally installed;<br>1.1.3. any custom software installed;<br>1.1.4. any logical network accessible ports; and<br>1.1.5. any security patches applied. | Examples of evidence may include, but are not limited to:<br>• a spreadsheet identifying the required items of the baseline configuration for each **cyber asset**, individually or by group; or<br>• a record in an asset management system that identifies the required items of the baseline configuration for each **cyber asset**, individually or by group. |
| 1.2 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and | Authorize and document changes that deviate from the existing baseline configuration. | Examples of evidence may include, but are not limited to:<br>• a change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a |

| CIP-010-AB-1 Table R1 – Configuration Change Management | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | | change management system for each change; or<br>• documentation that the change was performed in accordance with the requirement. |
| 1.3 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 **days** of completing the change. | An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 **days** of the date of the completion of the change. |
| 1.4 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated: | For a change that deviates from the existing baseline configuration:<br>1.4.1. prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;<br>1.4.2. following the change, verify that required cyber security controls determined | An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results. |

| CIP-010-AB-1 Table R1 – Configuration Change Management | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets** | in 1.4.1 are not adversely affected; and<br>1.4.3. document the results of the verification. | |
| 1.5 | High Impact **BES cyber systems** | Where technically feasible, for each change that deviates from the existing baseline configuration:<br>1.5.1. prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and<br>1.5.2. document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. | An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test. |

**R2.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R2 – Configuration Monitoring*.

**M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R2 – Configuration*

*Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-010-AB-1 Table R2 – Configuration Monitoring | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **protected cyber assets** | Monitor at least once every 35 **days** for changes to the baseline configuration (as described in requirement R1, part 1.1). Document and investigate detected unauthorized changes. | An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected. |

**R3.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R3– Vulnerability Assessments*.

**M3.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-010-AB-1 Table R3 – Vulnerability Assessments | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | At least once every 15 **months**, conduct a paper or active vulnerability assessment. | Examples of evidence may include, but are not limited to:<br>• a document listing the date of the assessment (performed at least once every 15 **months**), the controls assessed for each **BES cyber system** along with the method of assessment; or<br>• a document listing the date of the assessment and the output of any tools used to perform the assessment. |

| CIP-010-AB-1 Table R3 – Vulnerability Assessments | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.2 | High Impact **BES cyber systems** | Where technically feasible, at least once every 36 **months**:<br>3.2.1 perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the **BES cyber system** in a production environment; and<br>3.2.2 document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. | An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 **months**), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. |
| 3.3 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **protected cyber assets** | Prior to adding a new applicable **cyber asset** to a production environment, perform an active vulnerability assessment of the new **cyber asset**, except for **CIP exceptional circumstances** and like replacements of the same type of **cyber asset** with a baseline configuration that models an existing baseline configuration of the previous or other existing **cyber asset**. | An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new **cyber asset**) and the output of any tools used to perform the assessment. |
| 3.4 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access** | Document the results of the assessments conducted according to parts 3.1, 3.2, and 3.3 and the action plan to | An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a |

| CIP-010-AB-1 Table R3 – Vulnerability Assessments | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | **control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**;<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items. | list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items). |

## Revision History

| Date | Description |
|---|---|
| 2017-10-01 | Initial release. |

# Alberta Reliability Standard
# Cyber Security – Information Protection
# CIP-011-AB-1

## A. Introduction

1. Title: Cyber Security – Information Protection
2. Number: CIP-011-AB-1
3. Purpose: To prevent unauthorized access to **BES cyber system information** by specifying information protection requirements in support of protecting **BES cyber systems** against compromise that could lead to misoperation or instability in the **bulk electric system**.
4. Applicability:

4.1. For the purpose of the requirements contained herein, the following list of entities will be collectively referred to as "Responsible Entities". For requirements in this **reliability standard** where a specific entity or subset of entities are the applicable entity or entities, the entity or entities are specified explicitly.

4.1.1. [Intentionally left blank.]

4.1.2. a **legal owner** of an **electric distribution system** that owns one or more of the following facilities, systems, and equipment for the protection or restoration of the **bulk electric system**:

4.1.2.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.1.2.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.1.2.1.2. performs automatic load shedding under a common control system owned by the entity in subsection 4.1.2., without human operator initiation, of 300 MW or more;

4.1.2.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.1.2.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.1.2.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.1.3. the **operator** of a **generating unit** and the **operator** of an **aggregated generating facility**;

4.1.4. the **legal owner** of a **generating unit** and the **legal owner** of an **aggregated generating facility**;

4.1.5. [Intentionally left blank.]

4.1.6. [Intentionally left blank.]

4.1.7. the **operator** of a **transmission facility**;

4.1.8. the **legal owner** of a **transmission facility**; and

4.1.9. the **ISO**.

4.2. For the purpose of the requirements contained herein, the following facilities, systems, and equipment owned by each Responsible Entity in subsection 4.1 above are those to which these requirements are applicable. For requirements in this **reliability standard** where a specific type of facilities, system, or equipment or subset of facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. One or more of the following facilities, systems and equipment that operate at, or control elements that operate at, a nominal voltage of 25 kV or less and are owned by a **legal owner** of an **electric distribution system** or a **legal owner** of a **transmission facility** for the protection or restoration of the **bulk electric system**:

4.2.1.1. each **underfrequency load shedding** or **under voltage load shed** system that:

4.2.1.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.2.1.1.2. performs automatic load shedding under a common control system owned by one or more of the entities in subsection 4.2.1, without human operator initiation, of 300 MW or more;

4.2.1.2. each **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**;

4.2.1.3. each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to transmission where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.2.1.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.2.2. Responsible Entities listed in subsection 4.1 other than a **legal owner** of an **electric distribution system** are responsible for:

4.2.2.1. each **transmission facility** that is part of the **bulk electric system** except each **transmission facility** that:

4.2.2.1.1. is a transformer with fewer than 2 windings at 100 kV or higher and does not connect a contracted **blackstart resource**;

4.2.2.1.2. radially connects only to load;

4.2.2.1.3. radially connects only to one or more **generating units** or **aggregated generating facilities** with a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**; or

4.2.2.1.4. radially connects to load and one or more **generating units** or **aggregated generating facilities** that have a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart**

**resource**;

4.2.2.2. a **reactive power** resource that is dedicated to supplying or absorbing **reactive power** that is connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, except those **reactive power** resources operated by an end-use customer for its own use;

4.2.2.3. a **generating unit** that is:

4.2.2.3.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW unless the **generating unit** is part of an industrial complex;

4.2.2.3.2. within a power plant which:

4.2.2.3.2.1. is not part of an **aggregated generating facility**;

4.2.2.3.2.2. is directly connected to the **bulk electric system**; and

4.2.2.3.2.3. has a combined **maximum authorized real power** rating greater than 67.5 MW unless the power plant is part of an industrial complex;

4.2.2.3.3. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.3.4. a contracted **blackstart resource**;

4.2.2.4. an **aggregated generating facility** that is:

4.2.2.4.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW unless the **aggregated generating facility** is part of an industrial complex;

4.2.2.4.2. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.4.3. a contracted **blackstart resource**;

and

4.2.2.5. **control centres** and backup **control centres**.

4.2.3. The following are exempt from this **reliability standard**:

4.2.3.1. [Intentionally left blank.]

4.2.3.2. **cyber assets** associated with communication networks and data communication links between discrete **electronic security perimeters**.

4.2.3.3. [Intentionally left blank.]

4.2.3.4. for the **legal owner** of an **electric distribution system**, the systems and equipment that are not included in subsection 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no **BES cyber systems** categorized as High Impact or Medium Impact according to the CIP-002-AB-5.1 identification and categorization processes.

5. [Intentionally left blank.]
6. [Intentionally left blank.]

## B. Requirements and Measures

**R1.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-AB-1 Table R1 – Information Protection*.

**M1.** Evidence for the information protection program must include the applicable requirement parts in *CIP-011-AB-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| **CIP-011-AB-1 Table R1 – Information Protection** | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems** | Method(s) to identify information that meets the definition of **BES cyber system information**. | Examples of acceptable evidence include, but are not limited to:<br>• documented method to identify **BES cyber system information** from entity's information protection program; or<br>• indications on information (e.g., labels or classification) that identify **BES cyber system information** as designated in the entity's information protection program; or<br>• training materials that provide personnel with sufficient knowledge to recognize **BES cyber system information**; or<br>• repository or electronic and physical location designated for housing **BES cyber system information** in the entity's information protection program. |
| 1.2 | High Impact **BES cyber** | Procedure(s) for protecting | Examples of acceptable |

| CIP-011-AB-1 Table R1 – Information Protection | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | **systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems** | and securely handling **BES cyber system information**, including storage, transit, and use. | evidence include, but are not limited to:<br>• procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of **BES cyber system information**; or<br>• records indicating that **BES cyber system information** is handled in a manner consistent with the entity's documented procedure(s). |

**R2.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-011-AB-1 Table R2 – BES Cyber Asset Reuse and Disposal*.

**M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-AB-1 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-011-AB-1 Table R2 – BES Cyber Asset Reuse and Disposal | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.1 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and | Prior to the release for reuse of applicable **cyber assets** that contain **BES cyber system information** (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of **BES cyber system information** from the **cyber asset** data storage media. | Examples of acceptable evidence include, but are not limited to:<br>• records tracking sanitization actions taken to prevent unauthorized retrieval of **BES cyber system information** such as clearing, purging, or destroying; or<br>• records tracking actions such as encrypting, retaining in the **physical security perimeter** or |

| CIP-011-AB-1 Table R2 – BES Cyber Asset Reuse and Disposal | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | 2. **physical access control systems**; and<br>3. **protected cyber assets** | | other methods used to prevent unauthorized retrieval of **BES cyber system information**. |
| 2.2 | High Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems**; and<br>3. **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>1. **electronic access control or monitoring systems**; and<br>2. **physical access control systems**; and<br>3. **protected cyber assets** | Prior to the disposal of applicable **cyber assets** that contain **BES cyber system information**, the Responsible Entity shall take action to prevent the unauthorized retrieval of **BES cyber system information** from the **cyber asset** or destroy the data storage media. | Examples of acceptable evidence include, but are not limited to:<br>• records that indicate that data storage media was destroyed prior to the disposal of an applicable **cyber asset**; or<br>• records of actions taken to prevent unauthorized retrieval of **BES cyber system information** prior to the disposal of an applicable **cyber asset**. |

## Revision History

| Date | Description |
|---|---|
| 2017-10-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to protect the confidentiality and integrity of real-time assessment and real-time monitoring data transmitted between **control centres.**

## 2. Applicability

This **reliability standard** applies to the following entities, referred to as "Responsible Entities":

(a) the **operator** of a **generating unit**;

(b) the **legal owner** of a **generating unit**;

(c) the **operator** of an **aggregated generating facility**;

(d) the **legal owner** of an **aggregated generating facility**;

(e) the **operator** of a **transmission facility**;

(f) the **legal owner** of a **transmission facility**; and

(g) the **ISO**,

that own or operate a **control centre**.

Exemptions: The following are exempt from this **reliability standard**:

(a) **cyber assets** at facilities regulated by the Canadian Nuclear Safety Commission; and

(b) a **control centre** that transmits to another **control centre** real-time assessment or real-time monitoring data pertaining only to the generating resource, transmission station, or substation co-located with the transmitting **control centre.**

## 3. Requirements

**R1** Each Responsible Entity must implement, except under **CIP exceptional circumstances**, one or more documented plans to mitigate the risks posed by unauthorized disclosure and unauthorized modification of real-time assessment and real-time monitoring data while being transmitted between any applicable **control centres.** The Responsible Entity is not required to include oral communications in its plan. The plan must include:

**R1.1** identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of real-time assessment and real-time monitoring data while being transmitted between **control centres**;

**R1.2** identification of where the Responsible Entity applied security protection for transmitting real-time assessment and real-time monitoring data between **control centres**; and

**R1.3** if the **control centres** are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of real-time assessment and real-time monitoring data between those **control centres**.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of implementing one or more documented plans and including the required elements of the plan as required in requirement R1 exists. Evidence may include documentation demonstrating the implementation of the plan and a documented plan, or other equivalent evidence.

## 5. Appendices

Appendix 1 – *Implementation Plan*

### Revision History

| Date | Description |
|---|---|
| 2022-07-01 | Initial release. |

## Appendix 1 – Implementation Plan

### 1. Purpose

The purpose of this appendix is to set the effective dates and the implementation timelines for **reliability standard** CIP-012-AB-1, *Cyber Security – Communications between Control Centres* ("CIP-012-AB-1").

### 2. Compliance with Reliability Standards

The Responsible Entities identified in section 2 of this **reliability standard** must comply with the requirements of CIP-012-AB-1 in accordance with the implementation schedule.

### 3. Effective Date

CIP-012-AB-1 will become effective on July 1, 2022. Responsible Entities must follow the phased implementation plan set out in sections 4 and 5 below.

### 4. Implementation Plan for the ISO

(a) Where the **ISO** has communications with a **control centre** external to Alberta the **ISO** must be compliant with requirement R1 of CIP-012-AB-1 on July 1, 2022.

(b) Where the **ISO** has communications with a **control centre** internal to Alberta the **ISO** must be compliant with requirement R1 of CIP-012-AB-1 on July 1, 2023.

### 5. Implementation Plan for all Responsible Entities, Excluding the ISO

All Responsible Entities listed in section 2 of this **reliability standard**, excluding the **ISO**, must be compliant with requirement R1 of CIP-012-AB-1 on July 1, 2023.

# Alberta Reliability Standard
# Physical Security
# CIP-014-AB-2

## 1. Purpose

The purpose of this **reliability standard** is to identify and protect transmission substations and their associated primary **control centres**, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or **cascading** within an **Interconnection.**

## 2. Applicability

This **reliability standard** applies to:

(a) the **legal owner** of a **transmission facility** that the **ISO** notifies pursuant to requirement R2;

(b) the **operator** of a **transmission facility** that the **legal owner** of a **transmission facility** notifies pursuant to requirement R3; and

(c) the **ISO**.

## 3. Requirements

**R1** The **ISO** must perform an initial risk assessment and subsequent risk assessments of existing transmission substations and those planned to be in service within 24 **months** that meet any of the following criteria:

(i) **transmission facilities** operated at 500 kV or higher;

(ii) **transmission facilities** that are operating between 200 kV and 499 kV at a single substation, where the substation is connected at 200 kV or higher voltages to 3 or more other substations and has an aggregate weighted value exceeding 3000 according to the table below, with the "aggregate weighted value" for a substation determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing **bulk electric system** transmission line that is connected to another transmission substation:

| Voltage Value of a Line | Weight Value per Line |
|---|---|
| 200 kV to 299 kV | 700 |
| 300 kV to 499 kV | 1300 |

(iii) **transmission facilities** at a single substation location that are critical to the derivation of **interconnection reliability operating limits** and their associated contingencies;

and those risk assessments must consist of a transmission analysis or transmission analyses designed to identify those transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or **cascading**.

**R1.1** The **ISO** must perform subsequent risk assessments at least once every 30 **months** on a rolling basis.

**R1.2** Intentionally left blank

**R2** The **ISO** must notify the **legal owner** of a **transmission facility** of the transmission substations identified through the application of requirement R1 within 30 **days** following the completed requirement R1 risk assessment.

**R2.1** The **ISO** must, if a transmission substation previously identified under requirement R1 is removed from the identification during a subsequent risk assessment performed according to requirement R1, within 30 **days** following the subsequent risk assessment, notify the **legal owner** of a **transmission facility** of the removal.

**R3** The **legal owner** of a **transmission facility** must,

(a) if a transmission substation is identified under requirement R1; and

(b) if the **legal owner** of a **transmission facility** does not operate the transmission substation; then

within 7 **days** following the notification under requirement R2, provide notification of the identification to the **operator** of a **transmission facility** that has operational control of the associated primary **control centre**.

**R3.1** The **legal owner** of a **transmission facility** must,

(a) if a transmission substation previously identified under requirement R1 is removed from the identification during a subsequent risk assessment performed according to requirement R1; and

(b) if the **legal owner** of a **transmission facility** does not operate the transmission substation; then

within 7 **days** following the notification under requirement R2.1, provide notification of the removal to the **operator** of a **transmission facility** that has operational control of the associated primary **control centre**.

**R4** Each of:

(a) the **legal owner** of a **transmission facility** with a transmission substation identified in the notification provided under requirement R2;

(b) the **operator** of a **transmission facility** with a primary **control centre** that controls any of the substations identified in the notification provided under requirement R3; and

(c) the **ISO** in respect of its primary **control centre**;

must conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of those respective facilities, which evaluation must consider the following:

**R4.1** unique characteristics of the identified transmission substations and primary **control centres**;

**R4.2** prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

**R4.3** intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization, the Electricity Information Sharing and Analysis Center, U.S. federal governmental agencies, Canadian governmental agencies, or their successors.

**R5** Each of the **legal owner** of a **transmission facility** with a transmission substation identified in accordance with requirement R2, the **operator** of a **transmission facility** with a primary **control centre** that controls any of the substations identified in the notification provided under requirement R3, and the **ISO** in respect of its primary **control centre**, must:

(a) develop and implement one or more documented physical security plans that covers any respective transmission substations, and primary **control centre**;

(b) develop such physical security plans:

(i) within 180 **days** following the applicable notifications received in accordance with requirement R2 or requirement R3; or

(ii) for the **ISO**'s primary **control centre**, within 180 **days** of the effective date of this **reliability standard**; and

(c) implement such physical security plans according to the timeline specified in the physical security plans.

**R5.1** Each physical security plan must include the following attributes:

**R5.1.1** resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in requirement R4;

**R5.1.2** law enforcement contact and coordination information;

**R5.1.3** a timeline for executing the physical security enhancements and modifications specified in the physical security plan; and

**R5.1.4** provisions to evaluate evolving physical threats, and their corresponding security measures, to each transmission substations, or primary **control centres**.

**R6** Each of:

(a) the **legal owner** of a **transmission facility** with a transmission substation identified in accordance with requirement R2;

(b) the **operator** of a **transmission facility** with a primary **control centre** that controls any of the substations identified in the notification provided under requirement R3; and

(c) the **ISO** in respect of its primary control centre,

must have an unaffiliated third party review the evaluation performed under requirement R4 and any security plans developed under requirement R5.

**R6.1** Each **legal owner** of a **transmission facility**, **operator** of a **transmission facility**, and the **ISO** must select an unaffiliated third party reviewer from the following:

(a) an entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional or Physical Security Professional certification;

(b) an entity or organization approved by the **NERC**;

(c) a governmental agency with physical security expertise; or

(d) an entity or organization with demonstrated law enforcement, government, or military physical security expertise.

**R6.2** Each of the **legal owner** of a **transmission facility**, the **operator** of a **transmission facility**, and the **ISO** must ensure that the unaffiliated third party review is completed within 90 **days** of completing the security plans developed in requirement R5.

**R6.3** Each of the **legal owner** of a **transmission facility**, the **operator** of a **transmission facility,** and the **ISO** must, if the unaffiliated third party reviewer recommends changes to the evaluation performed under requirement R4 or any security plans developed under requirement R5 and within 60 **days** of the completion of the unaffiliated third party review, for each recommendation:

(a) modify its evaluation or security plans consistent with the recommendation; or

(b) document the reasons for not modifying the evaluation or security plans consistent with the recommendation.

**R6.4** Each of the **legal owner** of a **transmission facility**, the **operator** of a **transmission facility,** and the **ISO** must implement procedures for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this **reliability standard** from public disclosure.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of performing an initial risk assessment and subsequent risk assessments as required in requirement R1 exists. Evidence may include dated written or electronic documentation of the risk assessment of the transmission substations, or other equivalent evidence.

**MR1.1** Evidence of performing subsequent risk assessments as required in requirement R1.1 exists. Evidence may include dated written or electronic documentation of the subsequent risk assessments, or other equivalent evidence.

**MR2** Evidence of notifying the **legal owner** of a **transmission facility** of the transmission substations identified through the application of requirements R1 as required in requirement R2. Evidence may include dated emails or other equivalent evidence.

**MR2.1** Evidence of notifying the **legal owner** of a **transmission facility** of the transmission substations removed through the application of requirements R1 as required in requirement R2. Evidence may include dated emails or other equivalent evidence.

**MR3** Evidence of notifying the **operator** of the **transmission facility** of the transmission substations identified through the application of requirements R1 as required in requirement R3 exists. Evidence may include dated written or electronic notifications or communications, or other equivalent evidence.

**MR3.1** Evidence of notifying the **operator** of the **transmission facility** of the transmission substations removed through the application of requirements R1 as required in requirement R3.1 exists. Evidence may include dated written or electronic notifications or communications, or other equivalent evidence.

**MR4** Evidence of conducting an evaluation of the potential threats and vulnerabilities of a physical attack as required in requirement R4 exists. Evidence may include dated written or electronic documentation that each of the **legal owner** of a **transmission facility**, the **operator** of a **transmission facility**, and the **ISO** conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective transmission stations, transmission substations and primary **control centres**, or other equivalent evidence.

**MR5** Evidence of developing and implementing one or more documented physical security plans as required in requirement R5 exists. Evidence may include dated written or electronic documentation of its physical security plans that covers their respective identified and verified transmission substations, and primary **control centres**, and additional evidence demonstrating execution of the physical security plan according to the timeline specified in the physical security plan, or other equivalent evidence.

**MR6** Evidence of having an unaffiliated third party review the evaluation performed as required in requirement R6 exists. Evidence may include written or electronic documentation demonstrating that each of the **legal owner** of a **transmission facility**, **operator** of a **transmission facility**, and the **ISO** had an unaffiliated third party review the evaluation performed under requirement R4 and any security plans developed under requirement R5, or other equivalent evidence.

**MR6.1** Evidence of selecting an unaffiliated third party reviewer as required in requirement R6.1 exists. Evidence may include documentation demonstrating the selection of an unaffiliated third party reviewer and a statutory declaration confirming that the third party is unaffiliated, or other equivalent evidence.

**MR6.2** Evidence of ensuring that the unaffiliated third party review is completed as required in requirement R6.2 exists. Evidence may include a dated documented review performed by the unaffiliated third party, or other equivalent evidence.

**MR6.3** Evidence of modifying, or documenting the reasons for not modifying, the evaluation or security plans as required in requirement R6.3 exists. Evidence may include a modified evaluation or security plans, or documented reasons for not modifying the evaluation or security plans in accordance with the recommended change, or other equivalent evidence.

**MR6.4** Evidence of implementing procedures as required in requirement R6.4 exists. Evidence may include written or electronic documentation of procedures to protect information, such as a non-disclosure agreement, or other equivalent evidence.

## 5. Implementation Plan

Each of the **legal owner** of a **transmission facility**, the **operator** of a **transmission facility**, and the **ISO** must implement requirement R1 through requirement R6 in accordance with the implementation plan in Appendix 1.

## 6. Appendices

Appendix 1 – *Implementation plan effective dates*

## Revision History

| Date | Description |
|---|---|
| 2020-07-01 | Initial release. |

**Appendix 1**
**Effective Dates:**

1. CIP-014-AB-2 becomes effective on the first **day** of the calendar quarter (January 1, April 1, July 1 or October 1) that follows 6 full calendar quarters after approval by the **Commission**.

2. The initial risk assessment required by CIP-014-AB-2, requirement R1, must be completed on or before the effective date of this **reliability standard**.

3. The initial performance of CIP-014-AB-2, requirements R2 and R2.1 must be completed within 30 **days** of the effective date of this **reliability standard**.

# Alberta Reliability Standard
# Cyber Security – Implementation Plan for Version 5 CIP Security Standards
# CIP-PLAN-AB-1

## 1. Purpose

The purpose of this **reliability standard** is to set the effective dates for the Version 5 CIP Cyber Security **reliability standards** and describe compliance timelines for planned and unplanned changes that result in a higher categorization for a **BES cyber system**.

## 2. Applicable Reliability Standards

This **reliability standard** applies to the Version 5 CIP Cyber Security **reliability standards**, which are:

- CIP–002–AB-5.1, *Cyber Security — BES Cyber System Categorization*;
- CIP–003–AB-5, *Cyber Security — Security Management Controls*;
- CIP–004–AB-5.1, *Cyber Security — Personnel and Training*;
- CIP–005–AB-5, *Cyber Security — Electronic Security Perimeter(s)*;
- CIP–006–AB-5, *Cyber Security — Physical Security of BES Cyber Systems*;
- CIP–007–AB-5, *Cyber Security — Systems Security Management*;
- CIP–008–AB-5, *Cyber Security — Incident Reporting and Response Planning*;
- CIP–009–AB-5, *Cyber Security — Recovery Plans for BES Cyber Systems*;
- CIP–010–AB-1, *Cyber Security — Configuration Change Management and Vulnerability Assessments*; and
- CIP–011–AB-1, *Cyber Security — Information Protection*.

## 3. Compliance with Reliability Standards

Once the Version 5 CIP Cyber Security **reliability standards** become effective, the “Responsible Entities” identified in the applicability section of each Version 5 CIP Cyber Security **reliability standard** must comply with the requirements of those **reliability standards**.

## 4. Proposed Effective Date

The Version 5 Cyber Security **reliability standards**, except for requirement R2 of CIP-003-AB-5, become effective on the first **day** of the calendar quarter (January 1, April 1, July 1 or October 1) that follows eight (8) full calendar quarters after approval by the **Commission**. Requirement R2 of CIP-003-AB-5 becomes effective on the first **day** of the calendar quarter (January 1, April 1, July 1 or October 1) that follows twelve (12) full calendar quarters after approval by the **Commission**.

## 5. Initial Performance of Certain Periodic Requirements

Specific Version 5 CIP Cyber Security **reliability standards** have periodic requirements that contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, “. . . at least once every fifteen (15) **months** . . .”, and “Responsible Entities” must comply initially with those periodic requirements as follows:

1. on or before the effective date of the Version 5 CIP Cyber Security **reliability standards** for the following requirements:

- CIP-002-5, requirement R2; and
- CIP-003-5, requirement R1;

2. on or before the Effective Date of CIP-003-5, Requirement R2 for the following requirement:
   - CIP-003-5, requirement R2;
3. within fourteen (14) **days** after the effective date of the Version 5 CIP Cyber Security **reliability standards** for the following requirement:
   - CIP-007-5, requirement R4, Part 4.4;
4. within thirty-five (35) **days** after the effective date of the Version 5 CIP Cyber Security **reliability standards** for the following requirements:
   - CIP-010-1, requirement R2, Part 2.1;
5. within three (3) **months** after the effective date of the Version 5 CIP Cyber Security **reliability standards** for the following requirement:
   - CIP-004-5, requirement R4, Part 4.2;
6. within twelve (12) **months** after the effective date of the Version 5 CIP Cyber Security **reliability standards** for the following requirements:
   - CIP-004-5, requirement R2, Part 2.3;
   - CIP-004-5, requirement R4, Parts 4.3 and 4.4;
   - CIP-006-5, requirement R3, Part 3.1;
   - CIP-008-5, requirement R2, Part 2.1;
   - CIP-009-5, requirement R2, Parts 2.1 and 2.2; and
   - CIP-010-1, requirement R3, Part 3.1; and
7. within twenty-four (24) **months** after the effective date of the Version 5 CIP Cyber Security **reliability standards** for the following requirements:
   - CIP-009-5, requirement R2, Part 2.3; and
   - CIP-010-1, requirement R3, Part 3.2.

## 6. Planned or Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or **BES cyber system** as identified through the annual assessment under CIP-002-AB-5.1, requirement R2, which were planned and implemented by the “Responsible Entity” identified in the applicability section of each Version 5 CIP Cyber Security **reliability standard**.

In contrast, unplanned changes refer to any changes of the electric system or **BES cyber system**, as identified through the annual assessment under CIP-002-AB-5.1, Requirement R2, which were not planned by the “Responsible Entity” identified in the applicability section of each Version 5 CIP Cyber Security **reliability standard**.

For planned changes resulting in a higher categorization, the "Responsible Entity" identified in the applicability section of each Version 5 CIP Cyber Security **reliability standard** shall comply with all applicable requirements in the Version 5 CIP Cyber Security **reliability standards** on the update of the identification and categorization of the affected **BES cyber system** and any applicable and associated **physical access control systems**, **electronic access control or monitoring systems** and **protected cyber assets**, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

For unplanned changes resulting in a higher categorization, the "Responsible Entity" identified in the applicability section of each Version 5 CIP Cyber Security **reliability standard** shall comply with all applicable requirements in the Version 5 CIP Cyber Security **reliability standards**, according to the following timelines, following the identification and categorization of the affected **BES cyber system** and any applicable and associated **physical access control systems**, **electronic access control or monitoring systems** and **protected cyber assets**, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

| Scenario of Unplanned Changes After the Effective Date for Each Version 5 CIP Cyber Security Reliability Standard | Compliance Implementation |
|---|---|
| New High Impact **BES cyber system** | twelve (12) **months** |
| New Medium Impact **BES cyber system** | twelve (12) **months** |
| Newly categorized High Impact **BES cyber system** from Medium Impact **BES cyber system** | twelve (12) **months** for requirements not applicable to Medium Impact **BES Cyber Systems** |
| Newly categorized Medium Impact **BES cyber system** | twelve (12) **months** |
| The "Responsible Entity" identified in the applicability section of each Version 5 CIP Cyber Security **reliability standard** identifies first Medium Impact or High Impact **BES cyber system** (i.e., the "Responsible Entity" identified in the applicability section of each Version 5 CIP Cyber Security **reliability standard** previously had no **BES cyber systems** categorized as High Impact or Medium Impact according to the CIP-002-AB-5.1 identification and categorization processes) | twenty-four (24) **months** |

## Revision History

| Date | Description |
|---|---|
| 2017-10-01 | Initial release. |

# Alberta Reliability Standard
# Telecommunications
# COM-001-AB1-1.1

## 1. Purpose

The purpose of this **reliability standard** is to ensure the **ISO** and each **operator** of a **transmission facility** have adequate and reliable voice and message telecommunication facilities internally and with others for the exchange of **interconnection** and operating information necessary to maintain reliability.

## 2. Applicability

This **reliability standard** applies to the following:

(a) the **operator** of a **transmission facility** that is:

(i) part of the **bulk electric system**; or

(ii) not part of the **bulk electric system** but which the **ISO**:

(A) determines is necessary for the reliable operation of either the **interconnected electric system** or the City of Medicine Hat electric system; and

(B) publishes on the AESO website and may amend from time to time in accordance with the process set out in Appendix 1; and

(b) the **ISO**.

## 3. Requirements

**R1** The **ISO** must, as necessary to maintain reliability, provide adequate, reliable, and, where applicable, diverse and redundant voice and message telecommunication facilities for the exchange of **interconnection** and internal Alberta operating information with the following:

(a) each **operator** of a **transmission facility**;

(b) each adjacent **interconnected transmission operator** directly connected to Alberta;

(c) each adjacent **balancing authority** directly connected to Alberta; and

(d) the adjacent **reliability coordinators**.

**R2** Each **operator** of a **transmission facility** must, as necessary to maintain reliability, provide adequate, reliable, and, where applicable, diversely routed and redundant voice and message telecommunication facilities for the exchange of **interconnection** and Alberta operating information with the following:

(a) each adjacent **operator** of a **transmission facility**;

(b) each adjacent **interconnected transmission operator** that is directly connected to Alberta; and

(c) the **ISO**.

**R3** The **ISO** and each **operator** of a **transmission facility** must manage and test its alternate voice and message telecommunication facilities.

**R4** The **ISO** must provide a means to coordinate voice and message telecommunications with each **operator** of a **transmission facility**, adjacent **interconnected transmission operator**, adjacent

**balancing authority** and adjacent **reliability coordinators**, which coordination must include the ability to investigate and recommend solutions to voice and message telecommunications problems within Alberta.

**R5** Each **operator** of a **transmission facility** must provide a means to coordinate voice and message telecommunications with the **ISO** and adjacent **interconnected transmission operators**, which coordination must include the ability to investigate and recommend solutions to voice and message telecommunications problems within Alberta.

**R6** The **ISO** and each **operator** of a **transmission facility** must use the English language for all communications between their respective operating personnel responsible for the real-time generation control and operation of the **interconnected electric system**.

**R7** The **ISO** and each **operator** of a **transmission facility** must have written operating instructions and procedures to enable continued operation of the **interconnected electric system** during the loss of voice and message telecommunications facilities.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for R1.

**MR1** Evidence of providing voice and message telecommunication facilities as required in requirement R1 exists. Evidence may include:

(a) a list identifying each telecommunication facility for the exchange of **interconnection** and Alberta operating information; and

(b) documentation demonstrating the implementation of diverse routing and redundancy capability.

**MR2** Evidence of providing voice and message telecommunication facilities as required in requirement R2 exists. Evidence may include:

(a) a list identifying each telecommunication facility for the exchange of **interconnection** and Alberta operating information; and

(b) documentation demonstrating the implementation of diverse routing and redundancy capability, if applicable.

**MR3** Evidence of managing and testing its alternate voice and message telecommunication facilities as required in requirement R3 exists. Evidence may include:

(a) a list identifying each telecommunication facility as determined to be alternate;

(b) documented procedures describing how to manage and test its alternate telecommunication facilities; and

(c) records of testing.

**MR4** Evidence of providing a means to coordinate voice and message telecommunications as required in requirement R4 exists. Evidence may include a documented procedure in place which identifies a process for coordinating telecommunications and a process for investigating and recommending solutions to telecommunications problems.

**MR5** Evidence of providing a means to coordinate voice and message telecommunications as required in requirement R5 exists. Evidence may include a documented procedure in place which identifies a process for coordinating telecommunications and a process for investigating and recommending solutions to telecommunications problems.

**MR6** Evidence of using the English language as required in requirement R6 exists. Evidence may include **operator** logs, voice recordings, electronic communications or **e-tag** records.

**MR7** Evidence of having written operating instructions and procedures as required in requirement R7 exists. Evidence may include electronic or hard copy of the operating instructions and procedures.

## 5. Appendices

Appendix 1 – *Amending Process for List of Facilities*

### Revision History

| Effective | Description |
|---|---|
| 2013-10-01 | Initial Release |
| 2015-05-01 | Revised for ISO assumption of RC functionality for the Alberta footprint |

## Appendix 1
## Amending Process for List of Facilities

In order to amend the list referenced in subsections (a)(ii)(B) of section 2, *Applicability*, the **ISO** must:

(a) upon determining that a **transmission facility** is to be added, notify the **operator** in writing and determine an effective date, which must be no less than thirty (30) **days** after the date of notice, for the **operator** to meet the applicable requirements;

(b) upon determining that a **transmission facility** is to be deleted, notify the **operator** in writing and determine an effective date for the **operator** to no longer be required to meet the applicable requirements; and

(c) publish the amended list with effective dates on the AESO website.

## 1. Purpose

The purpose of this **reliability standard** is to ensure the **ISO** and entities subject to this **reliability standard** have adequate communications and that these communications capabilities are staffed and available for addressing a real-time emergency condition, and to ensure communications by operating personnel are effective.

## 2. Applicability

This **reliability standard** applies to:

(a) the **operator** of a **generating unit** that is:

(i) directly connected to the **transmission system** or to **transmission facilities** within the City of Medicine Hat; and

(ii) not part of an **aggregated generating facility**;

(b) the **operator** of an **aggregated generating facility** that is directly connected to the **transmission system** or to **transmission facilities** within the City of Medicine Hat;

(c) the **operator** of a **transmission facility**; and

(d) the **ISO**.

## 3. Requirements

**R1** The **ISO** must have voice and data communication facilities with:

(a) each **operator** of a **transmission facility**;

(b) each adjacent **interconnected transmission operator** directly connected to Alberta; and

(c) each **adjacent balancing authority** directly connected to Alberta;

**R2** The **operator** of a **transmission facility** must have voice and data communication facilities with:

(a) each adjacent **operator** of a **transmission facility**;

(b) each adjacent **interconnected transmission operator** directly connected to Alberta; and

(c) the **ISO**.

**R3** Each **operator** of a **generating unit** and each **operator** of an **aggregated generating facility** must have voice and data communication facilities with:

(a) each **operator** of a **transmission facility** to which it is directly connected; and

(b) the **ISO**.

**R4** The **ISO**, each **operator** of a **transmission facility**, each **operator** of an **aggregated generating facility** and each **operator** of a **generating unit** must have personnel available for all hours of the **day**, seven (7) **days** a week, to receive and respond to any voice or data communication regarding a real-time **system emergency** condition via the communication facilities as identified in requirements R1 through R3.

**R5** The **ISO** must notify all potentially affected adjacent **interconnected transmission operators** and **adjacent balancing authorities** through predetermined communication paths:

(a) of any threat to the **reliability** of the **interconnected electric system**; or

(b) if the **ISO** anticipates shedding **firm load**.

**R6** The **ISO** must, when issuing a verbal **directive**, do so in a clear, concise and definitive manner, identify the instruction as a **directive**, and:

(a) if the recipient of the **directive** does not respond by repeating the information in the **directive**, then the **ISO** must request the recipient to repeat the information in the **directive**;

(b) if the information in the response is not correct, the **ISO** must repeat the **directive** to resolve any misunderstandings; and

(c) if the information is repeated correctly, the **ISO** must acknowledge this to the recipient.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for R1.

**MR1** Evidence of having voice and data communication facilities as required in requirement R1 exists. Evidence may include a list of communication facilities or other equivalent evidence that confirms that the communications have been provided.

**MR2** Evidence of having voice and data communications as required in requirement R2 exists. Evidence may include a list of communication facilities or other equivalent evidence that confirms that the communications have been provided.

**MR3** Evidence of having voice and data communications as required in requirement R3 exists. Evidence may include a list of communication facilities or other equivalent evidence that confirms that the communications have been provided.

**MR4** Evidence of having personnel available as required in requirement R4 exists. Evidence may include **operator** logs, timesheets, on-call lists or shift schedules.

**MR5** Evidence of notifying entities as required in requirement R5 exists. Evidence may include **operator** logs or voice recordings.

**MR6** Evidence of issuing verbal **directives** as required in requirement R6 exists. Evidence may include voice recordings or **operator** logs.

## Revision History

| Effective | Description |
|---|---|
| 2013-10-01 | Initial release |
| 2014-01-01 | Administrative update to standardize formatting, definitions and drafting style.<br>Removed references to the WECC Reliability Coordinator. |

# Alberta Reliability Standard
# Event Reporting
# EOP-004-AB-2

## 1. Purpose

The purpose of this **reliability standard** is to improve the reliability of the **bulk electric system** by requiring the reporting of events by the **ISO**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must have an event reporting operating plan to report the events identified in Appendix 1 to the **NERC** and other organizations, as appropriate.

**R2** The **ISO** must, upon recognition of a reportable event identified in Appendix 1, report the event in accordance with its event reporting operating plan as soon as practicable, but no more than five (5) **business days** following such recognition.

**R3** The **ISO** must validate all contact information contained in its event reporting operating plan each calendar year.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of having an event reporting operating plan as required in requirement R1 exists. Evidence may include, but is not limited to, an event reporting operating plan for the events identified in Appendix 1.

**MR2** Evidence of reporting events as required in requirement R2 exists. Evidence may include, but is not limited to, a copy of the completed report, operator logs, voice recordings, electronic communications, or other equivalent evidence.

**MR3** Evidence of validating all contact information contained in the event reporting operating plan as required in requirement R3 exists. Evidence may include, but is not limited to, dated records showing contact information, electronic communications or other equivalent evidence.

## 5. Appendices

Appendix 1 – *Reportable Events*

### Revision History

| Date | Description |
|---|---|
| 2016-08-30 | Initial release. |

## Appendix 1

## Reportable Events

The following are the reportable events to be contained in the **ISO**’s event reporting operating plan, as described in requirement R1:

1. a physical threat to a **control centre** of the **ISO**, excluding a weather or natural disaster related threat, which has the potential to degrade the normal operation of a **control centre** of the **ISO**;
2. a suspicious device or activity at a **control centre** of the **ISO**;
3. a situation on the **bulk electric system** requiring a public appeal for load reduction;
4. a situation on the **bulk electric system** requiring a system-wide voltage reduction greater than or equal to 3%;
5. a situation on the **bulk electric system** requiring manual firm load shedding greater than or equal to 100 MW;
6. exceeding an **interconnection reliability operating limit** within the **interconnected electric system** for an amount of time that is greater than **interconnection reliability operating limit Tv**, or exceeding a **system operating limit** for a major transmission path identified in the table “Major WECC Transfer Paths in the Bulk Electric System”, as provided by the **WECC**, for more than thirty (30) minutes;
7. a loss of firm load greater than or equal to 300 MW for fifteen (15) minutes or more;
8. an unintended **transmission system** separation within the **interconnected electric system** that results in an island of greater than or equal to 100 MW, excluding an island created by the loss of:
   a) a **transmission system** radial connection;
   b) non-**transmission system** facilities (distribution level); or
   c) the **interconnection**;
9. total generation loss, within one (1) minute, of greater than or equal to 2000 MW;
10. an unplanned evacuation of the **control centre** of the **ISO** for thirty (30) continuous minutes or more;
11. a complete loss, for thirty (30) continuous minutes or more, of voice communication systems for the **control centre** of the **ISO**; or
12. a complete loss of monitoring capability affecting the **control centre** of the **ISO** for thirty (30) continuous minutes or more that renders analysis capability, such as state estimator or contingency analysis, inoperable.

# Alberta Reliability Standard
# System Restoration from Blackstart Resources
# EOP-005-AB-2

## 1. Purpose

The purpose of this **reliability standard** is to ensure plans, facilities, and personnel are prepared to enable restoration of the **interconnected electric system** starting from **blackstart resources**, to ensure **reliability** is maintained during restoration, and priority is placed on restoring the **interconnected electric system** and the **interconnection** in accordance with the **ISO**'s restoration plan.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**;

(b) the **operator** of a **transmission facility** that the **ISO** includes in its restoration plan and in a list published on the AESO website that the **ISO** may amend from time to time in accordance with the process set out in Appendix 1;

(c) the **operator** of a **generating unit** that:

(i) is not part of an **aggregated generating facility**;

(ii) has a **maximum authorized real power** rating greater than 18 MW; and

(iii) is directly connected to either the **transmission system** or to **transmission facilities** within the City of Medicine Hat; and

(d) the **operator** of an **electric distribution system** that is identified in the restoration plan of an **operator** of a **transmission facility**.

## 3. Requirements

**R1** Each **operator** of a **transmission facility** must have a restoration plan approved by the **ISO** that allows for the restoration of the **transmission facilities** that it operates to a state whereby the choice of the next load to be restored is not driven by the need to control frequency or voltage, regardless of where the **blackstart resource** is located, following a **disturbance** in which:

(a) one or more areas of the **interconnected electric system** shuts down; and

(b) the use of **blackstart resources** is required to restore the shut-down area(s) to service.

The restoration plan must include:

**R1.1** Strategies for system restoration that are coordinated with the **ISO**'s restoration plan.

**R1.2** Intentionally left blank.

**R1.3** Procedures for restoring:

(a) connections with other **operators** of **transmission facilities**; and

(b) **interconnections** with any adjacent **interconnected transmission operators** under the direction of the **ISO**.

**R1.4** The characteristics of each **blackstart resource** that is connected to the **transmission facilities** of the **operator** of a **transmission facility**, including but not limited to the:

(a) name;

(b) location;

(c) megawatt and megavar capacity; and

(d) type of **generating unit**.

**R1.5** The identification of the initial switching requirements for any facilities, operated by the **operator** of a **transmission facility**, that are a part of the **cranking paths** identified in the **ISO**'s restoration plan.

**R1.6** Acceptable operating voltage and frequency limits during restoration.

**R1.7** Operating processes to reestablish connections between the **transmission facilities** of the **operator** of a **transmission facility** for areas that have been restored and are prepared for reconnection.

**R1.8** Operating processes to restore loads required to restore the **interconnected electric system**, such as:

(a) station service for substations;

(b) **generating units** to be restarted or stabilized; and

(c) load needed to stabilize generation and frequency, and to provide voltage control.

