
Project QC-2015-01**Retirement of Standard Requirements Approved or Under Study by
the Régie**

1. Assessment of relevance

On March 15, 2012, FERC issued an order in paragraph 81 (P81) of which it invited NERC, regional entities and other interested parties to coordinate and propose appropriate mechanisms to identify and retire any requirements deemed unnecessary or redundant. Following that decision, NERC initiated a review project entitled "Project 2013-02 Paragraph 81", which consisted in identifying, based on various criteria, requirements to be modified or retired.

To consider retiring it, a requirement should meet the criteria below.

1. Criterion A (overarching criterion): The requirement obligates responsible entities to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES.
2. At least one of the B criteria (identifying criteria):
 - Administrative. The requirement obligates responsible entities to perform a function that is administrative in nature, does not support reliability and is needlessly burdensome.
 - Data. The requirement obligates responsible entities to produce and retain data that documents prior events or activities, and that should be collected through some other method under NERC rules and processes.
 - Documentation. The requirement obligates responsible entities to develop a document that is not necessary to protect BES reliability.
 - Reporting. The requirement obligates responsible entities to periodically update documentation without any operational benefit to reliability.
 - Commercial or business practice. The requirement is a commercial or business practice, or implicates commercial rather than reliability issues.
 - Redundant. The requirement is redundant with other FERC-approved reliability standard requirements, the NERC compliance monitoring program or governmental regulation (e.g., that in the Open Access Transmission Tariff (OATT), by the North American Energy Standards Board (NAESB), etc.).

A further series of criteria (criteria C) gave additional information to assist in determining whether to retire requirements satisfying both criteria A and B. Entities desiring further information on the mechanism for determining requirements to be retired can consult the following technical document: [http://www.nerc.com/pa/Stand/Project%20201302%20Paragraph%2081%20RF/P81_Phase I technical white paper FINAL.pdf](http://www.nerc.com/pa/Stand/Project%20201302%20Paragraph%2081%20RF/P81_Phase_I_technical_white_paper_FINAL.pdf).

Following this process, NERC identified 34 requirements to be retired in 19 reliability standards. The retirement of these requirements was approved by FERC on November 21, 2013 and became effective on January 21, 2014. To ensure coordination of practices with neighboring jurisdictions, the Reliability Coordinator thus proposes to retire the same requirements. Note that this proposal only

applies to standards approved or under study by the Régie de l'énergie. The retirement of requirements in standards not yet filed will be proposed in those standards in later filings.

2. Retirement of requirements

The requirements listed below satisfied the above-mentioned criteria and have been retired from the specified reliability standards. To avoid version changes, the requirements have not been removed from the standards. Retirement is clearly indicated, however, under each specific requirement in the standard and in the Québec appendices.¹ The Reliability Coordinator has identified in 10 standards now approved or under study by the Régie, 15 requirements to be retired.

Standard	Requirement	Registered entity	Criterion A	Criterion B
BAL-005-0.2b	R2	BA	X	Redundant (BAL-001-0.1a R1 and E2)
CIP-003-1 ¹	R1.2	RC, BA, IA, TSP, TO, TOP, GO, GOP and LSE	X	Administrative
CIP-003-1 ¹	R3 R3.1 R3.2 R3.3	RC, BA, IA, TSP, TO, TOP, GO, GOP and LSE	X	Administrative and Documentation
CIP-003-1 ¹	R4.2	RC, BA, IA, TSP, TO, TOP, GO, GOP and LSE	X	Administrative, Documentation and Redundant (CIP-003-1 R4)
CIP-005-1 ¹	R2.6	RC, BA, IA, TSP, TO, TOP, GO, GOP and LSE	X	Administrative and Documentation
CIP-007-1 ¹	R7.3	RC, BA, IA, TSP, TO, TOP, GO, GOP and LSE	X	Administrative and Data
FAC-002-1	R2	PA, TOP, GO, TO, LSE and DP	X	Administrative and Data
FAC-010-2.1	R5	PA	X	Administrative, Reporting and Commercial practice
FAC-011-2	R5	RC	X	Administrative, Reporting and Commercial practice
IRO-016-1	R2	RC	X	Administrative and Data
PRC-010-0	R2	LSE, TO, TOP and DP, which implements undervoltage load shedding	X	Administrative and Data
PRC-022-1	R2	TOP, LSE and DP	X	Administrative and Data

¹ NERC examined version 3 of the CIP standards, for which the requirements retired match those in version 1, which was filed with the Régie. The original NERC CIP version 1 standards, retired prior to the requirement retirement process, thus do not contain these amendments. For those standards, retired requirements are thus only incorporated into the Québec appendices as specific provisions for application in Québec.

3. Proposed effective dates

In the U.S., retirement of the requirements came into effect on January 21, 2014. Since the proposed amendments only involve retiring requirements, the proposed effective date of the amended Québec standards is the first day of the first calendar quarter following their approval by the Régie.