**R1.9** Operating processes for accepting authority from and transferring authority back to the **ISO** in accordance with the **ISO**'s restoration plan.

**R2** In the event of changes to the roles and specific tasks of entities identified in a restoration plan:

(a) the **ISO** must provide the affected entities identified in its restoration plan with a description of any changes to their roles and specific tasks prior to the effective date of the plan; and

(b) each **operator** of a **transmission facility** must provide the affected entities identified in its approved restoration plan with a description of their roles and any changes to their roles and specific tasks prior to the effective date of the plan.

**R3** Each **operator** of a **transmission facility** must within sixty (60) **days**, or another time period agreed to by the **ISO,** after receiving an updated copy of the **ISO**'s restoration plan:

(a) review its restoration plan;

(b) align its restoration plan, as necessary, with the **ISO**'s restoration plan; and

(c) submit its plan to the **ISO** for approval.

**R3.1** The **operator** of a **transmission facility** must, where the **ISO** disapproves a restoration plan submitted pursuant to requirement R3(c), resolve the issues described in the reasons provided by the **ISO** within a timeframe agreed to by the **ISO**.

**R4** Each **operator** of a **transmission facility** must update and submit its revised restoration plan to the **ISO** for approval:

(a) within ninety (90) **days** after identifying an unplanned permanent **interconnected electric system** modification; and

(b) no less than ninety (90) **days** prior to implementing a planned **interconnected electric system** modification

that would change the implementation of its restoration plan.

**R4.1** The **operator** of a **transmission facility** must, where the **ISO** disapproves a revised restoration plan submitted pursuant to requirement R4, resolve the issues described in the reasons provided by the **ISO** within a timeframe agreed to by the **ISO**.

**R5** Each **operator** of a **transmission facility** must have a copy of its current **ISO** approved restoration plan within its primary and backup control rooms for the purpose of ensuring it is available to its real time operating personnel.

**R5.1** Each **operator** of a **transmission facility** must provide a copy of its current **ISO** approved restoration plan to each **operator** of an **electric distribution system** identified in that plan.

**R6** The **ISO** must verify through analysis of actual events, steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This must be completed every five (5) years at a minimum. Such analysis, simulations or testing must verify:

**R6.1** the capability of **blackstart resources** to meet the **real power** and **reactive power** requirements of the **cranking paths** and the dynamic capability to supply initial loads;

**R6.2** the location and magnitude of loads required to control voltages and frequency within acceptable operating limits; and

**R6.3** the capability of **generating units** required to control voltages and frequency within acceptable operating limits.

**R7** Each affected **operator** of a **transmission facility** must, following a **disturbance** in which one or more areas of the **interconnected electric system** shuts down and the use of **blackstart resources** is required to restore the shut-down area to service, implement its restoration plan. If the restoration plan cannot be executed as expected, the **operator** of a **transmission facility** must use the strategies for system restoration referred to in requirement R1.1 to facilitate restoration.

**R8** Each affected **operator** of a **transmission facility** must, following a **disturbance** in which one or more areas of the **interconnected electric system** shuts down and the use of **blackstart resources** is required to restore the shut-down area to service, resynchronize these areas with each applicable:

(a) neighbouring **operator** of a **transmission facility**'s area; and

(b) **interconnected transmission operator**'s area,

but only with the prior authorization of the **ISO** and in accordance with the procedures included in the **ISO**'s restoration plan.

**R9** The **ISO** must have **blackstart resource** testing requirements to verify that each **blackstart resource** is capable of meeting the requirements of the **ISO**'s restoration plan. These **blackstart resource** testing requirements must include:

**R9.1** The frequency of testing such that each **blackstart resource** is tested at least once every three (3) calendar years.

**R9.2** A list of required tests including:

(a) a test to verify the ability of the **blackstart resource** to:

(i) start the **generating unit(s)** associated with the **blackstart resource** when isolated with no support from the **interconnected electric system**; or

(ii) remain energized without connection to the remainder of the **interconnected electric system**, if designed to do so; and

(b) upon completion of (a), a test to verify the ability of the **generating unit(s)** associated with the **blackstart resource** to energize a bus. If it is not possible to energize a bus during the test, the testing entity must otherwise demonstrate that the **generating unit(s)** associated with the **blackstart resource** has the capability to energize a bus.

**R9.3** The minimum duration of each of the required tests.

**R10** Each **operator** of a **transmission facility** must include system restoration training for its operating personnel once each calendar year in its operations training program. This training program must include training on the following:

(a) the **operator** of a **transmission facility**'s restoration plan including coordination with the **ISO** and each **operator** of a **generating unit** and **operator** of an **aggregated generating facility** included in its restoration plan;

(b) restoration priorities;

(c) the building of **cranking paths** as included in its restoration plan; and

(d) synchronizing re-energized sections of the **interconnected electric system**.

**R11** Each **operator** of a **transmission facility** and **operator** of an **electric distribution system** must provide a minimum of two (2) hours of system restoration training every two (2) calendar years to its field switching personnel identified as performing unique tasks associated with the **operator** of a **transmission facility**'s restoration plan that are outside of their normal tasks.

**R12** Each **operator** of a **transmission facility** must participate in the **ISO**'s restoration drills, exercises, or simulations if requested by the **ISO**.

**R13** The **ISO** must have written **blackstart resource** agreements or mutually agreed upon procedures or protocols with each **operator** of a **generating unit** with a **blackstart resource**, specifying the terms and conditions of their arrangement. Such agreements must include references to the **blackstart resource** testing requirements, including those specified in requirement R9.

**R14** Each **operator** of a **generating unit** with a **blackstart resource** must have documented procedures for starting each **blackstart resource** and energizing a bus.

**R15** Each **operator** of a **generating unit** with a **blackstart resource** must notify the **ISO** of any known changes to the capabilities of that **blackstart resource** affecting the ability of the **operator** of a **generating unit** to fulfill the requirements of the **ISO**'s restoration plan within twenty-four (24) hours of becoming aware of such change.

**R16** Each **operator** of a **generating unit** with a **blackstart resource** must perform **blackstart resource** tests, and maintain records of such testing, in accordance with the testing requirements set by the **ISO** as referenced in the **blackstart resource** agreements or mutually agreed upon procedures or protocols.

**R16.1** Testing records must include at a minimum:

(a) name of the **blackstart resource**;

(b) **generating unit** tested;

(c) date of the test;

(d) duration of the test;

(e) time required to start the **generating unit**; and

(f) an indication of any testing requirements not met under requirement R9.

**R16.2** Each **operator** of a **generating unit** with a **blackstart resource** must provide the **blackstart resource** test results within thirty (30) **days** after receiving a request from the **ISO**.

**R17** Each operator of a **generating unit** with a **blackstart resource** must provide a minimum of two (2) hours of training every two (2) calendar years to each of its operating personnel responsible for:

(a) the startup of its **blackstart resource**; and

(b) energizing a bus.

**R17.1** The training program must include training on the following:

(a) those elements of the **ISO**'s restoration plan that are applicable to the **blackstart resource**, including coordination with the **ISO** and the adjacent **operator** of a **transmission facility**; and

(b) the procedures documented in requirement R14.

**R18** Each **operator** of a **generating unit** must participate in the **ISO**'s restoration drills, exercises, or simulations if requested by the **ISO**.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of having a restoration plan that is approved by the **ISO** and includes the elements as required in requirement R1 exists. Evidence may include, but is not limited to:

(a) email, mail or other equivalent evidence demonstrating approval of the restoration plan by the **ISO**; and

(b) a documented restoration plan including the elements identified in requirement R1.

**MR2** Evidence of providing a description of any changes to the roles and specific tasks of affected entities identified in the restoration plan as required in requirement R2 exists. Evidence may include, but is not limited to, a documented restoration plan showing the effective date and dated emails with receipts or registered mail with receipts, including a description of any changes to roles and specific tasks, or other equivalent evidence.

**MR3** Evidence of reviewing, aligning and submitting the restoration plan as required in requirement R3 exists. Evidence may include, but is not limited to, a documented restoration plan, including a review or revision history, and emails with receipts or registered mail with receipts, or other equivalent evidence.

**MR3.1** Evidence of resolving the issues described in the reasons provided by the **ISO** within a timeframe agreed to by the **ISO** as required in requirement R3.1 exists. Evidence may include, but is not limited to, emails with receipts or registered mail with receipts, or other equivalent evidence.

**MR4** Evidence of updating and submitting the revised restoration plan as required in requirement R4 exists. Evidence may include, but is not limited to:

(a) for the date of identifying any unplanned permanent modifications: logs, a dated report, emails, or other equivalent evidence;

(b) for the date of implementing planned modifications: logs, a dated report, emails, or other equivalent evidence;

(c) for updating the restoration plan: a dated documented restoration plan and revision histories, or other equivalent evidence; and

(d) for submitting the revised restoration plan: emails with receipts or registered mail receipts including submission date, or other equivalent evidence.

**MR4.1** Evidence of resolving the issues described in the reasons provided by the **ISO** within a timeframe agreed to by the **ISO** as required in requirement R4.1 exists. Evidence may include, but is not limited to, emails with receipts or registered mail with receipts, or other equivalent evidence.

**MR5** Evidence of having a copy of the current **ISO** approved restoration plan within the primary and backup control rooms as required in requirement R5 exists. Evidence may include but is not limited to dated records to show that the latest **ISO** approved copy of the restoration plan is available in the primary and backup control rooms and to the real time operating personnel in accordance with requirement R5, or other equivalent evidence.

**MR5.1** Evidence of providing a copy of the current **ISO** approved restoration plan to each **operator** of an **electric distribution system** as required in requirement R5.1 exists. Evidence may include dated emails with receipts or registered mail receipts, or other equivalent evidence.

**MR6** Evidence of verifying every five (5) years that the restoration plan accomplishes its intended function as required in requirement R6 exists. Evidence may include, but is not limited to, dated event analysis assessments, dated study results, or other equivalent evidence.

**MR7** Evidence of executing the restoration plan or using the restoration strategies as required in requirement R7 exists. Evidence may include, but is not limited to, sequence of events records, data files, **operator** logs, voice recordings, electronic communications, or other equivalent evidence.

**MR8** Evidence of resynchronizing shut down area(s) with the **ISO**’s prior authorization and in accordance with the procedures included in the **ISO**’s restoration plan as required in requirement R8 exists. Evidence may include, but is not limited to, a dated copy of the **ISO**’s restoration plan and a combination of the following evidence as appropriate:

(a) sequence of events records;

(b) data files;

(c) **operator** logs;

(d) voice recordings;

(e) electronic communications,

or other equivalent evidence.

**MR9** Evidence of having **blackstart resource** testing requirements as required in requirement R9 exists. Evidence may include, but is not limited to, **blackstart resource** testing requirement documentation, or other equivalent evidence.

**MR10** Evidence of including system restoration training within the operations training program as required in requirement R10 exists. Evidence may include, but is not limited to, a documented operations training program including system restoration training for operating personnel, or other equivalent evidence.

**MR11** Evidence of providing a minimum of two (2) hours of system restoration training every two (2) calendar years as required in requirement R11 exists. Evidence may include, but is not limited to, training records, training documentation including dates and duration, or other equivalent evidence.

**MR12** Evidence of participating in the **ISO**'s restoration drills, exercises, or simulations as required in requirement R12 exists. Evidence may include, but is not limited to:

(1) documentation of the **ISO**'s request; and

(2) training records, participation records, training documentation, or other equivalent evidence.

**MR13** Evidence of having written **blackstart resource** agreements or mutually agreed upon procedures or protocols as required in requirement R13 exists. Evidence may include, but is not limited to, executed agreements, procedures or protocols, or other equivalent evidence.

**MR14** Evidence of having documented procedures for starting each **blackstart resource** and energizing a bus as required in requirement R14 exists. Evidence may include, but is not limited to, documented procedures, or other equivalent evidence.

**MR15** Evidence of notifying the **ISO** of any known changes to the capabilities of the **blackstart resource** as required in requirement R15 exists. Evidence may include, but is not limited to, emails with receipts, registered mail receipts, time stamped voice record(ing)s or operator logs, showing when the **operator** of a **generating unit** with a **blackstart resource** became aware of changes to the **blackstart resource** capabilities and that it notified the **ISO** within twenty-four (24) hours of becoming aware of such changes as required in requirement R15, or other equivalent evidence.

**MR16** Evidence of performing **blackstart resource** tests, maintaining records of such testing, and providing the **blackstart resource** test results as required in requirement R16 exists. Evidence may include, but is not limited to, test records, test results, and emails with receipts or registered mail receipts that show that it provided these records to the **ISO** when requested, or other equivalent evidence.

**MR17** Evidence of providing a minimum of two (2) hours of training every two (2) calendar years as required in requirement R17 exists. Evidence may include, but is not limited to, training records, training dates, durations and training materials provided, or other equivalent evidence.

**MR18** Evidence of participating in the **ISO**'s restoration drills, exercises, or simulations as required in requirement R18 exists. Evidence may include, but is not limited to:

(1) documentation of the **ISO**'s request; and

(2) training records, participation records, training documentation, or other equivalent evidence.

## 5. Appendices

Appendix 1 – *Amending Process for List of Operators of Transmission Facilities Included in the AESO Restoration Plan*

### Revision History

| Date | Description |
|---|---|
| 2019-12-01 | Unbolded “real time” |
| 2018-07-01 | Initial release. |

## Appendix 1

### Amending Process for List of Operators of Transmission Facilities included in the AESO Restoration Plan

In order to amend the list referenced in subsection (b) of section 2, *Applicability*, the **ISO** must:

(a) upon determining that an **operator** of a **transmission facility** is to be added to the list, notify each affected **operator** of a **transmission facility** in writing and determine the date on which the amended list comes into effect, which must be no less than the first day of the month following three (3) full calendar quarters (January 1, April 1, July 1, October 1) after the date of notice, for the **operator** to meet the applicable requirements;

(b) upon determining that an **operator** of a **transmission facility** is to be deleted, notify each affected **operator** of a **transmission facility** in writing and determine the date on which the amended list comes into effect such that the **operator** will no longer be required to meet the applicable requirements; and

(c) post the amended list with effective dates on the AESO website.

# Alberta Reliability Standard
# System Restoration Coordination
# EOP-006-AB-2

## 1. Purpose

Ensure plans are established and personnel are prepared to enable effective coordination of the system restoration process to ensure **reliability** is maintained during restoration of the **interconnected electric system** in the event of a complete or partial **blackout**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R.1.** The **ISO** must have a restoration plan for its area. The scope of the **ISO**'s restoration plan starts when contracted **blackstart resources** are utilized to re-energize a shut down area of the **bulk electric system**. The scope of the **ISO**'s restoration plan ends when each **operator** of a **transmission facility** is interconnected and the **ISO**'s area is connected to all of its neighbouring **reliability coordinator areas**, provided facilities are available to be returned to service. The restoration plan shall include:

**R1.1.** a strategy to be employed during restoration events for restoring the **interconnected electric system** including minimum criteria for meeting the objectives of the **ISO**'s restoration plan;

**R1.2.** operating processes for restoring the **interconnected electric system**;

**R1.3.** the elements of coordination between the **ISO** and each **operator** of a **transmission facility** in accordance with the **ISO**'s system restoration plan;

**R1.4.** descriptions of the elements of coordination of restoration plans with neighbouring **reliability coordinators**;

**R1.5.** criteria and conditions for reestablishing connections between each **operator** of a **transmission facility** within its area, with **transmission operators** in other **reliability coordinator areas**, and with other **reliability coordinators**;

**R1.6.** reporting requirements for the entities within the **ISO**'s area during a restoration event;

**R1.7.** criteria for sharing information regarding restoration with neighbouring **reliability coordinators** and with **operators** of **transmission facilities** within the **ISO**'s area; and

**R1.8.** identification of the **ISO** as the primary contact for disseminating information regarding restoration to neighbouring **reliability coordinators**, and to **operators** of **transmission facilities** within its area.

**R1.9.** Intentionally left blank.

**R2.** The **ISO** must distribute its most recent restoration plan to each **operator** of a **transmission facility**, as referenced in the **ISO**'s restoration plan, and to neighbouring **reliability coordinators** within thirty (30) **days** of creation or revision.

**R3**. The **ISO** must review its restoration plan within thirteen (13) **months** of the last review.

**R4.** The **ISO** must review its neighbouring **reliability coordinator**'s restoration plans.

**R4.1.** If the **ISO** finds conflicts between its restoration plans and any of its neighbours, the conflicts must be resolved in thirty (30) **days**.

**R5.** The **ISO** must review the restoration plans or procedures of **operators** of **transmission facilities** within its area that are required to be submitted to the **ISO** under any **ISO rules** or **reliability standards**.

**R5.1.** The **ISO** must determine whether each of the restoration plans or procedures referenced in requirement R5 is coordinated and compatible with the **ISO**'s restoration plan and each of the other restoration plans or procedures referenced in requirement R5. The **ISO** must approve or disapprove, with stated reasons, the restoration plan or procedure submitted by an **operator** of a **transmission facility** within thirty (30) **days** following the receipt of the restoration plan or procedure.

**R6.** The **ISO** must have, within its primary and backup control rooms, so that it is available to all of its operating personnel, a copy of its latest restoration plan and copies of the latest restoration plans or procedures of each **operator** of a **transmission facility** in the **ISO**'s area that is required to have an approved plan or procedure in accordance with any **ISO rule** or **reliability standard.**

**R7.** The **ISO** must work with each affected **operator** of a **generating unit**, **operator** of an **aggregated generating facility**, and **operator** of a **transmission facility** as well as neighbouring **reliability coordinators** to monitor restoration progress, coordinate restoration, and take actions to restore the **bulk electric system** frequency within acceptable operating limits. If the restoration plan cannot be completed as expected, the **ISO** must utilize its restoration plan strategies to facilitate restoration of the **interconnected electric system**.

**R8.** The **ISO** must coordinate or authorize resynchronizing islanded areas that bridge boundaries between each **operator** of a **transmission facility** or a boundary between the **ISO**'s area and a **reliability coordinator area**. If the resynchronization cannot be completed as expected the **ISO** must utilize its restoration plan strategies to facilitate resynchronization.

**R9.** The **ISO** must include within its operations training program, annual **interconnected electric system** restoration training for its operating personnel to assure the proper execution of its restoration plan. This training program must address the following

**R9.1.** the coordination role of the **ISO**; and

**R9.2.** reestablishing **WECC** Paths 1 and 83.

**R10.** The **ISO** must conduct two (2) scheduled instances of a system restoration drill, exercise, or simulation per calendar year, which must provide an opportunity for each **operator** of a **transmission facility**, **operator** of a **generating unit** and **operator** of an **aggregated generating**

**facility** to attend as dictated by the particular scope of the drill, exercise, or simulation that is being conducted.

**R10.1.** The **ISO** must request each **operator** of a **transmission facility**, **operator** of a **generating unit** and **operator** of an **aggregated generating facility**, as identified in the **ISO**'s restoration plan, to participate in a drill, exercise, or simulation at least once every two calendar years

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of having a restoration plan as required in requirement R1 exists. Evidence may include, but is not limited to, a dated copy of the restoration plan.

**MR2** Evidence of distributing the restoration plan as required in requirement R2 exists. Evidence may include, but is not limited to, e-mails with receipts or other equivalent evidence.

**MR3.** Evidence of reviewing the restoration plan as required in requirement R3 exists. Evidence may include, but is not limited to, a review signature sheet, or revision histories, or other equivalent evidence.

**MR4.** Evidence of reviewing neighboring **reliability coordinator**'s restoration plans and resolving any conflicts within thirty (30) **days** as required in requirement R4 exists.

**MR5.** Evidence of reviewing, approving or disapproving, and notifying each **operator** of a **transmission facility** as required in requirement R5 exists. Evidence may include, but is not limited to, a review signature sheet or emails, or other equivalent evidence.

**MR6.** Evidence of having copies of restoration plans as required in requirement R6 exists. Evidence may include, but is not limited to, e-mails, restoration plans or procedures documentation, or other equivalent evidence.

**MR7.** Evidence of monitoring and coordinating restoration progress as required in requirement R7 exists. Evidence may include, but is not limited to, voice recordings, e-mail, dated computer printouts, **operator** logs or other equivalent evidence.

**MR8.** If there has been a resynchronizing of an islanded area, the **ISO** and each **reliability coordinator** involved may have evidence that it coordinated or authorized resynchronizing in accordance with requirement R8. Evidence may include, but is not limited to, voice recordings, e-mails, **operator** logs or other equivalent evidence.

**MR9.** The **ISO** may have an electronic or hard copy of its training records available showing that it has provided training in accordance with requirement R9.

**MR10.** The **ISO** may have evidence that it conducted two scheduled instances of a system restoration drill, exercise, or simulation per calendar year and that **operators** of a **transmission facility** and **operators** of a **generating unit** and **operators** of an **aggregated generating facility** as identified in the **ISO**'s restoration plan were invited in accordance with requirement R10. Evidence may include, but is not limited to, e-mails or other equivalent evidence.

## Revision History

| Effective Date | Description |
|---|---|
| 2015-09-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to ensure continued reliable operations of the **bulk electric system** in the event that a **control centre** becomes inoperable.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**; and

(b) the **operator** of a **transmission facility** who operates a **control centre** that controls **transmission facilities** that are part of the **bulk electric system**.

This **reliability standard** does not apply to the **operator** of a **transmission facility** whose **transmission facilities** are only:

(a) radial **transmission facilities** connecting to:

- load;
- one or more **generating units**; and / or
- one or more **aggregated generating facilities**; or

(b) either part of an industrial complex or connected to an industrial complex and cannot interrupt power flow on the **interconnected electric system**, other than power flow on its own **transmission facilities**.

## 3. Requirements

**R1** The **ISO** and each **operator** of a **transmission facility** must have a current operating plan describing the manner in which it continues to meet its functional obligations with regard to the reliable operations of the **bulk electric system** in the event that its primary **control centre** functionality is lost.

This operating plan for backup functionality must include the following, at a minimum:

(a) the location and method of implementation for providing backup functionality;

(b) a summary description of the items required to support the backup functionality. These items must include, at a minimum:

(i) tools and applications to ensure that system operators have situational awareness of the **bulk electric system**;

(ii) data communications;

(iii) voice communications;

(iv) power source(s); and

(v) physical and cyber security;

(c) an operating process for keeping the backup functionality consistent with the primary **control centre**;

(d) operating procedures, including decision authority, for use in determining when to implement the operating plan for backup functionality;

(e) a transition period between the decision to transfer functionality to the back up **control centre** following the loss of primary **control centre** functionality and the time to fully implement the backup functionality that is less than or equal to two (2) hours; and

(f) an operating process describing the actions to be taken during the transition period between the loss of primary **control centre** functionality and the time to fully implement the backup functionality items identified in requirement R1, part (b). The operating process must include at a minimum:

(i) a list of all entities to notify when there is a change in operating locations;

(ii) actions to manage the risk to the **bulk electric system** during the transition from primary to backup functionality, as well as during outages of the primary or backup functionality; and

(iii) identification of the roles for personnel involved during the initiation and implementation of the operating plan for backup functionality.

**R2** The **ISO** and each **operator** of a **transmission facility** must have a copy of its current operating plan for backup functionality available at its primary **control centre** and at the location providing backup functionality.

**R3** The **ISO** must have a backup **control centre** facility (provided through its own dedicated backup facility or at another entity's **control centre** staffed with **NERC** certified "reliability coordinator operators" when control has been transferred to the backup facility) that provides the functionality required for maintaining compliance with all **reliability standards** that depend on primary **control centre** functionality. To avoid requiring a tertiary facility, a backup facility is not required during:

(a) planned outages of the primary or backup facilities of two (2) weeks or less; or

(b) unplanned outages of the primary or backup facilities.

**R4** Each **operator** of a **transmission facility** must, when control has been transferred to the backup functionality location, have backup functionality provided either through:

(a) a facility staffed by operators that are certified in accordance with any applicable **reliability standards**; or

(b) contracted services staffed by operators that are certified in accordance with any applicable **reliability standards**

that includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all **reliability standards** that depend on the **operator** of a **transmission facility**'s primary **control centre** functionality.

To avoid requiring tertiary functionality, backup functionality is not required during:

(i) planned outages of the primary or backup functionality of two (2) weeks or less; or

(ii) unplanned outages of the primary or backup functionality.

**R5** The **ISO** and each **operator** of a **transmission facility** must annually review and approve its operating plan for backup functionality.

**R5.1** An update and approval of the operating plan for backup functionality must take place within sixty (60) **days** of identifying any necessary changes to any part of the operating plan described in requirement R1.

**R6** The **ISO** and each **operator** of a **transmission facility** must have primary and backup functionality that do not depend on each other for the **control centre** functionality required to maintain compliance with **reliability standards**.

**R7** The **ISO** and each **operator** of a **transmission facility** must conduct and document results of an annual test of its operating plan that demonstrates:

**R7.1** The transition time between the decision to transfer functionality to the backup **control centre** following the simulated loss of primary **control centre** functionality and the time to fully implement the backup functionality; and

**R7.2** The backup functionality for a minimum of two (2) continuous hours.

**R8** The following requirements apply in the event of a loss of primary or backup functionality that is anticipated to last for more than six (6) months:

**R8.1** Where the **operator** of a **transmission facility** loses primary or backup functionality as described in requirement R8, it must provide a plan to the **ISO** within six (6) **months** of the date when the functionality is lost, showing how it will re-establish primary or backup functionality; and

**R8.2** Where the **ISO** loses primary or backup functionality as described in requirement R8, it must provide a plan to the **WECC** within six (6) **months** of the date when the functionality is lost, showing how it will re-establish primary or backup functionality.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of having a current operating plan for backup functionality as required in requirement R1 exists. Evidence may include, but is not limited to, a dated, current operating plan with specified elements or other equivalent evidence.

**MR2** Evidence of having an electronic or paper copy of the current operating plan for backup functionality available at its primary **control centre** and at the location providing backup functionality as required in requirement R2 exists.

Evidence may include, but is not limited to, a current electronic or paper copy of the operating plan, operator log identifying when the plan was put into the **control centre**, or other equivalent evidence.

**MR3** Evidence of having a backup **control centre** facility that provides the functionality and is staffed as required in requirement R3 exists. Evidence may include, but is not limited to, documentation identifying that the backup **control centre** facility is staffed with **NERC** certified “reliability coordinator operators” and provides the same functionality to maintain compliance with all **reliability standards** as the primary **control centre**, or other equivalent evidence.

**MR4** Evidence of having backup functionality provided either through a facility or contracted services staffed as required in requirement R4 exists. Evidence may include, but is not limited to, documentation identifying that the backup functionality includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all **reliability standards** that depend on the primary **control centre** functionality, or other equivalent evidence.

**MR5** Evidence of reviewing and approving annually the operating plan for backup functionality as required in requirement R5 exists. Evidence may include, but is not limited to, a dated, current, operating plan for backup functionality, including a revision and approval history, or other equivalent evidence.

**MR5.1** Evidence of updating and approving the operating plan for backup functionality as required in requirement R5.1 exits. Evidence may include, but is not limited to, an updated and approved operating plan for backup functionality within sixty (60) **days** of any changes to any part of the operating plan described in requirement R1, or other equivalent evidence.

**MR6** Evidence of having primary and backup functionality that do not depend on each other for the **control centre** functionality required to maintain compliance with **reliability standards** as required in requirement R6 exists. Evidence may include, but is not limited to, documentation or drawings that show the independence of the two (2) **control centres**, or other equivalent evidence.

**MR7** Evidence of conducting an annual test for backup functionality and documenting the results of the operating plan as required in requirement R7 exists. Evidence may include, but is not limited to, testing documentation or other equivalent evidence.

**MR8** Evidence for requirement R8 is included in the following measures:

**MR8.1** Evidence of providing a plan to the **ISO** as required in requirement R8.1 exists. Evidence may include, but is not limited to, a dated email or letter providing the plan to the **ISO**, or other equivalent evidence.

**MR8.2** Evidence of providing a plan to the **WECC** as required in requirement R8.2 exists. Evidence may include, but is not limited to, a dated email or letter to the **WECC**, or other equivalent evidence.

### Revision History

| Date | Description |
|---|---|
| 2019-07-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to address the effects of operating emergencies by ensuring the **ISO** and each applicable **operator** of a **transmission facility** has developed one or more operating plans to mitigate operating emergencies, and that those plans are coordinated within Alberta.

## 2. Applicability

This **reliability standard** applies to:

(a) the **operator** of a **transmission facility** that is part of the **bulk electric system**; and

(b) the **ISO**

This **reliability standard** does not apply to the **operator** of a **transmission facility** whose **transmission facilities** are only:

(c) **radial circuits** connecting to any one or more of:

(i) load;

(ii) one or more **generating units**; and

(iii) one or more **aggregated generating facilities**; or

(d) part of an industrial complex, or connected to an industrial complex, and cannot interrupt power flow on the **interconnected electric system** other than power flow on its own **transmission facilities**.

## 3. Requirements

**R1** Each **operator** of a **transmission facility** must develop, maintain, and, in the event of an operating emergency, implement one or more **ISO**-reviewed operating plans to mitigate operating emergencies in its area. The operating plans must include the following, as applicable:

**R1.1** roles and responsibilities for activating the operating plans;

**R1.2** processes to prepare for and mitigate operating emergencies including:

**R1.2.1** notification to the **ISO**, to include current and projected conditions, when experiencing an operating emergency;

**R1.2.2** coordination with the **ISO** for the cancellation or recall of **transmission facility** outages;

**R1.2.3** requests to the **ISO** for **transmission system** reconfiguration;

**R1.2.4** requests to the **ISO** to change generation level;

**R1.2.5** provisions for manual load shedding that minimizes the overlap with automatic load shedding and are capable of being implemented in a timeframe adequate for mitigating the emergency; and

**R1.2.6 reliability** impacts of extreme weather conditions.

**R1A** The **ISO** must develop, maintain, and implement one or more operating plans to mitigate operating emergencies on the **interconnected electric system**. The operating plans must include the following, as applicable:

**R1A.1** roles and responsibilities for activating the operating plans;

**R1A.2** processes to prepare for and mitigate operating emergencies including:

**R1A.2.1** intentionally left blank;

**R1A.2.2** cancellation or recall of **transmission facility** and **generating unit** outages;

**R1A.2.3** **transmission system** reconfiguration;

**R1A.2.4** provisions to issue **directives** for managing generation level;

**R1A.2.5** provisions to issue **directives** for manual load shedding for mitigating the emergency; and;

**R1A.2.6** **reliability** impacts of extreme weather conditions.

**R2** The **ISO** must develop, maintain, and implement one or more operating plans to mitigate capacity emergencies and energy emergencies within its **balancing authority area**. The operating plans must include the following, as applicable:

**R2.1** roles and responsibilities for activating the operating plans;

**R2.2** processes to prepare for and mitigate emergencies including:

**R2.2.1** intentionally left blank;

**R2.2.2** declaring an energy emergency alert, in accordance with Appendix 1;

**R2.2.3** managing generating resources in its **balancing authority area** to address:

**R2.2.3.1** capability and availability;

**R2.2.3.2** fuel supply and inventory concerns;

**R2.2.3.3** fuel switching capabilities; and

**R2.2.3.4** environmental constraints;

**R2.2.4** public appeals for voluntary load reductions;

**R2.2.5** intentionally left blank;

**R2.2.6** intentionally left blank;

**R2.2.7** use of **interruptible demand**, curtailable load and demand response;

**R2.2.8** provisions to issue **directives** for manual load shedding for mitigating the emergency; and

**R2.2.9** **reliability** impacts of extreme weather conditions.

**R3** The **ISO** must review the operating plans to mitigate operating emergencies submitted by an **operator** of a **transmission facility** regarding any **reliability** risks that are identified between operating plans,

**R3.1** within 60 **days** of receiving the initial operating plans and within 30 **days** of receiving subsequent operating plans, the **ISO** must:

**R3.1.1** review each submitted operating plan on the basis of compatibility and inter-dependency with operating plans of the **ISO** and other **operators** of a **transmission facility**;

**R3.1.2** review each submitted operating plan for coordination to avoid risk to wide-area **reliability**; and

**R3.1.3** notify each **operator** of a **transmission facility** of the results of its review, specifying any time frame for resubmittal of its operating plans if revisions are identified.

**R4** Each **operator** of a **transmission facility** must address any **reliability** risks the **ISO** identifies pursuant to requirement R3 and resubmit the related operating plans to the **ISO** within a time period the **ISO** specifies.

**R5** The **ISO** must, when it identifies an operating emergency, notify within 30 minutes from the time of identification, any affected adjacent **reliability coordinators**.

**R6** The **ISO** must, when experiencing a potential or actual energy emergency within Alberta declare an energy emergency alert, as detailed in Appendix 1.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of developing, maintaining, and implementing operating plans, and having operating plans reviewed as required in requirement R1 exists. Evidence of:

- developing an operating plan may include documented operating plans with effective dates;
- maintaining an operating plan may include documented operating plans with version history;
- implementing an operating plan may include **operator** logs, voice recordings, system logs, sequence of events records or disturbance reports;
- having operating plan reviewed by the **ISO**, as applicable, which may include emails; or
- other equivalent evidence.

**MR2** Evidence of developing, maintaining, and implementing one or more operating plans to mitigate capacity emergencies and energy emergencies as required in requirement R2 exists. Evidence may include documented operating plans with effective dates, **operator** logs, voice recordings, system logs, sequence of events records, disturbance reports, or other equivalent evidence.

**MR3** Evidence of reviewing operating plans as required in requirement R3 exists. Evidence may include dated e-mails, other correspondence, or other equivalent evidence.

**MR4** Evidence of addressing **reliability** risks identified in an operating plan as required in requirement R4 exists. Evidence may include dated emails, other correspondence, version history showing that the **operator** of a **transmission facility** has responded and updated the operating plan, or other equivalent evidence.

**MR5** Evidence of notifying affected adjacent **reliability coordinators** as required in requirement R5 exists. Evidence may include **operator** logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence.

**MR6** Evidence of declaring an energy emergency alert as required in requirement R6 exists. Evidence may include **operator** logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence.

## 5. Appendices

Appendix 1 - *Energy Emergency Alerts*

### Revision History

| Date | Description |
|---|---|
| 2022-01-01 | Initial release. |

## Appendix 1
## Energy Emergency Alerts

**Introduction**

This Appendix 1 provides the process and descriptions of the levels the **ISO** uses to communicate the condition of its **balancing authority area** when it is experiencing an energy emergency.

**A. General Responsibilities**

1. Initiation. The **ISO** may initiate an energy emergency alert.
2. Notification. The **ISO** must, when it declares an energy emergency alert, notify all adjacent **reliability coordinators**.

**B. Energy Emergency Alert Levels**

The **ISO** may declare whatever energy emergency alert level is necessary and need not proceed through the energy emergency alerts sequentially.

**1. EEA 1 — All available generation resources in use.**

Circumstances:

- The **ISO** is experiencing conditions where all available generation resources are committed to meet firm load, firm transactions, and reserve commitments, and is concerned about sustaining its required **contingency reserve**.
- Non-firm wholesale energy sales, other than those that are recallable to meet reserve requirements, have been curtailed.

**2. EEA 2 — Load management procedures in effect**.

Circumstances:

- The **ISO** is no longer able to provide its expected energy requirements and is energy deficient.
- The **ISO** has implemented its operating plans to mitigate emergencies.
- The **ISO** is still able to maintain minimum **contingency reserve** requirements.

During EEA 2, the **ISO** has the following responsibilities:

2.1 notify **adjacent balancing authorities**.

2.2 the **ISO** must update the energy emergency alert levels as changes occur and pass this information on to the adjacent **reliability coordinators**, **adjacent balancing authorities**, and adjacent **interconnected transmission operators.**

2.3 sharing information on resource availability: The **ISO** must coordinate, as appropriate, with the **reliability coordinator** that has an energy deficient **balancing authority**.

2.4 evaluating and mitigating transmission limitations: The **ISO** must review **transmission facility** outages and work with the **operator** of a **transmission facility** to see if it is possible to return to service any transmission elements that may relieve the loading on **system operating limits** or **interconnection reliability operating limits**.

2.5 before declaring an EEA 3, the **ISO** must make use of all available resources; including:

2.5.1 all available **generating units** are online: All **generating units** capable of being online in the time frame of the emergency are online.

2.5.2 **demand-side management**: Activate **demand-side management** within provisions of any applicable agreements.

**3. EEA 3 — Firm Load interruption is imminent or in progress.**

Circumstances:

- The **ISO** is unable to meet minimum **contingency reserve** requirements.

During EEA 3, the **ISO** has the following responsibilities:

3.1 continue actions from EEA 2. The **ISO** must continue to take all actions initiated during EEA 2.

3.2 the **ISO** must update its information as changes occur and pass this information on to the adjacent **reliability coordinators**, **adjacent balancing authorities** and adjacent **interconnected** transmission **operators** until the EEA 3 is terminated.

3.3 re-evaluating and revising **system operating limits** and **interconnection reliability operating limits**. The **ISO** must evaluate the risks of revising **system operating limits** and **interconnection reliability operating limits**. The **ISO** must coordinate the re-evaluation of **system operating limits** and **interconnection reliability operating limits** with other affected **reliability coordinators**. The **ISO** may only revise **system operating limits** and **interconnection reliability operating limits** as long as an EEA 3 condition exists. The following are minimum requirements that the **ISO** must meet before **system operating limits** or **interconnection reliability operating limits** are revised:

3.3.1 the **ISO** must, when it is energy deficient, immediately take whatever actions are necessary to mitigate any undue risk to the **Interconnection** which may include load shedding.

3.4 returning to pre-emergency conditions: Whenever energy is made available such that the systems can be returned to its pre-emergency **system operating limits** and **interconnection reliability operating limits**, the **ISO** may downgrade the alert level.

3.4.1 notification of other parties. Upon the **ISO** downgrading an alert level, it must notify the adjacent **reliability coordinators**, **adjacent balancing authorities** and adjacent **transmission operators** that systems can be returned to normal limits.

Alert 0 - Termination. When the **ISO** is able to meet its load and **operating reserve** requirements, it must terminate the energy emergency alert. The **ISO** must notify all other adjacent **reliability coordinators**, **adjacent balancing authorities** and adjacent **transmission operators** of the termination.

# FAC–001–AB–0 Facility Connection Requirements

## 1. Purpose

The purpose of this *reliability standard* is to establish connection and performance requirements for *facilities* connecting to the *AIES*.

## 2. Applicability

This *reliability standard* applies to:

- *ISO*

## 3. Definitions

Italicized terms used in this *reliability standard* have the meanings as set out in the Alberta Reliability Standards Glossary of Terms and Part 1 of the ISO Rules.

## 4. Requirements

**R1** The *ISO* must document transmission *interconnection* requirements to comply with all *reliability standards*. The *ISO's* transmission *interconnection* requirements must address connection requirements for:

**R1.1** Generating units

**R1.2** *Transmission facilities*

**R1.3** *Transmission connected end-use customer's facilities*

**R2** The *ISO's* transmission *interconnection* requirements or project functional specification must address, but is not limited to, the following items:

**R2.1** Voltage level and *MW* and *MVAR* capacity or *demand* at point of connection

**R2.2** Breaker duty and *surge* protection

**R2.3** *System* protection and coordination

**R2.4** Metering and telecommunications

**R2.5** Grounding and safety issues

**R2.6** Insulation and insulation coordination

**R2.7** Voltage, *reactive power*, and *power factor* control

**R2.8** Power quality impacts

**R2.9** Equipment *ratings*

**R2.10** Synchronizing of *facilities*

**R2.11** Maintenance coordination

**R2.12** Operational issues (abnormal frequency and voltages)

**R2.13** Inspection requirements for existing or new *facilities*

**R2.14** Communications and procedures during normal and emergency operating conditions

**R3** The *ISO* must assess the long term implications to the AIES of any facility to be connected to it.

**R4** The *ISO* must maintain and update as required and post on its website its transmission *interconnection* requirements.

## 5. Processes and Procedures

No procedures have been defined for this *reliability standard*.

## 6. Measures

The following measures correspond to the requirements identified in Section 4 of this *reliability standard*. For example, MR1 is the measure for R1.

**MR1** The *ISO* transmission *interconnection* requirements include requirements for generating units, *transmission facilities* and *transmission connected end use customer facilities*.

The *ISO* transmission *interconnection* requirements include content that is compliant and consistent with all *reliability standards*.

**MR2** The *ISO* transmission *interconnection* requirements or project functional specifications contain information addressing each item identified in R2.

**MR3** The assessment made in R3 is included in either the transmission *interconnection* requirements or project functional specification.

**MR4** The *ISO* transmission *interconnection* requirements are posted on its website.

A revision history for the *ISO* transmission *interconnection* requirements shows that updates were made for each change to *reliability standards*, as appropriate.

Changes to the *ISO* transmission *interconnection* requirements are completed within 12 months of the *Commission* approving a change in the *reliability standards.*

## 7. Appendices

No appendices have been defined for this *reliability standard*.

## 8. Guidelines

No guidelines have been defined for this *reliability standard*.

## Revision History

| Effective | Description |
|---|---|
| 2010-09-24 | New Issue |

# FAC–002–AB–0 Coordination of Plans for New Facilities

## 1. Purpose

The purpose of this *reliability standard* is to demonstrate that proper evaluation of potential *reliability* impacts of new *transmission facilities* to be connected to the *AIES* has occurred.

## 2. Applicability

This *reliability standard* applies to:

- *ISO*

## 3. Definitions

Italicized terms used in this *reliability standard* have the meanings as set out in the Alberta Reliability Standards Glossary of Terms and Part 1 of the ISO Rules.

## 4. Requirements

**R1** The *ISO* must retain the documentation of its evaluation of the potential *reliability* impact of the new *transmission facilities* and their connections on the *AIES* for three years after energization.

**R2** The *ISO* must provide the documentation referred to in requirement R1 to the *WECC* within 30 calendar *days* of its request, provided such request is made with the three year period referred to in requirement R1.

## 5. Processes and Procedures

No procedures have been defined for this *reliability standard*.

## 6. Measures

The following measures correspond to the requirements identified in Section 4 of this *reliability standard*. For example, MR1 is the measure for R1.

**MR1** Documentation exists for the past three years and is made available when requested per R1.

**MR2** Confirmation exists that documentation was received if requested.

## 7. Appendices

No appendices have been defined for this *reliability standard*.

## 8. Guidelines

No guidelines have been defined for this *reliability standard*.

## Revision History

| Effective | Description |
|---|---|
| 2010-03-22 | New Issue |

# FAC-003-AB1-1 Transmission Vegetation Management Program

## 1. Purpose

The purpose of this *reliability standard* is to improve the *reliability* of electric transmission systems by preventing *outages* from vegetation located on a right-of-way, corridor or other route (collectively "ROW") and minimizing *outages* from vegetation located adjacent to a ROW, maintaining clearances between *transmission facilities* and vegetation on and along a ROW, and reporting vegetation related *outages* of electric transmission systems to the *ISO* and *WECC.*

## 2. Applicability

This *reliability standard* applies to:

(a) the *legal owner* of a *transmission facility* with *transmission facilities* operated at 200 kV and above and any lower voltage *transmission facilities* designated by the *ISO* as critical to the *reliability* of the *AIES* as identified in Appendix A; provided that *transmission facilities* on ROWs that are assessed and identified on an annual basis not to have vegetation capable of growing higher than 2 meters are excluded; and

(b) the *ISO.*

## 3. Definitions

Italicized terms used in this *reliability standard* have the meanings as set out in the Consolidated Authoritative Document Glossary.

## 4. Requirements

**R1** Each *legal owner* of a *transmission facility* must prepare a *TVMP*. This program is to be updated at least annually. The *TVMP* must include the objectives, practices, approved procedures, and work specifications [1] of the *legal owner* of a *transmission facility*.

**R1.1** The *TVMP* must define a schedule for and the type (aerial or ground) of ROW vegetation inspections. This schedule must be flexible enough to adjust for changing conditions. The inspection schedule must be based on the anticipated growth of vegetation and any other environmental or operational factors that could impact the relationship of vegetation to the *transmission facilities* of the *legal owner* of a *transmission facility*. The *legal owner* of a *transmission facility* must perform vegetation inspections as identified in the schedule.