4. Assessment of impact

The impact of the proposed amendments is positive since it reduces the number of requirements that entities must satisfy by retiring those that are unnecessary or redundant. The Reliability Coordinator thus considers it unnecessary to assess the impact of such amendments. Entities so desiring may nevertheless submit an assessment of the impact of these amendments on their activities, which the Reliability Coordinator will file with the Régie in support of its application.

A. Introduction

- 1. Title:** Automatic Generation Control
- 2. Number:** BAL-005-0.2b
- 3. Purpose:** This standard establishes requirements for Balancing Authority Automatic Generation Control (AGC) necessary to calculate Area Control Error (ACE) and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved.
- 4. Applicability:**
 - 4.1.** Balancing Authorities
 - 4.2.** Generator Operators
 - 4.3.** Transmission Operators
 - 4.4.** Load Serving Entities
- 5. Effective Date:** May 13, 2009

B. Requirements

- R1.** All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.
 - R1.1.** Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.
 - R1.2.** Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are included within the metered boundaries of a Balancing Authority Area.
 - R1.3.** Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.
- R2.** Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard. (Retirement approved by FERC effective January 21, 2014.)
- R3.** A Balancing Authority providing Regulation Service shall ensure that adequate metering, communications, and control equipment are employed to prevent such service from becoming a Burden on the Interconnection or other Balancing Authority Areas.
- R4.** A Balancing Authority providing Regulation Service shall notify the Host Balancing Authority for whom it is controlling if it is unable to provide the service, as well as any Intermediate Balancing Authorities.
- R5.** A Balancing Authority receiving Regulation Service shall ensure that backup plans are in place to provide replacement Regulation Service should the supplying Balancing Authority no longer be able to provide this service.
- R6.** The Balancing Authority's AGC shall compare total Net Actual Interchange to total Net Scheduled Interchange plus Frequency Bias obligation to determine the Balancing Authority's ACE. Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control. If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator.

- R7.** The Balancing Authority shall operate AGC continuously unless such operation adversely impacts the reliability of the Interconnection. If AGC has become inoperative, the Balancing Authority shall use manual control to adjust generation to maintain the Net Scheduled Interchange.
- R8.** The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.
 - R8.1.** Each Balancing Authority shall provide redundant and independent frequency metering equipment that shall automatically activate upon detection of failure of the primary source. This overall installation shall provide a minimum availability of 99.95%.
- R9.** The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.
 - R9.1.** Balancing Authorities with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection may choose to omit the Interchange Schedule related to the HVDC link from the ACE equation if it is modeled as internal generation or load.
- R10.** The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.
- R11.** Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE.
- R12.** Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.
 - R12.1.** Balancing Authorities that share a tie shall ensure Tie Line MW metering is telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. Balancing Authorities shall ensure that megawatt-hour data is telemetered or reported at the end of each hour.
 - R12.2.** Balancing Authorities shall ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service are not filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.
 - R12.3.** Balancing Authorities shall install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.
- R13.** Each Balancing Authority shall perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment. The Balancing Authority shall adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (I_{ME}) term of the ACE equation to compensate for any equipment error until repairs can be made.
- R14.** The Balancing Authority shall provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance. As a minimum, the Balancing Authority shall provide its operating personnel with real-time values for ACE, Interconnection frequency and Net Actual Interchange with each Adjacent Balancing Authority Area.
- R15.** The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing Authority's control center and other critical

locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.

R16. The Balancing Authority shall sample data at least at the same periodicity with which ACE is calculated. The Balancing Authority shall flag missing or bad data for operator display and archival purposes. The Balancing Authority shall collect coincident data to the greatest practical extent, i.e., ACE, Interconnection frequency, Net Actual Interchange, and other data shall all be sampled at the same time.

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25 % of full scale
Remote terminal unit	≤ 0.25 % of full scale
Potential transformer	≤ 0.30 % of full scale
Current transformer	≤ 0.50 % of full scale

C. Measures

Not specified.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Balancing Authorities shall be prepared to supply data to NERC in the format defined below:

- 1.1.1.** Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization CPS source data in daily CSV files with time stamped one minute averages of: 1) ACE and 2) Frequency Error.
- 1.1.2.** Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization DCS source data in CSV files with time stamped scan rate values for: 1) ACE and 2) Frequency Error for a time period of two minutes prior to thirty minutes after the identified Disturbance.

1.2. Compliance Monitoring Period and Reset Timeframe

Not specified.

1.3. Data Retention

- 1.3.1.** Each Balancing Authority shall retain its ACE, actual frequency, Scheduled Frequency, Net Actual Interchange, Net Scheduled Interchange, Tie Line meter error correction and Frequency Bias Setting data in digital format at the same scan rate at which the data is collected for at least one year.
- 1.3.2.** Each Balancing Authority or Reserve Sharing Group shall retain documentation of the magnitude of each Reportable Disturbance as well as the ACE charts and/or samples used to calculate Balancing Authority or

Reserve Sharing Group disturbance recovery values. The data shall be retained for one year following the reporting quarter for which the data was recorded.

1.4. Additional Compliance Information

Not specified.

2. Levels of Non-Compliance

Not specified.

E. Regional Differences

None identified.