[1] ANSI A300, Tree Care Operations – Tree, Shrub, and Other Woody Plant Maintenance – Standard Practices, while not a requirement of this *reliability standard*, is considered by *NERC* to be an industry best practice.

**R1.2** The *TVMP* must identify and document clearances between vegetation and any overhead ungrounded supply conductors, taking into consideration transmission line voltage, the effects of ambient temperature on conductor sag under maximum design loading, and the effects of wind velocities on conductor sway. Specifically, the *legal owner* of a *transmission facility* must establish clearances to be achieved at the time of vegetation management work identified herein as Clearance 1, and must also establish and maintain a set of clearance requirements identified herein as Clearance 2 to prevent flashover between vegetation and overhead ungrounded supply conductors.

**R1.2.1** Clearance 1 — Each *legal owner* of a *transmission facility* must determine and document appropriate clearance distances to be achieved at the time of vegetation management work based upon local conditions and the expected time frame in which the *legal owner* of a *transmission facility* plans to return for future vegetation management work. Local conditions may include, but are not limited to: operating voltage, appropriate vegetation management techniques, fire risk, reasonably anticipated tree and conductor movement, species types and growth rates, species failure characteristics, local climate and rainfall patterns, line terrain and elevation, location of the vegetation within the span, and worker approach distance requirements. Clearance 1 distances must be greater than those defined in Clearance 2.

**R1.2.2** Clearance 2 — Each *legal owner* of a *transmission facility* must determine and document specific minimum radial clearance distances to be maintained between vegetation and conductors under all rated electrical operating conditions. These minimum radial clearance distances are necessary to prevent flashover between vegetation and conductors and will vary due to such factors as altitude and operating voltage. Subject to R1.2.2.1 and R1.2.2.2, the documented specific minimum radial clearance distances must be no less than those set forth in the Institute of Electrical and Electronics Engineers (IEEE) Standard 516-2003 (*Guide for Maintenance Methods on Energized Power Lines*) and as specified in its Section 4.2.2.3, Minimum Air Insulation Distances without Tools in the Air Gap.

**R1.2.2.1** Where transmission system transient overvoltage factors are not known, clearances must be derived from Table 5, IEEE 516-2003, phase-to-ground distances, with appropriate altitude correction factors applied.

**R1.2.2.2** Where transmission system transient overvoltage factors are known, clearances must be derived from Table 7, IEEE 516-2003, phase-to-phase voltages, with appropriate altitude correction factors applied.

**R1.3** All personnel directly involved in the design and implementation of the *TVMP* must hold appropriate qualifications and must have taken appropriate training, as defined by the *legal owner* of a *transmission facility*, to perform their duties.

**R1.4** Each *legal owner* of a *transmission facility* must develop mitigation measures to achieve sufficient clearances for the protection of its *transmission facilities* when it identifies locations on the ROW where it is restricted from attaining Clearance 1 distances.

**R1.5** Each *legal owner* of a *transmission facility* must establish and document a process for the immediate communication of vegetation conditions that present an imminent threat of a transmission line *outage*.

This is so that action (temporary reduction in line rating, switching line out of service, etc.) may be taken until the threat is relieved.

**R2** The *legal owner* of a *transmission facility* must create and implement an annual plan for vegetation management work to ensure the *reliability* of its *transmission facilities*. The plan must describe the methods used, such as manual clearing, mechanical clearing, herbicide treatment, or other actions. The plan must be flexible enough to adjust to changing conditions, taking into consideration anticipated growth of vegetation and all other environmental factors that may have an impact on the *reliability* of the *AIES*. Adjustments to the plan must be documented as they occur. The plan must include the time required to obtain permissions or permits from landowners or regulatory authorities. Each *legal owner* of a *transmission facility* must have systems and procedures for documenting and tracking the planned vegetation management work and ensuring that the vegetation management work was completed according to its work specifications.

**R3** Each *legal owner* of a *transmission facility* must report quarterly to the *ISO*, *sustained outages* to its transmission lines determined by the *legal owner* of a *transmission facility* to have been caused by vegetation.

**R3.1** Multiple *sustained outage*s on an individual transmission line, if caused by the same vegetation, must be reported as one *outage* regardless of the actual number of *outages* within a 24-hour period.

**R3.2** The *legal owner* of a *transmission facility* is not required to report to the *ISO, sustained outages* to its transmission lines caused by either:

- vegetation falling onto a transmission line from outside the ROW caused by a natural disasters are not considered reportable (examples of disasters include, but are not limited to, earthquakes, fires, tornados, hurricanes, landslides, wind shear, ice storms, floods, major storms as defined either by the *legal owner* of a *transmission facility* or an applicable regulatory body); or
- vegetation falling onto a transmission line caused by human or animal activity are not considered reportable (examples of human or animal activity include, but are not limited to, logging, animal severing tree, vehicle contact with tree, arboricultural, horticultural or agricultural activities, or removal/digging of vegetation).

**R3.3** The *outage* information provided by the *legal owner* of a *transmission facility* to the *ISO* must include at a minimum:

- number or name of the transmission line(s) forced out of service;
- date and time;
- duration of the *outage*;

- description of the cause of the *outage*;
- other pertinent comments; and
- remedial action taken by the *legal owner* of a *transmission facility*.

**R3.4** An *outage* must be categorized by the *legal owner* of a *transmission facility* as one of the following:

**R3.4.1** Category 1 — Grow-ins: *Outages* caused by vegetation growing into transmission lines from vegetation inside and/or outside of the ROW;

**R3.4.2** Category 2 — Fall-ins: *Outages* caused by vegetation falling into transmission lines from inside the ROW; or

**R3.4.3** Category 3 — Fall-ins: *Outages* caused by vegetation falling into transmission lines from outside the ROW.

**R4** The *ISO* must report quarterly to *WECC*, *sustained outages* to transmission lines determined by the *legal owner* of a *transmission facility* to have been caused by vegetation.

**R4.1** Multiple *sustained outages* within a 24-hour period on an individual transmission line, if caused by the same vegetation, must be reported as one *outage* regardless of the actual number of *outages*.

**R4.2** The *ISO* is not required to report to *WECC*, *sustained outages* to transmission lines caused by either:

- *outages* from vegetation falling onto transmission lines from outside the ROW caused by natural disasters are not reportable (examples of disasters include, but are not limited to, earthquakes, fires, tornados, hurricanes, landslides, wind shear, ice storms, floods, major storms as defined either by the *legal owner* of a *transmission facility,* or an applicable regulatory body); or
- *outages* from vegetation caused by human or animal activity are not considered reportable (examples of human or animal activity include, but are not limited to, logging, animal severing tree, vehicle contact with tree, arboricultural, horticultural or agricultural activities, or removal/digging of vegetation).

**R4.3** The *outage* information provided by the *ISO* to *WECC* must include at a minimum:

- number or name of the transmission line(s) forced out of service;
- date and time;
- duration of the *outage*;
- description of the cause of the *outage*;
- other pertinent comments; and
- remedial action taken by the *legal owner* of a *transmission facility*.

**R4.4** An *outage* must be categorized by the *legal owner* of a *transmission facility* as one of the following:

**R4.4.1** Category 1 — Grow-ins: *Outages* caused by vegetation growing into transmission lines from vegetation inside and/or outside of the ROW;

**R4.4.2** Category 2 — Fall-ins: *Outages* caused by vegetation falling into transmission lines from inside the ROW; or

**R4.4.3** Category 3 — Fall-ins: *Outages* caused by vegetation falling into transmission lines from outside the ROW.

## 5. Procedures

No procedures have been defined for this *reliability standard*.

## 6. Measures

The following measures correspond to the requirements identified in Section 4 of this *reliability standard*. For example, MR1 is the measure for R1.

These measures will be used by the *ISO* in carrying out its compliance monitoring duties in accordance with *ISO rule* 12. The *ISO* may consider other data and information, including any provided by a *market participant*.

**MR1** A revision history of the *TVMP* is provided annually to the *ISO*. A *TVMP* exists and is provided in the format specified in the *ISO TVMP* template. The *TVMP* is provided within 30 *days* of request. The *TVMP* is complete and includes the required component sections specified in the template.

**MR1.1** A vegetation inspection schedule exists in the *TVMP*. The schedule is completed in accordance with the *ISO TVMP* template. The schedule includes all applicable transmission lines. Documentation exists to show that the vegetation inspections have been performed.

**MR1.2** Clearance 1 and Clearance 2 values exist in the *TVMP*

**MR1.2.1** Clearance 1 values exist for every transmission line. Clearance 1 values specified are greater than those of Clearance 2.

**MR1.2.2** Clearance 2 values exist for every transmission line. Clearance 2 values specified are greater than the minimum clearances set in IEEE standards for the applicable scenarios.

**MR1.3** Requirements, training, and qualifications for positions responsible for preparing and implementing the *TVMP* exist. Documentation exists to confirm that personnel meet the requirements, training, and qualifications of the position. Acceptable documentation includes training records, licenses, certificates, and resumes.

**MR1.4** A list exists and specifies locations on the ROW where Clearance 1 is not attainable. Mitigation measures exist where there are restrictions. Mitigating measures are appropriate and meet the intent of this *reliability standard*.

**MR1.5** A documented process or procedure for communication exists. The process is appropriate and of sufficient detail to meet the intent of the requirement.

**MR2** A work plan exists in the form of the *ISO* vegetation management work plan template. The work plan is complete. The work plan is submitted annually and within 30 *days* of being requested.

Evidence exists to show that the work plan is implemented. Evidence may include status and inspection reports, work orders, and/or contracts. The work plan is being followed in accordance to the schedule. The work is completed in accordance with the work plan. Revision documentation exists where the plan has been revised. Evidence is provided to the *ISO* within 30 *day*s of a request.

**MR3 to 3.4.3** Quarterly reports are submitted to the *ISO* by the dates specified by the *ISO*. Quarterly reports contain all sustained outages caused by vegetation for that reporting period. Quarterly reports contain the specific information in the requirement.

**MR4 to 4.4.3** Quarterly reports are submitted to the *WECC* by dates specified by *WECC*. Quarterly reports contain all sustained *outages* caused by vegetation received by the *ISO* for that reporting period. Quarterly reports contain the specific information in the requirement.

## 7. Appendices

### Appendix A - Transmission Facilities Designated as Critical to the AIES

The following facilities have been identified as critical to the *AIES* and require the application of this *reliability standard*:

- 887L (Pocaterra T48S - Alberta / BC border);
- 777L (Pocaterra T48S - Seebe T245S);
- 786L (Coleman T799S - Alberta / BC border); and
- 170L (Coleman T799S - Pincher Creek T396S).

## 8. Guidelines

No guidelines have been defined for this *reliability standard*.

### Revision History

| Date | Description |
|---|---|
| 2012-12-17 | Administrative update – “*TFO*” replaced with the “*legal owner* of a *transmission facility*”; and other minor cleanup items. |
| 2010-01-26 | R1 and R2 |
| 2013-10-01 | New Issue |

## 1. Purpose

The purpose of this **reliability standard** is to ensure that the **facility ratings** used in the reliable planning and operation of the **transmission system** are determined based on technically sound principles. A **facility rating** is an essential component in the determination of **system operating limits**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **legal owner** of a **transmission facility**:

(i) that is part of the **bulk electric system**, except for transformers that do not have a primary terminal and at least one (1) secondary terminal engerized at 100 kV or higher;

(ii) that the **ISO**:

(A) determines is necessary for the reliable operation of either the **interconnected electric system** or the City of Medicine Hat electric system; and

(B) publishes on the AESO website and may amend from time to time on notice to **market participants** in accordance with the process set out in Appendix 1;

(iii) who owns a **generating unit** step-up transformer for those generating units listed in subsection (b); or

(iv) who owns a transformer connected to a **blackstart resource**;

(b) the **legal owner** of a **generating unit** that is:

(i) directly connected to the **bulk electric system** and has a **maximum authorized real power rating** greater than 18 MW, unless the **generating unit** is part of an industrial complex;

(ii) within a power plant that:

(A) is not part of an **aggregated generating facility**;

(B) is directly connected to the **bulk electric system**; and

(C) has a combined **maximum authorized real power rating** greater than 67.5 MW,

unless the power plant is part of an industrial complex;

(iii) a **blackstart resource**;

(iv) directly connected to the **bulk electric system** and within an industrial complex with **supply transmission service** greater than 67.5 MW; or

(v) material to this **reliability standard** and to the **reliability** of the **bulk electric system**, regardless of **maximum authorized real power** rating, as the **ISO** determines and publishes on the AESO website and may amend from time to time in accordance with the process set out in Appendix 1; and

(c) the **legal owner** of an **aggregated generating facility** that is:

(i) directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW, unless the **aggregated generating facility** is part of an industrial complex;

(ii) a **blackstart resource**;

(iii) directly connected to the **bulk electric system** and within an industrial complex with **supply transmission service** greater than 67.5 MW; or

(iv) regardless of **maximum authorized real power rating**, material to this **reliability standard** and to the reliability of the **bulk electric system** as the **ISO** determines and publishes on the AESO website and may amend from time to time in accordance with the process set out in Appendix 1.

## 3. Requirements

**R1** Each **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** must have documentation for determining the **facility ratings** of its facilities:

(a) up to the low side terminals of the step-up transformer if the **legal owner** of the **generating unit** or **legal owner** of the **aggregated generating facility** does not own the step-up transformer; or

(b) including the step-up transformer and associated terminal equipment (as applicable based on ownership) if the **legal owner** of the **generating unit** or **legal owner** of the **aggregated generating facility** owns the step-up transformer.

**R1.1** The documentation must contain assumptions used to rate the facilities and at least one (1) of the following:

(a) design or construction information such as design criteria, ratings provided by equipment manufacturers, equipment drawings and/or specifications, engineering analyses, method(s) consistent with industry standards (e.g. the American National Standards Institute and the Institute of Electrical and Electronic Engineers ("IEEE")), or an established engineering practice that has been verified by testing or engineering analysis; or

(b) operational information such as commissioning test results, performance testing or historical performance records, any of which may be supplemented by engineering analyses.

**R1.2** The documentation must be consistent with the principle that the **facility ratings** do not exceed the most limiting applicable **equipment rating** of the individual equipment that comprises that facility.

**R2** Each **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** must have a documented methodology for determining the **facility ratings** of its facilities connected between the location specified in requirement R1 and the interface with a **transmission facility** (based on equipment ownership) that contains all of the following:

**R2.1** the method used to establish the **equipment ratings** of the equipment that comprises the facility must be consistent with at least one (1) of the following:

(a) ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications, such as the nameplate rating;

(b) one (1) or more industry standards developed through an open process such as the IEEE or the International Council on Large Electric Systems ("CIGRE"); or

(c) a practice that has been verified by testing, performance history or engineering analysis;

**R2.2** the underlying assumptions, design criteria, and methods used to determine the **equipment ratings** identified in requirement R2.1, including identification of how each of the following were considered:

(a) **equipment rating** standard(s) used in development of this method;

(b) ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications;

(c) ambient conditions (for particular or average conditions or as they vary in real time);

(d) operating limitations; and

(e) both summer and winter season operations, where summer is defined as May 1st at 12:01 AM Mountain Time to October 31st at 12:00 midnight Mountain Time and winter is defined as November 1st at 12:01 AM Mountain Time to April 30th at 12:00 midnight Mountain Time;

**R2.3** a statement that a **facility rating** must not exceed the most limiting applicable **equipment rating** of the individual equipment that comprises that facility;

**R2.4** the process by which the **equipment ratings** of the equipment that comprises a facility are determined, where:

**R2.4.1** the scope of equipment that comprises the facility, addressed in accordance with requirement R2.4 must include (based on equipment ownership), but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices; and

**R2.4.2** the scope of **equipment ratings** addressed in accordance with requirement R2.4 must include, as a minimum, both **normal ratings** and **emergency ratings**, such that:

**R2.4.2.1** the **emergency ratings** for equipment comprising power transformers must be specified for a 30 minute duration and the next 3.5 hour duration; and

**R2.4.2.2** the **emergency ratings** for transmission lines must be specified for a ten (10) minute duration.

**R3** Each **legal owner** of a **transmission facility** must have a documented methodology for determining the **facility ratings** of its facilities (except for those facilities associated with a **generating unit** or **aggregated generating facility** addressed in requirements R1 and R2) that contains all of the following:

**R3.1** the method used to establish the **equipment ratings** of the equipment that comprises the facility must be consistent with at least one (1) of the following:

(a) ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications, such as the nameplate rating;

(b) one (1) or more industry standards developed through an open process such as the IEEE or CIGRE; or

(c) a practice that has been verified by testing, performance history or engineering analysis;

**R3.2** the underlying assumptions, design criteria, and methods used to determine the **equipment ratings** identified in requirement R3.1, including identification of how each of the following were considered:

(a) **equipment rating** standard(s) used in development of this method;

(b) ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications;

(c) ambient conditions (for particular or average conditions or as they vary in);

(d) operating limitations; and

(e) both summer and winter season operations, where summer is defined as May 1st at 12:01 AM Mountain Time to October 31st at 12:00 midnight Mountain Time and winter is defined as November 1st at 12:01 AM Mountain Time to April 30th at 12:00 midnight Mountain Time;

**R3.3** a statement that a **facility rating** must not exceed the most limiting applicable **equipment rating** of the individual equipment that comprises that facility; and

**R3.4** the process by which the **equipment ratings** of the equipment that comprises a facility are determined, where:

**R3.4.1** the scope of equipment that comprises the facility, addressed in accordance with requirement R3.4, must include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices; and

**R3.4.2** the scope of **equipment ratings** addressed in accordance with requirement R3.4 must include, at a minimum, both **normal ratings** and **emergency ratings**, such that:

**R3.4.2.1** the **emergency ratings** for equipment comprising power transformers must be specified for a 30 minute duration and the next 3.5 hour duration; and

**R3.4.2.2** the **emergency ratings** for transmission lines must be specified for a ten (10) minute duration.

**R4** Intentionally left blank.

**R5** Intentionally left blank.

**R6** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** must have **facility ratings** for its facilities that are consistent with:

(a) the **facility ratings** methodology in accordance with requirements R2 or R3, for a **transmission facility**, a **generating unit** and an **aggregated generating facility**; and

(b) the documentation in accordance with requirement R1, for a **generating unit** and an **aggregated generating facility**.

**R7** Intentionally left blank.

**R8** Intentionally left blank.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of having documentation for determining the **facility ratings** as required in requirements R1, R1.1 and R1.2 exists.

**MR2** Evidence of having a documented **facility ratings** methodology as described in requirement R2 exists.

**MR3** Evidence of having a documented **facility ratings** methodology as described in requirement R3 exists.

**MR4** Intentionally left blank.

**MR5** Intentionally left blank.

**MR6** Evidence of having **facility ratings** that are consistent with the **facility ratings** methodology in accordance with requirements R2 and R3, and the documentation in accordance with requirement R1 exists.

**MR7** Intentionally left blank.

**MR8** Intentionally left blank.

## 5. Appendices

Appendix1 – Amending Process for List of Facilities

### Revision History

| Date | Description |
|---|---|
| 2019-12-01 | Unbolded “real time” |
| 2019-01-01 | Initial release |

**Appendix 1**

**Amending Process for List of Facilities**

In order to amend a list referenced in subsections (a)(ii), (b)(iv) and (c)(iii) of section 2, Applicability, the **ISO** must:

(a) upon determining that a **transmission facility**, **generating unit** or **aggregated generating facility** is to be added, notify the **legal owner** and **operator** in writing and determine an effective date, which must be no less than:

  (i) eight (8) full calendar quarters after the date of notice, where the **transmission facility**, **generating unit** or **aggregated generating facility** is commissioned prior to the date of notice; and

  (ii) no less than four (4) full calendar quarters after the date of notice, where the **transmission facility**, **generating unit** or **aggregated generating facility** is commissioned on or after the date of notice;

(b) upon determining that a **transmission facility**, **generating unit** or **aggregated generating facility** is to be deleted, notify the **legal owner** and **operator** in writing and determine an effective date on which the **legal owner** and **operator** will no longer be required to meet the applicable requirements; and

(c) publish the amended list with effective dates on the AESO website.

# Alberta Reliability Standard
# System Operating Limits Methodology for the Planning Horizon
# FAC-010-AB1-2.1

## 1. Purpose

The purpose of this **reliability standard** is to ensure that **system operating limits** used in the reliable planning of the **bulk electric system** are determined based on an established methodology or methodologies.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must have a documented **system operating limit** methodology for use in developing **system operating limits** that:

(a) is applicable for developing **system operating limits** used in the **ISO**'s planning horizon;

(b) states that **system operating limits** must not exceed any associated **facility rating**; and

(c) includes a description of how to identify the subset of **system operating limits** that qualify as **interconnected reliability operating limits**.

**R2** The **system operating limit** methodology of the **ISO** must include a requirement:

**R2.1** That **system operating limits** developed in the pre-**contingency** state, and with all facilities in service:

(a) result in:

i. **bulk electric system** performance that demonstrates transient, dynamic and voltage stability;

ii. all facilities operating within their **facility ratings**; and

iii. system conditions within thermal, voltage and stability limits;

and

(b) reflect expected system conditions and changes to **bulk electric system** topology.

**R2.2** That **system operating limits** developed starting with all facilities in service and following any single **contingency** including:

(a) single line to ground **fault** or three-phase **fault**, whichever is most severe, with **normal clearing**, on any **generating unit**, line, transformer or shunt device;

(b) loss of any **generating unit**, line, transformer or shunt device without a **fault**; or

(c) single pole block, with **normal clearing**, in a monopolar or bipolar high voltage direct current system;

result in **bulk electric system** performance that:

(d) demonstrates transient, dynamic and voltage stability;

(e) has all facilities operating within their **facility ratings**;

(f) is within voltage and stability limits; and

(g) has no **cascading** or uncontrolled separation,

with either or both of the following responses to the single **contingency** being acceptable:

(h) planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the facility on which the **fault** occurred or by the affected area; or

(i) **bulk electric system** reconfiguration through manual or automatic control or protection actions.

**R2.3** Intentionally left blank.

**R2.4** That following a single **contingency**, in preparation for the next **contingency** when developing **system operating limits**, the **ISO** may make system adjustments, including changes to generation, uses of the **transmission system**, and the **transmission system** topology.

**R2.5** That **system operating limits** developed starting with all facilities in service and following any of the multiple **contingencies** identified in **reliability standard** TPL-003-AB, result in **bulk electric system** performance that:

(a) demonstrates transient, dynamic and voltage **stability**;

(b) has all facilities operating within their **facility ratings**;

(c) is within voltage and stability limits; and

(d) has no **cascading** or uncontrolled separation,

with any of the following responses to such multiple **contingencies** being acceptable:

(e) planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the facility on which the **fault** occurred or by the affected area;

(f) **bulk electric system** reconfiguration through manual or automatic control or protection actions; or

(g) planned or controlled interruption of **demand** to **demand customers**, the planned removal of a **generating unit**, or the curtailment of firm, non-recallable power transfers.

**R2.6** Intentionally left blank.

**R3** In addition to requirements R1 through R2, the **ISO** must include within the **system operating limit** methodology a description of the:

(a) study model, which must include at least the Alberta system as well as the critical modeling details from other interconnected jurisdictions that would impact any facility under study;

(b) selection of applicable **contingencies**;

(c) level of system detail included in the study model used to determine **system operating limits**;

(d) allowed uses of **remedial action schemes**;

(e) anticipated **transmission system** configuration, generation **dispatch** and **load** level;

(f) criteria for determining when violating a **system operating limit** qualifies as an **interconnection reliability operating limit** and criteria for developing any associated **interconnection reliability operating limit** $T_v$; and

(g) any reliability margins applied.

**R4** The **ISO** must provide its **system operating limit** methodology, and any update to that methodology, to all of the following prior to implementation of the methodology or any update to the methodology:

(a) each adjacent planning authority; and

(b) each planning authority that indicated it has a **reliability**-related need for the methodology.

**R5** Intentionally left blank.

**R6** The **system operating limit** methodology of the **ISO** must include a requirement that:

**R6.1** for **interconnections** with other systems within the **WECC**, starting with all facilities in service and following any of the multiple **contingencies** identified in **reliability standard** TPL-003-AB or any of the following multiple **contingencies**:

(a) simultaneous permanent phase to ground **faults** of each of two (2) adjacent transmission circuits on a multiple circuit tower with **normal clearing**. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five (5) towers at each station, this condition is an acceptable risk and therefore can be excluded;

(b) a permanent phase to ground **fault** on any **generating unit**, transmission circuit, transformer, or **collector bus** section with delayed **fault** clearing except for **collector bus** sectionalizing breakers or **collector bus** tie breakers as specified in requirement R6.2;

(c) simultaneous permanent loss of both poles of a direct current bipolar facility without an alternating current **fault**;

(d) the failure of a circuit breaker associated with a remedial action scheme to operate when required following the loss of any **system element** without a **fault**, or a permanent phase to ground **fault**, with **normal clearing**, on any transmission circuit, transformer or **collector bus** section; or

(e) a single-line-to-ground **fault** with **normal clearing** on common mode **contingency** of two (2) adjacent circuits on separate towers unless the **ISO** determines the event frequency is less than one (1) in thirty (30) years, the **system operating limits** result in **bulk electric system** performance that:

(f) demonstrates transient, dynamic and voltage **stability**;

(g) has all facilities operating within their **facility ratings**;

(h) is within voltage and stability limits; and

(i) has no **cascading** or uncontrolled separation,

with any of the following responses to such multiple **contingencies** being acceptable:

(j) planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the facility on which the **fault** occurred or by the affected area;

(k) **bulk electric system** reconfiguration through manual or automatic control or protection actions; or

(l) planned or controlled interruption of **demand** to **demand customers**, the planned removal of a **generating unit**, or the curtailment of firm, non-recallable power transfers.

**R6.2** for **interconnections** with other systems within the **WECC**, starting with all facilities in service and following either of these multiple **contingencies**:

(a) a common mode **outage** of two (2) **generating units** connected to the same switchyard not otherwise addressed by **reliability standard** FAC-010-AB; or

(b) the loss of multiple **collector bus** sections as a result of failure or delayed clearing of a **collector bus** tie or **collector bus** sectionalizing breaker to clear a permanent phase to ground **fault**, the **system operating limits** result in **bulk electric system** performance such that **cascading** does not occur on other systems in other jurisdictions within the **WECC**.

**R6.3** where the **ISO** makes changes to any **contingencies** and required responses identified in requirements R6.1 and R6 .2 for specific facilities on **interconnections** to other systems within the **WECC** in accordance with the **WECC** performance category adjustment process based upon system performance and robust design, the **system operating limits** result in **bulk electric system** performance that satisfies the performance requirements in requirements R2.4.

## 4. Measures

The following measures correspond to the requirements identified in Section 3 of this **reliability standard**. For example, MR1 is the measure for R1.

**MR1** Evidence of having a documented **system operating limit** methodology as required in requirement R1 exists.

**MR2** Evidence of the **system operating limit** methodology including requirements as required in sub requirements R2.1, R2.2, R2.4 and R2.5 exists.

**MR3** Evidence of the **system operating limit** methodology including the description(s) as required in requirement R3 exists.

**MR4** Evidence of providing the **system operating limit** methodology as required in requirement R4 exists. Evidence may include, but is not limited to, email or mail to an appropriate recipient that identifies contents submitted.

**MR5** Intentionally left blank.

**MR6** Evidence of the **system operating limit** methodology including requirements as required in sub requirements R6.1 through R6.3 exists.

## Revision History

| Effective | Description |
|---|---|
| 2012-07-01 | Initial Release |
| 2015-09-01 | Revised for ISO assumption of RC functionality for the Alberta footprint |
| 2016-08-30 | Inclusion of the defined term **system element**. |

## 1. Purpose

To ensure that **system operating limits** used in the reliable operation of the **bulk electric system** are determined based on an established methodology or methodologies.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must have a documented methodology for use in developing **system operating limits** (**system operating limit** methodology) within its area. This **system operating limit** methodology must:

**R1.1** be applicable for developing **system operating limits** used in the operations horizon;

**R1.2** state that **system operating limits** must not exceed associated **facility ratings**; and

**R1.3** include a description of how to identify the subset of **system operating limits** that qualify as **interconnection reliability operating limits**.

**R2** The **system operating limit** methodology of the **ISO** must include a requirement that **system operating limits** provide **bulk electric system** performance consistent with the following:

**R2.1** in the **pre-contingency** state, the **bulk electric system** must demonstrate transient, dynamic and voltage stability; all facilities must be within their **facility ratings** and within their thermal, voltage and stability limits. In the determination of **system operating limits**, the **bulk electric system** condition used must reflect current or expected system conditions and must reflect changes to system topology such as facility outages;

**R2.2** following the single **contingencies**[1] identified in requirement 2.2.1 through requirement 2.2.3, the system must demonstrate transient, dynamic and voltage stability; all facilities must be operating within their **facility ratings** and within their thermal, voltage and stability limits; and **cascading** or uncontrolled separation must not occur:

**R2.2.1** single line to ground or three (3) -phase **fault** (whichever is more severe), with **normal clearing**, on any **generating unit**, **aggregated generating facility**, line, transformer, or shunt device that is **faulted**;

**R2.2.2** loss of any **generating unit**, **aggregated generating facility**, line, transformer, or shunt device without a **fault**; and

**R2.2.3** single pole block, with **normal clearing**, in a monopolar or bipolar high voltage direct current system;

**R2.3** in determining the system's response to a single **contingency**, the following will be acceptable:

**R2.3.1** planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the **faulted** facility or by the affected area;

---

[1] The **contingencies** identified in FAC-011-AB-2 requirement R2.2.1 through requirement R2.2.3 are the minimum **contingencies** that must be studied but are not necessarily the only **contingencies** that are studied.

**R2.3.2** interruption of other network customers, (a) only if the system has already been adjusted, or is being adjusted, following at least one prior outage, or (b) if the real-time operating conditions are more adverse than anticipated in the corresponding studies; and

**R2.3.3** system reconfiguration through manual or automatic control or protection actions; and

**R2.4** to prepare for the next **contingency**, system adjustments may be made, including changes to generation, uses of the **transmission system**, and the **transmission system** topology.

**R3** The **ISO**'s methodology for determining **system operating limits**, must include, as a minimum, a description of the following, along with any **reliability** margins applied for each:

**R3.1** study model (must include at least the entire **ISO** area as well as the critical modeling details from other **reliability coordinator areas** that would impact the facility or facilities under study);

**R3.2** selection of applicable **contingencies**;

**R3.3** a process for determining which of the stability limits associated with the list of multiple **contingencies** (as determined by the **ISO** in accordance with FAC-014 requirement R6) are applicable for use in the operating horizon given the actual or expected system conditions;

**R3.3.1** this process must address the need to modify these limits, to modify the list of limits, and to modify the list of associated multiple **contingencies**;

**R3.4** level of detail of system models used to determine **system operating limits**;

**R3.5** allowed uses of **remedial action schemes** or remedial action plans;

**R3.6** anticipated **transmission system** configuration, generation **dispatch** and load level; and

**R3.7** criteria for determining when violating a **system operating limit** qualifies as an **interconnection reliability operating limit** and criteria for developing any associated **interconnection reliability operating limit Tv**.

**R4** The **ISO** must issue its **system operating limit** methodology and any changes to that methodology, prior to the effective date of the methodology or of a change to the methodology, to all of the following:

**R4.1** each adjacent **reliability coordinator** and each **reliability coordinator** that indicated it has a reliability-related need for the methodology.

**R4.2** each **planning authority** and **transmission planner** that models any portion of the **ISO**'s area.

**R4.3** each **operator** of a **transmission facility** that operates in the **ISO**'s area.

**R5** Intentionally left blank.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** The **system operating limit** methodology of the **ISO** may address all of the items listed in requirement R1.1 through requirement R1.3. Evidence may include, but is not limited to, a documented **system operating limit** methodology, or other equivalent evidence as required in requirement R1.

**MR2** Evidence of including requirements in the **system operating limit** methodology as set out in requirement R2. Evidence may include, but is not limited to, a documented **system operating limit** methodology, or other equivalent evidence as set out in requirement R2.

**MR3** Evidence of including all of the items as required in requirement R3.1 through R3.7 in the **system operating limit** methodology. Evidence may include, but is not limited to, a documented **system operating limit** methodology, documented processes or other equivalent evidence as required in requirement R2.

**MR4** The **ISO** may have evidence of issuing the **system operating limit** methodology, and any changes to that methodology, including the date they were issued, as required in requirement R4. Evidence may include, but is not limited to, emails, or other equivalent evidence.

**MR5** Intentionally left blank.

### Revision History

| Date | Description |
|---|---|
| 2019-12-01 | Unbolded “real-time” |
| 2015-09-01 | Initial release. |

# Alberta Reliability Standard
# Establish and Communicate System Operating Limits
# FAC-014-AB1-2

## 1. Purpose

The purpose of this **reliability standard** is to establish and communicate **system operating limits** to be used in the reliable planning and operation of the **bulk electric system**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must ensure that **system operating limits**, including **interconnection reliability operating limits**, for its area are established and that the **system operating limits** (including **interconnection reliability operating limits**) are consistent with its **system operating limit** methodology.

**R2** Intentionally left blank.

**R3** Intentionally left blank.

**R4** Intentionally left blank.

**R5** The **ISO** must provide its **system operating limits** and **interconnection reliability operating limits** in the operating horizon to:

(a) each adjacent **reliability coordinator**;

(b) each **operator** of a **transmission facility** within its area that has a **reliability**-related need for those limits; and

(c) each entity that has a **reliability**-related need for those limits and provides a written request for delivery of those limits.

**R5.1** For each **interconnection reliability operating limit**, the **ISO** must provide the following supporting information:

**R5.1.1** identification and status of the associated **system element** (or group of **system elements**) that is (are) critical to the derivation of the **interconnection reliability operating limit**;

**R5.1.2** the value of the **interconnection reliability operating limit** and its associated Tv;

**R5.1.3** the associated **contingency**(ies); and

**R5.1.4** the type of limitation represented by the **interconnection reliability operating limit** (e.g., voltage collapse, angular stability).

**R5.2** Intentionally left blank.

**R5.3** The **ISO** must provide its **system operating limits** (including the subset of **system operating limits** that are **interconnection reliability operating limits**) in the planning horizon to adjacent **planning authorities.**

**R5.4** Intentionally left blank.

**R6** The **ISO** must identify and develop a list of the subset of multiple **contingencies** from **reliability standard** TPL-003-AB, which result in stability limits as determined if any that exist in its planning horizon.[1]

**R6.1** Intentionally left blank.

**R6.2** Intentionally left blank.

## 4 Measures

The following measures correspond to the requirements identified in Section 3 of this **reliability standard**. For example, MR1 is the measure for R1.

**MR1** Evidence that the **ISO**'s **system operating limits**, including **interconnection reliability operating limits**, for its area are established and consistent with its **system operating limit** methodology. Evidence may include, but is not limited to, dated reports, voice recordings, business practices or other equivalent evidence.

**MR2** Intentionally left blank.

**MR3** Intentionally left blank.

**MR4** Intentionally left blank.

**MR5** Evidence to confirm the **ISO** provided its **system operating limits** and **interconnection reliability operating limits** and supporting information as required in requirement R5 exists. Evidence may include, but is not limited to, records of email communication to appropriate recipients that identify contents submitted, or other equivalent evidence.

**MR6** Evidence that the **ISO** identified and listed the subset of multiple **contingencies** as required in requirement R6 exists. Evidence may include, but is not limited to, dated reports, letters, or other documentation containing the list of multiple **contingencies**.

**MR6.1** Intentionally left blank.

**MR6.2** Intentionally left blank.

## 5. Appendices

No appendices have been defined for this **reliability standard**.

## Revision History

| Date | Description |
|---|---|
| 2016-08-30 | Inclusion of the defined term **system element**. |
| 2015-09-01 | Revised for ISO assumption of RC functionality for the Alberta footprint |
| 2012-10-01 | Initial Release |

[1] Requirement R6 is referenced in requirement R3.3 of FAC-011-AB

## 1. Purpose

The purpose of this **reliability standard** is to ensure the **legal owner** of a **transmission facility** of a major transmission path, including any associated **transmission facility**, has a *Transmission Maintenance and Inspection Plan* such that a reliable path is available*.*

## 2. Applicability

This **reliability standard** applies to the **legal owner** of a **transmission facility** that is, or is part of, a major transmission path identified in the table "*Major WECC Transfer Paths in the Bulk Electric System*" as provided by the **WECC**.

## 3. Requirements

**R1** The *Transmission Maintenance and Inspection Plan* of the **legal owner** of a **transmission facility** must detail its inspection and maintenance requirements and must apply to each **transmission facility** that is associated with each of the transmission paths identified by the **ISO**.

**R1.1** The **legal owner** of a **transmission facility** must review its *Transmission Maintenance and Inspection Plan* annually and update it as required.

**R1.2** The **legal owner** of a **transmission facility** must annually submit its *Transmission Maintenance and Inspection Plan* and any updates to the **ISO**.

**R2** The *Transmission Maintenance and Inspection Plan* of the **legal owner** of a **transmission facility** must include without limitation the following maintenance categories:

**R2.1** Transmission line maintenance details:

**R.2.1.1** patrol/inspection;

**R.2.1.2** contamination control; and

**R.2.1.3** tower and wood pole structure management;

**R2.2** Station maintenance details:

**R.2.2.1** inspections;

**R.2.2.2** contamination control; and

**R.2.2.3** equipment maintenance for the following:

(a) circuit breakers;

(b) power transformers (including phase-shifting transformers);

(c) regulators; and

(d) **reactive power** devices (including, but not limited to, shunt capacitors, series capacitors, static VAR compensators, synchronous condensers, shunt reactors, and tertiary reactors).

**R3** The maintenance practices of the **legal owner** of a **transmission facility** in the *Transmission Maintenance and Inspection Plan* must be either performance-based, time-based, or condition-based, or a combination of all three (3).

The *Tranmsision Maintenance and Inspection Plan* of the **legal owner** of a **transmission facility** must include scheduled intervals for any time-based maintenance activities and/or a description supporting condition or performance-based maintenance practices including a description of the condition or performance based trigger.

**R4** The **legal owner** of a **transmission facility** must implement its *Transmission Maintenance and Inspection Plan* and retain records that demonstrate such implementation including without limitation the following:

**R4.1** The names of individual or crew members responsible for performing the work or inspection;

**R4.2** The date(s) the work or inspection was performed;

**R4.3** The **transmission facility** on which the work or inspection was performed; and

**R4.4** A description of the inspection or maintenance performed.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** A documented *Transmission Maintenance and Inspection Plan* as identified in requirement R1 exists and covers each **transmission facility** as identified by the **ISO**.

**MR1.1** Evidence exists that shows the **legal owner** of a **transmission facility** reviewed their *Transmission Maintenance and Inspection Plan* annually and updated it as needed.

**MR1.2** The *Transmission Maintenance and Inspection Plan* and updates, if any, are received by the **ISO** annually.

**MR2** The *Transmission Maintenance and Inspection Plan* addresses the required maintenance details of requirement R2.

**MR3** The *Transmission Maintenance and Inspection Plan* addresses the items in requirement R3.

**MR4** Records exist that show the **legal owner** of a **transmission facility** implemented and followed its *Transmission Maintenance and Inspection Plan* .

## Revision History

| Effective | Description |
|---|---|
| 2015-07-01 | Transmission paths identified by the AESO for the purposes of requirement R1 updated to include new Bennett 520S equipment and 632 Russell equipment and moved from the Appendix to another document.<br>Administrative update to standardize formatting, definitions and drafting style. |
| 2012-12-17 | Administrative update – "*TFO*" replaced with "*legal owner* of a *transmission facility*"; and other minor clean up items. |
| 2010-09-10 | Initial Release |

# Alberta Reliability Standard
# Evaluation of Interchange Transactions
# INT-006-AB-4

## 1. Purpose

The purpose of this **reliability standard** is to ensure that responsible entities conduct a **reliability** assessment of each **arranged interchange** before it is implemented.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must approve or deny each on-time **arranged interchange** or emergency **arranged interchange** that it receives and must do so prior to the expiration of the time period defined in Appendix 1, column B.

**R1.1** The **ISO** must, when it is either the source **balancing authority** or sink **balancing authority** deny the **arranged interchange** or curtail **confirmed interchange** if it does not expect to be capable of supporting the magnitude of the **interchange**, including ramping, throughout the duration of the **arranged interchange**.

**R1.2** The **ISO** must deny the **arranged interchange** or curtail **confirmed interchange** if the **scheduling path** (proper connectivity of **adjacent balancing authorities**) between it and its **adjacent balancing authorities** is invalid.

**R2** The **ISO** must approve or deny each on-time **arranged interchange** or emergency **arranged interchange** that it receives and must do so prior to the expiration of the time period defined in Appendix 1, column B.

**R2.1** The **ISO** must deny the **arranged interchange** or curtail **confirmed interchange** if the transmission path (proper connectivity of adjacent transmission service providers) between it and its adjacent transmission service providers is invalid.

**R3** The **ISO** must, when it receives a **reliability** adjustment **arranged interchange**, approve or deny it prior to the expiration of the time period defined in Appendix 1, column B.

**R4** The **ISO** must when it is a sink **balancing authority** confirm that none of the following conditions exist prior to transitioning an **arranged interchange** to **confirmed interchange**:

(a) it is a **reliability** adjustment **arranged interchange**, the time period specified in Appendix 1, column B has elapsed, and the **ISO** or the source **balancing authority** associated with the **arranged interchange** has not communicated its approval of the transition;

(b) it is not a **reliability** adjustment **arranged interchange**, the time period specified in Appendix 1, column B, has elapsed, and not all **balancing authorities** and transmission service providers associated with the **arranged interchange** have communicated their approval of the transition; or

(c) it is not a **reliability** adjustment **arranged interchange**, the time period specified in Appendix 1, column B, has elapsed, and any entity associated with the **arranged interchange** has communicated its denial of the transition.

**R5** For each **arranged interchange** that is transitioned to **confirmed interchange**, the **ISO** must, when it is the sink **balancing authority**, notify the following entities of the on-time **confirmed interchange** such that the notification is delivered in time to be incorporated into scheduling systems prior to ramp start as specified in Appendix 1, column D:

**R5.1** the source **balancing authority**;

**R5.2** each intermediate **balancing authority**;

**R5.3** each **reliability coordinator** associated with each **balancing authority** included in the **arranged interchange**;

**R5.4** each transmission service provider included in the **arranged interchange**; and

**R5.5** each purchasing selling entity included in the **arranged interchange**.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of either approving or denying **arranged interchange** as required in requirement R1 exists. Evidence may include, but is not limited to, dated and time stamped electronic logs or other equivalent evidence.

**MR2** Evidence of either approving or denying **arranged interchange** as required in requirement R2 exists. Evidence may include, but is not limited to, dated and time stamped electronic logs or other equivalent evidence.

**MR3** Evidence of either approving or denying **reliability** adjustment **arranged interchange** as required in requirement R3 exists. Evidence may include, but is not limited to, dated and time stamped electronic logs, studies or other equivalent evidence.

**MR4** Evidence of confirming none of the conditions exist prior to transitioning an **arranged interchange** to **confirmed interchange** as required in requirement R4 exists. Evidence may include, but is not limited to, an interchange transaction without an implemented e-tag, or other equivalent evidence.

**MR5** Evidence of notifying entities of the on-time **confirmed interchange** as required in requirement R5 exists. Evidence may include, but is not limited to, dated and time stamped electronic logs, voice recordings or other equivalent evidence.

## 5. Appendices

Appendix 1 – Timing Tables

### Revision History

| Date | Description |
|---|---|
| 2018-10-01 | Initial release. |

**Appendix 1 – Timing Tables**
**Timing Requirements for WECC**

| | | A | B | C | D |
|---|---|---|---|---|---|
| If **arranged interchange**[1] is submitted | Time Classification | Sink BA makes initial distribution of **arranged interchange**[2] | BA and TSP conduct reliability assessments | Compilation and distribution status[2] | BA prepares **confirmed interchange** for implementation |
| >1 hour after the start time | ATF | | Entities have up to 2 hours to respond. | | N/A |
| <10 minutes prior to ramp start and ≤1 hour after transaction start time where transaction start time is at the top of the hour | Late | | Entities have up to 10 minutes to respond. | | ≤ 3 minutes after receipt of **confirmed interchange** |
| <15 minutes prior to ramp start and ≤1 hour after transaction start time where transaction start time is not at the top of the hour | Late | | Entities have up to 10 minutes to respond. | | ≤ 3 minutes after receipt of **confirmed interchange** |
| 10 minutes prior to ramp start where transaction start time is at the top of the hour | On-time | | ≤ 5 minutes from **arranged interchange** receipt | | ≥ 3 minutes prior to ramp start |
| 11 minutes prior to ramp start where transaction start time is at the top of the hour | On-time | | ≤ 6 minutes from **arranged interchange** receipt | | ≥ 3 minutes prior to ramp start |
| 12 minutes prior to ramp start where transaction start time is at the top of the hour | On-time | | ≤ 7 minutes from **arranged interchange** receipt | | ≥ 3 minutes prior to ramp start |

1 Time classifications and deadlines apply to both initial **arranged interchange** submittal and any subsequent modifications to the **arranged interchange**.
2 See NAESB WEQ004. The times are being retained in the NAESB tables but are removed here since they are not being referenced in requirements.

| | | A | B | C | D |
|---|---|---|---|---|---|
| If **arranged interchange**[1] is submitted | Time Classification | Sink BA makes initial distribution of **arranged interchange**[2] | BA and TSP conduct reliability assessments | Compilation and distribution status[2] | BA prepares **confirmed interchange** for implementation |
| 13 minutes prior to ramp start where transaction start time is at the top of the hour | On-time | | ≤ 8 minutes from **arranged interchange** receipt | | ≥ 3 minutes prior to ramp start |
| 14 minutes prior to ramp start where transaction start time is at the top of the hour | On-time | | ≤ 9 minutes from **arranged interchange** receipt | | ≥ 3 minutes prior to ramp start |
| < 1 hour and ≥ 15 minutes prior to ramp start | On-time | | ≤ 10 minutes from **arranged interchange** receipt | | ≥ 3 minutes prior to ramp start |
| ≥ 1 hour and < 4 hours prior to ramp start | On-time | | < 20 minutes from **arranged interchange** receipt | | ≥ 39 minutes prior to ramp start |
| ≥ 4 hours prior to ramp start | On-time | | ≤ 2 hours from **arranged interchange** receipt | | ≥ 1 hour 58 minutes prior to ramp start |
| Submitted before 10:00 PPT with start time ≥ 00:00 PPT of following day | On-time | | By 12:00 PPT of day the **arranged interchange** was recieved | | ≥ 1 hour 58 minutes prior to ramp start |

# Alberta Reliability Standard
# Implementation of Interchange
# INT-009-AB-2.1

## 1. Purpose

The purpose of this **reliability standard** is to ensure that **balancing authorities** implement the **interchange** as agreed upon in the **interchange** confirmation process.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must agree with each of its **adjacent balancing authorities** that its composite **confirmed interchange** with that **adjacent balancing authority**, at mutually agreed upon time intervals, excluding **dynamic schedules** and pseudo-ties and including any **interchange** per INT-010-AB not yet captured in the **composite confirmed interchange**, is:

**R1.1** identical in magnitude to that of the **adjacent balancing authority**; and

**R1.2** opposite in sign or direction to that of the **adjacent balancing authority**.

**R2** The **ISO** when it is either the attaining **balancing authority** or the native **balancing authority** must use a dynamic value emanating from a common source that is agreed upon with the other **balancing authority** to account for the pseudo-tie in the **net actual interchange** term of its control **area control error** or alternate control process.

**R3** The **ISO** must, if it is the **balancing authority** in whose area the high-voltage direct current **intertie** is controlled, coordinate the **confirmed interchange** prior to its implementation with the **operator** of the high-voltage direct current **intertie**.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of agreeing on composite **confirmed interchange** with **adjacent balancing authorities** as required in requirement R1 exists. Evidence may include, but is not limited to dated logs, voice recordings, electronic records or other equivalent evidence.

**MR2** Evidence of using a dynamic value emanating from an agreed upon common source as required in requirement R2 exists. Evidence may include, but is not limited to dated logs, voice recordings, electronic records, written agreement or other equivalent evidence.

**MR3** Evidence of coordinating the **confirmed interchange** prior to its implementation with the **operator** of the high-voltage direct current **intertie** as required in requirement R3 exists. Evidence may include, but is not limited to dated logs, electronic records or other equivalent evidence.

## Revision History

| Date | Description |
|---|---|
| 2018-10-01 | Initial release. |

# Alberta Reliability Standard
# Interchange Initiation and Modification for Reliability
# INT-010-AB-2.1

## 1. Purpose

The purpose of this **reliability standard** is to provide guidance for required actions on **confirmed interchange** or **implemented interchange** to address **reliability**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must, if it experiences a loss of resources covered by an energy sharing agreement or other **reliability** needs covered by an energy sharing agreement, ensure that a request for **interchange** is submitted with a start time no more than sixty (60) minutes beyond the resource loss or **reliability** need. If the use of the energy sharing agreement does not exceed sixty (60) minutes from the time of the resource loss or **reliability** need, no request for **interchange** is required.

**R2** The **ISO** must, when it is the sink **balancing authority**, after modifying a **confirmed interchange** or **implemented interchange** for actual or anticipated **reliability**-related reasons, ensure that a **reliability** adjustment **arranged interchange** reflecting the modification is submitted within sixty (60) minutes of the start of the modification.

**R3** The **ISO** must, when it is a sink **balancing authority**, after scheduling **interchange** for actual or anticipated **reliability**-related reasons, ensure that a request for **interchange** is submitted reflecting that **interchange schedule** within sixty (60) minutes of the start of the scheduled **interchange**.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of ensuring that a **request for interchange** is submitted as required in requirement R1 exists. Evidence may include, but is not limited to, dated and time-stamped request for **interchange**, electronic logs or other equivalent evidence.

**MR2** Evidence of ensuring that a **reliability** adjustment **arranged interchange** is submitted as required in requirement R2 exists. Evidence may include, but is not limited to, dated and time-stamped **reliability** adjustment **arranged interchange**, electronic logs or other equivalent evidence.

**MR3** Evidence of ensuring that a **reliability** adjustment **arranged interchange** is submitted as required in requirement R2 exists. Evidence may include, but is not limited to, dated and time-stamped **reliability** adjustment **arranged interchange**, electronic logs or other equivalent evidence.

## Revision History

| Date | Description |
|---|---|
| 2018-10-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to provide the **ISO** with the capabilities necessary to monitor and analyze data needed to perform their **reliability** functions.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO.**

## 3. Requirements

**R1** The **ISO** must have data exchange capabilities with entities, that the **ISO** deems necessary, for it to perform operational planning analysis.

**R2** The **ISO** must have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the **ISO**'s primary **control centre**, for the exchange of real time data with entities it deems necessary, for performing its real time monitoring and real time assessments.

**R3A** The **ISO** must test its primary **control centre** data exchange capabilities specified in requirement R2 for redundant functionality at least once every 90 **days**.

**R3B** The **ISO** must, if the test conducted pursuant to requirement R3A is unsuccessful, initiate action within 2 hours to restore redundant functionality.

**R4** The **ISO** must provide its real time operating personnel with the authority to approve planned outages and maintenance of its telecommunication, monitoring, and analysis capabilities.

**R5** The **ISO** must, as necessary, monitor:

(a) **system elements** that are part of the **bulk electric system**;
(b) the status of **remedial action schemes**; and
(c) **system elements** that are not part of the **bulk electric system**,

within Alberta and neighbouring **reliability coordinator areas**, to identify any **system operating limit** exceedances and to determine any **interconnection reliability operating limit** exceedances within Alberta.

**R6** The **ISO** must have monitoring systems that provide information utilized by the **ISO**'s operating personnel, giving particular emphasis to alarm management and awareness systems, automated data transfers, and synchronized information systems, over a redundant infrastructure.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of having data exchange capabilities as required in requirement R1 exists. Evidence may include a document that lists the **ISO**'s data exchange capabilities with entities, that the **ISO** deems necessary, for it to perform operational planning analysis, or other equivalent evidence.

**MR2** Evidence of having data exchange capabilities as required in requirement R2 exists. Evidence may include system specifications, system diagrams, other documentation that lists the **ISO**'s data exchange capabilities, or other equivalent evidence.

**MR3A** Evidence of testing the **ISO**'s primary **control centre** data exchange capabilities for redundant functionality as required in requirement R3A exists. Evidence may include dated and time-stamped test records, operator logs, voice recordings, electronic communications, or other equivalent evidence.

**MR3B** Evidence of initiating action within 2 hours to restore redundant functionality of the **ISO**’s primary **control centre** data exchange capabilities as required in requirement R3B exists. Evidence may include dated and time-stamped test records, operator logs, voice recordings, electronic communications, or other equivalent evidence.

**MR4** Evidence of providing the **ISO**’s real time operating personnel with the authority as required in requirement R4 exists. Evidence may include a documented procedure, or other equivalent evidence.

**MR5** Evidence of monitoring **system elements** and **remedial action schemes** as required in requirement R5 exists. Evidence may include energy management system description documents, computer printouts, SCADA data collection, or other equivalent evidence.

**MR6** Evidence of having monitoring systems as required in requirement R6 exists. Evidence may include energy management system description documents, computer printouts, SCADA data collection, or other equivalent evidence.

### Revision History

| Date | Description |
|---|---|
| 2019-12-01 | Initial release. |

# Alberta Reliability Standard
# Reliability Coordination Current Day Operations
# IRO-005-AB1-3.1a

## 1. Purpose

The **ISO** must be continuously aware of conditions within its area and include this information in its reliability assessments. The **ISO** must monitor **bulk electric system** parameters that may have significant impacts upon its area and neighbouring **reliability coordinator areas**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** Intentionally left blank.

**R1.1** Intentionally left blank.

**R1.2** Intentionally left blank.

**R1.3** Intentionally left blank.

**R1.4** Intentionally left blank.

**R1.5** Intentionally left blank.

**R1.6** Intentionally left blank.

**R1.7** Intentionally left blank.

**R1.8** Intentionally left blank.

**R1.9** Intentionally left blank.

**R1.10** Intentionally left blank.

**R2** Intentionally left blank.

**R3** The **ISO** must ensure that it is aware of geomagnetic disturbance forecast information and develop any required response plans.

**R4** Intentionally left blank.

**R5** Intentionally left blank.

**R6** Intentionally left blank.

**R7** Intentionally left blank.

**R8** Intentionally left blank.

**R9** Intentionally left blank.

**R10** Intentionally left blank.

**R11** Intentionally left blank.

**R12** Intentionally left blank.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this reliability standard. For example, MR1 is the measure for requirement R1.

**MR1** Intentionally left blank.

**MR2** Intentionally left blank.

**MR3** The **ISO** may have evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications or equivalent evidence to demonstrate that it was aware of geomagnetic disturbance (GMD) forecast information and evidence of the development of any required response plans.

**MR4** Intentionally left blank.

**MR5** Intentionally left blank.T

**MR6** Intentionally left blank.

**MR7** Intentionally left blank.

**MR8** Intentionally left blank.

**MR9** Intentionally left blank.

**MR10** Intentionally left blank.

**MR11** Intentionally left blank.

**MR12** Intentionally left blank.

## Revision History

| Effective Date | Description |
|---|---|
| 2019-12-01 | Removed all requirements that have been retired at NERC. requirement R3 will be retained until NERC EOP-010-1 is adopted for application in Alberta. |
| 2016-08-30 | Inclusion of the defined term **system element**. |
| 2015-04-01 | Initial release. |

# Alberta Reliability Standard
# Reliability Coordination – Transmission Loading Relief
# IRO-006-AB-5

## 1. Purpose

To ensure coordinated action between **Interconnections** when implementing **Interconnection**-wide transmission loading relief procedures to prevent or manage potential or actual **system operating limit** and **interconnection reliability operating limit** exceedances to maintain reliability of the **bulk electric system**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** When the **ISO** receives a request pursuant to an **Interconnection**-wide transmission loading relief procedure (such as Eastern Interconnection Transmission Loading Relief, WECC Unscheduled Flow Mitigation, or congestion management procedures from the ERCOT Protocols) from any **reliability coordinator**, **balancing authority**, or **transmission operator** in another **Interconnection** to curtail an **interchange transaction** that crosses an **Interconnection** boundary, the **ISO** must comply with the request, unless it provides a reliability reason to the requestor why it cannot comply with the request.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this reliability standard. For example, MR1 is the measure for requirement R1.

**MR1** The **ISO** may have evidence (such as dated logs, voice recordings, **e-tag** histories, and studies, in electronic or hard copy format) that, when a request to curtail an **interchange transaction** crossing an **Interconnection** boundary pursuant to an **Interconnection**-wide transmission loading relief procedure was made from another **reliability coordinator**, **balancing authority**, or **transmission operator** in that other **Interconnection**, the **ISO** complied with the request or provided a reliability reason why it could not comply with the request.

## Revision History

| Effective Date | Description |
|---|---|
| 2015-04-01 | Initial release. |

# Alberta Reliability Standard
# Qualified Transfer Path Unscheduled Flow Relief
# IRO-006-WECC-AB-2

## 1. Purpose

The purpose of this **reliability standard** is to mitigate transmission overloads due to unscheduled flow on **qualified transfer paths**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must approve schedule curtailment requests submitted to mitigate transmission overloads on **qualified transfer paths**, implement alternative actions, or a combination thereof that collectively meets the relief requirement.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard.** For example, MR1 is the measure for requirement R1.

**MR1** **E-tags**, voice recordings or operator logs exist and are provided on request. **E-tags**, voice recordings or operator logs contain content confirming requirement R1 is met.

## Revision History

| Date | Description |
|---|---|
| 2015-04-01 | Initial release. |

# Alberta Reliability Standard
# Reliability Coordinator Operational Analyses and Real-time Assessments
# IRO-008-AB-2

## 1. Purpose

The purpose of this **reliability standard** is to perform analyses and assessments to prevent instability, uncontrolled separation, and **cascading**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must perform an operational planning analysis that will allow it to assess whether the planned operations for the next day will exceed **system operating limits** and **interconnection reliability operating limits** within its **wide-area**.

**R2** The **ISO** must have an operating plan for next-day operations to address potential **system operating limit** and **interconnection reliability operating limit** exceedances identified as a result of its operational planning analysis as performed in requirement R1.

**R3** Intentionally left blank.

**R4** The **ISO** must perform a real time assessment at least once every 30 minutes.

**R5** Intentionally left blank.

**R6** Intentionally left blank.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of performing an operational planning analysis as required in requirement R1 exists. Evidence may include a completed operational planning analysis, dated power flow study results, or other equivalent evidence.

**MR2** Evidence of having an operating plan as required in requirement R2 exists. Evidence may include plans for precluding operating in excess of each **system operating limit** and **interconnected reliability operating limit** that were identified as a result of the operational planning analysis, or other equivalent evidence**.**

**MR3** Intentionally left blank.

**MR4** Evidence of performing a real time assessment at least once every 30 minutes as required in requirement R4 exists. Evidence may include dated computer logs showing times of assessment as conducted, dated checklists, or other equivalent evidence.

**MR5** Intentionally left blank.

**MR6** Intentionally left blank.

## Revision History

| Date | Description |
|---|---|
| 2019-12-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to prevent instability, uncontrolled separation, or **cascading** outages that adversely impact the **reliability** of the **Interconnection** by ensuring prompt action to prevent or mitigate instances of exceeding **interconnection reliability operating limits**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO.**

## 3. Requirements

**R1** The **ISO** must, for each **interconnection reliability operating limit** that the **ISO** identifies one or more **days** prior to the current **day**, have one or more operating processes, procedures, or plans that identify actions to take, or actions to direct others to take, up to and including load shedding, that:

**R1.1** can be implemented in time to prevent the identified **interconnection reliability operating limit** exceedance; and

**R1.2** mitigate the magnitude and duration of an **interconnection reliability operating limit** exceedance such that the **interconnection reliability operating limit** exceedance is relieved within the **interconnection reliability operating limit Tv**.

**R2** The **ISO** must initiate one or more operating processes, procedures, or plans that are intended to prevent an **interconnection reliability operating limit** exceedance, as identified in the **ISO**'s real time monitoring or real time assessment.

**R3** The **ISO** must act or direct others to act so that the magnitude and duration of an **interconnection reliability operating limit** exceedance is mitigated within the **interconnection reliability operating limit Tv**, as identified in the **ISO**'s real time monitoring or real time assessment.

**R4** The **ISO** must operate to the most limiting **interconnection reliability operating limit** or **interconnection reliability operating limit Tv** in instances where there is a difference in an **interconnection reliability operating limit** or its **interconnection reliability operating limit Tv** and that of another **reliability coordinator** where both entities are responsible for that facility or group of facilities.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of having one or more operating processes, procedures, or plans to address both preventing and mitigating the magnitude and duration of **interconnection reliability operating limit** exceedances as required in requirement R1 exists. Evidence may include a list of any **interconnection reliability operating limit** (and each associated **interconnection reliability operating limit Tv**) identified in advance, along with one or more dated operating processes, procedures, or plans that will be used, or other equivalent evidence.

**MR2** Evidence of initiating one or more operating processes, procedures, or plans to prevent an **interconnection reliability operating limit** exceedance as required in requirement R2 exists. Evidence may include operating processes, procedures, or plans from requirement R1, dated operating logs, dated voice recordings, dated transcripts of voice recordings, or other equivalent evidence.

**MR3** Evidence of acting or requesting others to act so that the magnitude and duration of an **interconnection reliability operating limit** exceedance is mitigated as required in requirement R3 exists. Evidence may include operating processes, procedures, or plans, dated operating logs, dated voice recordings, dated transcripts of voice recordings, or other equivalent evidence.

**MR4** Evidence of operating to the most limiting **interconnection reliability operating limit** or **interconnection reliability operating limit Tv** in instances where there was a difference as required in requirement R4 exists. Evidence may include dated computer printouts, dated operator logs, dated voice recordings, dated transcripts of voice recordings, or other equivalent evidence.

### Revision History

| Date | Description |
|---|---|
| 2019-12-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to prevent instability, uncontrolled separation, or **cascading** outages that adversely impact **reliability**, by ensuring the **ISO** has the data it needs to monitor and assess the operation of the area for which it has **reliability** coordination responsibility.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO.**

## 3. Requirements

**R1** Intentionally left blank.

**R2** Intentionally left blank.

**R3** The **ISO** must provide data and information, as requested and agreed upon to each **reliability coordinator** with which it has a **reliability** relationship using**:**

**R3.1** a mutually agreeable format;

**R3.2** a mutually agreeable process for resolving data conflicts; and

**R3.3** a mutually agreeable security protocol.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Intentionally left blank.

**MR2** Intentionally left blank.

**MR3** Evidence of providing data and information as required in requirement R3 exists. Evidence may include electronic or hard copies of data transmittals, or other equivalent evidence.

## Revision History

| Date | Description |
|---|---|
| 2019-12-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to ensure that the **ISO**'s operations are coordinated such that they will not adversely impact other **reliability coordinator areas** and to preserve the **reliability** benefits of interconnected operations.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must have and implement operating procedures, operating processes, or operating plans, for activities that require notification or coordination of actions that may impact adjacent **reliability coordinator areas**, to support the **reliability** of the **Interconnection**. These operating procedures, operating processes, or operating plans must include the following:

**R1.1** criteria and processes for notifications;

**R1.2** energy and capacity shortages;

**R1.3** control of voltage, including the coordination of reactive resources;

**R1.4** exchange of information including planned and unplanned outage information to support its operational planning analysis and real time assessments; and

**R1.5** provisions for periodic communications to support reliable operations.

**R2** The **ISO** must maintain its operating procedures, operating processes, and operating plans identified in requirement R1 as follows:

**R2.1** review and update annually with no more than 15 **months** between reviews;

**R2.2** obtain written agreement from all of the **reliability coordinators** required to take the indicated actions for each update; and

**R2.3** distribute to all **reliability coordinators** that are required to take the indicated actions within 30 **days** of an update.

**R3** The **ISO**, upon identification of an expected or actual emergency in Alberta, must notify other impacted **reliability coordinators**.

**R4** The **ISO** must operate as though the emergency exists during each instance where the **ISO** and another **reliability coordinator** disagree on the existence of an emergency.

**R5** The **ISO** must, when it identifies an emergency in Alberta, develop an action plan to resolve the emergency during those instances where another impacted **reliability coordinator** disagrees on the existence of an emergency.

**R6** The **ISO** must, when impacted, implement the action plan developed by another **reliability coordinator** that identifies an emergency during those instances where the **ISO** and the other **reliability coordinator** disagree on the existence of an emergency, unless such actions would violate safety, equipment, regulatory, or statutory requirements.

**R7** The **ISO** must, when requested and able, assist another **reliability coordinator** if the requesting **reliability coordinator** has implemented its emergency procedures, unless such actions cannot be physically implemented or would violate safety, equipment, regulatory, or statutory requirements.

## Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of having and implementing operating procedures, operating processes, or operating plans as required in requirement R1 exists. Evidence may include dated, current in effect documentation with the specified elements, notes from periodic communications, or other equivalent evidence.

**MR2** Evidence of maintaining its operating procedures, operating processes, and operating plans as required in requirement R2 exists. Evidence may include dated documentation with confirmation of receipt, dated notice of acceptance or agreement to take specified actions, dated electronic communications with confirmation of receipt and acceptance or agreement to take specified actions, or other equivalent evidence.

**MR3** Evidence of notifying impacted **reliability coordinators** as required in requirement R3 exists. Evidence may include voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence.

**MR4** Evidence of operating as though an emergency existed as required in requirement R4 exists. Evidence may include dated operator logs, voice recordings or transcripts of voice recordings, electronic communication, or other equivalent evidence.

**MR5** Evidence of developing an action plan to resolve the emergency as required in requirement R5 exists. Evidence may include dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence.

**MR6** Evidence of implementing the action plan as required in requirement R6 exists. Evidence may include dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or dated documentation, or other equivalent evidence.

**MR7** Evidence of assisting **reliability coordinators** as required in requirement R7 exists. Evidence may include dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence.

## Revision History

| Date | Description |
|---|---|
| 2019-12-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to ensure that outages are properly coordinated in the operations planning time horizon and near-term transmission planning horizon.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** Intentionally left blank.

**R2** Intentionally left blank.

**R3** The **ISO** must provide its planning assessment to impacted **reliability coordinators**.

**R4** Intentionally left blank.

## Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Intentionally left blank.

**MR2** Intentionally left blank.

**MR3** Evidence of providing the **ISO**'s planning assessment to impacted **reliability coordinators** as required in requirement R3 exists. Evidence may include web postings with an electronic notice of the posting, e-mail records, or other equivalent evidence.

**MR4** Intentionally left blank.

## Revision History

| Date | Description |
|---|---|
| 2019-12-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to establish requirements for real time monitoring and analysis capabilities to support reliable system operations.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must implement an operating process or operating procedure, to address the quality of the real time data necessary to perform its real time monitoring and real time assessments, which must include:

**R1.1** criteria for evaluating the quality of real time data;

**R1.2** provisions to indicate the quality of real time data to the system operator; and

**R1.3** actions to address real time data quality issues with each entity responsible for providing the data when data quality affects real time assessments.

**R2** The **ISO** must implement an operating process or operating procedure to address the quality of analysis used in its real time assessments which must include:

**R2.1** criteria for evaluating the quality of analysis used in its real time assessments;

**R2.2** provisions to indicate the quality of analysis used in its real time assessments; and

**R2.3** actions to address analysis quality issues affecting its real time assessments.

**R3** The **ISO** must have an alarm process monitor that provides notification to its real time operating personnel when a failure of its real time monitoring alarm processor has occurred.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of implementing an operating process or operating procedure as required in requirement R1 exists. Evidence may include an operating process or operating procedure in electronic or hard copy format meeting all provisions of requirement R1 and evidence that the **ISO** implemented the operating process or operating procedure as called for in the operating process or operating procedure, such as dated operator or supporting logs, dated checklists, voice recordings, voice transcripts, or other equivalent evidence.

**MR2** Evidence of implementing an operating process or operating procedure as required in requirement R2 exists. Evidence may include an operating process or operating procedure in electronic or hard copy format meeting all provisions of requirement R2 and evidence the **ISO** implemented the operating process or operating procedure as called for in the operating process or operating procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other equivalent evidence.

**MR3** Evidence of having an alarm process monitor that provides notification to the **ISO**'s real time operating personnel as required in requirement R3 exists. Evidence may include operator logs, computer printouts, system specifications, or other equivalent evidence.

### Revision History

| Date | Description |
|---|---|
| 2019-12-01 | Initial release. |

# Alberta Reliability Standard
# Steady-State and Dynamic Data for Transmission System Modeling and Simulation
# MOD-010&012-AB-0

## 1 Purpose

The purpose of this **reliability standard** is to provide for the delivery of data and information necessary to establish consistent power flow and dynamic models to be used in the analysis of the reliability of the **Interconnection**.

## 2 Applicability

This **reliability standard** applies to:

(a) the **legal owner** of a **generating unit** that is:

  (i) directly connected to the **transmission system** or to **transmission facilities** within the City of Medicine Hat; and

  (ii) not part of an **aggregated generating facility**;

(b) the **legal owner** of an **aggregated generating facility** that is directly connected to the **transmission system** or to **transmission facilities** within the City of Medicine Hat;

(c) the **legal owner** of a **transmission facility**; and

(d) the **ISO**.

## 3 Requirements

**R1** Each **legal owner** of a **generating unit**, **legal owner** of an **aggregated generating facility** and **legal owner** of **a transmission facility** must provide, within thirty (30) **days** of the **ISO**'s written request, equipment characteristics and system data that the **ISO** requires to meet requirements R2 and R3.

**R2** Subject to requirement R3, the **ISO** must provide equipment characteristics and system data, including dynamics system modeling, simulation data and interchange schedules, to the **WECC** in compliance with the appropriate **Interconnection**-wide **WECC** steady-state and dynamics system modeling and simulation data requirements and reporting procedures.

**R3** The **ISO** must provide the equipment characteristics and system data, including modeling data and information specified in requirement R2, according to the data bank compilation schedule the **WECC** publishes but if no such schedule has been published, then the **ISO** must provide such equipment characteristics and system data no later than:

(a) thirty (30) **days** from the date the **WECC** requests it if the **ISO** has received the requested information prior to the date that **WECC** requested it; or

(b) sixty (60) **days** from the date the **WECC** requests it if the **ISO** has not received the information prior to the date that **WECC** requested it.

## 4 Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for R1.

**MR1** Evidence of providing equipment characteristics and system data as required in requirement R1. Evidence may include data files, email or mail.

**MR2** Evidence of providing equipment characteristics and system data as required in requirement R2. Evidence may include data files, email or mail.

**MR3** Evidence of providing equipment characteristics and system data within the timelines specified in requirement R3. Evidence may include email or mail.

## Revision History

| Effective | Description |
|---|---|
| 2014-01-01 | Initial Release – The first day of the calendar quarter that follows three full calendar quarters after approval by the Commission |
| | |

# Alberta Reliability Standard
# Demand and Energy Data
# MOD-031-AB-2

## 1. Purpose

The purpose of this **reliability standard** is to identify the requirements for the **ISO** to provide to the **WECC**, demand, energy and related data to support **reliability** studies and assessments.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** Intentionally left blank.

**R2** Intentionally left blank.

**R3** The **ISO** must provide the data listed below, for the Alberta **balancing authority area**, to the **WECC** within 75 **days** of receiving a request for such data, unless the **WECC** and the **ISO** agree otherwise:

**R3.1** any or all of the following actual data:

**R3.1.1** integrated hourly **demands** in MWs for the prior calendar year;

**R3.1.2** **monthly** and annual integrated peak hour **demands** in MWs for the prior calendar year;

**R3.1.2.1** if the annual peak hour actual **demand** varies due to weather related conditions (e.g., temperature, humidity or wind speed), the **ISO** must also provide the weather normalized annual peak hour actual **demand** for the prior calendar year;

**R3.1.3** **monthly** and annual net energy for load in GWhs for the prior calendar year; and

**R3.1.4** **monthly** and annual peak hour controllable and dispatchable **demand** side management under the control or supervision of the **ISO** in MWs for the prior calendar year including, reporting for each hour: 1) the committed MWs (the amount under control or supervision); 2) the MWs issued in a **dispatch** (the amount, if any, activated for use by the system operator); and 3) the realized MWs (the amount of actual demand reduction);

**R3.2** any or all of the following forecast data:

**R3.2.1** **monthly** peak hour forecast total internal **demands** in MWs for the next 2 calendar years;

**R3.2.2** **monthly** forecast net energy for load in GWhs for the next 2 calendar years;

**R3.2.3** peak hour forecast total internal **demands** (summer and winter) in MWs for 10 calendar years into the future;

**R3.2.4** annual forecast net energy for load in GWhs for 10 calendar years into the future; and

**R3.2.5** total and available peak hour forecast of controllable and dispatchable **demand** side management (summer and winter), in MWs, under the control or supervision of the system operator for 10 calendar years into the future;

**R3.3** any or all of the following summary explanations:

**R3.3.1** the assumptions and methods used in the development of aggregated peak **demand** and net energy for load forecasts;

**R3.3.2** the **demand** and energy effects of controllable and dispatchable **demand** side management under the control or supervision of the system operator;

**R3.3.3** how **demand** side management is addressed in the forecasts of its peak **demand** and annual net energy for load;

**R3.3.4** how the controllable and dispatchable **demand** side management forecast compares to actual controllable and dispatchable **demand** side management for the prior calendar year and, if applicable, how the assumptions and methods for future forecasts were adjusted; and

**R3.3.5** how the peak **demand** forecast compares to actual **demand** for the prior calendar year with due regard to any relevant weather-related variations (e.g., temperature, humidity, or wind speed) and, if applicable, how the assumptions and methods for future forecasts were adjusted.

**R4** Intentionally left blank.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Intentionally left blank.

**MR2** Intentionally left blank.

**MR3** Evidence of providing the data as required in requirement R3 exists. Evidence may include dated emails or dated transmittal letters, or other equivalent evidence.

**MR4** Intentionally left blank.

## Revision History

| Date | Description |
| --- | --- |
| 2018-08-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to ensure that operating personnel performing the reliability-related tasks of an **operator** of a **transmission facility** are certified through the NERC System Operator Certification Program when filling a real time operating position responsible for control of the **bulk electric system**.

## 2. Applicability

This **reliability standard** applies to:

(a) an **operator** of a **transmission facility** that is part of the **bulk electric system**.

This **reliability standard** does not apply to the **operator** of a **transmission facility** who only operates **transmission facilities** that are:

(a) radial **transmission facilities** connected to:

  (i) load;

  (ii) one or more **generating unit**; and/or

  (iii) one or more **aggregated generating facility**;

(b) connected to an industrial complex, or part of an industrial complex, and the removal of any or all of these **transmission facilities** cannot interrupt power flow on the **interconnected electric system**, other than power flow on its own **transmission facilities** when all transmission facilities in the rest of the **interconnected electric system** are in service; or

(c) **transmission facilities** where the operation of all these facilities is covered by an operating agreement with a NERC-certified operator whereby the NERC-certified operator has the operating authority for these facilities.

## 3. Requirements

**R1** Intentionally left blank.

**R2** An **operator** of a **transmission facility** must staff each of its real time operating positions performing reliability-related tasks with operating personnel who have obtained and maintained one of the following NERC certificates:

(a) Reliability Operator;

(b) Balancing, Interchange and Transmission Operator; or

(c) Transmission Operator.

**R3** Intentionally left blank.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Intentionally left blank.

**MR2** Evidence of staffing its real time operating positions performing reliability-related tasks with operating personnel certified in accordance with the requirement R2 exists. This evidence may include, but it is not limited to:

(a) the list of real time operating positions performing reliability-related tasks;

(b) the list of operating personnel assigned to the real time operating positions performing reliability-related tasks;

(c) a copy of each of its operating personnel's NERC certificate; and

(d) work schedules, logs, or other equivalent evidence showing which operating personnel were assigned to work in real time operating positions performing reliability-related tasks.

**MR3** Intentionally left blank.

## Revision History

| Date | Description |
|---|---|
| 2019-12-01 | Unbolded "real time" |
| 2019-01-01 | Initial release. |

# Alberta Reliability Standard
# Reliability Coordination - Staffing
# PER-004-AB-2

## 1. Purpose

The **ISO** must have sufficient, competent staff to perform the functions of the **ISO**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must be staffed with adequately trained operating personnel, each possessing a valid NERC Reliability Operator certificate, 24 hours per **day**, seven **days** per week.

**R2** The **ISO** must ensure that **ISO** operating personnel have adequate information regarding **system operating limits**, **interconnection reliability operating limits** and **intertie** facility limits available.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence may include, but is not limited to, NERC certificate / certification records, shift schedules or other equivalent evidence that will be used to confirm that the **ISO** is staffed with operating personnel possessing a valid NERC Reliability Operator certificate 24 hours per **day**, seven **days** per week.

**MR2** Evidence may include but is not limited to, EMS screenshots, methodology documentation or other equivalent documentation that will be used to confirm that **ISO** operating personnel have adequate information regarding **system operating limits** and **interconnection reliability operating limits** and **intertie** facility limits.

## Revision History

| Effective Date | Description |
|---|---|
| 2015-05-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to ensure that personnel performing or supporting real time operations on the **bulk electric system** are trained using a systematic approach.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**;

(b) the **operator** of a **transmission facility** that has personnel who can act independently to operate in real time, or to direct the real time operation of, those **transmission facilities** that are part of the **bulk electric system** from a **control centre**. This does not include field switching personnel.

This reliability standard does not apply to the **operator** of a **transmission facility** whose only **transmission facilities** are:

(i) radial **transmission facilities** connecting to:

(a) load;

(b) one or more **generating units**; and / or

(c) one or more **aggregated generating facilities**; or

(ii) either part of an industrial complex or connected to an industrial complex and cannot interrupt power flow on the **interconnected electric system**, other than power flow on its own **transmission facilities**.

## 3. Requirements

**R1** The **ISO** and each **operator** of a **transmission facility** must use a systematic approach to develop and implement a training program for its real time operating personnel, as follows:

**R1.1** The **ISO** and each **operator** of a **transmission facility** must:

(a) create a definition of a company-specific real time reliability-related task;

(b) develop a documented methodology for determining company-specific real time reliability-related tasks; and

(c) create a list of **bulk electric system** company-specific real time reliability-related tasks based on that methodology.

**R1.1.1** The **ISO** and each **operator** of a **transmission facility** must review, and update if necessary, its list of **bulk electric system** company-specific real time reliability-related tasks identified in R1.1 each calendar year.

**R1.2** The **ISO** and each **operator** of a **transmission facility** must design and develop training materials according to its training program, based on the **bulk electric system** company-specific real time reliability-related task list created in R1.1.

**R1.3** The **ISO** and each **operator** of a **transmission facility** must deliver training to its real time operating personnel according to its training program.

**R1.4** The **ISO** and each **operator** of a **transmission facility** must conduct an evaluation each calendar year of the training program established in requirement R1 to identify any needed changes to the training program, and must implement the changes identified.

**R2** Intentionally left blank.

**R3** The **ISO** and each **operator** of a **transmission facility** must verify, at least once, the capabilities of its real time operating personnel, identified in requirement R1, assigned to perform each of the **bulk electric system** company-specific real time reliability-related tasks identified under requirement R1.1.

**R3.1** Within six (6) months of a modification or addition of a **bulk electric system** company-specific real time reliability-related task, the **ISO** and each **operator** of a **transmission facility** must verify the capabilities of each of its real time operating personnel identified in requirement R1 to perform the new or modified **bulk electric system** company-specific real time reliability-related tasks identified in requirement R1.1.

**R4** The **ISO** must provide its real time operating personnel identified in requirement R1 with emergency operations training using simulation technology such as a simulator, virtual technology, or other technology that replicates the operational behavior of the **bulk electric system** if the **ISO**:

(1) has operational authority or control over **facilities** with established **interconnection reliability operating limits**, or

(2) has established **protection systems** or operating guides to mitigate **interconnection reliability operating limit** violations,

**R4.1** The **ISO** must comply with requirement R4 within twelve (12) months of meeting either of the criteria identified in requirements R4(1) or R4(2).

**R5** The **ISO** and each **operator** of a **transmission facility** must use a systematic approach to develop and implement training for its identified **operations support personnel** on how their job function(s) impact those **bulk electric system** company-specific **real time** reliability-related tasks that it has identified pursuant to requirement R1.1.

**R5.1** The **ISO** and each **operator** of a **transmission facility** must conduct an evaluation each calendar year of the training established in requirement R5 to identify and implement changes to the training.

**R6** Intentionally left blank.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this reliability standard. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of using a systematic approach to develop and implement a training program for its real time operating personnel as required in requirement R1 exists. Evidence may include, but is not limited to, training program descriptions, meeting minutes, design notes, or other equivalent evidence.

**MR1.1** Evidence of having a definition, methodology and **bulk electric system** company-specific real time reliability-related task list and review history, as required in requirement R1.1 exists. Evidence may include, but is not limited to, a definition for real time reliability-related tasks, a documented methodology for determining company-specific real time reliability-related tasks, a list of real time reliability related tasks, a documented revision history or other equivalent evidence.

**MR1.2** Evidence of designing and developing training materials as required in requirement R1.2 exists. Evidence may include, but is not limited to, course design documents and examples of training materials or other equivalent evidence.

**MR1.3** Evidence of delivering real time operating personnel training, as required in requirement R 1.3 exists. Evidence may include, but is not limited to, training records showing the names of the attendees, the title of the training delivered, and the dates of delivery or other equivalent evidence.

**MR1.4** Evidence of conducting an evaluation of the training program each calendar year and implementing the identified changes, as required in requirement R1.4 exists. Evidence may include, but is not limited to, instructor observations, trainee feedback, course evaluations, meeting minutes, training program document revision history, or other equivalent evidence.

**MR2** Intentionally left blank.

**MR3** Evidence of verifying, at least once, the capabilities of the real time operating personnel, as required in requirement R3 exists.

Evidence may include, but is not limited to, documented records to show that it verified the capability of each of its real time personnel on company-specific real time reliability-related tasks with the date of verification, employee name, supervisor signature and check sheets for each company-specific real time reliability-related task completed, the results of learning assessments, or other equivalent evidence.

**MR3.1** Evidence of verifying the capabilities of real time operating personnel within six (6) months of a modification or addition of a **bulk electric system** company-specific **real time** reliability-related task, as required in requirement R3.1 exists. Evidence may include, but is not limited to, documented records to show that it verified the capability of each of its personnel on company-specific real time reliability-related tasks with the date of verification, employee name, supervisor signature and check sheets for each company-specific real time reliability-related task completed, the results of learning assessments, or other equivalent evidence.

**MR4** Evidence of providing emergency operations training as required in requirement R4 exists. Evidence may include, but is not limited to, dated training records or other equivalent evidence.

**MR4.1** Evidence of complying with requirement R4 as required in requirement R4.1 exists. Evidence may include, but is not limited to, dated training records or other equivalent evidence.

**MR5** Evidence of using a systematic approach to develop and implement training for identified **operations support personnel** as required in requirement R5 exists. Evidence may include, but is not limited to, training records showing employee name, date of training and completion of training, or other equivalent evidence.

**MR5.1** Evidence of conducting an evaluation each calendar year of the training established in requirement R5 and that any identified changes were implemented as required in requirement R5.1 exists. Evidence may include, but is not limited to, instructor observations, trainee feedback, course evaluations, meeting minutes, training program document revision history or other equivalent evidence.

**MR6** Intentionally left blank.

### Revision History

| Date | Description |
| --- | --- |
| 2019-12-01 | Unbolded “real time” |
| 2018-04-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to ensure that personnel are trained on specific topics essential to reliability to perform or support real time operations of the **interconnected electric system.**

## 2. Applicability

This **reliability standard** applies to:

(a) the **operator** of a **generating unit** that:

(i) is part of the **bulk electric system**; or

(ii) the **ISO**:

(A) determines is necessary for the reliable operation of either **the interconnected electric system** or the City of Medicine Hat electric system; and

(B) publishes on the AESO website and may amend from time to time on notice to **market participants** in accordance with the process set out in Appendix 1;

and

(b) the **operator** of an **aggregated generating facility** that:

(i) is part of the **bulk electric system**; or

(ii) the **ISO**:

(A) determines is necessary for the reliable operation of either **the interconnected electric system** or the City of Medicine Hat electric system; and

(B) publishes on the AESO website and may amend from time to time on notice to **market participants** in accordance with the process set out in Appendix 1,

that has personnel who are responsible for the real time control of a **generating unit** or **aggregated generating facility** and directly or indirectly receives operating instructions from the **ISO** or **operator** of a **transmission facility**.

## 3. Requirements

**R1** Each **operator** of a **generating unit** or **operator** of an **aggregated generating facility** must provide training to personnel identified in the Applicability section on the operational functionality of **protection systems** and **remedial action schemes** that affect the output of a **generating unit** or an **aggregated generating facility** it operates.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of providing training to the personnel responsible for the real time control of a **generating unit** or an **aggregated generating facility** as required in requirement R1 exists. Evidence may include documents such as training records showing successful completion of training that includes training materials, the name of the person, and date of training, or other equivalent evidence.

## 5. Appendices

Appendix 1 – Amending Process for List of Generating Units and Aggregated Generating Facilities

## Revision History

| Date | Description |
|---|---|
| 2023-07-01 | Initial release |

**Appendix 1**

**Amending Process for List of Generating Units and Aggregated Generating Facilities**

In order to amend a list referenced in subsections (a)(ii) and (b)(ii) of section 2, Applicability, the **ISO** must:

(a) upon determining that a **generating unit** or **aggregated generating facility** is to be added, notify the **operator** in writing and determine an effective date, which must be no less than 4 full calendar quarters after the date of notice;

(b) upon determining that a **generating unit** or **aggregated generating facility** is to be deleted, notify the **operator** in writing and determine and effective date on which the operator will no longer be required to meet the applicable requirements; and

(c) publish the amended list with effective dates on the AESO website.

# Alberta Reliability Standard
# Protection System Coordination
# PRC-001-AB3-1.1(ii)

## 1. Purpose

The purpose of this **reliability standard** is to ensure **protection systems** are coordinated among operating entities.

## 2. Applicability

This **reliability standard** applies to:

(a) the **legal owner** of a **transmission facility** that is:

(i) part of the **bulk electric system**; or

(ii) not part of the **bulk electric system** and which the **ISO**:

(A) determines is necessary for the reliable operation of either the **interconnected electric system** or the City of Medicine Hat electric system; and

(B) publishes on the AESO website and may amend from time to time in accordance with the process set out in Appendix 1;

(b) the **legal owner** of a **generating unit** that is:

(i) directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW;

(ii) within a power plant which:

(A) is not part of an **aggregated generating facility**;

(B) is directly connected to the **bulk electric system**; and

(C) has a combined **maximum authorized real power** rating greater 67.5 MW;

(iii) a **blackstart resource**; or

(iv) material to this **reliability standard** and to the reliability of the **bulk electric system**, regardless of its **maximum authorized real power** rating, as the **ISO** determines and publishes on the AESO website and may amend from time to time in accordance with the process set out in Appendix 1;

(c) the **legal owner** of an **aggregated generating facility** that is:

(i) directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW;

(ii) within a power plant or industrial complex which:

(A) is directly connected to the **bulk electric system**; and

(B) has a combined **maximum authorized real power** rating greater than 67.5 MW;

(iii) a **blackstart resource**; or

(iv) material to this **reliability standard** and to the reliability of the **bulk electric system**, regardless of its **maximum authorized real power** rating, as the **ISO** determines and publishes on the AESO website and may amend from time to time in accordance with the process set out in Appendix 1;

(d) the **operator** of a **transmission facility** that is:

   (i) part of the **bulk electric system**; or

   (ii) not part of the **bulk electric system** and which the **ISO**:

      (A) determines is necessary for the reliable operation of either the **interconnected electric system** or the City of Medicine Hat electric system; and

      (B) publishes on the AESO website and may amend from time to time in accordance with the process set out in Appendix 1;

(e) the **operator** of a **generating unit** that is:

   (i) directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW;

   (ii) within a power plant which:

      (A) is not part of an **aggregated generating facility**;

      (B) is directly connected to the **bulk electric system**; and

      (C) has a combined **maximum authorized real power** rating greater than 67.5 MW;

   (iii) a **blackstart resource**; or

   (iv) material to this **reliability standard** and to the reliability of the **bulk electric system**, regardless of its **maximum authorized real power** rating, as the **ISO** determines and publishes on the AESO website and may amend from time to time in accordance with the process set out in Appendix 1; and

(f) the **operator** of an **aggregated generating facility** that is:

   (i) directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW;

   (ii) within a power plant or industrial complex which:

      (A) is directly connected to the bulk electric system; and

      (B) has a combined maximum authorized real power rating greater than 67.5 MW;

   (iii) a **blackstart resource**; or

   (iv) material to this **reliability standard** and to the reliability of the **bulk electric system**, regardless of its **maximum authorized real power** rating, as the **ISO** determines and publishes on the AESO website and may amend from time to time in accordance with the process set out in Appendix 1.

## 3. Requirements

**R1** Each **operator** of a **generating unit** and **operator** of an **aggregated generating facility** must, upon failure of any component of a **protection system** of a **generating unit** or an **aggregated generating facility** which it operates, take the actions listed in requirement R1.1 and R1.2.

**R1.1** Notify the **operator** of a **transmission facility** to which the **generating unit** or **aggregated generating facility** is connected as soon as possible, but no longer than twenty-four (24) hours after becoming aware of such a failure, and provide the following information, regardless of whether or not the **generating unit** or **aggregated generating facility** remains on-line:

(a) identify the **protection system** that failed; and

(b) identify whether or not a **functionally equivalent protection system** remains in service.

**R1.2** Correct the failure as soon as possible.

**R2** Each **operator** of a **transmission facility**, **operator** of a **generating unit** and **operator** of an **aggregated generating facility** must take the actions listed in requirements R2.1 through R2.3 after becoming aware of the failure of any of the following **protection systems** or teleprotection communication channels under its authority:

(a) a **protection system**, other than a related teleprotection communication channel referred to in requirement R2(c) or R2(d), that protects a **transmission facility** operated at a nominal voltage greater than 200 kV, whether or not a **functionally equivalent protection system** remains in service;

(b) a **protection system**, other than a related teleprotection communication channel referred to in requirement R2(c) or R2(d), that protects a **transmission facility** that is part of the **bulk electric system** where a **functionally equivalent protection system** is not available;

(c) a teleprotection communication channel, that is part of a **protection system** for a **transmission facility** operated at a nominal voltage greater than 200 kV, where there is an equivalent backup teleprotection communication channel, and where the failure lasts for more than twenty-four (24) continuous hours; or

(d) a teleprotection communication channel, where there is no equivalent backup teleprotection communication channel, and where the failure lasts for more than ten (10) consecutive minutes.

**R2.1** Provide notification to the **ISO**, and to each directly affected **operator** of a **transmission facility**, directly affected **operator** of a **generating unit**, directly affected **operator** of an **aggregated generating facility** and directly affected **interconnected transmission operator** as soon as possible, but no longer than twenty-four (24) hours after becoming aware of a failure identified in requirements R2(a), R2(b) and R2(d), and no longer than forty-eight (48) hours after becoming aware of a failure identified in requirement R2(c), regardless of whether or not the **transmission facility** is removed from service following the awareness of such failure, that includes the following information:

(a) the identification of the **protection system** or teleprotection communication channel(s) that failed;

(b) when the **protection system** or teleprotection communication channel(s) failed or when such failure was first discovered; and

(c) an estimate of the date when the **protection system** or teleprotection communication channel(s) will be returned to service.

**R2.2** Where the protection system or teleprotection communication channel(s) are not returned to service by the estimated return to service date identified in requirement R2.1, provide a new estimate of the return to service date up to five (5) **days** after the previous estimated return to service date to the entities that received the notification in accordance with requirement R2.1.

**R2.3** Correct the failure as soon as possible.

**R3** Each **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** must coordinate all new **protection systems** and all **protection system** changes with each affected interconnecting **legal owner** of a **transmission facility** and notify the **ISO** that such coordination has occurred.

**R4** Each **legal owner** of a **transmission facility** must coordinate all new **protection systems** and all **protection system** changes with:

(a) each affected adjacent **legal owner** of a **transmission facility**;

(b) each affected **legal owner** of a **generating unit**;

(c) each affected **legal owner** of an **aggregated generating facility**;

(d) each affected **interconnected transmission operator**; and

(e) the **ISO**, as affected,

and must notify the **ISO** that such coordination has occurred.

**R5** Each **operator** of a **generating unit**, **operator** of an **aggregated generating facility** and **operator** of a **transmission facility** must identify, notify and coordinate planned changes that may require changes in the **protection systems** of others as described in requirements R5.1 and R5.2.

**R5.1** Each **operator** of a **generating unit** and **operator** of an **aggregated generating facility** must identify planned changes to its generation, load, or operating conditions that may require changes to the **protection systems** of others, and must notify the **ISO** and coordinate with each affected **operator** of a **transmission facility** in advance of making such changes.

**R5.2** Each **operator** of a **transmission facility** must identify planned changes to its transmission, load or operating conditions that may require changes to the **protection systems** of others, and must notify the **ISO** and coordinate with each affected:

(a) **operator** of a **transmission facility**;

(b) adjacent **interconnected transmission operator**;

(c) **operator** of a **generating unit**; and

(d) **operator** of an **aggregated generating facility**,

in advance of making such changes.

**R6** Each **operator** of a **transmission facility** must monitor the status (on/off) of each **remedial action scheme** in its area, and must notify the **ISO** and each affected:

(a) **operator** of a **transmission facility**;

(b) adjacent **interconnected transmission operator**;

(c) **operator** of a **generating unit**; and

(d) **operator** of an **aggregated generating facility**,

of each change in status.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this reliability standard. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of notifying, providing information and correcting failures of any component of a **protection system** as required in requirement R1 exists. Evidence may include, but is not limited to:

**MR1.1** voice recordings, operator logs, electronic notifications (emails) or other equivalent evidence; and

**MR1.2** work orders, setting change files, electronic records or other equivalent evidence.

**MR2** Evidence of providing notification, providing an estimate and correcting failures of any of the **protection systems** or teleprotection communication channel(s) as required in requirement R2 exists. Evidence may include, but is not limited to:

**MR2.1** voice recordings, operator logs, electronic notifications (emails) or other equivalent evidence;

**MR2.2** voice recordings, operator logs, electronic notifications (emails) or other equivalent evidence; and

**MR2.3** work orders, setting change files, electronic records or other equivalent evidence.

**MR3** Evidence of coordinating **protection systems** and notifying the **ISO** as required in requirement R3 exists.

Evidence of coordinating **protection systems** may include, but is not limited to, a fault analysis study, letters of agreement on settings, notifications of changes or other equivalent evidence.

Evidence of notifying the **ISO** may include, but is not limited to, electronic notifications (emails), hard copy notifications, or other equivalent evidence.

**MR4** Evidence of coordinating **protection systems** and notifying the **ISO** as required in requirement R4 exists.

Evidence of coordinating **protection systems** may include, but is not limited to, a fault analysis study, letters of agreement on settings, notifications of changes or other equivalent evidence.

Evidence of notifying the **ISO** may include, but is not limited to, electronic notifications (emails), hard copy notifications or other equivalent evidence.

**MR5** Measures for this requirement are identified in the subsections below:

**MR5.1** Evidence of identifying, notifying and coordinating planned changes that may require changes to the **protection systems** of others as required in requirement R5.1 exists.

Evidence may include, but is not limited to, voice recordings, operator logs, electronic notifications (emails) or other equivalent evidence.

**MR5.2** Evidence of identifying, notifying and coordinating planned changes that may require changes to the **protection systems** of others as required in requirement R5.2 exists.

Evidence may include, but is not limited to, voice recordings, operator logs, electronic notifications (emails) or other equivalent evidence.

**MR6** Evidence of monitoring the status of each **remedial action scheme** in its area and notifying entities of each change in status as required in requirement R6 exists.

Evidence of monitoring the status of each **remedial action scheme** may include, but is not limited to, SCADA data, wiring diagrams or other equivalent evidence.

Evidence of notifying entities may include, but is not limited to, SCADA data, voice recordings, operator logs, electronic notifications (emails) or other equivalent evidence.

## Revision History

| Date | Description |
|---|---|
| 2017-10-01 | Alberta specific revisions made to improve clarity. |
| 2015-05-01 | Revised for ISO assumption of RC functionality for the Alberta footprint |
| 2013-01-02 | Administrative update – “TFO” and “GFO” replaced with “legal owner of a transmission facility”, “operator of a transmission facility”, “legal owner of a generating unit”, “operator of a generating unit”, “legal owner of an aggregated generating facility”, and “operator of an aggregated generating facility”; applied standard at the bulk electric system level; added Appendix 1; and other minor cleanup items. |
| 2011-01-13 | R1 |
| 2010-01-22 | New Issue |

Appendix 1
Amending Process for List of Facilities

In order to amend any list referenced in subsections (a)(ii)(B), (b)(iv), (c)(iv), (d)(ii)(B), (e)(iv) and (f)(iv) of section 2, *Applicability*, the **ISO** must:

(a) upon determining that a **transmission facility**, **generating unit** or **aggregated generating facility** is to be added, notify the **legal owner** and **operator** in writing and determine an effective date, which must be no less than thirty (30) **days** after the date of notice, by which the **transmission facility**, **generating unit** or **aggregated generating facility** is to meet the applicable requirements;

(b) upon determining that a **transmission facility**, **generating unit** or **aggregated generating facility** is to be deleted, notify the **legal owner** and **operator** in writing and determine an effective date on which the **transmission facility**, **generating unit** or **aggregated generating facility** will no longer be required to meet the applicable requirements; and

(c) publish the amended list with effective dates on the AESO website.

# Alberta Reliability Standard
# Disturbance Monitoring and Reporting Requirements
# PRC-002-AB-2

## 1. Purpose

The purpose of this **reliability standard** is to ensure that adequate data is available to facilitate analysis of **disturbances** on the **bulk electric system**.

## 2. Applicability

This **reliability standard** applies to the following:

(a) the **legal owner** of a **transmission facility** that is part of the **bulk electric system**;

(b) the **legal owner** of a **generating unit** that is part of the **bulk electric system**;

(c) the **legal owner** of an **aggregated generating facility** that is part of the **bulk electric system**; and

(d) the **ISO**.

## 3. Requirements

**R1** Each **legal owner** of a **transmission facility** must:

**R1.1** identify **bulk electric system** buses for which sequence of events recording and **fault** recording data is required by using the methodology in Appendix 1;

**R1.2** notify other **legal owners** of **system elements** on the **bulk electric system** connected to those **bulk electric system** buses, if any, within 90 **days** of completion of requirement R1.1, that those **system elements** require either one or both of sequence of events recording data and **fault** recording data; and

**R1.3** re-evaluate all **bulk electric system** buses at least once every 5 calendar years in accordance with requirement R1.1 and notify other **legal owners**, if any, in accordance with requirement R1.2, and implement the re-evaluated list of **bulk electric system** buses as per the *Implementation Plan* in Appendix 2.

**R2** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** must have sequence of events recording data for circuit breaker position, open or close, for each circuit breaker it owns connected directly to the **bulk electric system** buses identified in requirement R1 and associated with the **system elements** on the **bulk electric system** at those **bulk electric system** buses.

**R3** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** must have **fault** recording data to determine the following electrical quantities for each triggered **fault** recording for the **system elements** on the **bulk electric system** it owns connected to the **bulk electric system** buses identified in requirement R1:

**R3.1** phase-to-neutral voltage for each phase of each specified **bulk electric system** bus; and

**R3.2** each phase current and the residual or neutral current for the following **system elements** on the **bulk electric system**:

**R3.2.1** transformers that have a low-side operating voltage of 100 kV or above; and

**R3.2.2** transmission lines.

**R4** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** must have **fault** recording data as specified in requirement R3 that meets the following:

**R4.1** a single record or multiple records that include:

(a) a pre-trigger record length of at least 2 cycles and a total record length of at least 30 cycles for the same trigger point, or

(b) at least 2 cycles of the pre-trigger data, the first 3 cycles of the post-trigger data, and the final cycle of the **fault** as seen by the **fault** recorder;

**R4.2** a minimum recording rate of 16 samples per cycle; and

**R4.3** trigger settings for at least the following:

**R4.3.1** neutral (residual) overcurrent; and

**R4.3.2** phase under voltage or overcurrent**.**

**R5** The **ISO** must:

**R5.1** identify **system elements** on the **bulk electric system** for which dynamic **disturbance** recording data is required, including the following:

**R5.1.1** generating resources with:

**R5.1.1.1** an individual **generating unit** with a **maximum authorized real power** rating greater than or equal to 450 MW; and

**R5.1.1.2** an individual **generating unit** with a **maximum authorized real power** rating greater than or equal to 270 MW where the plant/facility aggregate **maximum authorized real power** rating is greater than or equal to 900 MW;

**R5.1.2** any one **system element** on the **bulk electric system** that is part of an angular stability or voltage stability related **system operating limit**;

**R5.1.3** each terminal of a high voltage direct current circuit with a nameplate rating greater than or equal to 270 MW, on the alternating current portion of the converter;

**R5.1.4** one or more **system elements** on the **bulk electric system** that are part of an **interconnection reliability operating limit**; and

**R5.1.5** any one **system element** on the **bulk electric system** within a major voltage sensitive area as defined by an area with an in-service **under voltage load shed** program;

**R5.2** identify a minimum dynamic **disturbance** recording coverage, inclusive of those **system elements** on the **bulk electric system** identified in requirement R5.1, of at least:

**R5.2.1** one **system element** on the **bulk electric system**; and

**R5.2.2** one **system element** on the **bulk electric system** per 3,000 MW of the **ISO**'s historical simultaneous peak **demand** of the **interconnected electric system**;

**R5.3** notify all **legal owners** of identified **system elements** on the **bulk electric system**, within 90 **days** of completion of requirement R5.1, that their respective **system elements** on the **bulk electric system** require dynamic **disturbance** recording data when requested; and

**R5.4** re-evaluate all **system elements** on the **bulk electric system** at least once every 5 calendar years in accordance with requirements R5.1 and R5.2, and notify **legal owners** in accordance with requirement R5.3 to implement the re-evaluated list of **system elements** on the **bulk electric system** as per the implementation plan in Appendix 2.

**R6** Each **legal owner** of a **transmission facility** must have dynamic **disturbance** recording data to determine the following electrical quantities for each **system element** on the **bulk electric system** it owns for which it received notification as identified in requirement R5:

**R6.1** one phase-to-neutral or positive sequence voltage;

**R6.2** the phase current for the same phase at the same voltage corresponding to the voltage in requirement R6.1, or the positive sequence current;

**R6.3** **real power** and **reactive power** flows expressed on a 3-phase basis corresponding to all circuits where current measurements are required; and

**R6.4** frequency of any one of the voltages in requirement R6.1.

**R7** Each **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** must have dynamic **disturbance** recording data to determine the following electrical quantities for each **system element** on the **bulk electric system** it owns for which it received notification as identified in requirement R5:

**R7.1** one phase-to-neutral, phase-to-phase, or positive sequence voltage at either the generator step-up transformer high-side or low-side voltage level;

**R7.2** the phase current for the same phase at the same voltage corresponding to the voltage in requirement R7.1, phase currents for any phase-to-phase voltages, or positive sequence current;

**R7.3** **real power** and **reactive power** flows expressed on a 3-phase basis corresponding to all circuits where current measurements are required; and

**R7.4** frequency of at least one of the voltages in requirement R7.1.

**R8** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** responsible for dynamic **disturbance** recording data for the **system elements** on the **bulk electric system** for which it received notification as identified in requirement R5 must, unless it complies with subsection 7(1) of Section 502.9 of the **ISO rules**, *Synchrophasor Measurement Unit Technical Requirements,* have continuous data recording and storage, unless the equipment was installed prior to the effective date of this **reliability standard** and is not capable of continuous recording, in which case, triggered records must meet the following:

**R8.1** triggered record lengths of at least 3 minutes; or

**R8.2** at least one of the following 3 triggers:

(a) off nominal low frequency trigger set at < 59.55 Hz and off nominal high frequency trigger set at > 61.0 Hz;

(b) rate of change of frequency trigger set at < -0.05625 Hz/sec and > 0.125 Hz/sec; or

(c) undervoltage trigger set no lower than 85% of normal operating voltage for a duration of 5 seconds.

**R9** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** responsible for dynamic **disturbance** recording data for the **system elements** on the **bulk electric system** identified in requirement R5 must have dynamic **disturbance** recording data that meet the following:

**R9.1** input sampling rate of at least 960 samples per second; and

**R9.2** output recording rate of electrical quantities of at least 30 times per second.

**R10** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** must time synchronize all sequence of events recording and **fault** recording data for the **bulk electric system** buses identified in requirement R1 and dynamic **disturbance** recording data for the **system elements** on the **bulk electric system** identified in requirement R5 to meet the following:

**R10.1** synchronization to Coordinated Universal Time with or without a local time offset; and

**R10.2** synchronized device clock accuracy within ± 2 milliseconds of Coordinated Universal Time.

**R11** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** must provide to the **ISO**, upon written request, all sequence of events recording and **fault** recording data for the **bulk electric system** buses identified in requirement R1 and dynamic **disturbance** recording data for the **system elements** on the **bulk electric system** identified in requirement R5, in accordance with the following:

**R11.1** data is retrievable for the period of 10 **days**, inclusive of the **day** the data was recorded;

**R11.2** data subject to requirement R11.1 is provided within 30 **days** of a request unless an extension is granted by the **ISO**;

**R11.3** sequence of events recording data are provided in ASCII Comma Separated Value format following Appendix 3;

**R11.4** **fault** recording and dynamic **disturbance** recording data are provided in electronic files that are formatted in conformance with C37.111, *IEEE Standard for Common Format for Transient Data Exchange (COMTRADE)*, revision C37.111-1999 or later; and

**R11.5** data files will be named in conformance with C37.232, *IEEE Standard for Common Format for Naming Time Sequence Data Files (COMNAME)*, revision C37.232-2011 or later.

**R11-A** The **ISO** must provide to the **WECC** or the **NERC** upon written request, all sequence of events recording and **fault** recording data that the **ISO** subsequently receives, through making the same request of responsible entities in Alberta, in accordance with requirement R11, within 60 **days** of a request unless an extension is granted by the either the **WECC** or the **NERC**.

**R12** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** must, within 90 **days** of the discovery of a failure of the recording capability for the sequence of events recording, **fault** recording or dynamic **disturbance** recording data, either:

(a) restore the recording capability, or

(b) submit a corrective action plan to the **ISO** and implement it.

**R12.1** the **ISO** must submit a corrective action plan to the **WECC** within 15 **days** of receiving a corrective action plan from any of a **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, or **legal owner** of an **aggregated generating facility**.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of identifying **bulk electric system** buses, notifying **legal owners**, re-evaluating all **bulk electric system** buses, and implementing the re-evaluated list as required in requirement R1 exists. Evidence may include lists, dated correspondence, or other equivalent evidence.

**MR2** Evidence of having sequence of events recording data for circuit breaker positions as required in requirement R2 exists. Evidence may include documents describing the device interconnections and configurations which may include a single design standard as representative for common installations, station drawings, and data recordings, or other equivalent evidence.

**MR3** Evidence of having **fault** recording data as required in requirement R3 exists. Evidence may include documents describing the device specifications and configurations which may include a single design standard as representative for common installations, station drawings, and data recordings, or other equivalent evidence.

**MR4** Evidence of having **fault** recording data as required in requirement R4 exists. Evidence may include data recordings, technical specification sheets, settings documentation, or other equivalent evidence.

**MR5** Evidence of identifying **system elements** on the **bulk electric system**, identifying a minimum dynamic **disturbance** recording coverage, and notifying all **legal owners** of identified **system elements** on the **bulk electric system** as required in requirement R5 exists. Evidence may include lists and related documentation, dated correspondence, or other equivalent evidence.

**MR6** Evidence of having dynamic **disturbance** recording data as required in requirement R6 exists. Evidence may include data records, documents describing the device specifications and configurations, which may include a single design standard as representative for common installations, station drawings, or other equivalent evidence.

**MR7** Evidence of having dynamic **disturbance** recording data as required in requirement R7 exists. Evidence may include data records, documents describing the device specifications and configurations, which may include a single design standard as representative for common installations, station drawings, or other equivalent evidence.

**MR8** Evidence of having continuous data recording and storage, or of having triggered records that meet the criteria required in requirement R8 exists. Evidence may include data recordings, technical specification sheets, settings documentation, or other equivalent evidence.

**MR9** Evidence of having dynamic **disturbance** recording data as required in requirement R9 exists. Evidence may include data recordings, technical specification sheets, settings documentation or other equivalent evidence.

**MR10** Evidence of time synchronizing all sequence of events recording and **fault** recording data, and dynamic **disturbance** recording data as required in requirement R10 exists. Evidence may include technical specification sheets, settings documentation, or other equivalent evidence.

**MR11** Evidence of providing all sequence of events recording and **fault** recording data as required in requirement R11 exists. Evidence may include dated correspondence, documents describing data storage capability, device specification, configuration or settings, data records, or other equivalent evidence.

**MR11-A** Evidence of providing all sequence of events recording and **fault** recording data as required in requirement R11-A exists. Evidence may include dated correspondence, or other equivalent evidence.

**MR12** Evidence of either restoring the recording capability or submitting a corrective action plan and implementing it as required in requirement R12 exists. Evidence may include dated reports of discovery of a failure, documentation noting the date the data recording was restored, SCADA records, work orders, dated correspondence, a corrective action plan, or other equivalent evidence.

**MR12.1** Evidence of submitting a corrective action plan to the **WECC** as required in requirement R12.1 exists. Evidence may include dated correspondence, or other equivalent evidence.

## 5. Appendices

Appendix 1 - *Methodology for Selecting Bulk Electric System Buses for Capturing Sequence of Events Recording and Fault Recording Data*

Appendix 2 - *Implementation Plan*

Appendix 3 - *Sequence of Events Recording Data Format*

### Revision History

| Date | Description |
|---|---|
| 2019-10-01 | Initial release. |

**Appendix 1**

**Methodology for Selecting Bulk Electric System Buses for Capturing Sequence of Events Recording and Fault Recording Data**

**(Requirement R1)**

To identify monitored **bulk electric system** buses for sequence of events recording and **fault** recording data required by requirement R1, each **legal owner** of a **transmission facility** must follow sequentially, unless otherwise noted, the steps listed below:

Step 1 Determine a complete list of **bulk electric system** buses that it owns.

For the purposes of this **reliability standard**, a single **bulk electric system** bus includes physical buses with breakers connected at the same voltage level within the same physical location sharing a common ground grid. These buses may be modeled or represented by a single node in **fault** studies. For example, ring bus or breaker-and-a-half bus configurations are considered to be a single bus.

Step 2 Reduce the list to those **bulk electric system** buses that have a maximum available calculated 3-phase short circuit MVA of 1,500 MVA or greater. If there are no buses on the resulting list, proceed to Step 7.

Step 3 Determine the 11 **bulk electric system** buses on the list with the highest maximum available calculated 3-phase short circuit MVA level. If the list has 11 or fewer **bulk electric system** buses, proceed to Step 7.

Step 4 Calculate the median MVA level of the 11 **bulk electric system** buses determined in Step 3.

Step 5 Multiply the median MVA level determined in Step 4 by 20%.

Step 6 Reduce the **bulk electric system** buses on the list to only those that have a maximum available calculated 3-phase short circuit MVA higher than the greater of:

(a) 1,500 MVA; or

(b) 20% of median MVA level determined in Step 5.

Step 7 <u>If there are no **bulk electric system** buses on the list</u>: the procedure is complete and no **fault** recording and sequence of events recording data is required. Proceed to Step 9.

<u>If the list has one or more, but less than or equal to 11 **bulk electric system** buses</u>: **fault** recording and sequence of events recording data is required at the **bulk electric system** bus with the highest maximum available calculated 3-phase short circuit MVA as determined in Step 3. Proceed to Step 9.

<u>If the list has more than 11 **bulk electric system** buses</u>: sequence of events recording and **fault** recording data is required on at least the 10% of the **bulk electric system** buses determined in Step 6 with the highest maximum available calculated 3-phase short circuit MVA. Proceed to Step 8.

Step 8 Sequence of events recording and **fault** recording data is required at additional **bulk electric system** buses on the list determined in Step 6. The aggregate of the number of **bulk electric system** buses determined in Step 7 and in this Step 8 are at least 20% of the **bulk electric system** buses determined in Step 6. The additional **bulk electric system** buses are selected, at the discretion of the **legal owner** of a **transmission facility**, to provide maximum wide-area coverage for sequence of events recording and **fault** recording data. The following **bulk electric system** bus locations are recommended:

(a) electrically distant **bulk electric system** buses or electrically distant from other **disturbance monitoring equipment** devices;

(b) voltage sensitive areas;

(c) cohesive load and generation zones;

(d) **bulk electric system** buses with a relatively high number of incident transmission circuits

(e) **bulk electric system** buses with **reactive power** devices; and

(f) major facilities interconnecting outside the area of the **legal owner** of a **transmission facility**.

Step 9 The list of monitored **bulk electric system** buses for sequence of events recording and **fault** recording data for requirement R1 is the aggregate of the **bulk electric system** buses determined in Steps 7 and 8.

**Appendix 2**

**Implementation Plan**

**Effective Date**

This **reliability standard** is effective on the first **day** 3 full calendar quarters after the date that it is approved by the **Commission**.

**Implementation Plan for PRC-002-AB-2 Requirements R1 and R5:**

Entities must be 100% compliant on the first **day** following 3 full calendar quarters after the date that the **reliability standard** is approved by the **Commission**.

**Implementation Plan for PRC-002-AB-2 Requirements R2, R3, R4, R6, R7, R8, R9, R10,and R11:**

Entities must be at least 50% compliant within 4 calendar years of the effective date of PRC-002-AB-2 and 100% compliant within 6 calendar years of the effective date.

Entities that own only one identified **bulk electric system** bus, **system element** on the **bulk electric system**, or **generating unit** must be 100% compliant within 6 calendar years of the effective date.

Entities must be 100% compliant with a re-evaluated list from requirements R1 or R5 within 3 calendar years following the notification by the **ISO** or the **legal owner** of a **transmission facility** that re-evaluated the list.

**Standards for Retirement**

**PRC-018-AB-1**

Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** must maintain documentation to demonstrate compliance with PRC-018-AB-1 until that entity meets the requirements of PRC-002-AB-2 in accordance with this Implementation Plan. **Reliability standard** PRC-018-AB-1 remains effective throughout the phased implementation period of PRC-002-AB-2 and is applicable to an entity's **disturbance** monitoring and reporting activities not yet transitioned to PRC-002-AB-2. PRC-018-AB-1 will be retired following full implementation of PRC-002-AB-2 as noted below.

PRC-018-AB-1 Midnight of the day immediately prior to 6 years after the effective date of PRC-002-AB-2.

## Appendix 3
## Sequence of Events Recording Data Format
## (Requirement R11, R11.3)

Date, Time, Local Time Code, Substation, Device, State[1]

08/27/13, 23:58:57.110, -5, Sub 1, Breaker 1, Close

08/27/13, 23:58:57.082, -5, Sub 2, Breaker 2, Close

08/27/13, 23:58:47.217, -5, Sub 1, Breaker 1, Open

08/27/13, 23:58:47.214, -5, Sub 2, Breaker 2, Open

[1] "OPEN" and "CLOSE" are used as examples. Other terminology such as TRIP, TRIP TO LOCKOUT, RECLOSE, etc. is also acceptable.

# Alberta Reliability Standard
# Analysis and Mitigation of Transmission and Generation Protection System Misoperation
# PRC-004-AB2-1

## 1. Purpose

The purpose of this **reliability standard** is to ensure all **misoperations** of transmission and generation **protection systems** affecting the **reliability** of the **bulk electric system** are analyzed and mitigated.

## 2. Applicability

This **reliability standard** applies to:

(a) the **legal owner** of a **transmission facility**;

(b) the **legal owner** of a **generating unit** that:

(i) is not part of an **aggregated generating facility**;

(ii) has a **maximum authorized real power** rating greater than 4.5 MW;

(iii) is directly connected to the **transmission system** or to **transmission facilities** within the City of Medicine Hat; and

(iv) has **protection systems** that directly affect the **reliability** of the **bulk electric system**;

(c) the **legal owner** of an **aggregated generating facility** that:

(i) is directly connected to the **transmission system** or to **transmission facilities** within the City of Medicine Hat;

(ii) has a **maximum authorized real power** rating greater than 4.5 MW; and

(iii) has **protection systems** that directly affect the **reliability** of the **bulk electric system**; and

(d) the **ISO**.

## 3. Requirements

**R1** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facilit**y must analyze **misoperations** of its **protection systems** affecting the **reliability** of the **bulk electric system**, and develop and implement a corrective action plan to avoid future **misoperation**s of a similar nature.

**R2** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** must provide to the **ISO** documentation of its **misoperations** analyses and corrective action plans upon request by the **ISO**.

**R3** The **ISO** must provide to the **WECC** documentation of the **misoperations** analyses and corrective action plans upon request by the **WECC**.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of analyzing **misoperations**, and developing and implementing a corrective action plan as required in requirement R1 exists. Evidence may include reports that include analysis and corrective action plans, emails, work orders, or other equivalent evidence.

**MR2** Evidence of providing to the **ISO** documentation of **misoperations** analyses and corrective action plans as required in requirement R2 exists. Evidence may include emails, dated correspondence, or other equivalent evidence.

**MR3** Evidence of providing to the **WECC** documentation of the **misoperations** analyses and corrective action plans as required in requirement R3 exists. Evidence may include emails, dated correspondence, or other equivalent evidence

## Revision History

| Date | Description |
|---|---|
| 2019-04-01 | Clarification to ensure the protections system misoperations that must be analyzed are those affecting the reliability of the bulk electric system. Administrative update: existing PRC-004-AB1-1 is being renamed PRC-004-AB2-1; and amendments to ensure consistent use of defined terms as included in the AESO's Consolidated Authoritative Document Glossary ("CADG"); formatting and grammatical corrections; the deletion of the following sections: (a) "Definitions"; (b) "Processes and Procedures", (c) "Appendices"; and (d) "Guidelines" |
| 2013-01-02 | Administrative update – "TFO" and "GFO" replaced with "legal owner of a transmission facility", "legal owner of a generating unit" and "legal owner of an aggregated generating facility"; and other minor clean up items. |
| 2010-02-11 | Initial release. |

# Alberta Reliability Standard
# Protection System and Remedial Action Scheme Misoperation
# PRC-004-WECC-AB1-1

## 1. Purpose

The purpose of this **reliability standard** is to ensure all **misoperations** of transmission and generation **protection systems** and RASs on transmission paths are analyzed and mitigated.

## 2. Applicability

This **reliability standard** applies to:

(a) the **legal owner** of a **transmission facility** that is the **legal owner** of a **WECC** major transmission path **facility** or **RAS** listed in the tables titled “Major WECC Transfer Paths in the Bulk Electric System” and “Major WECC Remedial Action Schemes (RAS)” as provided by the **WECC;**

(b) the **operator** of a **transmission facility** that operates a **WECC** major transmission path **facility** or **RAS** listed in the tables titled “Major WECC Transfer Paths in the Bulk Electric System” and “Major WECC Remedial Action Schemes (RAS)” as provided by the **WECC;**

(c) the legal owner of a generating unit that owns components of RASs listed in the table titled “Major WECC Remedial Action Schemes (RAS)” as provided by the WECC;

(d) the **legal owner** of an **aggregated generating facility** that owns components of **RASs** listed in the table titled “Major WECC Remedial Action Schemes (RAS)” as provided by the **WECC;**

(e) the **operator** of a **generating unit** that operates **RASs** listed in the table titled “Major WECC Remedial Action Schemes (RAS)” as provided by the **WECC;**

(f) the **operator** of an **aggregated generating facility** that operates **RASs** listed in the table titled “Major WECC Remedial Action Schemes (RAS)” as provided by the **WECC**; and

(g) the **ISO**.

## 3. Definitions

Bold terms used in this **reliability standard** have the meanings as set out in the ***Consolidated Authoritative Document Glossary***.

## 4. Requirements

**R1** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, **legal owner** of an **aggregated generating facility**, **operator** of a **transmission facility**, **operator** of a **generating unit** and **operator** of an **aggregated generating facility** must ensure that its **system operator**s and protection personnel analyze all **protection system** and **RAS** operations as follows:

**R1.1** Each **operator** of a **transmission facility**, **operator** of a **generating unit** and **operator** of an **aggregated generating facility** must review all tripping of transmission **system elements** and **RAS** operations to identify apparent **misoperations** within 24 hours.

**R1.2** Protection personnel of the **legal owner** of a **transmission facility**, the **legal owner** of a **generating unit** and the **legal owner** of an **aggregated generating facility** must analyze all operations of **protection systems** and **RAS** within 20 business **days** of the operation of either such system or **RAS** to determine whether a **misoperation** has occurred.

**R2** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** must perform the actions listed in requirements R2.1 to R2.4 inclusive for each **misoperation** of the **protection system** or **RAS**, subject to the following:

Requirements R2.1 to R2.4 inclusive do not apply to **protection system** and/or **RAS** operations that appear to have operated correctly at the time of occurrence. If the **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** or **legal owner** of an **aggregated generating facility** later finds through **system** protection personnel analysis that the **protection system** or **RAS** misoperated, the requirements of R2.1 to R2.4 inclusive become applicable at the time the **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** or **legal owner** of an **aggregated generating facility** identifies the **misoperation.**

Table 1 is provided as a simplified summary of the requirements in R2.1 to R2.4 inclusive.

**2.1** If the **protection system** or **RAS** has a **security-based misoperation** and two or more **FEPS** or **FERAS** remain in service to ensure **BES reliability**, the **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** or **legal owner** of an **aggregated generating facility** must remove from service the **protection system** or **RAS** that misoperated, within 22 hours following the identification of the **misoperation.**

Repair or replacement of the failed **protection system** or **RAS** is at the discretion of the **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** or **legal owner** of an **aggregated generating facility.**

**R2.2** If the **protection system** or **RAS** has a **security-based misoperation** and only one **FEPS** or **FERAS** remains in service to ensure **BES reliability**, the **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** or **legal owner** of an **aggregated generating facility** responsible for the **protection system** or **RAS**, as the case may be, must perform the following:

**R2.2.1** Remove from service, within 22 hours for repair or modification, the **protection system** or **RAS** that misoperated.

**R2.2.2** Repair or replace any **protection system** or **RAS** that misoperated with a **FEPS** or **FERAS** within 20 business **days** of the date of removal.

**R2.2.3** Remove the **system element** from service or disable the **RAS** if repair or replacement is not completed within 20 business **days.**

**R2.3** If the **protection system** or **RAS** has a **security-based** or **dependability-based misoperation** and a **FEPS** or **FERAS** is not in service to ensure **BES reliability,** the **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** or **legal owner** of an **aggregated generating facility** responsible for the **protection system** or **RAS**, as the case may be, must repair and place back in service within 22 hours the **protection system** or **RAS** that misoperated.

If this cannot be done, the responsible legal owner of a transmission facility, legal owner of a generating unit or legal owner of an aggregated generating facility must perform the following:

**R2.3.1** When a **FEPS** is not available, remove the associated **system element** from service.

**R2.3.2** When **FERAS** is not available, meet one of the following requirements:

**R2.3.2.1** If the responsible entity is a **legal owner** of a **generating unit** or **legal owner** of an **aggregated generating facility,** it must advise the **ISO**, and the **operator** of a **generating unit** or **operator** of an **aggregated generating facility** must adjust generation to a reliable operating level as directed by the **ISO.**

**R2.3.2.2** If the responsible entity is a **legal owner** of a **transmission facility**, it must advise the **ISO**, and the **operator** of a **transmission facility** must operate the **facilities** within the adjusted **SOL** as determined and directed by the **ISO**.

**R2.4** If the **protection system** or **RAS** has a **dependability-based misoperation**, but has one or more **FEPS** or **FERAS** that operated correctly, the associated **system element** or transmission path may remain in service without removing from service the **protection system** or **RAS** that failed, provided one of the following is performed

**R2.4.1** The **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** or **legal owner** of an **aggregated generating facility** must repair or replace any **protection system** or RAS that misoperated with **FEPS** and **FERAS** within 20 business **days** of the date of the **misoperation** identification, or

**R2.4.2** The **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** or **legal owner** of an **aggregated generating facility** must remove from service the associated **system element** or **RAS**.

**R3** The **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** or **legal owner** of an **aggregated generating facility** must submit a **misoperation** incident report to the **ISO** within six business **days** of identifying the **misoperation** for the following:

**R3.1** Identification of a **misoperation** of a **protection system** and/or **RAS**

**R3.2** Completion of repairs or the replacement of the protection system and/or **RAS** that misoperated.

**R4** The **ISO** must submit **misoperation** incident reports to **WECC** within 10 business **days** of identifying the **misoperation**.

## 5. Processes and Procedures

No procedures have been defined for this **reliability standard**.

## 6. Measures

The following measures correspond to the requirements identified in Section 4 of this **reliability standard**. For example, MR1 is the measure for R1.

**MR1** Measures for this requirement are identified in the subsections below.

**MR1.1** Documentation exists that confirms a review was completed within the timelines as specified in requirement R1.1.

**MR1.2** Documentation exists that confirms an analysis was completed and in the timelines as specified in requirement R1.2.

**MR2** Measures for this requirement are identified in the subsections below.

**MR2.1** Evidence exists and shows that required actions were taken in the timelines as specified in requirement R2.1.

**MR2.2** Measures for this requirement are identified in the subsections below**.**

**MR2.2.1** Evidence exists and shows that required actions were taken in the timelines as specified in requirement R2.2.1.

**MR2.2.2** Evidence exists and shows that required actions were taken in the timelines as specified in requirement R2.2.2.

**MR2.2.3** Evidence exists and shows that required actions were taken in the timelines as specified in requirement R2.2.3.

**MR2.3** Evidence exists and shows that required actions were taken in the timelines as specified in requirement R2.3**.**

**MR2.3.1** Evidence exists and shows that required actions were taken in the timelines as specified in requirement R2.3.1.

**MR2.3.2** Measures for this requirement are identified in the subsections below.

**MR2.3.2.1** Evidence exists and shows that required actions were taken in the timelines as specified in requirement R2.3.2.1.

**MR2.3.2.2** Evidence exists and shows that required actions were taken in the timelines as specified in requirement R2.3.2.2.

**MR2.4** Measures for this requirement are identified in the subsections below

**MR2.4.1** Evidence exists and shows that required actions were taken in the timelines as specified in requirement R2.4.1.

**MR2.4.2** Evidence exists and shows that required actions were taken in the timelines as specified in requirement R2.4.2.

**MR3** **Misoperation** incident report is submitted within timelines as specified in requirement R3.

**MR3.1** **Misoperation** incident report contains content as specified in requirement R3.1.

**MR3.2** **Misoperation** incident report contains content as specified in requirements R3.2.

**MR4** Confirmation exists that incident reports as specified in requirement R4 were received within the timelines specified, or evidence that requests for confirmation were made for the incident reports provided as specified in requirement R4**.**

## 7. Appendices

**Appendix 1 – Requirement R2: Table of Required Actions for Protection System or RAS Misoperation** (see below)

## 8. Guidelines

No guidelines have been defined for this **reliability standard**.

## Revision History

| Date | Description |
|---|---|
| 2016-08-30 | Inclusion of the defined term **system element**. |
| 2013-01-02 | Administrative update – "**TFO** and **GFO**" replaced with "**legal owner** of a **transmission facility**" "**legal owner** of a **generating unit**" and "**legal owner** of an **aggregated generating facility**"; and other minor cleanup items. |
| 2010-02-11 | New Issue |

**Appendix 1 – Requirement R2: Table of Required Actions for Protection System or RAS Misoperation**

| PRC-004-WECC-1 Requirement R2 - Table of Required Actions for **Protection System** or **RAS Misoperation** | | | | | |
|---|---|---|---|---|---|
| Protective System/RAS Situation | | | Required Mitigating Actions | | |
| Protection Basis: | Number of **FEPS** or **RAS** in place after **misoperation** | Misoperating **protection system** is: | **Protection System/RAS** Removal Requirement | **Protection System/RAS** Repair or Replacement Requirement | **System Element** Removal Requirement |
| | | | | | |
| Security | 2 or more | PS | Remove within 22h. | At owners discretion. | |
| | 1 | PS | Remove within 22h. | Repair within 20 **days**. | Remove **system element** from service. |
| | 0 | PS | None. | Repair within 22 hours. | If not repaired in 22 hours then remove **system element** from service. |
| | 2 or more | **RAS** | Remove within 22h. | At owners discretion. | |
| | 1 | **RAS** | Remove within 22h. | Repair within 20 **days**. | If not repaired in 20 days then disable **RAS** or remove **system element** from service. |
| | 0 | **RAS** | None. | Repair within 22 hours. | Either the **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** or **legal owner** of an **aggregated generating facility** must advise the **ISO**, and the **operator** of a **generating unit** or **operator** of an **aggregated generating facility** must adjust generating operating levels to a reliable operating level as directed by the **ISO** or the **ISO** will adjust the **SOL** and the **operator** of a **transmission facility** will operate the **facilities** within established limits. |

| | | | | | |
|---|---|---|---|---|---|
| Dependability | 1 or more that operated correctly | PS | Can leave in service. | Repair in 20 **days** or remove **system element** from service. | |
| | 0 | PS | None. | Repair within 22 hours. | If not repaired in 22 hours then remove **system element** from service. |
| | 1 or more that operated correctly | PS | Can leave in service. | Repair in 20 **days** or remove **RAS** or **system element** from service. | |
| | 0 | **RAS** | None. | Repair within 22 hours. | Either the **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** or **legal owner** of an **aggregated generating facility** must advise the **ISO**, and the **operator** of a **generating unit** or **operator** of an **aggregated generating facility** must adjust generating operating levels to a reliable operating level as directed by the **ISO** or the **ISO** will adjust the **SOL** and the **operator** of a **transmission facility** will operate the **facilities** within established limits. |

# Alberta Reliability Standard
# Protection System, Automatic Reclosing and Sudden Pressure Relaying Maintenance
# PRC-005-AB2-6

## 1. Purpose

The purpose of this **reliability standard** is to document and implement programs for the maintenance of all **protection systems**, automatic reclosing, and sudden pressure relaying affecting the reliability of the **transmission system** so that they are kept in working order.

## 2. Applicability

The entities identified in subsection 2.1 must apply the requirements of this **reliability standard** to the devices listed in subsection 2.2, unless exempted under subsection 2.3.

**2.1** This **reliability standard** applies to:

(a) the **legal owner** of a **transmission facility** that:

(i) is part of the **bulk electric system**, excluding any transformer with less than 2 terminals energized at 100 kV or higher;

(ii) is not part of the **bulk electric system**, and owns any of the following:

(A) the **protection systems** used for the **ISO**'s **underfrequency load shedding program**;

(B) the **protection systems** used for **undervoltage load shed systems** installed to prevent system voltage collapse or voltage instability for the **reliability** of the **interconnected electric system**;

(C) **protection systems** installed as a **remedial action scheme**, including automatic reclosing applied as an integral part of a **remedial action scheme**, for the **reliability** of the **interconnected electric system**; or

(iii) is material to this **reliability standard** and to the **reliability** of either the **interconnected electric system** or the City of Medicine Hat electric system, as the **ISO** determines and includes on a list published on the AESO website, which the **ISO** may amend from time to time in accordance with the process set out in Appendix 3.

(b) the **legal owner** of a **generating unit** that:

(i) has a **maximum authorized real power** rating greater than 18 MW and is either:

(A) directly connected to the **transmission system**,

(B) directly connected to **transmission facilities** within the City of Medicine Hat, or

(C) part of an industrial complex that is directly connected to the **transmission system** or to **transmission facilities** within the City of Medicine Hat;

(ii) is within a power plant that:

(A) is not part of an **aggregated generating facility**;

(B) is directly connected to the **transmission system** or to **transmission facilities** within the City of Medicine Hat; and

(C) has a combined **maximum authorized real power** rating greater than 67.5 MW;

(iii) is a **black start resource**; or

(iv) is material to this **reliability standard** and to the **reliability** of either the **interconnected electric system** or the City of Medicine Hat electric system, regardless of the **maximum authorized real power** rating of the **generating unit**, as the **ISO** determines and includes on a list published on the AESO website, which the **ISO** may amend from time to time in accordance with the process set out in Appendix 3;

(c) the **legal owner** of an **aggregated generating facility** that:

(i) has a **maximum authorized real power** rating greater than 67.5 MW and is either:

(A) directly connected to the **transmission system**;

(B) directly connected to **transmission facilities** within the City of Medicine Hat; or

(C) part of an industrial complex that is directly connected to the **transmission system** or to **transmission facilities** within the City of Medicine Hat;

(ii) is a **black start resource**; or

(iii) is material to this **reliability standard** and to the **reliability** of either the **interconnected electric system** or the City of Medicine Hat electric system, regardless of the **maximum authorized real power** rating of the **aggregated generating facility**, as the **ISO** determines and includes on a list published on the AESO website, which the **ISO** may amend from time to time in accordance with the process set out in Appendix 3.

**2.2** This **reliability standard** applies to the following devices:

(a) **protection systems** and sudden pressure relaying that are installed for the purpose of detecting faults on **system elements** as identified in section 2.1;

(b) **protection systems** used for the **ISO**’s **underfrequency load shedding** program;

(c) **protection systems** used for **undervoltage load shed** systems installed to prevent system voltage collapse or voltage instability for the reliability of the **interconnected electric system**;

(d) **protection systems** installed as a **remedial action scheme** for the **reliability** of the **interconnected electric system**;

(e) **protection systems** and sudden pressure relaying for **generating units**, including:

(i) **protection systems** that act to trip the **generating unit** either directly or via lockout or auxiliary tripping relays;

(ii) **protection systems** and sudden pressure relaying for **generating unit** step-up transformers; and

(iii) **protection systems** and sudden pressure relaying for station service or excitation transformers connected to the **generating unit** bus, that act to trip the **generating unit** either directly or via lockout or tripping auxiliary relays;

(f) **protection systems** and sudden pressure relaying for **aggregated generating facilities** from and including the **collector bus** to a common point of connection at 100 kV or above;

(g) automatic reclosing :

(i) applied on all transmission lines connected to a bus operated at a voltage level of 100 kV or higher located at generating plant substations where the combined **maximum authorized real power** is greater than 500 MW;

(ii) applied on all transmission line terminals operated at a voltage level of 100 kV or higher at substations one bus away from generating plants specified in Section 2.2 (g)(i) when the substation is less than 10 circuit-miles from the generating plant substation; and

(iii) applied as an integral part of a **remedial action scheme** specified in subsection (d) above.

**2.3** Automatic reclosing addressed in subsections 2.2(g)(i) and 2.2(g)(ii) may be excluded if the equipment owner can demonstrate to the **ISO** that a close-in three-phase fault present for twice the normal clearing time (capturing a minimum trip-close-trip time delay) does not result in a total loss of gross generation in either the **interconnected electric system** or the City of Medicine Hat electric system exceeding the gross capacity of the largest **generating unit** where the automatic reclosing is applied.

## 3. Requirements

**R1** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** must establish a **protection system** maintenance program for its **protection systems**, automatic reclosing, and sudden pressure relaying.

The **protection system** maintenance program must:

**R1.1** identify which maintenance method (a time-based method, the performance-based method per Appendix 2, or a combination of these maintenance methods) is used to address each **protection system**, automatic reclosing, and sudden pressure relaying component type (as identified in Appendix 1). All batteries associated with the station dc supply component type of a **protection system** must be included in a time-based program as described in Table 1-4 and Table 3 of Appendix 1.

**R1.2** include the applicable monitored component attributes applied to each **protection system**, automatic reclosing, and sudden pressure relaying component type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-3, and Table 5 of Appendix 1, where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored **protection system**, automatic reclosing, and sudden pressure relaying components.

**R2** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** that uses performance-based maintenance intervals in its **protection system** maintenance program must follow the procedure established in Appendix 2 to establish and maintain its performance-based intervals.

**R3** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** that uses time-based maintenance program(s) must maintain its **protection system**, automatic reclosing, and sudden pressure relaying components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-3, and Table 5 of Appendix 1.

**R4** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** that uses performance-based maintenance program(s) in accordance with requirement R2 must implement and follow its **protection system** maintenance program for its **protection system**, automatic reclosing, and sudden pressure relaying components that are included within the performance-based program(s).

**R5** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** must demonstrate efforts to correct identified unresolved maintenance issues.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of having a documented **protection system** maintenance program in accordance with requirement R1 exists. Evidence may include, but is not limited to a documented **protection system** maintenance program that may include supporting information such as manufacturer's specifications or engineering drawings or other equivalent evidence.

**MR2** Evidence of following the procedure for performance-based maintenance intervals as required in requirement R2 exists. Evidence may include, but is not limited to, component lists, dated maintenance records and dated analysis records and results or other equivalent evidence.

**MR3** Evidence of maintaining **protection system**, automatic reclosing, and sudden pressure relaying components in accordance with the minimum maintenance activities and maximum maintenance intervals as required in requirement R3 exists. Evidence may include, but is not limited to, dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders or other equivalent evidence.

**MR4** Evidence of following the **protection system** maintenance program for performance-based maintenance program(s) as required in requirement R4 exists. Evidence may include, but is not limited to, dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders or other equivalent evidence.

**MR5** Evidence of demonstrating efforts to correct identified unresolved maintenance issues as required in requirement R5 exists. Evidence may include, but is not limited to, work orders, replacement component orders, invoices, project schedules with completed milestones, return material authorizations or purchase orders or other equivalent evidence.

## 5. Implementation Plan

Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** must implement requirements R1 through R5 in accordance with the implementation plan in Appendix 5.

## 6. Appendices

Appendix 1 – *Tables describing protection system, automatic reclosing, and sudden pressure relaying component types, maintenance activities and intervals*:

| | |
|---|---|
| Table 1-1 | Maintenance Activities and Intervals for Protection Systems for Protective Relay Excluding distributed UFLS and distributed UVLS |
| Table 1-2 | Maintenance Activities and Intervals for Protection Systems for Communications Systems Excluding distributed UFLS and distributed UVLS |
| Table 1-3 | Maintenance Activities and Intervals for Protection Systems for Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS |
| Table 1-4(a) | Maintenance Activities and Intervals for Protection Systems for Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS |

| | |
|---|---|
| Table 1-4(b) | Maintenance Activities and Intervals for Protection Systems for Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS |
| Table 1-4(c) | Maintenance Activities and Intervals for Protection Systems for Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS |
| Table 1-4(d) | Maintenance Activities and Intervals for Protection Systems for Protection System Station dc Supply Using Non Battery Based Energy Storage Excluding distributed UFLS and distributed UVLS |
| Table 1-4(e) | Maintenance Activities and Intervals for Protection Systems for Protection System Station dc Supply for non-bulk electric system Interrupting Devices for RAS, non-distributed UFLS, and non-distributed UVLS systems |
| Table 1-4(f) | Exclusions for Protection System Station dc Supply Monitoring Devices and Systems |
| Table 1-5 | Maintenance Activities and Intervals for Protection Systems for Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS, Automatic Reclosing, and Sudden Pressure Relaying |
| Table 2 | Alarming Paths and Monitoring |
| Table 3 | Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems |
| Table 4-1 | Maintenance Activities and Intervals for Automatic Reclosing Components for Reclosing and Supervisory Relay |
| Table 4-2(a) | Maintenance Activities and Intervals for Automatic Reclosing Components for Control Circuitry Associated with Reclosing and Supervisory Relays that are NOT an Integral Part of RAS |
| Table 4-2(b) | Maintenance Activities and Intervals for Automatic Reclosing Components for Control Circuitry Associated with Reclosing and Supervisory Relays that are an Integral Part of RAS |
| Table 4-3 | Maintenance Activities and Intervals for Automatic Reclosing Components for Voltage Sensing Devices Associated with Supervisory Relays |
| Table 5-1 | Maintenance Activities and Intervals for Sudden Pressure Relaying for Fault Pressure Relay |
| Table 5-2 | Maintenance Activities and Intervals for Sudden Pressure Relaying for Control Circuitry Associated with a Fault Pressure Relay |

Appendix 2 – *Performance-Based Protection System Maintenance Program*;

Appendix 3 – *Amending Process for List of Facilities*;

Appendix 4 – *Amending Process for List of Devices*; and

Appendix 5 – *Implementation Plan*

### Revision History

| Date | Description |
|---|---|
| 2020-10-13 | Revised Applicability section 2.2(g) to clearly identify the reclosers that this reliability standard applies to. |
| 2019-10-01 | Revised:<br>- the Applicability section to clearly apply the reliability standard to protection systems associated with underfrequency load shedding, under voltage load shedding, and remedial action schemes that are not part of the bulk electric system, add clarity regarding the reference to the bulk electric system and the exclusion of certain types of transformers, and to add a provision enabling the ISO to add transmission facilities it determines are material to this reliability standard;<br>- the Implementation Plan to add references to Tables 4 and 5 in subsection 5.5 in Appendix 5; and<br>- reliability standard to correct various typos, update references, and replace the descriptions of compliance dates in Appendix 5 with the actual calendar dates. |
| 2019-10-01 | Initial release. |

**Appendix 1 – Protection system, automatic reclosing, and sudden pressure relaying component types, maintenance activities and intervals**

| Table 1-1<br>Maintenance Activities and Intervals for Protection Systems<br>Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3) | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Any unmonitored protective relay not having all the monitoring attributes of a category below. | 6 calendar years | For all unmonitored relays:<br>- Verify that settings are as specified.<br><br>For non-microprocessor relays:<br>- Test and, if necessary, calibrate.<br><br>For microprocessor relays:<br>- Verify operation of the relay inputs and outputs that are essential to proper functioning of the **protection system**; and<br>- Verify acceptable measurement of power system input values. |

| Table 1-1<br>Maintenance Activities and Intervals for Protection Systems<br>Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3) | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Monitored microprocessor protective relay with the following:<br>- Internal self-diagnosis and alarming (see Table 2);<br>- Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics; and<br>- Alarming for power supply failure (see Table 2). | 12 calendar years | Verify:<br>- Settings are as specified;<br>- Operation of the relay inputs and outputs that are essential to proper functioning of the **protection system**; and<br>- Acceptable measurement of power system input values. |

| Table 1-1<br>Maintenance Activities and Intervals for Protection Systems<br>Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3) | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Monitored microprocessor protective relay with preceding row attributes and the following:<br>• Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2);<br>• Some or all inputs and outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2); and<br>• Alarming for change of settings (See Table 2). | 12 calendar years | Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the **protection system**. |

| Table 1-2<br>Maintenance Activities and Intervals for Protection Systems<br>Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3) | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below. | 4 **months** | Verify that the communications system is functional. |
| | 6 calendar years | Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate).<br>Verify operation of communications system inputs and outputs that are essential to proper functioning of the **protection system**. |
| Any communications system necessary for correct operation of protective functions with continuous monitoring or periodic automated testing for the presence of the channel function, and alarming for loss of function (See Table 2). | 12 calendar years | Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate).<br>Verify operation of communications system inputs and outputs that are essential to proper functioning of the **protection system**. |

| Table 1-2<br>Maintenance Activities and Intervals for Protection Systems<br>Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3) | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Any communications system with all of the following:<br>• Continuous monitoring or periodic automated testing for the performance of the channel using criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate, and alarming for excessive performance degradation); (See Table 2); and<br>• Some or all inputs and outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). | 12 calendar years | Verify only the unmonitored communications system inputs and outputs that are essential to proper functioning of the **protection system** |

| Table 1-3<br>Maintenance Activities and Intervals for Protection Systems<br>Component Type - Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS (see Table 3) | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Any voltage and current sensing devices not having monitoring attributes of the category below. | 12 calendar years | Verify that current and voltage signal values are provided to the protective relays. |
| Voltage and current sensing devices connected to microprocessor relays with ac measurements that are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure (see Table 2). | No periodic maintenance specified | None. |

| Table 1-4(a)<br>Maintenance Activities and Intervals for Protection Systems<br>Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3)<br>Protection System Station dc supply used only for non-bulk electric system interrupting devices for RAS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)). | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| **Protection system** station dc supply using Vented Lead-Acid (VLA) batteries not having monitoring attributes of Table 1-4(f). | 4 **months** unless a variance is granted by the AESO | Verify:<br>• Station dc supply voltage<br>Inspect:<br>• Electrolyte level; and<br>• For unintentional grounds |
| | 18 **months** | Verify:<br>• Float voltage of battery charger<br>• Battery continuity<br>• Battery terminal connection resistance<br>• Battery intercell or unit-to-unit connection resistance |

| Table 1-4(a)<br>Maintenance Activities and Intervals for Protection Systems<br>Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3)<br><br>Protection System Station dc supply used only for non-bulk electric system interrupting devices for RAS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)). | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| | | Inspect:<br>• Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible; and<br>• Physical condition of battery rack. |
| | 18 **months**<br>-or-<br>6 calendar years | Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline.<br>-or-<br>Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank. |

| Table 1-4(b)<br>Maintenance Activities and Intervals for Protection Systems<br>Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3)<br><br>Protection System Station dc supply used only for non-bulk electric system interrupting devices for RAS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)). | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| **Protection system** station dc supply with Valve Regulated Lead-Acid (VRLA) batteries not having monitoring attributes of Table 1-4(f). | 4 **months** unless a variance is granted by the AESO | Verify:<br>- Station dc supply voltage<br><br>Inspect:<br>- For unintentional grounds |
| | 6 **months** | Inspect:<br>- Condition of all individual units by measuring battery cell/unit internal ohmic values. |
| | 18 **months** | Verify:<br>- Float voltage of battery charger;<br>- Battery continuity; |

| Table 1-4(b)<br>Maintenance Activities and Intervals for Protection Systems<br>Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3)<br><br>Protection System Station dc supply used only for non-bulk electric system interrupting devices for RAS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)). | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| | | • Battery terminal connection resistance; and<br>• Battery intercell or unit-to-unit connection resistance.<br><br>Inspect:<br>• Physical condition of battery rack. |
| | 6 **months**<br>-or-<br>3 calendar years | Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline.<br>-or-<br>Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank. |

| Table 1-4(c)<br>Maintenance Activities and Intervals for Protection Systems<br>Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3)<br><br>Protection System Station dc supply used only for non-bulk electric system interrupting devices for RAS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)). | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| **Protection system** station dc supply Nickel-Cadmium (NiCad) batteries not having monitoring attributes of Table 1-4(f). | 4 **months** unless a variance is granted by the AESO | Verify:<br>• Station dc supply voltage.<br>Inspect:<br>• Electrolyte level; and<br>• For unintentional grounds. |
| | 18 **months** | Verify:<br>• Float voltage of battery charger;<br>• Battery continuity;<br>• Battery terminal connection resistance; and<br>• Battery intercell or unit-to-unit connection resistance. |

| Table 1-4(c)<br>Maintenance Activities and Intervals for Protection Systems<br>Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3)<br>Protection System Station dc supply used only for non-bulk electric system interrupting devices for RAS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)). | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| | | Inspect:<br>• Cell condition of all individual battery cells; and<br>• Physical condition of battery rack. |
| | 6 calendar years | Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank. |

| Table 1-4(d)<br>Maintenance Activities and Intervals for Protection Systems<br>Component Type – Protection System Station dc Supply Using Non Battery Based Energy Storage Excluding distributed UFLS and distributed UVLS (see Table 3)<br><br>Protection System Station dc supply used only for non-bulk electric system interrupting devices for RAS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)). | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Any **protection system** station dc supply not using a battery and not having monitoring attributes of Table 1-4(f). | 4 **months** | Verify:<br>• Station dc supply voltage<br><br>Inspect:<br>• For unintentional grounds |
| | 18 **months** | Inspect:<br>Condition of non-battery based dc supply |
| | 6 calendar years | Verify that the dc supply can perform as manufactured when ac power is not present. |

| Table 1-4(e)<br>Maintenance Activities and Intervals for Protection Systems<br><br>Component Type – Protection System Station dc Supply for non-bulk electric system Interrupting Devices for RAS, non-distributed UFLS, and non-distributed UVLS systems | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Any **protection system** dc supply used for tripping only non- **bulk electric system** interrupting devices as part of a **remedial action scheme**, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f). | When control circuits are verified (See Table 1-5) | Verify station dc supply voltage. |

| Table 1-4(f)<br>Exclusions for Protection System Station dc Supply Monitoring Devices and Systems | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Any station dc supply with high and low voltage monitoring and alarming of the battery charger voltage to detect charger overvoltage and charger failure (See Table 2). | No periodic maintenance specified | No periodic verification of station dc supply voltage is required. |
| Any battery based station dc supply with electrolyte level monitoring and alarming in every cell (See Table 2). | | No periodic inspection of the electrolyte level for each cell is required. |
| Any station dc supply with unintentional dc ground monitoring and alarming (See Table 2). | | No periodic inspection of unintentional dc grounds is required. |
| Any station dc supply with charger float voltage monitoring and alarming to ensure correct float voltage is being applied on the station dc supply (See Table 2). | | No periodic verification of float voltage of battery charger is required. |
| Any battery based station dc supply with monitoring and alarming of battery string continuity (See Table 2). | | No periodic verification of the battery continuity is required. |

| Table 1-4(f)<br>Exclusions for Protection System Station dc Supply Monitoring Devices and Systems | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Any battery based station dc supply with monitoring and alarming of the intercell and/or terminal connection detail resistance of the entire battery (See Table 2). | | No periodic verification of the intercell and terminal connection resistance is required. |
| Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with internal ohmic value or float current monitoring and alarming, and evaluating present values relative to baseline internal ohmic values for every cell/unit (See Table 2). | | No periodic evaluation relative to baseline of battery cell/unit measurements indicative of battery performance is required to verify the station battery can perform as manufactured. |
| Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with monitoring and alarming of each cell/unit internal ohmic value (See Table 2). | | No periodic inspection of the condition of all individual units by measuring battery cell/unit internal ohmic values of a station VRLA or Vented Lead-Acid (VLA) battery is required. |

**Table 1-5**

**Maintenance Activities and Intervals for Protection Systems**

**Component Type - Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS (see Table 3), Automatic Reclosing (see Table 4), and Sudden Pressure Relaying (see Table 5)**

**Note: Table requirements apply to all Control Circuitry Components of Protection Systems, and RAS except as noted.**

| Component Attributes | Maximum Maintenance Interval | Maintenance Activities |
|---|---|---|
| Trip coils or actuators of circuit breakers, interrupting devices, or mitigating devices (regardless of any monitoring of the control circuitry). As long as there is monitoring on the mitigating devices for high-voltage direct current/ flexible alternating current transmission system (HVDC/FACTS) devices no maintenance is required. | 6 calendar years | Verify that each trip coil is able to operate the circuit breaker, interrupting device, or mitigating device. |
| Electromechanical lockout devices which are directly in a trip path from the protective relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry). | 6 calendar years | Verify electrical operation of electromechanical lockout devices. |
| Unmonitored control circuitry associated with RAS. (See Table 4-2(b) for RAS which include automatic reclosing.) | 12 calendar years | Verify all paths of the control circuits essential for proper operation of the RAS. |

| | | |
|---|---|---|
| Unmonitored control circuitry associated with protective functions inclusive of all auxiliary relays. | 12 calendar years | Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices. |
| Control circuitry associated with protective functions and/or RAS whose integrity is monitored and alarmed (See Table 2). | No periodic maintenance specified | None. |

| Table 2 – Alarming Paths and Monitoring<br><br>In Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-3, and Table 5 alarm attributes used to justify extended maximum maintenance intervals and/or reduced maintenance activities are subject to the following maintenance requirements | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Any alarm path through which alarms in Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-3, and Table 5 are conveyed from the alarm origin to the location where corrective action can be initiated, and not having all the attributes of the "Alarm Path with monitoring" category below.<br><br>Alarms are reported within 24 hours of detection to location where corrective action can be initiated. | 12 calendar years | Verify that the alarm path conveys alarm signals to a location where corrective action can be initiated. |
| Alarm Path with monitoring:<br><br>The location where corrective action is taken receives an alarm within 24 hours for failure of any portion of the alarming path from the alarm origin to the location where corrective action can be initiated. | No periodic maintenance specified | None. |

| Table 3<br>Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Any unmonitored protective relay not having all the monitoring attributes of a category below. | 6 calendar years | Verify that settings are as specified.<br>For non-microprocessor relays:<br>- Test and, if necessary calibrate.<br><br>For microprocessor relays:<br>- Verify operation of the relay inputs and outputs that are essential to proper functioning of the **protection system**; and<br>- Verify acceptable measurement of power system input values. |
| Monitored microprocessor protective relay with the following:<br>- Internal self-diagnosis and alarming (See Table 2); and<br>- Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics.<br><br>Alarming for power supply failure (See Table 2). | 12 calendar years | Verify:<br>- Settings are as specified;<br>- Operation of the relay inputs and outputs that are essential to proper functioning of the **protection system**; and<br>- Acceptable measurement of power system input values. |

| Table 3<br>Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Monitored microprocessor protective relay with preceding row attributes and the following:<br>- Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2); and<br>- Some or all inputs and outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2).<br>Alarming for change of settings (See Table 2). | 12 calendar years | Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the **protection system**. |
| Voltage and/or current sensing devices associated with UFLS or UVLS systems. | 12 calendar years | Verify that current and/or voltage signal values are provided to the protective relays. |
| **Protection system** dc supply for tripping non-**bulk electric system** interrupting devices used only for a UFLS or UVLS system. | 12 calendar years | Verify **protection system** dc supply voltage. |

| Table 3<br>Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Control circuitry between the UFLS or UVLS relays and electromechanical lockout and/or tripping auxiliary devices (excludes non-**bulk electric system** interrupting device trip coils). | 12 calendar years | Verify the path from the relay to the lockout and/or tripping auxiliary relay (including essential supervisory logic). |
| Electromechanical lockout and/or tripping auxiliary devices associated only with UFLS or UVLS systems (excludes non-**bulk electric system** interrupting device trip coils). | 12 calendar years | Verify electrical operation of electromechanical lockout and/or tripping auxiliary devices. |
| Control circuitry between the electromechanical lockout and/or tripping auxiliary devices and the non-**bulk electric system** interrupting devices in UFLS or UVLS systems, or between UFLS or UVLS relays (with no interposing electromechanical lockout or auxiliary device) and the non-**bulk electric system** interrupting devices (excludes non-**bulk electric system** interrupting device trip coils). | No periodic maintenance specified | None. |
| Trip coils of non-**bulk electric system** interrupting devices in UFLS or UVLS systems. | No periodic maintenance specified | None. |

**Table 4-1**

**Maintenance Activities and Intervals for Automatic Reclosing Components**
**Component Type – Reclosing and Supervisory Relay**

**Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-1 through 1-5, the Components only need to be tested once during a distinct maintenance interval.**

| Component Attributes | Maximum Maintenance Interval | Maintenance Activities |
|---|---|---|
| Any unmonitored reclosing relay or supervisory relay not having all the monitoring attributes of a category below. | 6 calendar years | Verify that settings are as specified.<br>For non-microprocessor reclosing or supervisory relays:<br>- Test and, if necessary calibrate<br>For microprocessor reclosing or supervisory relays:<br>- Verify operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.<br>For microprocessor supervisory relays:<br>- Verify acceptable measurement of power system input values. |

| Table 4-1<br><br>Maintenance Activities and Intervals for Automatic Reclosing Components<br>Component Type – Reclosing and Supervisory Relay<br><br>Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-1 through 1-5, the Components only need to be tested once during a distinct maintenance interval. | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
|  Monitored microprocessor reclosing relay or supervisory relay with the following: Internal self-diagnosis and alarming (See Table 2).<br> Alarming for power supply failure (See Table 2).<br><br>For supervisory relay:<br><br>Voltage waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. | 12 calendar years | Verify:<br> Settings are as specified.<br> Operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.<br><br>For supervisory relays:<br> Verify acceptable measurement of power system input values. |

| Table 4-1<br><br>Maintenance Activities and Intervals for Automatic Reclosing Components<br>Component Type – Reclosing and Supervisory Relay<br><br>Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-1 through 1-5, the Components only need to be tested once during a distinct maintenance interval. | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Monitored microprocessor reclosing relay or supervisory relay with preceding row attributes and the following:<br>• Some or all inputs and outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2).<br>• Alarming for change of settings (See Table 2).<br><br>For supervisory relay:<br>• Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). | 12 calendar years | Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the automatic reclosing. |

| Table 4-2(a)<br>Maintenance Activities and Intervals for Automatic Reclosing Components<br>Component Type – Control Circuitry Associated with Reclosing and Supervisory Relays that are NOT an Integral Part of RAS<br>Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-5, the Components only need to be tested once during a distinct maintenance interval. | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Unmonitored control circuitry associated with automatic reclosing that is not an integral part of an RAS. | 12 calendar years | Verify that automatic reclosing, upon initiation, does not issue a premature closing command to the close circuitry. |
| Control circuitry associated with automatic reclosing that is not part of an RAS and is monitored and alarmed for conditions that would result in a premature closing command. (See Table 2) | No periodic maintenance specified | None. |

**Table 4-2(b)**

**Maintenance Activities and Intervals for Automatic Reclosing Components**

**Component Type – Control Circuitry Associated with Reclosing and Supervisory Relays that are an Integral Part of RAS**

**Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-5, the Components only need to be tested once during a distinct maintenance interval.**

| Component Attributes | Maximum Maintenance Interval | Maintenance Activities |
|---|---|---|
| Close coils or actuators of circuit breakers or similar devices that are used in conjunction with automatic reclosing as part of an RAS (regardless of any monitoring of the control circuitry). | 6 calendar years | Verify that each close coil or actuator is able to operate the circuit breaker or mitigating device. |
| Unmonitored close control circuitry associated with automatic reclosing used as an integral part of an RAS. | 12 calendar years | Verify all paths of the control circuits associated with automatic reclosing that are essential for proper operation of the RAS. |
| Control circuitry associated with automatic reclosing that is an integral part of an RAS whose integrity is monitored and alarmed (See Table 2). | No periodic maintenance specified | None. |

| Table 4-3<br>Maintenance Activities and Intervals for Automatic Reclosing Components<br>Component Type – Voltage Sensing Devices Associated with Supervisory Relays<br>Note: In cases where Components of Automatic Reclosing are common to Components listed in Table 1-3, the Components only need to be tested once during a distinct maintenance interval. | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Any voltage sensing devices not having monitoring attributes of the category below. | 12 calendar years | Verify that voltage signal values are provided to the supervisory relays. |
| Voltage sensing devices that are connected to microprocessor supervisory relays with ac measurements that are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure. (See Table 2) | No periodic maintenance specified | None. |

| Table 5-1<br>Maintenance Activities and Intervals for Sudden Pressure Relaying<br><br>Component Type – Fault Pressure Relay<br>Note: In cases where Components of Sudden Pressure Relaying are common to Components listed in Table 1-5, the Components only need to be tested once during a distinct maintenance interval. | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Any fault pressure relay. | 6 calendar years unless a variance is granted by the AESO | Verify the pressure or flow sensing mechanism is operable. |

| Table 5-2<br>Maintenance Activities and Intervals for Sudden Pressure Relaying<br>Component Type – Control Circuitry Associated with a Fault Pressure Relay<br>Note: In cases where Components of Sudden Pressure Relaying are common to Components listed in Table 1-5, the Components only need to be tested once during a distinct maintenance interval. | | |
|---|---|---|
| **Component Attributes** | **Maximum Maintenance Interval** | **Maintenance Activities** |
| Electromechanical lockout devices which are directly in a trip path from the fault pressure relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry). | 6 calendar years unless a variance is granted by the AESO | Verify electrical operation of electromechanical lockout devices. |
| Unmonitored control circuitry associated with sudden pressure relaying. | 12 calendar years | Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices. |
| Control circuitry associated with sudden pressure relaying whose integrity is monitored and alarmed (See Table 2). | No periodic maintenance specified | None. |

## Appendix 2 – Performance-Based Protection System Maintenance Program

### Purpose:

1. To establish a technical basis for initial and continued use of a performance-based **protection system** maintenance program.
2. To establish the technical justification for the initial use of a performance-based **protection system** maintenance program:
   (a) Develop a list with a description of components included in each designated segment, with a minimum segment population of 60 components;
   (b) Maintain the components in each segment according to the time-based maximum allowable intervals established in Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-2, and Table 5 until results of maintenance activities for the segment are available for a minimum of 30 individual components of the segment;
   (c) Document the maintenance program activities and results for each segment, including maintenance dates and countable events for each included component;
   (d) Analyze the maintenance program activities and results for each segment to determine the overall performance of the segment and develop maintenance intervals; and
   (e) Determine the maximum allowable maintenance interval for each segment such that the segment experiences countable events on no more than 4% of the components within the segment, for the greater of either the last 30 components maintained or all components maintained in the previous year.
3. To maintain the technical justification for the ongoing use of a performance-based **protection system** maintenance program:
   (a) At least annually, update the list of components and segments, and/or description if any changes occur within the segment;
   (b) Perform maintenance on the greater of 5% of the components (addressed in the performance based **protection system** maintenance program) in each segment or 3 individual components within the segment in each year;
   (c) For the prior year, analyze the maintenance program activities and results for each segment to determine the overall performance of the segment; and
   (d) Using the prior year's data, determine the maximum allowable maintenance interval for each segment such that the segment experiences countable events on no more than 4% of the components within the segment, for the greater of either the last 30 components maintained or all components maintained in the previous year.

If the components in a segment maintained through a performance-based **protection system** maintenance program experience 4% or more countable events, develop, document and implement an action plan to reduce the countable events to less than 4% of the segment population within 3 years.

**Appendix 3 – Amending Process for List of Facilities**

In order to amend any list referenced in subsections 2.1(a)(iii), 2.1(b)(iv) and 2.1(c)(iii), of section 2, *Applicability* of this **reliability standard**, the **ISO** must:

(a) upon determining that a **transmission facility**, **generating unit** or **aggregated generating facility** is to be added, notify the **legal owner** in writing and determine when the **legal owner** is to be compliant with the requirements of this **reliability standard**, which from the date of notice must be at a minimum the maximum maintenance interval identified in Tables 1 to 5 plus six (6) full **months**;

(b) upon determining that a **transmission facility**, **generating unit** or **aggregated generating facility** is to be deleted, notify the **legal owner** in writing and determine an effective date for the **legal owner** to no longer be required to meet the applicable requirements; and

(c) publish the amended list with effective dates on the AESO website.

**Appendix 4 – Amending Process for List of Devices**

If devices are added or removed as described in subsections 2.2(b), 2.2(c) and 2.2(d) of section 2, *Applicability* of this **reliability standard** the **ISO** must:

(a) upon determining that a **protection system** that is to be used for **underfrequency load shedding**, **under voltage load shed** or that is to be installed as a **remedial action scheme** is to be added, notify the **legal owner** in writing and determine when the **legal owner** is to be compliant with the requirements of this **reliability standard**, which from the date of notice must be at a minimum the maximum maintenance interval identified in Tables 1 to 5 plus 6 full months;

(b) upon determining that a **protection system** that is used for **underfrequency load shedding**, **under voltage load shed** or that is installed as a **remedial action scheme** is to be removed, notify the **legal owner** in writing and determine an effective date for the **legal owner** to no longer be required to meet the applicable requirements.

**Appendix 5 – Implementation Plan**

## 1. Purpose

The purpose of this appendix is to set the effective dates and the implementation timelines for Alberta reliability standard PRC-005-AB, *Protection System, Automatic Reclosing and Sudden Pressure Relaying Maintenance* ("PRC-005-AB").

## 2. Compliance with Reliability Standards

The entities identified in section 2 of this **reliability standard** must comply with the requirements of PRC-005-AB in accordance with the implementation schedule.

## 3. Effective Date

PRC-005-AB will become effective on October 1, 2019. Entities must follow the phased implementation plan set out in sections 4 and 5 below.

## 4. Implementation Plan for Requirements R1, R2 and R5

Entities must be compliant with requirements R1, R2 and R5 of PRC-005-AB on October 1, 2019.

## 5. Implementation Plan for Requirements R3 and R4

1. For **protection system**, automatic reclosing, and sudden pressure relaying component maintenance activities with maximum allowable intervals of less than 1 calendar year, as established in Tables 1-1 through 1-5, the entity must be compliant with PRC-005-AB by April 1, 2020.
2. For **protection system**, automatic reclosing, and sudden pressure relaying component maintenance activities with maximum allowable intervals 1 calendar year or more, but 2 calendar years or less, as established in Tables 1-1 through 1-5, the entity must be compliant with PRC-005-AB by October 1, 2021.
3. For **protection system**, automatic reclosing, and sudden pressure relaying component maintenance activities with maximum allowable intervals of 3 calendar years, as established in Tables 1-1 through 1-5, maintenance must be completed in accordance with the following:
    - The entity must complete maintenance on 30% of identified components in accordance with their **protection system** maintenance program by October 1, 2020 or, for generating plants with scheduled outage intervals exceeding 2 years, at the conclusion of the first succeeding maintenance outage;
    - The entity must complete maintenance on 60% of the identified components in accordance with their **protection system** maintenance program by October 1, 2021.
    - The entity must complete maintenance on 100% of the identified components in accordance with their **protection system** maintenance program by October 1, 2022.
4. For **protection system**, automatic reclosing, and sudden pressure relaying component maintenance activities with maximum allowable intervals of 6 calendar years, as established in Tables 1-1 through 1-5, Table 3, Table 4-1, Table 4-2b, Table 5-1, and Table 5-2 maintenance must be completed in accordance with the following:
    - The entity must complete maintenance on 30% of the identified components in accordance with their **protection system** maintenance program by October 1, 2021 or, for generating plants with scheduled outage intervals exceeding 3 years, at the conclusion of the first succeeding maintenance outage.

- The entity must complete maintenance on 60% of the identified components in accordance with their **protection system** maintenance program by October 1, 2023.
- The entity must complete maintenance on 100% of the identified components in accordance with their **protection system** maintenance program by October 1, 2025.

5. For **protection system**, automatic reclosing, and sudden pressure relaying component maintenance activities with maximum allowable intervals of 12 calendar years, as established in Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-3, and Table 5-2 maintenance must be completed in accordance with the following:

- The entity must complete maintenance on 30% of the identified components in accordance with their **protection system** maintenance program by October 1, 2023.
- The entity must complete maintenance on 60% of the identified components in accordance with their **protection system** maintenance program by October 1, 2027.
- The entity must complete maintenance on 100% of the identified components in accordance with their **protection system** maintenance program by October 1, 2031.

## 1. Purpose

The purpose of this **reliability standard** is to establish design and documentation requirements for any automatic **underfrequency load shedding** program that arrests declining frequency, assists recovery of frequency following underfrequency events, and provides last resort system preservation measures.

## 2. Applicability

This **reliability standard** applies to:

(a) the **legal owner** of a **transmission facility** that has responsibility in an **underfrequency load shedding** program the **ISO** establishes;

(b) the **legal owner** of an **electric distribution system** that has responsibility in an **underfrequency load shedding** program the **ISO** establishes;

(c) a **market participant** receiving service under Rate DTS of the **ISO tariff** that has responsibility in an **underfrequency load shedding** program the **ISO** establishes; and

(d) the **ISO**.

Entities identified in item (a), (b) and (c) above are collectively referred to as "UFLS entities" in this **reliability standard**. For requirements in this **reliability standard** where a specific entity or subset of entities are the applicable entity or entities, the entity or entities are specified explicitly.

## 3. Requirements

**R1** Intentionally left blank.

**RD.B.1** The **ISO** must participate, through its involvement in the **WECC** UFLS Review Group or its successor, in a joint regional review with the other planning coordinators in the **WECC** regional entity area that develops and documents criteria, including consideration of historical events and system studies, to select portions of the **bulk electric system** that may form islands.

**R2** Intentionally left blank.

**RD.B.2** The **ISO** must identify one or more islands from the regional review, set out in requirement RD.B.1, to serve as a basis for designing a region-wide coordinated **underfrequency load shedding** program including:

**RD.B.2.1** those islands selected by applying the criteria in requirement RD.B.1; and

**RD.B.2.2** any portions of the **bulk electric system** designed to detach from the **Interconnection** as a result of the operation of a **protection system** or **remedial action scheme.**

**R3** Intentionally left blank.

**RD.B.3.** The **ISO** must adopt an **underfrequency load shedding** program;

(a) coordinated across the **WECC** regional entity area; and

(b) modified as appropriate for Alberta;

including notification to the UFLS entities of the adopted **underfrequency load shedding** program and a schedule for implementation within Alberta.

**R4** Intentionally left blank.

**RD.B.4** The **ISO** must participate in a coordinated **underfrequency load shedding** design assessment with the other planning coordinators in the **WECC** regional entity area at least once every five years.

**RD.B.4.1** Intentionally left blank.

**RD.B.4.2** Intentionally left blank.

**RD.B.4.3** Intentionally left blank.

**RD.B.4.4** Intentionally left blank.

**RD.B.4.5** Intentionally left blank.

**RD.B.4.6** intentionally left blank.

**RD.B.4.7** Intentionally left blank.

**R5** Intentionally left blank.

**R6** The **ISO** must maintain the set of **underfrequency load shedding** data necessary to model its **underfrequency load shedding** program for use in event analyses and assessments of the **underfrequency load shedding** program at least once each calendar year, with no more than 15 **months** between maintenance activities.

**R7** Intentionally left blank.

**R8** Each **legal owner** of a **transmission facility**, **legal owner** of an **electric distribution system** and **market participant** receiving service under Rate DTS of the **ISO tariff** must provide data to support maintenance of the **underfrequency load shedding** program, to the **ISO** according to the schedule the **ISO** specifies.

**R9** Each **legal owner** of a **transmission facility**, **legal owner** of an **electric distribution system** and **market participant** receiving service under Rate DTS of the **ISO tariff** must provide, as the **ISO** determines, automatic tripping of load in accordance with the **underfrequency load shedding** program design, and schedule for implementation, including any corrective action plan.

**R10** Each **legal owner** of a **transmission facility** must provide, as the **ISO** determines, automatic switching of its existing capacitor banks, transmission lines, and reactors to control over-voltage as a result of **underfrequency load shedding** if required by the **underfrequency load shedding** program and schedule for implementation, including any corrective action plan.

**R11** Intentionally left blank.

**RD.B.11** The **ISO** must, if a **bulk electric system** islanding event in Alberta results in system frequency excursions below the initializing set points of the **ISO**'s **underfrequency load shedding** program, participate in and document a coordinated event assessment with all affected planning coordinators within one year of event actuation to evaluate:

**RD.B.11.1** the performance of the **underfrequency load shedding** equipment; and

**RD.B.11.2** the effectiveness of the **underfrequency load shedding** program.

**R12** Intentionally left blank.

**RD.B.12** The **ISO** must, if an islanding event assessment (per RD.B.11) identifies deficiencies in the **underfrequency load shedding** program, participate in and document a coordinated **underfrequency load shedding** design assessment of the **underfrequency load shedding**

program with the other planning coordinators in the **WECC** regional area to consider the identified deficiencies within 2 years of event actuation.

**R13** Intentionally left blank.

**R14** Intentionally left blank.

**R15** Intentionally left blank.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MD.B.1 is the measure for requirement RD.B.1.

**MR1** Intentionally left blank.

**MD.B.1** Evidence of participating in a joint regional review as required in requirement RD.B.1 exists. Evidence may include reports, or other documentation of its criteria, developed as part of the joint regional review with other planning coordinators in the **WECC** regional entity area, to select portions of the **bulk electric system** that may form islands, including how system studies and historical events were considered to develop the criteria per requirement RD.B.1, meeting minutes showing attendance at the **WECC** UFLS Review Group or its successor, or other equivalent evidence.

**MR2** Intentionally left blank.

**MD.B.2** Evidence of identifying one or more islands from the regional review as required in requirement RD.B.2 exists. Evidence may include reports, memorandums, e-mails, or other documentation supporting its identification of an island, or other equivalent evidence.

**MR3** Intentionally left blank

**MD.B.3** Evidence of adopting an **underfrequency load shedding** program as required in requirement RD.B.3 exists. Evidence may include reports, memorandums, e-mails, program plans, or other documentation of its adoption of a **underfrequency load shedding** program, or other equivalent evidence.

**MR4** Intentionally left blank

**MD.B.4** Evidence of participating in a coordinated **underfrequency load shedding** design assessment as required in requirement RD.B.4 exists. Evidence may include dated documentation of the **ISO**'s participation in a coordinated **underfrequency load shedding** design assessment with the other planning coordinators in the **WECC** or other equivalent evidence.

**MR5** Intentionally left blank

**MR6** Evidence of maintaining **underfrequency load shedding** data as required in requirement R6 exists. Evidence may include **underfrequency load shedding** data, data requests, data input forms, other dated documentation or other equivalent evidence.

**MR7** Intentionally left blank.

**MR8** Evidence of providing data to the **ISO** as required in requirement R8 exists. Evidence may include responses to data requests, spreadsheets, letters or other dated documentation or other equivalent evidence.

**MR9** Evidence of providing automatic tripping of load as required in requirement R9 exists. Evidence may include:

- spreadsheets summarizing feeder load armed with **underfrequency load shedding** relays;
- the relay settings and implementation date;
- schedules for implementation of the **underfrequency load shedding** program or any required corrective action plan; or
- other equivalent evidence.

**MR10** Evidence of providing automatic switching of capacitor banks, transmission lines, and reactors as required in requirement R10 exists. Evidence may include:

- relay settings and, in some cases, the tripping logic and the implementation date;
- schedules for implementation of the **underfrequency load shedding** program or any required corrective action plan; or
- other equivalent evidence.

**MR11** Intentionally left blank.

**MD.B.11** Evidence of participating in and documenting a coordinated event assessment with all affected planning coordinators as required in requirement RD.B.11 exists. Evidence may include reports, data gathered from an historical event, other dated documentation, or other equivalent evidence.

**MR12** Intentionally left blank.

**MD.B.12** Evidence of participating in and documenting a coordinated **underfrequency load shedding** design assessment of the **underfrequency load shedding** program with the other planning coordinators as required in requirement RD.B.12 exists. Evidence may include reports, data gathered from an historical event, dated documentation, or other equivalent evidence.

**MR13** Intentionally left blank.

**MR14** Intentionally left blank.

**MR15** Intentionally left blank.

### Revision History

| Date | Description |
|---|---|
| 2022-01-01 | Initial release. |

## 1. Purpose

The purpose of this **reliability standard** is to establish an integrated and coordinated approach to the design, evaluation, and reliable operation of **under voltage load shed** programs.

## 2. Applicability

This **reliability standard** applies to:

(a) the **legal owner** of a **transmission facility** that has responsibility in an **under voltage load shed** program the **ISO** establishes;

(b) the **legal owner** of an **electric distribution system** that has responsibility in an **under voltage load shed** program the **ISO** establishes;

(c) a **market participant** receiving service under Rate DTS of the **ISO tariff** that has responsibility in an **under voltage load shed** program the **ISO** establishes; and

(d) the **ISO**.

## 3. Requirements

**R1** The **ISO** must, if it is developing an **under voltage load shed** program, evaluate its effectiveness and subsequently provide the **under voltage load shed** program's specifications and implementation schedule to the **under voltage load shed** entities responsible for implementing the **under voltage load shed** program. The evaluation must include studies and analyses that show that:

(a) the implementation of the **under voltage load shed** program resolves the identified under voltage issues that led to its development and design; and

(b) the **under voltage load shed** program is integrated with consideration given to the following at the discretion of the **ISO**:

coordination with **generating unit** and **aggregated generating facility** voltage ride-through capabilities and other protection and control systems, including transmission line protection, automatic reclosing, **remedial action schemes**, and other **under voltage load shed** programs or schemes.

**R2** Each **legal owner** of a **transmission facility**, **legal owner** of an **electric distribution system,** and **market participant** receiving service under Rate DTS of the **ISO tariff** must adhere to the **under voltage load shed** program specifications and implementation schedule the **ISO** determines and associated with any corrective action plans in accordance with requirement R5.

**R3** The **ISO** must perform a comprehensive assessment to evaluate the effectiveness of each of its **under voltage load shed** programs at least once every 60 **months**. Each assessment must include, studies and analyses that evaluate whether the **under voltage load shed** program:

(a) resolves the identified under voltage issues for which the **under voltage load shed** program is designed; and

(b) is integrated with consideration given to the following at the discretion of the **ISO**: coordination with **generating unit** and **aggregated generating facility** voltage ride-through capabilities and other protection and control systems, including transmission line protection, automatic reclosing, **remedial action schemes**, and other **under voltage load shed** programs or schemes.

**R4** The **ISO** must, within 12 **months** of an event that resulted in a voltage excursion for which its **under voltage load shed** programs were designed to operate, perform an assessment to evaluate:

(a) whether its **under voltage load shed** program resolved the under voltage issues associated with the event; and

(b) the performance (i.e., operation and non-operation) of the **under voltage load shed** program equipment.

**R5** The **ISO** must, when it identifies deficiencies during an assessment performed in either requirement R3 or R4, develop a corrective action plan to address the deficiencies and subsequently provide the corrective action plan, including an implementation schedule, to **under voltage load shed** entities within 3 **months** of completing the assessment in either requirement R3 or R4.

**R6** The **ISO** must, if it has an **under voltage load shed** program in its area, collect data necessary to model the **under voltage load shed** program in its area for use in event analyses and assessments of the **under voltage load shed** program at least once each calendar year.

**R7** Each **legal owner** of a **transmission facility, legal owner** of an **electric distribution system,** and **market participant** receiving service under Rate DTS of the **ISO tariff** must provide data to support maintenance of the **under voltage load shed** program, to the **ISO** according to the schedule the **ISO** specifies.

**R8** The **ISO** must, if it has an **under voltage load shed** program in its area, provide its **under voltage load shed** program data to:

(a)planning coordinators within its **Interconnection**;

(b)**transmission planners** within its **Interconnection**; and

(c)other entities with a **reliability** need,

within 30 **days** of a written request.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of evaluating **under voltage load shed** programs and providing its specifications and implementation schedule to the **under voltage load shed** entities as required in requirement R1 exists. Evidence may include date-stamped studies and analyses, reports, or other documentation detailing the effectiveness of the **under voltage load shed** program, and date-stamped communications showing that the **under voltage load shed** program specifications and implementation schedule were provided to **under voltage load shed** entities, or other equivalent evidence.

**MR2** Evidence of adhering to specifications, implementation of the **under voltage load shed** program and any corrective action plans as required in requirement R2 exists. Evidence may include date-stamped documentation on the completion of actions and may include identifying the equipment armed with **under voltage load shed** relays, the **under voltage load shed** relay settings, associated load summaries, work management program records, work orders, and maintenance records, or other equivalent evidence.

**MR3** Evidence of performing a comprehensive assessment to evaluate the effectiveness of each **under voltage load shed** program as required in requirement R3 exists. Evidence may include date-stamped reports or other documentation detailing the assessment of each **under voltage load shed** program, or other equivalent evidence.

**MR4** Evidence of performing an assessment to evaluate the **under voltage load shed** program as required in requirement R4 exists. Evidence may include date-stamped event data, event analysis reports, or other documentation detailing the assessment of the **under voltage load shed** program and performance of the associated equipment, or other equivalent evidence.

**MR5** Evidence of developing a corrective action plan and providing it to **under voltage load shed** entities as required in requirement R5 exists. Evidence may include:

- a date-stamped corrective action plan that addresses identified deficiencies and may also include date-stamped reports or other documentation supporting the corrective action plan;
- date-stamped communications showing that the corrective action plan and an associated implementation schedule were provided to **under voltage load shed** entities, or
- other equivalent evidence.

**MR6** Evidence of collecting data necessary to model each **under voltage load shed** program as required in requirement R6 exists. Evidence may include date-stamped spreadsheets, data reports, or other documentation demonstrating the **under voltage load shed** program data was updated, or other equivalent evidence.

**MR7** Evidence of providing data to the **ISO** in accordance with requirement R7 exists. Evidence may include date-stamped emails, letters, or other documentation demonstrating data was provided to the **ISO** as specified, or other equivalent evidence.

**MR8** Evidence of providing its **under voltage load shed** data as required in requirement R8 exists. Evidence may include date-stamped emails, letters, or other documentation demonstrating that the **under voltage load shed** program data was provided within 30 **days** of receipt of a written request, or other equivalent evidence.

### Revision History

| Date | Description |
| --- | --- |
| 2022-01-01 | Initial release. |

# Alberta Reliability Standard
# Disturbance Monitoring Equipment Installation and Data Reporting
# PRC-018-AB-1

## 1. Purpose

The purpose of this **reliability standard** is to ensure that **disturbance monitoring equipment** is installed and that **disturbance** data is reported in accordance with regional requirements to facilitate analyses of events.

## 2. Applicability

This **reliability standard** applies to:

(a) the **legal owner** of a **transmission facility** that owns **disturbance monitoring equipment** as identified in the list of *Disturbance Monitoring Equipment Locations* as required in requirement R1, as published by the **ISO** on the AESO website and as amended from time to time by the **ISO** on notice to **market participants**;

(b) the **legal owner** of a **generating unit** that owns **disturbance monitoring equipment** as identified in the list of *Disturbance Monitoring Equipment Locations* as required in requirement R1, as published by the **ISO** on the AESO website and as amended from time to time by the **ISO** on notice to **market participants**;

(c) the **legal owner** of an **aggregated generating facility** that owns **disturbance monitoring equipment** as identified in the list of *Disturbance Monitoring Equipment Locations* as required in requirement R1, as published by the **ISO** on the AESO website and as amended from time to time by the **ISO** on notice to **market participants**; and

(d) the **ISO**.

## 3. Requirements

**R1** The **ISO** must maintain and publish a list of all **disturbance monitoring equipment** that this **reliability standard** applies to which includes all **disturbance monitoring equipment** the **WECC** requires to be installed in Alberta.

**R2** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** that the **ISO** directs to install **disturbance monitoring equipment** must install such **disturbance monitoring equipment** with internal clocks synchronized to within two (2) milliseconds or less of the Universal Coordinated Time scale.

**R3** The **ISO** must have recorded **disturbance** data available for retrieval for at least ten (10) **days**.

**R4** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** must install **disturbance monitoring equipment** as directed by the **ISO**.

**R5** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** must report, within thirty (30) **days** of the **ISO**'s request, the following information on the **disturbance monitoring equipment**:

**R5.1** type of **disturbance monitoring equipment**;

**R5.2** make and model of **disturbance monitoring equipment**;

**R5.3** installation location;

**R5.4** operational status;

**R5.5** date last tested;

**R5.6** monitored **system elements** which may include transmission circuit and bus section;

**R5.7** monitored devices which may include circuit breaker, disconnect status and alarms; and

**R5.8** monitored electrical quantities, which may include voltage and current.

**R6** The **ISO** must provide the information received from the **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** in requirement R5 to the **WECC** within forty-five (45) **days** of the **WECC**'s written request.

**R7** If the **ISO** is unable to directly access **disturbance** data, then each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** must provide all available **disturbance** data recorded by **disturbance monitoring equipment** to the **ISO** within forty-five (45) **days** of the **ISO**'s written request.

**R8** The **ISO** must provide all available **disturbance** data recorded by the **disturbance monitoring equipment** of a **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** to the **WECC** within sixty (60) **days** of the **WECC**'s written request.

**R9** The **ISO** must archive all data recorded by **disturbance monitoring equipment** for all **WECC** or **ISO** identified events for at least three (3) years.

**R10** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** that the **ISO** directs to have **disturbance monitoring equipment** must develop, implement and maintain a maintenance and testing program for **disturbance monitoring equipment** that includes:

**R10.1** maintenance and testing intervals and their basis; and

**R10.2** a summary of maintenance and testing procedures.

## 4 Measures

The following measures correspond to the requirements identified in Section 4 of this **reliability standard**. For example, MR1 is the measure for R1.

**MR1** Evidence of maintaining and publishing a list as required in requirement R1 exists. Evidence may include a list published on the AESO's website that identifies the effective date and revision history.

**MR2** Evidence of having internal clocks in the installed **disturbance monitoring equipment** synchronized as required in requirement R2 exists. Evidence may include: the manufacturer's equipment specification, commissioning documents or GPS clock records that demonstrate each installed **disturbance monitoring equipment**'s internal clock is synchronized in accordance with R2.

**MR3** Evidence of having recorded **disturbance** data available for retrieval as required in requirement R3 exists. Evidence may include **disturbance** records.

**MR4** Evidence of installing **disturbance monitoring equipment** as required in requirement R4 exists. Evidence may include documentation of the installation of the **disturbance monitoring equipment**.

**MR5** Evidence of reporting information as required in requirement R5 exists. Evidence may include email or mail to the appropriate **ISO** recipient that identifies information submitted.

**MR6** Evidence of providing data as required in requirement R6 exists. Evidence may include email or mail to the appropriate **WECC** recipient that identifies data submitted.

**MR7** Evidence of providing data as required in requirement R7 exists. Evidence may include email or mail to the appropriate **ISO** recipient that identifies data submitted.

**MR8** Evidence of providing data as required in requirement R8 exists. Evidence may include email or mail to appropriate **WECC** recipient that identifies data submitted.

**MR9** Evidence of archiving data as required in requirement R9 exists. Evidence may include dated archived data files.

**MR10** Evidence of developing, implementing and maintaining a maintenance and testing program as required in requirement R10 exists. Evidence may include a documented maintenance and testing program, maintenance and testing records showing the test date, type of test, what was tested and test results.

**MR10.1** Evidence of developing, implementing and maintaining a maintenance and testing program as required in requirement R10.1 exists. Evidence may include a documented maintenance and testing program that includes the provision as required in requirement R10.1.

**MR10.2** Evidence of developing, implementing and maintaining a maintenance and testing program as required in requirement R10.2 exists. Evidence may include a documented maintenance and testing program that includes the provision as required in requirement R10.2.

## 5. Appendices

No appendices have been defined for this **reliability standard**.

## Revision History

| Effective | Description |
|---|---|
| 2013-01-01 | Initial Release |
| 2016-08-30 | Inclusion of the defined term **system element**. |

# Alberta Reliability Standard
# Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection
# PRC-019-AB-2

## 1. Purpose

The purpose of this **reliability standard** is to verify coordination of **generating unit** or synchronous condenser voltage regulating controls, limit functions, equipment capabilities, and protection system settings.

## 2. Applicability

This **reliability standard** applies to:

(a) the **legal owner** of a **transmission facility** that owns a synchronous condenser greater than 20 MVA (gross nameplate rating) directly connected to the **transmission system**;

(b) the **legal owner** of a **generating unit** whose **generating unit** has a **maximum authorized real power** rating greater than 18 MW that is:

(i) directly connected to the **transmission system**;

(ii) directly connected to **transmission facilities** within the City of Medicine Hat; or

(iii) part of an industrial complex that is directly connected to the **transmission system**;

(c) the **legal owner** of a **generating unit** whose **generating unit** is within a power plant that has a combined **maximum authorized real power** rating greater than 67.5 MW and that:

(i) is not part of an **aggregated generating facility**; and

(ii) is directly connected to the **transmission system** or to **transmission facilities** within the City of Medicine Hat;

(d) the **legal owner** of an **aggregated generating facility** that has a **maximum authorized real power** rating greater than 67.5 MW, where voltage regulating control for the facility is performed solely at the individual **generating units** of the **aggregated generating facility**, and the **aggregated generating facility** is:

(i) directly connected to the **transmission system**;

(ii) directly connected to **transmission facilities** within the City of Medicine Hat; or

(iii) part of an industrial complex that is directly connected to the **transmission system**;

(e) the **legal owner** of a **generating unit** whose **generating unit** is a **blackstart resource**; and

(f) the **legal owner** of a **generating unit**, the **legal owner** of a **aggregated generating facility** and the **legal owner** of a **transmission facility** whose resource is material to this **reliability standard** and to the **reliability** of either the **interconnected electric system** or the City of Medicine Hat electric system as the **ISO** determines and includes on a list published on the AESO website, which the **ISO** may amend from time to time in accordance with the process set out in Appendix 1.

## 3. Requirements

**R1** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** must, by the effective date of this **reliability standard** and at a maximum of every 5 calendar years, coordinate the voltage regulating system controls, including in-service limiters and protection functions, with the applicable equipment capabilities and settings of the applicable **protection system** devices and functions, assuming normal automatic voltage regulator control loop and steady-state system operating conditions, by verifying the following coordination items for each applicable facility:

(a) the in-service limiters are set to operate before the **protection system** of the applicable facility in order to avoid disconnecting the **generating unit** or synchronous condenser unnecessarily; and

(b) the applicable in-service **protection system** devices are set to operate to isolate or de-energize equipment in order to limit the extent of damage when operating conditions exceed equipment capabilities or stability limits.

**R2** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit** and **legal owner** of an **aggregated generating facility** must:

(a) by the later of either the effective date of this **reliability standard** or within 90 **days** following the identification of unplanned systems, equipment or setting changes that will affect the coordination described in requirement R1; or

(b) prior to electrically connecting to the **transmission system**:

(i) a **generating unit**;

(ii) a synchronous condenser; or

(iii) a **generating unit** that is part of an **aggregated generating facility**;

any of which are impacted by planned system, equipment or setting changes that will affect the coordination as described in requirement R1,

perform the coordination described in requirement R1.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of coordinating the voltage regulating system controls by verifying the coordination items as required in requirement R1 exists. Evidence may include dated documentation that demonstrates the coordination was performed, or other equivalent evidence.

**MR2** Evidence of performing the coordination as described in requirement R1 in accordance with the requirements in requirement R2 exists. Evidence may include dated documentation that demonstrates the specified interval in requirement R2(a) has been met or an operator log, or other equivalent evidence.

## 5. Appendices

Appendix 1 – *Amending Process for List of Generating Units, Synchronous Condensers and Aggregated Generating Facilities*

### Revision History

| Date | Description |
|---|---|
| 2022-01-01 | Initial release. |

## Appendix 1
## Amending Process for List of Generating Units, Synchronous Condensers and Aggregated Generating Facilities

In order to amend the list referenced in subsections (f) of section 2, Applicability, the **ISO** must:

(a) upon determining that a **generating unit**, synchronous condenser, or **aggregated generating facility** is to be added, notify the **legal owner** in writing and determine an effective date, which must be no less than 4 full calendar quarters after the date of notice, for the **legal owner** to meet the applicable requirements;

(b) upon determining that a **generating unit**, synchronous condenser, or **aggregated generating facility** is to be deleted, notify the **legal owner** in writing and determine an effective date for the **legal owner** to no longer be required to meet the applicable requirements; and

(c) publish the amended list with effective dates on the AESO website.

## 1. Purpose

The purpose of this **reliability standard** is to ensure the protection relay settings do not limit transmission loadability, do not interfere with an **operator**'s ability to take remedial action to protect the **reliability** of the **transmission system**, and are set to reliably detect all **fault** conditions and protect the electrical network from these **faults.**

## 2. Applicability

This **reliability standard** applies to:

(a) the **legal owner** of a **transmission facility** with load-responsive phase **protection systems**, as described in Appendix 1, applied at the terminals of any one or more of the following facilities:

(i) transmission lines operated at 200 kV and above, except **system elements** that are part of a radial circuit, including transmission step-up transformers and lines, that are only used to export energy directly from a **generating unit** or **aggregated generating facility** to a single **system element** on the networked **transmission system**;

(ii) transmission lines operated below 200 kV which the **ISO** identifies, as required in requirement R6.2, as essential to the **reliability** of the **bulk electric system**, except transmission lines that are part of a radial circuit that are only used to export energy directly from a **generating unit** or **aggregated generating facility** to a single **system element** on the networked **transmission system**;

(iii) transformers with low voltage terminals connected at 200 kV and above; or

(iv) transformers with low voltage terminals connected below 200 kV, which the **ISO** identifies in accordance with requirement R6.2, except transformers that are part of a radial circuit that are only used to export energy directly from a **generating unit** or **aggregated generating facility** to a single **system element** on the networked **transmission system**;

(b) the **legal owner** of a **generating unit**, that also owns the associated switch yard, with load-responsive phase **protection systems**, as described in Appendix 1, applied at the terminals of any one or more of the following facilities:

(i) transmission lines operated at 200 kV and above, except transmission lines that are part of a radial circuit that are only used to export energy directly from a **generating unit** to a single **system element** on the networked **transmission system**;

(ii) transmission lines operated below 200 kV which the **ISO** identifies, as required in requirement R6.2, as essential to the **reliability** of the **bulk electric system**, except transmission lines that are part of a radial circuit that are only used to export energy directly from a **generating unit** to a single **system element** on the networked **transmission system**;

(iii) transformers with low voltage terminals connected at 200 kV and above; or

(iv) transformers with low voltage terminals connected below 200 kV which the **ISO** identifies in accordance with requirement R6.2, except transformers that are part of a radial circuit that are only used to export energy directly from a **generating unit** to a single **system element** on the networked **transmission system**;

(c) the **legal owner** of an **aggregated generating facility**, that also owns the associated switch yard, with load-responsive phase **protection systems**, as described in Appendix 1, applied at the terminals of any one or more of the following facilities:

(i) transmission lines operated at 200 kV and above, except transmission lines that are part of a radial circuit that are only used to export energy directly from an **aggregated generating facility** to a single **system element** on the networked **transmission system**;

(ii) transmission lines operated below 200 kV which the **ISO** identifies, as required in requirement R6.2, as essential to the **reliability** of the **bulk electric system**, except transmission lines that are part of a radial circuit that are only used to export energy directly from an **aggregated generating facility** to a single **system element** on the networked **transmission system**; or

(iii) transformers with low voltage terminals connected below 200 kV which the **ISO** identifies in accordance with requirement R6.2, except transformers that are part of a radial circuit that are only used to export energy directly from an **aggregated generating facility** to a single **system element** on the networked **transmission system**; and

(d) the **ISO**.

## 3. Requirements

**R1** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** must:

(a) use one of the criteria set out in requirements R1.1 through R1.14, inclusive, for each specific circuit terminal, being either a transmission line or a transformer, to prevent its phase protection relay settings from limiting **transmission system** loadability; and

(b) for R1.1 through R1.14 evaluate the phase protection relay's loadability at 0.85 per unit voltage and a **power factor** angle of 30°.

A load encroachment function within protection relays may be used to meet (a) and (b).

**R1.1** Set transmission line protection relays so they do not operate at or below 150% of the highest seasonal facility rating of a circuit for the available defined loading duration nearest to 4 hours, expressed in amperes;

**R1.2** Set transmission line protection relays so they do not operate at or below 115% of the 10-minute emergency facility rating of a circuit, expressed in amperes;

**R1.3** Set transmission line protection relays so they do not operate at or below 115% of the maximum theoretical power transfer capability, using a 90° angle between the sending-end and receiving-end voltages and either reactance or complex impedance of the circuit, expressed in amperes, using one of the following to perform the power transfer calculation:

**R1.3.1** an infinite source, i.e. zero source impedance, with a 1.00 per unit bus voltage at each end of the transmission line; or

**R1.3.2** an impedance at each end of the transmission line, which reflects the actual system source impedance with a 1.05 per unit voltage behind each source impedance;

**R1.4** Set transmission line protection relays on series compensated transmission lines so they do not operate at or below the maximum power transfer capability of the transmission line, determined as the greater of:

(a) 115% of the highest emergency rating of the series capacitor, or

(b) 115% of the maximum power transfer capability of the circuit, expressed in amperes, calculated in accordance with requirement R1.3, using the full transmission line inductive reactance;

**R1.5** Set transmission line protection relays on weak source systems so they do not operate at or below 170% of the maximum end-of-line three-phase **fault** magnitude, expressed in amperes;

**R1.6** Set transmission line relays applied on transmission lines connected to a **generating unit** or **aggregated generating facility** remote to load so they do not operate at or below 230% of the total nameplate capability of all the **generating unit**s at the facility;

**R1.7** Set transmission line protection relays applied at the load center terminal, remote from a **generating unit** or **aggregated generating facility**, so they do not operate at or below 115% of the maximum current flow from the load to the generation source under any system configuration;

**R1.8** Set transmission line protection relays applied on the system-end of transmission lines that serve load remote to the system so they do not operate at or below 115% of the maximum current flow from the system to the load under any system configuration;

**R1.9** Set transmission line protection relays applied on the load-end of transmission lines that serve load remote to the system so they do not operate at or below 115% of the maximum current flow from the load to the system under any system configuration;

**R1.10** Set transformer **fault** protection relays and transmission line protection relays on transmission lines terminated only with a transformer so that they do not operate at or below the greater of:

(a) 150% of the applicable maximum transformer nameplate rating, expressed in amperes, including the forced cooled ratings corresponding to all installed supplemental cooling equipment; or

(b) 115% of the highest established emergency transformer rating;

**R1.11** Set load responsive transformer **fault** protection relays, if used, such that the protection settings do not expose the transformer to a **fault** level and duration that exceeds the transformer's mechanical withstand capability;

**R1.12** For transformer overload protection relays that do not comply with requirement R1.10:

(a) set the protection relays to allow the transformer to be operated at an overload level of at least 150% of the maximum applicable nameplate rating, or 115% of the highest emergency transformer rating, whichever is greater;

(b) the protection relay must allow overload in requirement R1.12(a) for at least 30 minutes to allow the **ISO** to take controlled action to relieve the overload;

(c) install supervision for the protection relays using either a top oil or simulated winding hot spot temperature element; and

(d) the protection relay setting should be no less than 100°C for the top oil or 140°C for the winding hot spot temperature;

**R1.13** When the desired transmission line capability is limited by the requirement to adequately protect the transmission line and a load encroachment function is not available within the protection relay, set the transmission line distance protection relays to a maximum of 125% of the apparent impedance, at the impedance angle of the transmission line, subject to the following constraints:

**R1.13.1** set the maximum torque angle to 90° or the highest setting supported by the manufacturer;

**R1.13.2** evaluate the protection relay loadability in amperes at the protection relay trip point 0.85 per unit voltage and a **power factor** angle of 30°; and

**R1.13.3** include a protection relay setting component of 87% of the current calculated in requirement R1.13.2 in the facility rating determination for the circuit; and

**R1.14** Where other extraordinary situations present practical limitations on circuit capability, as the **ISO** approves in writing, set the phase protection relays and associated current transformer ratios so they do not operate at or below 115% of such limitations.

**R2** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** must set its out-of-step blocking elements to allow tripping of phase protection relays for **faults** that occur during the loading conditions used to verify transmission line protection relay loadability per requirement R1.

**R3** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, or **legal owner** of an **aggregated generating facility** that uses a circuit capability with the practical limitations described in requirements R1.7, R1.8, R1.9, R1.13, or R1.14 must use the calculated circuit capability as the facility rating of the circuit and must obtain the **ISO**'s written agreement to use the calculated circuit capability.

**R4** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, or **legal owner** of an **aggregated generating facility** that uses requirement R1.2 as the basis for verifying transmission line protection relay loadability must provide the **ISO** with an updated list of circuits associated with those transmission line protection relays at least once each calendar year, with no more than 15 **months** between reports.

**R5** Each **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, or **legal owner** of an **aggregated generating facility** that uses requirement R1.13 as the basis for verifying transmission line protection relay loadability must provide the **ISO** with an updated list of circuits associated with those transmission line protection relays at least once each calendar year, with no more than 15 **months** between reports.

**R6** The **ISO** must conduct an assessment at least once each calendar year, with no more than 15 months between assessments, by applying the criteria in Appendix 2, to identify the circuits in its planning area for which the **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** must comply with requirements R1 through R5. The **ISO** must:

**R6.1** maintain a list of circuits per the application of Appendix 2, including an effective date that is no earlier than 24 **months** from identification of the circuits; and

**R6.2** provide the list of circuits to the **legal owner** of a **transmission facility**, **legal owner** of a **generating unit**, and **legal owner** of an **aggregated generating facility** within its planning area within 30 **days** of the establishment of the initial list and within 30 **days** of any changes to that list.

## 2. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for R1.

**MR1** Evidence of using one of the criteria set out in requirements R1.1 through R1.14, evaluating the phase protection relay's loadability, and implement transmission line protection relays settings, all as required in requirement R1 exists. Evidence may include:

(a) spreadsheets or summaries of calculations to show that each of its transmission line protection relays is set in accordance with one of the criteria set out in requirements R1.1 through R1.14;

(b) coordination curves or summaries of calculations that show that protection relays set per criterion set out in requirement R1.11 do not expose the transformer to **fault** levels and durations beyond those indicated in the **reliability standard**;

(c) evidence to demonstrate settings implementation,or

(d) other equivalent evidence.

**MR2** Evidence of setting its out-of-step blocking elements as required in requirement R2 exists. Evidence may include spreadsheets or summaries of calculations, or other equivalent evidence.

**MR3** Evidence of using, and obtaining the **ISO**'s written agreement to use, the calculated circuit capability as required in requirement R3 exists. Evidence may include:

(a) facility rating spreadsheets or facility rating database to show that the calculated circuit capability was used as the facility rating of the circuit;

(b) dated correspondence to show that the **ISO** agreed to the calculated circuit capability; or

(c) other equivalent evidence.

**MR4** Evidence of providing the **ISO** with an updated list of circuits as required in requirement R4 exists. Evidence may include dated correspondence to the appropriate **ISO** recipient with the updated list which may either be a full list, a list of incremental changes to the previous list, a statement that there are no changes to the previous list, or other equivalent evidence.

**MR5** Evidence of providing the **ISO** with an updated list of circuits as required in requirement R5 exists. Evidence may include dated correspondence to the appropriate **ISO** recipient with the updated list which may either be a full list, a list of incremental changes to the previous list, a statement that there are no changes to the previous list, or other equivalent evidence.

**MR6** Evidence of conducting an assessment as required in requirement R6 exists. Evidence may include power flow results, calculation summaries or study reports that the **ISO** used the criteria established within Appendix 2 to identify the circuits in its planning area, or other equivalent evidence.

**MR6.1** Evidence of maintaining the list of circuits as required in requirement R6.1 exists. Evidence may include a documented list of circuits with the effective date and the revision history captured, or other equivalent evidence.

**MR6.2** Evidence of providing the list of circuits as required in requirement R6.2 exists. Evidence may include dated correspondence to the applicable entities, or other equivalent evidence.

## 3. Appendices

Appendix 1 – *Associated Switch Yard with Load-Responsive Phase Protection Systems*

Appendix 2 – *Criteria for Identifying Circuits and Establishing a List*

Appendix 3 – *Retirement of Requirement R1.6*

## Revision History

| Effective | Description |
|---|---|
| 2020-07-01 | Initial Release |

## Appendix 1

### Associated Switch Yard with Load-Responsive Phase Protection Systems

1. This **reliability standard** includes any protection functions which could trip with or without time delay, on load current, including:
   (a) phase distance;
   (b) out-of-step tripping;
   (c) switch-on-to-**fault**;
   (d) overcurrent relays;
   (e) communications aided **protection system** including:
      (i) permissive overreach transfer trip;
      (ii) permissive under-reach transfer trip;
      (iii) directional comparison blocking;
      (iv) directional comparison unblocking; and
   (f) phase overcurrent supervisory elements (i.e. phase **fault** detectors) associated with current-based, communication-assisted schemes (i.e. pilot wire, phase comparison, and line current differential) where the scheme is capable of tripping for loss of communications.
2. The following **protection systems** are excluded from the requirements of this **reliability standard**:
   (a) relay elements that are only enabled when other relays or associated systems fail, including:
      (i) overcurrent elements that are only enabled during loss of potential conditions; and
      (ii) relay elements that are only enabled during a loss of communications except as noted in subsection 1(f) above;
   (b) **protection systems** intended for the detection of ground **fault** conditions;
   (c) **protection systems** intended for protection during stable power swings;
   (d) Not used;
   (e) relay elements used only for **remedial action scheme** purposes;
   (f) **protection systems** that are designed only to respond in time periods which allow 15 minutes or greater to respond to overload conditions;
   (g) thermal emulation relays which are used in conjunction with dynamic facility ratings; and
   (h) relay elements associated with direct current lines.

## Appendix 2

## Criteria for Identifying Circuits and Establishing a List

The **ISO** must evaluate the following circuits:

(a) transmission lines operated at 100 kV to 200 kV and transformers with low voltage terminals connected at 100 kV to 200 kV; and

(b) transmission lines operated below 100 kV and transformers with low voltage terminals connected below 100 kV that are essential to the **reliability** of the **bulk electric system**.

### Criteria

If any of the following criteria apply to a circuit, the **ISO** must identify the circuit as required in requirement R6.

1 A major transfer path within the Western **Interconnection** as defined by the Regional Entity.

2 The circuit is a monitored facility of an **interconnection reliability operating limit**, where the **interconnection reliability operating limit** was determined in the planning horizon pursuant to **reliability standard** FAC-010-AB.

3 The circuit is identified through the following sequence of power flow analyses:

(a) simulate double **contingency** combinations selected by engineering judgment, without manual system adjustments in between the 2 **contingencies** (reflects a situation where real time operating personnel may not have time between the 2 **contingencies** to make appropriate system adjustments), performed by the **ISO** for the one-to-five-year planning horizon;

(b) for circuits operated between 100 kV and 200 kV, evaluate the post-**contingency** loading, in consultation with the **legal owner**, against a threshold based on the facility rating assigned for that circuit and used in the power flow case by the **ISO**;

(c) when more than one facility rating for that circuit is available in the power flow case, the **ISO** must base the threshold for selection on the facility rating for the loading duration nearest 4 hours;

(d) the threshold for selection of the circuit will vary based on the loading duration assumed in the development of the facility rating:

(i) if the facility rating is based on a loading duration of up to and including 4 hours, the circuit must comply with this **reliability standard** if the loading exceeds 115% of the facility rating;

(ii) if the facility rating is based on a loading duration greater than 4 and up to and including 8 hours, the circuit must comply with this **reliability standard** if the loading exceeds 120% of the facility rating; or

(iii) if the facility rating is based on a loading duration of greater than 8 hours, the circuit must comply with this **reliability standard** if the loading exceeds 130% of the facility rating; and

(e) radially operated circuits serving only load are excluded.

4 The **ISO** must select the circuit based on technical studies or assessments, other than those specified in criteria 1 through 3, in consultation with the **legal owner**.

5 The **ISO** and the **legal owner** must mutually agree upon the circuit for inclusion.

## Appendix 3

### Appendix 3 – Retirement of Requirement R1.6

Requirement R1.6 will be retired as of midnight the **day** before the effective date of **reliability standard** PRC-025-AB-2, *Generator Load Reliability*.

# Alberta Reliability Standard
# System Performance Under Normal Conditions
# TPL-001-AB-0

## 1. Purpose

The purpose of this **reliability standard** is to ensure that a reliable transmission system is planned that meets specified performance requirements, with sufficient lead time. The transmission system must continue to be modified or upgraded as required to meet present and future system specified performance requirements as identified by periodically performed system simulations and associated planning assessments.

## 2. Applicability

This **reliability standard** applies to:

(a) **ISO**

## 3. Definitions

Bold terms used in this **reliability standard** have the meanings as set out in the *Consolidated Authoritative Document Glossary* and Part 1 of the ISO Rules.

## 4. Requirements

**R1** The **ISO** must demonstrate through a planning assessment that a transmission system is planned such that, with all **transmission facilities** in service and with pre-**contingency** operating procedures in effect, the transmission system can be operated to accommodate forecasted customer **demands**, supply and forecasted **firm** (non- recallable reserved) transmission services at all **demand** levels over the range of forecast system **demands**, under the conditions defined in Category A of Appendix 1.

The **ISO** planning assessment must:

**R1.1** Be carried out annually.

**R1.2** Be conducted for years one through five and years six through ten planning horizons.

**R1.3** Be supported by a study and/or system simulation testing, conducted within the last five years, that addresses each of the requirements in requirement R1.3.1 to R1.3.9, showing system performance for the conditions defined in Category A of Appendix 1.

**R1.3.1** Cover critical system conditions and study years as determined necessary by the **ISO**.

**R1.3.2** Be conducted annually unless the **ISO** determines that changes to system conditions do not warrant such analyses.

**R1.3.3** Be conducted beyond the five year planning horizon only as needed to address identified marginal conditions that may have longer lead time solutions.

**R1.3.4** Have pre-**contingency** operating procedures established and in place.

**R1.3.5** Have all projected firm transfers modeled, if any.

**R1.3.6** Be performed for selected **demand** levels over the range of forecast system **demands** as considered necessary by the **ISO**.

**R1.3.7** Demonstrate that system performance meets the conditions defined in Category A of Appendix 1.

**R1.3.8** Include existing and planned **facilities** as considered necessary by the **ISO**.

**R1.3.9** Include **reactive power** resources to ensure that adequate reactive resources are available to meet system performance.

**R1.4** Address any planned upgrades needed to meet the performance requirements for the conditions defined in Category A of Appendix 1.

**R2** When system simulations indicate an inability of the systems to respond as set out in R1.3.7 in this **reliability standard**, the **ISO** must:

**R2.1** Develop corrective plans to achieve the required system performance as described above throughout the planning horizon.

**R2.1.1** Including a schedule for implementation.

**R2.1.2** Including a discussion of expected required in-service dates of **facilities**.

**R2.1.3** Consider lead times necessary to implement corrective plans**.**

**R2.2** Review in subsequent annual assessments, where sufficient lead time exists, the continuing need for identified system **facilities**. Detailed implementation plans are not needed.

**R3** The **ISO** must provide the planning assessment to **WECC** on an annual basis.

## 5. Processes and Procedures

No procedures have been defined for this **reliability standard**.

## 6. Measures

The following measures correspond to the requirements identified in Section 4 of this **reliability standard**. For example, MR1 is the measure for R1.

**MR1** The planning assessment will be valid and meet requirement in R1 through the following measures:

(a) The scope of the planning assessment identifies where area studies have been conducted in the past year. It also identifies area studies that have been conducted in previous years and are still valid. Where area studies have not been conducted, a plan and schedule to conduct one is included in the planning assessment.

(b) The planning assessment includes time horizons as specified in R1.2.

(c) The planning assessment has been prepared within the last year.

(d) A certification that the planning assessment complies with each of the R1 technical requirements is provided and states that the planning assessment meets all requirements, identifies requirements not met, and states reasons where the requirement was not met.

(e) A summary list of supporting area studies and needs identification documents is provided. The summary list includes the title and date of the study. The area studies and needs identification documents are provided if requested.

**MR2** The area studies and needs identification documents contain recommendations and projects for corrective plans where an inability of the systems to respond to requirements specified in R1 has been identified. The area studies and needs identification documents are provided on request. The area studies and needs identification documents contain the technical components as specified in R2 and its subsections.

**MR3** A written or email confirmation from **WECC** that it has received the planning assessment from the **ISO**. The confirmation includes the date of when the planning assessment was received and source identification information.

## 7. Appendices

**Appendix 1 - Transmission System Standards – Normal and Emergency Conditions** (see below)

## 8. Guidelines

No guidelines have been defined for this **reliability standard**.

## Revision History

| Date | Description |
|---|---|
| 2010-09-24 | New Issue |
| 2016-08-30 | Inclusion of the defined term **system element**. |

**Appendix 1 - Transmission System Standards – Normal and Emergency Conditions**

| Category | Contingencies | System Limits or Impacts | | |
|---|---|---|---|---|
| | Initiating Event(s) and Contingency **System Element(s)** | System Stable and Both Thermal and Voltage Limits Within Applicable **Rating**[a] | Loss of **Demand** or Curtailed Firm Transmission Service Transfers | **Cascading** |
| **A**<br>No **contingencies** | All **facilities** in service | Yes | No | No |
| **B**<br>Event resulting in the loss of a single **system element** | Single Line Ground (SLG) or 3-Phase (3Ø) fault, with **normal clearing**: | Yes | No[b] | No |
| | 1. Generator | Yes | No[b] | No |
| | 2. Transmission circuit | Yes | No[b] | No |
| | 3. Transformer | Yes | No[b] | No |
| **C**<br>Event(s) resulting in the loss of two or more (multiple) **system elements** | SLG fault, with **normal clearing**[e]: | | | |
| | 1. Bus section | Yes | Planned/ Controlled[c] | No |
| | 2. Breaker (failure or internal fault) | Yes | Planned/ Controlled[c] | No |
| | SLG or 3Ø fault, with **normal clearing**[e], manual system adjustments, followed by another SLG or 3Ø fault, with **normal clearing**[e]<br>3. Category B (B1, B2, B3, or B4) **contingency**, manual system adjustments, followed by another Category B (B1, B2, B3, or B4) **contingency** | Yes | Planned/ Controlled[c] | No |
| | Bipolar block, with **normal clearing**[e]: | | | |
| | 4. Bipolar (dc) line fault (non 3Ø), with **normal clearing**[e]: | Yes | Planned/ Controlled[c] | No |
| | 5. Any two circuits of a multiple circuit towerline[f] | Yes | Planned/ Controlled[c] | No |
| | SLG fault, with delayed clearing[e] (stuck breaker or **protection system** failure) | | | |

| | | | | |
|---|---|---|---|---|
| | 6. Generator | Yes | Planned/ Controlled[c] | No |
| | 7. Transformer | Yes | Planned/ Controlled[c] | No |
| | 8. Transmission circuit | Yes | Planned/ Controlled[c] | No |
| | 9. Bus section | Yes | Planned/ Controlled[c] | No |
| **D** [d]<br><br>Extreme event resulting in two or more (multiple) **system elements** removed or **cascading** out of service | 3Ø fault, with delayed clearing[e] (stuck breaker or **protection system** failure):<br>1. Generator 2. Transmission circuit<br>3. Transformer 4. Bus section<br><br>3Ø fault, with **normal clearing**[e]:<br>5. Breaker (failure or internal fault)<br>6. Loss of towerline with three or more circuits<br>7. All transmission lines on a common right-of -way<br>8. Loss of a substation (one voltage level plus transformers)<br>9. Loss of a switching station (one voltage level plus transformers)<br>10. Loss of all generating units at a station<br>11. Loss of a large **load** or major **load** center<br>12. Failure of a fully redundant **special protection system** (or **remedial action scheme**) to operate when required<br>13. Operation, partial operation, or **misoperation** of a fully redundant **special protection system** (or **remedial action scheme**) in response to an event or abnormal system<br>14. Impact of severe power swings or oscillations from disturbances in another Regional Reliability Organization | Evaluate for risks and consequences<br>• May involve substantial loss of customer demand and generation in a widespread area or areas<br>• Portions or all of the **interconnected** systems may or may not achieve a new, stable operating point<br>• Evaluation of these events may require joint studies with neighboring systems | | |

a) Applicable **rating** refers to the applicable normal and emergency **facility** thermal and voltage **rating** as applied by the **facility** owner or system voltage limit as determined and consistently applied by the ISO. Applicable **ratings** may include emergency **ratings** applicable for short durations as required to permit operating steps necessary to maintain system control. All **ratings** must be established by the applicable entity consistent with applicable **ISO** rules addressing **facility ratings**.

b) Planned or controlled interruption of electric supply to radial customers or some local network customers, connected to or supplied by the faulted **system element** or by the affected area, may occur in certain areas without impacting the overall **reliability** of the **interconnected** transmission systems. To prepare for the next **contingency**, system adjustments are permitted, including curtailments of contracted firm (non-recallable reserved) transmission service electric power transfers.

c) Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (**load** shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) transmission service electric power transfers may be necessary to maintain the overall **reliability** of the **interconnected** transmission systems.

d) A number of extreme **contingencies** that are listed under Category D and judged to be critical by the transmission planning entity(ies) will be selected for evaluation. It is not expected that all possible **facility outages** under each listed **contingency** of Category D will be evaluated.

e) **Normal clearing** is when the **protection system** operates as designed and the fault is cleared in the time normally expected with proper functioning of the installed **protection systems**. Delayed clearing of a fault is due to failure of any **protection system** component such as a relay, circuit breaker, or current transformer, and not because of an intentional design delay.

f) System assessments may exclude these events where multiple circuit towers are used over short distances (i.e., station entrance, river crossings) in accordance with exemption criteria.

# Alberta Reliability Standard
# System Performance Following Loss of a Single BES Element
# TPL-002-AB1-0

## 1. Purpose

The purpose of this **reliability standard** is to ensure that a reliable transmission system is planned that meets specified performance requirements with sufficient lead time. The transmission system must continue to be modified or upgraded as required to meet present and future system specified performance requirements as identified by periodically performed system simulations and associated planning assessments.

## 2. Applicability

This **reliability standard** applies to:

(a) **ISO**

## 3. Definitions

Bold terms used in this **reliability standard** have the meanings as set out in the *Consolidated Authoritative Document Glossary* and Part 1 of the ISO Rules.

## 4. Requirements

**R1** The **ISO** must demonstrate for **transmission facilities** rated 69 kV and above, through a planning assessment, that a transmission system is planned such that the transmission system can be operated to accommodate forecasted customer **demands** and forecasted firm (non-recallable reserved) transmission services, at all **demand** levels over the range of forecast system **demands**, under the **contingency** conditions as defined in Category B of Appendix 1.

The **ISO** planning assessments must:

**R1.1** Be carried out annually.

**R1.2** Be conducted for near term (year one through five) and longer term (year six through ten) planning horizons.

**R1.3** Be supported by a study and/or system simulation testing, conducted within the last five years that addresses each of the requirements in requirement R1.3.1 to R1.3.12, showing system performance for the conditions defined in Category B of Appendix 1.

**R1.3.1** Be performed and evaluated only for those Category B **contingencies** that the **ISO** has determined would produce the more severe system results or impacts. The rationale for the **contingencies** selected for evaluation and an explanation of why the remaining simulations would produce less severe system results must be included in the study.

**R1.3.2** Cover critical system conditions and study years as determined necessary by the **ISO**.

**R1.3.3** Be conducted annually unless the **ISO** determines that changes to system conditions do not warrant such analyses.

**R1.3.4** Be conducted beyond the five year horizon only as needed to address identified marginal conditions that may have longer lead time solutions.

**R1.3.5** Have all projected firm transfers modeled, if any.

**R1.3.6** Be performed and evaluated for selected **demand** levels over the range of forecast system **demands** as considered necessary by the *ISO*.

**R1.3.7** Demonstrate that system performance meets the conditions defined in Category B of Appendix 1.

**R1.3.8** Include existing and planned **facilities** as considered necessary by the **ISO**.

**R1.3.9** Include **reactive power** resources to ensure that adequate reactive resources are available to meet system performance.

**R1.3.10** Include the effects of existing and planned **protection systems**, including any backup or redundant systems.

**R1.3.11** Include the effects of existing and planned control devices.

**R1.3.12** Include the planned **outage** and maintenance of any bulk electric equipment (including **protection systems** or their components) at those **demand** levels for which planned (including maintenance) **outages** are performed. For stations supplied by two lines, if one line is out for maintenance, then those stations are considered to be supplied by a radial line.

**R1.4** Address any planned upgrades needed to meet the performance requirements for the conditions defined in Category B of Appendix 1.

**R1.5** Consider all **contingencies** applicable to Category B of Appendix 1.

**R2** When system simulations indicate an inability of the systems to respond as set out in R1.3.7 of this **reliability standard** the **ISO** must:

**R2.1** Provide corrective plans to achieve the required system performance as described above throughout the planning horizon:

**R2.1.1** Including a schedule for implementation.

**R2.1.2** Including a discussion of expected required in-service dates of **facilities**.

**R2.1.3** Consider lead times necessary to implement corrective plans**.**

**R2.2** Review, in subsequent annual assessments, where sufficient lead time exists, the continuing need for identified system **facilities**. Detailed implementation plans are not needed**.**

**R3** The **ISO** must provide the planning assessment to **WECC** on an annual basis.

## 5. Processes and Procedures

No procedures have been defined for this **reliability standard**.

## 6. Measures

The following measures correspond to the requirements identified in Section 4 of this **reliability standard**. For example, MR1 is the measure for R1.

**MR1** The planning assessment will be valid and meet requirements in R1 through the following measures:

(a) The scope of the planning assessment identifies where area studies have been conducted in the past year. It also identifies area studies that have been conducted in previous years and are still valid. Where area studies have not been conducted, a plan and schedule to conduct one is included in the planning assessment.

(b) The planning assessment includes time horizons as specified in R1.2.

(c) The planning assessment has been prepared within the last year.

(d) A certification that the planning assessment complies with each of the R1 technical requirements is provided and states that the planning assessment meets all requirements, identifies requirements not met, and states reasons where the requirement was not met.

(e) A summary list of supporting area studies and needs identification documents is provided. The summary list includes the title and date of the study. The area studies and needs identification documents are provided if requested.

**MR2** The area studies and needs identification documents contain recommendations and projects for the corrective plans where an inability of the systems to respond to requirements specified in R1 has been identified. The area studies and needs identification documents must be provided on request.

**MR3** A written or email confirmation from **WECC** that it has received the planning assessment from the **ISO**. The confirmation includes the date of when the planning assessment was received and source identification information.

## 7. Appendices

**Appendix 1 - Transmission System Standards – Normal and Emergency Conditions** (see below)

## 8. Guidelines

No guidelines have been defined for this **reliability standard**.

## Revision History

| Date | Description |
|---|---|
| 2017-10-30 | Initial release. |

**Appendix 1 - Transmission System Standards – Normal and Emergency Conditions**

| Category | Contingencies | System Limits or Impacts | | |
|---|---|---|---|---|
| | Initiating Event(s) and Contingency **System Element(s)** | System Stable and Both Thermal and Voltage Limits Within Applicable **Rating**[a] | Loss of **Demand** or Curtailed Firm Transmission Service Transfers | **Cascading** |
| **A**<br>No **contingencies** | All **facilities** in service | Yes | No | No |
| **B**<br>Event resulting in the loss of a single **system element** | Single Line Ground (SLG) or 3-Phase (3Ø) fault, with **normal clearing**: | Yes | No[b] | No |
| | 1. Generator | Yes | No[b] | No |
| | 2. Transmission circuit | Yes | No[b] | No |
| | 3. Transformer | Yes | No[b] | No |
| **C**<br>Event(s) resulting in the loss of two or more (multiple) **system elements** | SLG fault, with **normal clearing**[e]: | | | |
| | 1. Bus section | Yes | Planned/ Controlled[c] | No |
| | 2. Breaker (failure or internal fault) | Yes | Planned/ Controlled[c] | No |
| | SLG or 3Ø fault, with **normal clearing**[e], manual system adjustments, followed by another SLG or 3Ø fault, with **normal clearing**[e]<br>3. Category B (B1, B2, B3, or B4) **contingency**, manual system adjustments, followed by another Category B (B1, B2, B3, or B4) **contingency** | Yes | Planned/ Controlled[c] | No |
| | Bipolar block, with **normal clearing**[e]: | | | |
| | 4. Bipolar (dc) line fault (non 3Ø), with **normal clearing**[e]: | Yes | Planned/ Controlled[c] | No |
| | 5. Any two circuits of a multiple circuit towerline[f] | Yes | Planned/ Controlled[c] | No |
| | SLG fault, with delayed clearing[e] (stuck breaker or **protection system** failure) | | | |

| | | | | |
|---|---|---|---|---|
| | 6. Generator | Yes | Planned/ Controlled[c] | No |
| | 7. Transformer | Yes | Planned/ Controlled[c] | No |
| | 8. Transmission circuit | Yes | Planned/ Controlled[c] | No |
| | 9. Bus section | Yes | Planned/ Controlled[c] | No |
| **D** [d]<br><br>Extreme event resulting in two or more (multiple) **system elements** removed or **cascading** out of service | 3Ø fault, with delayed clearing[e] (stuck breaker or **protection system** failure):<br>1. Generator<br>2. Transmission circuit<br>3. Transformer<br>4. Bus section<br><br>3Ø fault, with **normal clearing**[e]:<br>5. Breaker (failure or internal fault)<br>6. Loss of towerline with three or more circuits<br>7. All transmission lines on a common right-of -way<br>8. Loss of a substation (one voltage level plus transformers)<br>9. Loss of a switching station (one voltage level plus transformers)<br>10. Loss of all generating units at a station<br>11. Loss of a large **load** or major **load** center<br>12. Failure of a fully redundant **special protection system** (or **remedial action scheme**) to operate when required<br>13. Operation, partial operation, or **misoperation** of a fully redundant **special protection system** (or **remedial action scheme**) in response to an event or abnormal system<br>14. Impact of severe power swings or oscillations from disturbances in another Regional Reliability Organization | Evaluate for risks and consequences<br>• May involve substantial loss of customer demand and generation in a widespread area or areas<br>• Portions or all of the **interconnected** systems may or may not achieve a new, stable operating point<br>• Evaluation of these events may require joint studies with neighboring systems | | |

a) Applicable **rating** refers to the applicable normal and emergency **facility** thermal and voltage **rating** as applied by the **facility** owner or system voltage limit as determined and consistently applied by the ISO. Applicable *ratings* may include emergency **ratings** applicable for short durations as required to permit operating steps necessary to maintain system control. All **ratings** must be established by the applicable entity consistent with applicable *ISO* rules addressing **facility ratings**.

b) Planned or controlled interruption of electric supply to radial customers or some local network customers, connected to or supplied by the faulted **system element** or by the affected area, may occur in certain areas without impacting the overall **reliability** of the **interconnected** transmission systems. To prepare for the next **contingency**, system adjustments are permitted, including curtailments of contracted firm (non-recallable reserved) transmission service electric power transfers.

c) Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (**load** shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) transmission service electric power transfers may be necessary to maintain the overall **reliability** of the **interconnected** transmission systems.

d) A number of extreme **contingencies** that are listed under Category D and judged to be critical by the transmission planning entity(ies) will be selected for evaluation. It is not expected that all possible **facility outages** under each listed **contingency** of Category D will be evaluated.

e) **Normal clearing** is when the **protection system** operates as designed and the fault is cleared in the time normally expected with proper functioning of the installed ***protection*** **systems**. Delayed clearing of a fault is due to failure of any **protection system** component such as a relay, circuit breaker, or current transformer, and not because of an intentional design delay.

f) System assessments may exclude these events where multiple circuit towers are used over short distances (i.e., station entrance, river crossings) in accordance with exemption criteria.

# Alberta Reliability Standard
# System Performance Following Loss of Two or more BES Elements
# TPL-003-AB-0

## 1. Purpose

The purpose of this **reliability standard** is to ensure that a reliable transmission system is planned that meets specified performance requirements, with sufficient lead time. The transmission system must continue to be modified or upgraded as required to meet present and future system specified performance requirements as identified by periodically performed system simulations and associated planning assessments.

## 2. Applicability

This **reliability standard** applies to:

(a) **ISO**

## 3. Definitions

Bold terms used in this **reliability standard** have the meanings as set out in the *Consolidated Authoritative Document Glossary* and Part 1 of the ISO Rules.

## 4. Requirements

**R1** The **ISO** must demonstrate for **transmission facilities** rated 100 kV and above, through a planning assessment that the **AIES** is planned such that the **AIES** can be operatedto accommodate forecasted customer **demands**, supply and forecasted firm (non- recallable reserved) transmission services, at all demand **levels** over the range of forecast system **demands**, under the **contingency** conditions as defined in Category C of Appendix 1. The controlled interruption of **demand** to **demand customers**, the planned removal of generating units, or the curtailment of firm (non-recallable reserved) power transfers may be necessary to meet this **reliability standard**.

The **ISO** planning assessments must:

**R1.1** Be carried out annually.

**R1.2** Be conducted for near term (year one through five) and longer term (year six through ten) planning horizons.

**R1.3** Be supported by a study and/or system simulation testing, conducted within the last five years that addresses each of the requirements in requirement R1.3.1 to R1.3.1, showing system performance for the conditions defined in Category C of Appendix 1.

**R1.3.1** Be performed and evaluated only for those Category C **contingencies** that the **ISO** determines would produce the more severe system results or impacts. The rationale for the **contingencies** selected for evaluation and an explanation of why the remaining simulations would produce less severe system results must be included in the study.

**R1.3.2** Cover critical system conditions and study years as determined necessary by the *ISO*.

**R1.3.3** Be conducted annually unless the ISO determines that changes to system conditions do not warrant such analyses.

**R1.3.4** Be conducted beyond the five year planning horizon only as needed to address identified marginal conditions that may have longer lead- time solutions.

**R1.3.5** Have all projected firm transfers modeled, if any.

**R1.3.6** Be performed and evaluated for selected **demand** levels over the range of forecast system **demands** as considered necessary by the **ISO**.

**R1.3.7** Demonstrate that system performance meets the conditions defined in Category C of Appendix 1.

**R1.3.8** Include existing and planned **facilities** as considered necessary by the **ISO**.

**R1.3.9** Include **reactive power** resources to ensure that adequate reactive resources are available to meet system performance.

**R1.3.7** Demonstrate that system performance meets the conditions defined in Category C of Appendix 1.

**R1.3.8** Include existing and planned **facilities** as considered necessary by the **ISO**.

**R1.3.9** Include **reactive power** resources to ensure that adequate reactive resources are available to meet system performance.

**R1.3.10** Include the effects of existing and planned protection systems, including any backup or redundant systems.

**R1.3.11** Include the effects of existing and planned control devices.

**R1.3.12** Include the planned **outage** and maintenance of any bulk electric equipment (including **protection systems** or their components) at those **demand** levels for which planned (including maintenance) **outages** are performed. This requirement applies only to **BES facilities** greater than 200 kV or other **facilities** as specified by the **ISO**.

**R1.4** Address any planned upgrades needed to meet the performance requirements for the conditions defined in Category C of Appendix 1.

**R1.5** Consider all **contingencies** applicable to Category C of Appendix 1.

**R2** When system simulations indicate an inability of the systems to respond as set out inR1.3.7 of this reliability standard, the **ISO** must:

**R2.1** Provide corrective plans to achieve the required system performance as described above throughout the planning horizon:

**R2.1.1** Including a schedule for implementation.

**R2.1.2** Including a discussion of expected required in-service dates of **facilities**.

**R2.1.3** Consider lead times necessary to implement plans.

**R2.2** Review in subsequent annual assessments where sufficient lead time exists, the continuing need for identified system **facilities**. Detailed implementation plans are not needed.

**R3** The **ISO** must provide the planning assessment to **WECC** on an annual basis.

## 5. Processes and Procedures

No procedures have been defined for this **reliability standard**.

## 6. Measures

The following measures correspond to the requirements identified in Section 4 of this **reliability standard**. For example, MR1 is the measure for R1.

**MR1** The planning assessment will be valid and meet requirements in R1 through the following measures:

(a) The scope of the planning assessment identifies where area studies have been conducted in the past year. It also identifies area studies that have been conducted in previous years and are still valid. Where area studies have not been conducted, a plan and schedule to conduct one is included in the planning assessment.

(b) The planning assessment includes time horizons as specified in R1.2.

(c) The planning assessment has been prepared within the last year.

(d) A certification that the planning assessment complies with each of the R1 technical requirements is provided and states that the planning assessment meets all requirements, identifies requirements not met, and states reasons where the requirement was not met.

(e) A summary list of supporting area studies and needs identification documents is provided. The summary list includes the title and date of the study. The area studies and needs identification documents are provided if requested.

**MR2** The area studies and needs identification documents contain recommendations and projects that correct the situations where an inability of the systems to respond to requirements specified in R1 has been identified. The area studies and needs identification documents are provided on request.

The area studies and needs identification documents contain the technical components as specified in R2 and its subsections.

**MR3** A written or email confirmation from **WECC** that it has received the planning assessment from the **ISO**. The confirmation includes the date of when the planning assessment was received and source identification information.

## 7. Appendices

**Appendix 1 - Transmission System Standards – Normal and Emergency Conditions** (see below)

## 8. Guidelines

No guidelines have been defined for this **reliability standard**.

## Revision History

| Date | Description |
|---|---|
| 2010-09-24 | Initial release. |
| 2016-08-30 | Inclusion of the defined term **system element**. |

**Appendix 1 - Transmission System Standards – Normal and Emergency Conditions**

| Category | Contingencies | System Limits or Impacts | | |
|---|---|---|---|---|
| | Initiating Event(s) and Contingency **System Element(s)** | System Stable and Both Thermal and Voltage Limits Within Applicable **Rating**[a] | Loss of **Demand** or Curtailed Firm Transmission Service Transfers | **Cascading** |
| **A**<br>No **contingencies** | All **facilities** in service | Yes | No | No |
| **B**<br>Event resulting in the loss of a single **system element** | Single Line Ground (SLG) or 3-Phase (3Ø) fault, with **normal clearing**: | Yes | No[b] | No |
| | 1. Generator | Yes | No[b] | No |
| | 2. Transmission circuit | Yes | No[b] | No |
| | 3. Transformer | Yes | No[b] | No |
| **C**<br>Event(s) resulting in the loss of two or more (multiple) **system elements** | SLG fault, with **normal clearing**[e]: | | | |
| | 1. Bus section | Yes | Planned/ Controlled[c] | No |
| | 2. Breaker (failure or internal fault) | Yes | Planned/ Controlled[c] | No |
| | SLG or 3Ø fault, with **normal clearing**[e], manual system adjustments, followed by another SLG or 3Ø fault, with **normal clearing**[e]<br>3. Category B (B1, B2, B3, or B4) **contingency**, manual system adjustments, followed by another Category B (B1, B2, B3, or B4) **contingency** | Yes | Planned/ Controlled[c] | No |
| | Bipolar block, with **normal clearing**[e]: | | | |
| | 4. Bipolar (dc) line fault (non 3Ø), with **normal clearing**[e]: | Yes | Planned/ Controlled[c] | No |
| | 5. Any two circuits of a multiple circuit towerline[t] | Yes | Planned/ Controlled[c] | No |
| | SLG fault, with delayed clearing[e] (stuck breaker or **protection system** failure) | | | |

| | | | | |
|---|---|---|---|---|
| | 6. Generator | Yes | Planned/ Controlled[c] | No |
| | 7. Transformer | Yes | Planned/ Controlled[c] | No |
| | 8. Transmission circuit | Yes | Planned/ Controlled[c] | No |
| | 9. Bus section | Yes | Planned/ Controlled[c] | No |
| **D** [d]<br>Extreme event resulting in two or more (multiple) **system elements** removed or **cascading** out of service | 3Ø fault, with delayed clearing[e] (stuck breaker or **protection system** failure):<br>1. Generator 2. Transmission circuit<br>3. Transformer 4. Bus section<br>3Ø fault, with **normal clearing**[e]:<br>5. Breaker (failure or internal fault)<br>6. Loss of towerline with three or more circuits<br>7. All transmission lines on a common right-of -way<br>8. Loss of a substation (one voltage level plus transformers)<br>9. Loss of a switching station (one voltage level plus transformers)<br>10. Loss of all generating units at a station<br>11. Loss of a large **load** or major **load** center<br>12. Failure of a fully redundant **special protection system** (or **remedial action scheme**) to operate when required<br>13. Operation, partial operation, or **misoperation** of a fully redundant **special protection system** (or **remedial action scheme**) in response to an event or abnormal system<br>14. Impact of severe power swings or oscillations from disturbances in another Regional Reliability Organization | | Evaluate for risks and consequences<br>• May involve substantial loss of customer demand and generation in a widespread area or areas<br>• Portions or all of the **interconnected** systems may or may not achieve a new, stable operating point<br>• Evaluation of these events may require joint studies with neighboring systems | |

a) Applicable **rating** refers to the applicable normal and emergency **facility** thermal and voltage **rating** as applied by the **facility** owner or system voltage limit as determined and consistently applied by the ISO. Applicable **ratings** may include emergency **ratings** applicable for short durations as required to permit operating steps necessary to maintain system control. All **ratings** must be established by the applicable entity consistent with applicable **ISO** rules addressing **facility ratings**.

b) Planned or controlled interruption of electric supply to radial customers or some local network customers, connected to or supplied by the faulted **system element** or by the affected area, may occur in certain areas without impacting the overall **reliability** of the **interconnected** transmission systems. To prepare for the next **contingency**, system adjustments are permitted, including curtailments of contracted firm (non-recallable reserved) transmission service electric power transfers.

c) Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (**load** shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) transmission service electric power transfers may be necessary to maintain the overall **reliability** of the **interconnected** transmission systems.

d) A number of extreme **contingencies** that are listed under Category D and judged to be critical by the transmission planning entity(ies) will be selected for evaluation. It is not expected that all possible **facility outages** under each listed **contingency** of Category D will be evaluated.

e) **Normal clearing** is when the **protection system** operates as designed and the fault is cleared in the time normally expected with proper functioning of the installed **protection systems**. Delayed clearing of a fault is due to failure of any **protection system** component such as a relay, circuit breaker, or current transformer, and not because of an intentional design delay.

f) System assessments may exclude these events where multiple circuit towers are used over short distances (i.e., station entrance, river crossings) in accordance with exemption criteria.

# Alberta Reliability Standard
# System Performance Following Extreme BES Events
# TPL-004-AB-0

## 1. Purpose

The purpose of this **reliability standard** is to ensure that a reliable transmission system is planned that meets specified performance requirements with sufficient lead time. The transmission system must continue to be modified or upgraded as required to meet present and future system specified performance requirements as identified by periodically performed system simulations and associated planning assessments.

## 2. Applicability

This **reliability standard** applies to:

(a) **ISO**

## 3. Definitions

Bold terms used in this **reliability standard** have the meanings as set out in the *Consolidated Authoritative Document Glossary* and Part 1 of the ISO Rules.

## 4. Requirements

**R1** The ISO must demonstrate for transmission facilities rated 100 kV and above, through a planning assessment that a transmission system is planned such that it has been evaluated for the risks and consequences of a number of each of the extreme contingencies that are listed under Category D of Appendix 1.

The **ISO** planning assessments must:

**R1.1** Be carried out annually.

**R1.2** Be conducted for near term (year one through five).

**R1.3** Be supported by a study and/or system simulation that addresses each of the following categories, showing system performance following Category D **contingencies** of Appendix 1.

**R1.3.1** Be performed and evaluated only for those Category D **contingencies that** *ISO* determines would produce the more severe system results or impacts. The rationale for the **contingencies** selected for evaluation and an explanation of why the remaining simulations would produce less severe system results must be included in the study.

**R1.3.2** Cover critical system conditions and study years as considered necessary by the **ISO**.

**R1.3.3** Be conducted annually unless the **ISO** determines that changes to system conditions do not warrant such analyses.

**R1.3.4** Have all projected firm transfers modeled, if any.

**R1.3.5** Include existing and planned **facilities** as considered necessary by the **ISO**.

**R1.3.6** Include **reactive power** resources to ensure that adequate reactive resources are available to meet system performance.

**R1.3.7** Include the effects of existing and planned **protection systems**, including any backup or redundant systems.

**R1.3.8** Include the effects of existing and planned control devices.

**R1.3.9** Include the planned **outage** and maintenance of any bulk electric equipment (including **protection systems** or their components) at those **demand** levels for which planned (including maintenance) **outages** are performed. This requirement applies only to **BES facilities** greater than 200 kV or other **facilities** as specified by the **ISO**.

**R1.4** Consider all **contingencies** applicable to Category D of Appendix 1.

**R2** The **ISO** must provide the planning assessment to **WECC** on an annual basis.

## 5. Processes and Procedures

No procedures have been defined for this **reliability standard**.

## 6. Measures

The following measures correspond to the requirements identified in Section 4 of this **reliability standard**. For example, MR1 is the measure for R1.

**MR1** The planning assessment will be valid and meet requirement in R1 and associated sub-sections through the following measures:

(a) The scope of the planning assessment identifies where area studies have been conducted in the past year. It also identifies area studies that have been conducted in previous years and are still valid. Where area studies have not been conducted, a plan and schedule to conduct one is included in the planning assessment.

(b) The planning assessment includes time horizons as specified in R1.2.

(c) The planning assessment has been prepared within the last year.

(d) A certification that the planning assessment complies with each of the R1 technical requirements is provided and states that the planning assessment meets all requirements, identifies requirements not met, and states reasons where the requirement was not met.

(e) A summary list of supporting area studies and needs identification documents is provided. The summary list includes the title and date of the study. The area studies and needs identification documents are provided if requested.

**MR2** A written or email confirmation from **WECC** that it has received the planning assessment from the **ISO**. The confirmation includes the date of when the planning assessment was received and source identification information.

## 7. Appendices

**Appendix 1 - Transmission System Standards – Normal and Emergency Conditions** (see below)

## 8. Guidelines

No guidelines have been defined for this **reliability standard**.

## Revision History

| Date | Description |
|---|---|
| 2010-09-24 | Initial release. |
| 2016-08-30 | Inclusion of the defined term **system element**. |

**Appendix 1 - Transmission System Standards – Normal and Emergency Conditions**

| Category | Contingencies | System Limits or Impacts | | |
|---|---|---|---|---|
| | Initiating Event(s) and Contingency **System Element(s)** | System Stable and Both Thermal and Voltage Limits Within Applicable **Rating**[a] | Loss of **Demand** or Curtailed Firm Transmission Service Transfers | **Cascading** |
| **A**<br>No **contingencies** | All **facilities** in service | Yes | No | No |
| **B**<br>Event resulting in the loss of a single **system element** | Single Line Ground (SLG) or 3-Phase (3Ø) fault, with **normal clearing**: | Yes | No[b] | No |
| | 1. Generator | Yes | No[b] | No |
| | 2. Transmission circuit | Yes | No[b] | No |
| | 3. Transformer | Yes | No[b] | No |
| **C**<br>Event(s) resulting in the loss of two or more (multiple) **system elements** | SLG fault, with **normal clearing**[e]: | | | |
| | 1. Bus section | Yes | Planned/ Controlled[c] | No |
| | 2. Breaker (failure or internal fault) | Yes | Planned/ Controlled[c] | No |
| | SLG or 3Ø fault, with **normal clearing**[e], manual system adjustments, followed by another SLG or 3Ø fault, with **normal clearing**[e]<br>3. Category B (B1, B2, B3, or B4) **contingency**, manual system adjustments, followed by another Category B (B1, B2, B3, or B4) **contingency** | Yes | Planned/ Controlled[c] | No |
| | Bipolar block, with **normal clearing**[e]: | | | |
| | 4. Bipolar (dc) line fault (non 3Ø), with **normal clearing**[e]: | Yes | Planned/ Controlled[c] | No |
| | 5. Any two circuits of a multiple circuit towerline[t] | Yes | Planned/ Controlled[c] | No |
| | SLG fault, with delayed clearing[e] (stuck breaker or **protection system** failure) | | | |

| | | | | |
|---|---|---|---|---|
| | 6. Generator | Yes | Planned/ Controlled[c] | No |
| | 7. Transformer | Yes | Planned/ Controlled[c] | No |
| | 8. Transmission circuit | Yes | Planned/ Controlled[c] | No |
| | 9. Bus section | Yes | Planned/ Controlled[c] | No |
| **D** [d]<br>Extreme event resulting in two or more (multiple) **system elements** removed or **cascading** out of service | 3Ø fault, with delayed clearing[e] (stuck breaker or **protection system** failure):<br>1. Generator 2. Transmission circuit<br>3. Transformer 4. Bus section | | Evaluate for risks and consequences<br>• May involve substantial loss of customer demand and generation in a widespread area or areas<br>• Portions or all of the **interconnected** systems may or may not achieve a new, stable operating point<br>• Evaluation of these events may require joint studies with neighboring systems | |
| | 3Ø fault, with **normal clearing**[e]:<br>5. Breaker (failure or internal fault)<br>6. Loss of towerline with three or more circuits<br>7. All transmission lines on a common right-of -way<br>8. Loss of a substation (one voltage level plus transformers)<br>9. Loss of a switching station (one voltage level plus transformers)<br>10. Loss of all generating units at a station<br>11. Loss of a large **load** or major **load** center<br>12. Failure of a fully redundant **special protection system** (or **remedial action scheme**) to operate when required<br>13. Operation, partial operation, or **misoperation** of a fully redundant **special protection system** (or **remedial action scheme**) in response to an event or abnormal system<br>14. Impact of severe power swings or oscillations from disturbances in another Regional Reliability Organization | | | |

a) Applicable **rating** refers to the applicable normal and emergency **facility** thermal and voltage **rating** as applied by the **facility** owner or system voltage limit as determined and consistently applied by the ISO. Applicable **ratings** may include emergency **ratings** applicable for short durations as required to permit operating steps necessary to maintain system control. All **ratings** must be established by the applicable entity consistent with applicable **ISO** rules addressing **facility ratings**.

b) Planned or controlled interruption of electric supply to radial customers or some local network customers, connected to or supplied by the faulted **system element** or by the affected area, may occur in certain areas without impacting the overall **reliability** of the **interconnected** transmission systems. To prepare for the next **contingency**, system adjustments are permitted, including curtailments of contracted firm (non-recallable reserved) transmission service electric power transfers.

c) Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (**load** shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) transmission service electric power transfers may be necessary to maintain the overall **reliability** of the **interconnected** transmission systems.

d) A number of extreme **contingencies** that are listed under Category D and judged to be critical by the transmission planning entity(ies) will be selected for evaluation. It is not expected that all possible **facility outages** under each listed **contingency** of Category D will be evaluated.

e) **Normal clearing** is when the **protection system** operates as designed and the fault is cleared in the time normally expected with proper functioning of the installed **protection systems**. Delayed clearing of a fault is due to failure of any **protection system** component such as a relay, circuit breaker, or current transformer, and not because of an intentional design delay.

f) System assessments may exclude these events where multiple circuit towers are used over short distances (i.e., station entrance, river crossings) in accordance with exemption criteria.

## 1. Purpose

To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real-time to protect equipment and the reliable operation of the **Interconnection**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **ISO**.

## 3. Requirements

**R1** The **ISO** must specify a system voltage range with an associated tolerance band, as part of its plan to operate within **system operating limits** and **interconnection reliability operating limits**.

**R1.1** The **ISO** must provide a copy of the system voltage range with an associated tolerance band to an **interconnected transmission operator** within thirty (30) **days** of a request.

**R2** The **ISO** must operate with sufficient **reactive power** resources available within Alberta to protect the voltage levels of the **transmission system** under normal and **contingency** conditions.

**R3** The **ISO** must be able to regulate transmission voltage and **reactive power** flow by issuing **directives** or instructions to operate the devices necessary to do so.

**R4** The **ISO** must specify the criteria that will exempt a **generating unit** or an **aggregated generating facility** from:

a) following a voltage or **reactive power** instruction or **directive**;

b) having its **automatic voltage regulator** or **voltage regulating system** in service or being in voltage control mode; or

c) making any associated notifications.

**R4.1** If the **ISO** determines that a **generating unit** or an **aggregated generating facility** has satisfied the exemption criteria, the **ISO** must notify the associated **operator** of a **generating unit** or **operator** of an **aggregated generating facility**.

**R5** The **ISO**, when issuing **directives** or instructions for voltage level or **reactive power**, to the **operator** of a **generating unit** or the **operator** of an **aggregated generating facility**, must specify the following:

a) the voltage level at the **point of connection** between the **transmission system** and a **generating unit** or an **aggregated generating facility**, including those in a power plant or an industrial complex; or

b) the **reactive power** to be achieved by the **generating unit**, **aggregated generating facility**, power plant or industrial complex.

**R6** The **ISO** must, after a review with the **legal owner** of a **generating unit** or the **legal owner** of an **aggregated generating facility** regarding necessary off-load tap changes for the step-up transformer that connects to the **transmission system**, provide documentation to the **legal owner** of a **generating**

**unit** or the **legal owner** of an **aggregated generating facility** specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard.** For example, MR1 is the measure for R1.

**MR1**. Evidence of specifying a system voltage range with an associated tolerance band as required in requirement R1 exists.

**MR1.1** Evidence of providing a copy of the system voltage range with an associated tolerance band as required in requirement R1.1 exists. Evidence may include, but is not limited to, emails, website postings, or any other equivalent evidence.

**MR2** Evidence of operating with sufficient **reactive power** resources as required in requirement R2 exists. Evidence may include, but is not limited to, data files or any other equivalent evidence.

**MR3** Evidence of being able to regulate transmission voltage and **reactive power** flow as required in requirement R3 exists. Evidence may include, but is not limited to, relevant **ISO** authoritative documents.

**MR4** Evidence of specifying the criteria that will exempt a **generating unit** or an **aggregated generating facility** as specified in requirement R4 exists.

**MR4.1** Evidence of notifying the associated **operator** of a **generating uni**t or **operator** of an **aggregated generating facility** if the **ISO** determines that the exemption criteria were satisfied. Evidence may include, but is not limited to, emails, data files or other equivalent evidence.

**MR5** Evidence of issuing **directives** or instructions to the **operator** of a **generating unit** or the **operator** of an **aggregated generating facility** as required in requirement R5 exists. Evidence may include, but is not limited to, voice recordings or other equivalent evidence.

**MR6** Evidence of providing documentation as required in requirement R6 exists. Evidence may include, but is not limited to, dated study results or email to appropriate recipients that identifies contents submitted or other equivalent evidence.

## 5. Appendices

Appendix 1 - *Exemptions*

### Revision History

| Date | Description |
|---|---|
| 2019-12-01 | Unbolded “real time” |
| 2016-04-01 | Revised to align with NERC version 4. |
| 2012-10-01 | Initial release |

## Appendix 1 - Exemptions

### 1. Exemption Criteria

A **generating unit** or **aggregated generating facility** must, in order to meet the exemption criteria referred to in requirement R4 of this **reliability standard**:

(a) be a wind **aggregated generating facility**;

(b) not be equipped with a **voltage regulating system**; and

(c) be the subject of an executed *Construction Commitment Agreement* and have completed the **ISO**'s approval process for connection to the **transmission system** under the *Technical Requirements for connecting generators (1999)*.

## 1. Purpose

The purpose of this **reliability standard** is to ensure **generating units** and **aggregated generating facilities** provide **reactive power** support and voltage control, within generating facility capabilities, in order to protect equipment and maintain reliable operation of the **interconnected electric system**.

## 2. Applicability

This **reliability standard** applies to:

(a) the **legal owner** of a **generating unit** that has a **maximum authorized real power** greater than or equal to 5 MW and where the **generating unit** is:
- (i) connected to a switchyard at which **system access service** is provided to:
  - (A) the **generating unit**; or
  - (B) an industrial complex of which the **generating unit** is a part; or
- (ii) directly connected to **transmission facilities** within the City of Medicine Hat;

(b) the **operator** of a **generating unit** that has a **maximum authorized real power** greater than or equal to 5 MW and where the **generating unit** is:
- (i) connected to a switchyard at which system access service is provided to:
  - (A) the **generating unit**; or
  - (B) an industrial complex of which the **generating unit** is a part; or
- (ii) directly connected to **transmission facilities** within the City of Medicine Hat;

(c) the **legal owner** of an **aggregated generating facility** that has a **maximum authorized real power** greater than or equal to 5 MW and is:
- (i) connected to a switchyard at which **system access service** is provided to:
  - (A) the **aggregated generating facility**; or
  - (B) an industrial complex of which the **aggregated generating facility** is a part; or
- (ii) directly connected to transmission facilities within the City of Medicine Hat; and

(d) the **operator** of an **aggregated generating facility** that has a **maximum authorized real power** greater than or equal to 5 MW and is:
- (i) connected to a switchyard at which **system access service** is provided to:
  - (A) the **aggregated generating facility**; or
  - (B) an industrial complex of which the **aggregated generating facility** is a part; or
- (ii) directly connected to **transmission facilities** within the City of Medicine Hat.

Notwithstanding subsections (c) and (d) above, this **reliability standard** does not apply to the **legal owner** of an **aggregated generating facility** or the **operator** of an **aggregated generating facility** that meets the criteria listed in Appendix 1 of VAR-001-AB.

## 3. Requirements

**R1** The **operator** of a **generating unit** and **operator** of an **aggregated generating facility** must, while a **generating unit** or **aggregated generating facility** is electrically connected to the **transmission system**, operate the **generating unit** or **aggregated generating facility** with its **automatic voltage regulator** or **voltage regulating system** in service and in automatic voltage control mode, or in a different control mode as instructed by the **ISO** unless:

(a) the **generating unit** or **aggregated generating facility** is exempted by the **ISO**;

(b) the **operator** of a **generating unit** or **operator** of an **aggregated generating facility** has notified the **ISO** in accordance with requirement R3 that the **generating unit** or **aggregated generating**

**facility** is not being operated in automatic voltage control mode or in the control mode that was instructed by the **ISO** for a reason other than start-up, shutdown, or testing. Such reasons may include a forced or unplanned change in control mode;

(c) the **generating unit** or **aggregated generating facility** is being operated during start-up or shut-down in accordance with the procedure of the **operator** of a **generating unit** or **operator** of an **aggregated generating facility**; or

(d) the **operator** of a **generating unit** or the **operator** of an **aggregated generating facility** has previously obtained approval from the **ISO** allowing the **generating unit** or **aggregated generating facility** to be in a testing mode.

**R2** Unless exempted by the **ISO**, each **operator** of a **generating unit** and each **operator** of an **aggregated generating facility** must, upon receiving an instruction from the **ISO** regarding voltage levels or **reactive power**, comply with that instruction.

**R2.1** Each **operator** of a **generating unit** and each **operator** of an **aggregated generating facility** must, when:

(a) the **automatic voltage regulator** of a **generating unit** or the **voltage regulating system** of an **aggregated generating facility** is out of service; or

(b) the **generating unit** does not have an **automatic voltage regulator**, or the **aggregated generating facility** does not have a **voltage regulating system**,

use an alternative method to control the generator **reactive power** output to comply with an instruction from the **ISO** regarding voltage levels or **reactive power**.

**R2.2** Notwithstanding requirement R2, where the **operator** of a **generating unit** or the **operator** of an **aggregated generating facility** cannot comply with an instruction to modify voltage, the **operator** of a **generating unit** or the **operator** of an **aggregated generating facility** must provide an explanation for why the instruction cannot be met.

**R2.3** Each **operator** of a **generating unit** and **operator** of an **aggregated generating facility** that does not monitor the voltage or **reactive power** at the location specified in an instruction or **directive** from the **ISO** must have a methodology for converting the voltage or **reactive power** at the location specified by the **ISO**.

**R3** Each **operator** of a **generating unit** and **operator** of an **aggregated generating facility** must notify the **ISO** within 30 minutes after a status or control mode change of the **automatic voltage regulator**, **voltage regulating system**, alternative voltage controlling device or power system stabilizer, as applicable, on any **generating unit** or **aggregated generating facility**.

**R3.1** If the status or control mode has been restored within 30 minutes of such change, then the **operator** of a **generating unit** or **operator** of an **aggregated generating facility** is not required to notify the **ISO** of the status or control mode change.

**R3.2** If a **generating unit** or an **aggregated generating facility** is in testing, start-up, shut-down or offline mode, requirement R3 does not apply.

**R3.3** If a **generating unit** or an **aggregated generating facility** is operating below the safe and stable level for power system stabilizer operation, then the **operator** of a **generating unit** or **operator** of an **aggregated generating facility** is not required to notify the **ISO** of a change in status of the power system stabilizer caused by the low output level of the **generating unit** or **aggregated generating facility**.

**R4** Each **operator** of a **generating unit** and **operator** of an **aggregated generating facility** must notify the **ISO** within 30 minutes after becoming aware of a change in **reactive power** capability due to factors other than a status or control mode change described in requirement R3, or unless:

**R4.1** the capability has been restored within 30 minutes of the **operator** of a **generating unit** or **operator** of an **aggregated generating facility** becoming aware of such change, then the **operator** is not required to notify the **ISO** of the change in **reactive power** capability; or

**R4.2** a **generating unit** or an **aggregated generating facility** is in testing, start-up, shut-down or offline mode, requirement R4 does not apply.

**R5** Each **legal owner** of a **generating unit** and each **legal owner** of an **aggregated generating facility** whose step-up transformer for connecting to the **transmission system** or auxiliary transformer has primary voltages equal to or greater than the **generating unit** terminal voltage must provide any one or more of the following to the **ISO** within 30 **days** of a request:

(a) tap settings;
(b) available fixed tap ranges; and
(c) impedance data.

**R6** Each **legal owner** of a **generating unit** and each **legal owner** of an **aggregated generating facility** that has a step-up transformer, with off-load taps for connecting to the **transmission system** must, change the tap positions according to the specifications the **ISO** provides.

**R6.1** Each **legal owner** of a **generating unit** and each **legal owner** of an **aggregated generating facility** that cannot comply with requirement R6 must notify the **ISO** within 30 **days** of the **ISO** providing the specifications and must include the technical justification along with the notice.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of operating the **generating unit** or **aggregated generating facility** in automatic voltage control mode as required in requirement R1 exists. Evidence may include exemption letters, data files, start-up or shut-down procedures, **operator** logs, voice recordings, e-mail, or other equivalent evidence.

**MR2** Evidence of complying with an instruction as required in requirement R2 exists. Evidence may include data files, **operator** logs, or other equivalent evidence.

**MR2.1** Evidence of using an alternative method to control generator **reactive power** output as required in requirement R2.1 exists. Evidence may include data files, **operator** logs, voice recordings, or other equivalent evidence.

**MR2.2** Evidence of providing an explanation to the **ISO**, as required in requirement R2.2 exists. Evidence may include voice recordings, **operator** logs, or other equivalent evidence

**MR2.3** Evidence of having a methodology as required in requirement R2.3 exists. Evidence may include a documented methodology, or other equivalent evidence.

**MR3** Evidence of notifying the **ISO** within 30 minutes of any status or control mode change as required in requirement R3 exists. Evidence may include data logs, SCADA logs, voice recordings, **operator** logs, or other equivalent evidence.

**MR4** Evidence of notifying the **ISO** within 30 minutes of becoming aware of a change in reactive power capability as required in requirement R4 exists. Evidence may include voice recordings, **operator** logs, or other equivalent evidence.

**MR5** Evidence of providing the **ISO** with information on its step-up and auxiliary transformers, as required in requirement R5 exists. Evidence may include dated written or electronic records, or other equivalent evidence.

**MR6** Evidence of changing step-up transformer taps in accordance with the **ISO**’s specifications as required in requirement R6 exists. Evidence may include written or electronic records, or other equivalent evidence.

**MR6.1** Evidence of notifying the **ISO** as required in requirement R6.1 exists. Evidence may include written or electronic notifications, or other equivalent evidence.

### Revision History

| Date | Description |
|---|---|
| 2021-06-24 | Initial release. |

# Alberta Reliability Standard
# Power System Stabilizer
# VAR-501-WECC-AB-1

## 1. Purpose

The purpose of this **reliability standard** is to ensure that **power system stabilizers** on **generating units** are kept in service.

## 2. Applicability

This **reliability standard** applies to:

(a) the o**perator** of a **generating unit** equipped with a **power system stabilizer** that is either:

- (i) directly connected to the **bulk electric system** or part of an industrial complex that is directly connected to the **bulk electric system**, and has a **maximum authorized real power** rating greater than eighteen (18) MW; or
- (ii) within a power plant which:
  - (A) is not part of an **aggregated generating facility**;
  - (B) is directly connected to the **bulk electric system**; and
  - (C) has a combined **maximum authorized real power rating** greater than sixty-seven point five (67.5) MW;
- (iii) a black start resource; or
- (iv) regardless of **maximum authorized real power** rating, material to this **reliability standard** and to the **reliability** of the **bulk electric system** as the **ISO** determines and publishes on the AESO website and may amend from time to time in accordance with the process set out in Appendix 1.

## 3. Requirements

**R1** Each **operator** of a **generating unit** equipped with a **power system stabilizer** must have the **power system stabilizer** in service ninety-eight (98%) of all operating hours except that the operating hours determined in accordance with requirements R 1.1 through 1.12 inclusive may be excluded to achieve the ninety-eight percent (98%) requirement.

**R1.1** The operating hours during which the **generating unit** operates for less than five percent (5%) of all hours during any calendar quarter.

**R1.2** The operating hours during which maintenance or testing on the **power system stabilizer** was performed, up to a maximum of seven (7) **days** per calendar quarter.

**R1.3** The operating hours during which the **power system stabilizer** exhibits instability due to abnormal system configuration.

**R1.4** The operating hours during which the **generating unit** is operating in the synchronous condenser mode and the **generating unit** is very near or at a zero (0) **real power** level.

**R1.5** The operating hours during which the **generating unit** is generating less **real power** than its design limit for effective **power system stabilizer** operation.

**R1.6** The operating hours during which the **generating unit** is passing through a range of output that is a known "rough zone" being a range in which a **generating unit** is experiencing excessive vibration.

**R1.7** The operating hours during which the **automatic voltage regulator** of the **generating unit** is not in service.

**R1.8** The operating hours, up to a maximum of sixty (60) consecutive **days** per incident, during which the **power system stabilizer** is out of service for repair due to a component failure.

**R1.9** The operating hours, up to a maximum of twelve (12) consecutive **months**, during which the **power system stabilizer** had a component failure, but only if the **operator** of a **generating unit** submitted documentation to the **ISO** identifying the need for time to obtain replacement parts and identifying a scheduled **outage**, if required.

**R1.10** The operating hours, up to a maximum of twenty-four (24) consecutive **months**, during which the **power system stabilizer** had a component failure, but only if the **operator** of a **generating unit** submitted documentation to the **ISO** identifying the need for time to replace the **power system stabilizer** and to schedule an **outage**.

**R1.11** The operating hours during which the **generating unit** is not in **commercial operation**.

**R1.12** The operating hours for which the **ISO** has issued a **directive** to the **operator** of a **generating unit** to operate the **generating unit** when the **power system stabilizer** is unavailable for service

**R2** Each **operator of a generating unit** must have documentation supporting the identification of the number of operating hours excluded for each requirement in requirements R1.1 through R1.12 inclusive.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for R1.

**MR1** Evidence of having the **power system stabilizer** in service as required in requirement R1 exists. Evidence may include documentation that summarizes for each calendar quarter:

(a) the number of hours the **power system stabilizer** was in service while the **generating unit** was operating;

(b) the number of hours the **power system stabilizer** was out of service while the **generating unit** was operating;

(c) the number of operating hours excluded in accordance with requirements R1.1 through R1.12; and

(d) the percentage of operating hours that the **power system stabilizer** was in service excluding the number of operating hours determined in accordance with requirements R1.1 through R1.12

**MR2** Evidence of having documentation as required in requirement R2 exists. Evidence may include a document identifying the subject of each exclusion, the date and the period of time that the exclusion refers to, reasons, the supporting data and the supporting logs.

## 5. Appendices

Appendix 1 – *Amending Process for List of Generating Units*

### Revision History

| Effective | Description |
|---|---|
| 2013-10-01 | |
| | |

## Appendix 1

## Amending Process for List of Generating Units

In order to amend the list referenced in subsection (a)(iv) of section 2, *Applicability*, the **ISO** must:

(a) upon determining that a **generating unit** is to be added, notify each affected **operator** of a **generating unit** in writing and determine an effective date, which must be no less than thirty (30) **days** after the date of notice, for the **operator** to meet the applicable requirements;

(b) upon determining that a **generating unit** is to be deleted, notify each affected **operator** of a **generating unit** in writing and determine an effective date for the **operator** to no longer be required to meet the applicable requirements; and

(c) post the amended list with effective dates on the AESO website.