F. Associated Documents

1. Appendix 1 — Interpretation of Requirement R17 (February 12, 2008).

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
0a	December 19, 2007	Added Appendix 1 – Interpretation of R17 approved by BOT on May 2, 2007	Addition
0a	January 16, 2008	Section F: added “1.”; changed hyphen to “en dash.” Changed font style for “Appendix 1” to Arial	Errata
0b	February 12, 2008	Replaced Appendix 1 – Interpretation of R17 approved by BOT on February 12, 2008 (BOT approved retirement of Interpretation included in BAL-005-0a)	Replacement
0.1b	October 29, 2008	BOT approved errata changes; updated version number to “0.1b”	Errata
0.1b	May 13, 2009	FERC approved – Updated Effective Date	Addition
0.2b	March 8, 2012	Errata adopted by Standards Committee; (replaced Appendix 1 with the FERC-approved revised interpretation of R17 and corrected standard version referenced in Interpretation by changing from “BAL-005-1” to “BAL-005-0)	Errata
0.2b	September 13, 2012	FERC approved – Updated Effective Date	Addition
0.2b	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
0.2b	November 21, 2013	R2 and associated elements approved by FERC	

		for retirement as part of the Paragraph 81 project (Project 2013-02) effective January 21, 2014.	
--	--	--	--

Appendix 1

Effective Date: August 27, 2008 (U.S.)

Interpretation of BAL-005-0 Automatic Generation Control, R17

Request for Clarification received from PGE on July 31, 2007

PGE requests clarification regarding the measuring devices for which the requirement applies, specifically clarification if the requirement applies to the following measuring devices:

- Only equipment within the operations control room
- Only equipment that provides values used to calculate AGC ACE
- Only equipment that provides values to its SCADA system
- Only equipment owned or operated by the BA
- Only to new or replacement equipment
- To all equipment that a BA owns or operates

BAL-005-0

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	$\leq 0.25\%$ of full scale
Remote terminal unit	$\leq 0.25\%$ of full scale
Potential transformer	$\leq 0.30\%$ of full scale
Current transformer	$\leq 0.50\%$ of full scale

Existing Interpretation Approved by Board of Trustees May 2, 2007

BAL-005-0, Requirement 17 requires that the Balancing Authority check and calibrate its control room time error and frequency devices against a common reference at least annually. The requirement to “annually check and calibrate” does not address any devices outside of the operations control room.

The table represents the design accuracy of the listed devices. There is no requirement within the standard to “annually check and calibrate” the devices listed in the table, unless they are included in the control center time error and frequency devices.

Interpretation provided by NERC Frequency Task Force on September 7, 2007 and Revised on November 16, 2007

As noted in the existing interpretation, BAL-005-0 Requirement 17 applies only to the time error and frequency devices that provide, or in the case of back-up equipment may provide, input into the reporting or compliance ACE equation or provide real-time time error or frequency information to the system operator. Frequency inputs from other sources that are for reference only are excluded. The time error and

frequency measurement devices may not necessarily be located in the system operations control room or owned by the Balancing Authority; however the Balancing Authority has the responsibility for the accuracy of the frequency and time error measurement devices. No other devices are included in R 17. The other devices listed in the table at the end of R17 are for reference only and do not have any mandatory calibration or accuracy requirements.

New or replacement equipment that provides the same functions noted above requires the same calibrations. Some devices used for time error and frequency measurement cannot be calibrated as such. In this case, these devices should be cross-checked against other properly calibrated equipment and replaced if the devices do not meet the required level of accuracy.

Appendix QC-BAL-005-0.2b
Provisions specific to the standard BAL-005-0.2b applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** Automatic Generation Control

2. **Number:** BAL-005-0.2b

3. **Purpose:** No specific provision

4. **Applicability:** No specific provision

5. **Effective Date:**

5.1. Adoption of the standard by the Régie de l'énergie: ~~October 30~~ Month xx, 2013~~x~~

5.2. Adoption of the appendix by the Régie de l'énergie: ~~October 30~~ Month xx, 2013~~x~~

5.3. Effective date of the standard and its appendix in Québec: Month xx, 201x

B. Requirements

~~No specific provision~~ Retirement of requirement R2.

C. Measures

No specific provision

D. Compliance

1. **Compliance Monitoring Process**

1.1. **Compliance Monitoring Responsibility**

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. **Compliance Monitoring Period and Reset Timeframe**

No specific provision

1.3. **Data Retention**

No specific provision

1.4. **Additional Compliance Information**

No specific provision

2. **Levels of Non-Compliance**

No specific provision

E. Regional Differences

No specific provision

Standard BAL-005-0.2b — Automatic Generation Control

Appendix QC-BAL-005-0.2b

Provisions specific to the standard BAL-005-0.2b applicable in Québec

F. Associated Documents

No specific provision

Appendix 1

No specific provision

Revision History

Revision	Adoption Date	Action	Change Tracking
0	October 30, 2013	New appendix	New
<u>1</u>	<u>Month xx, 201x</u>	<ul style="list-style-type: none">• <u>Modification of adoption dates</u>• <u>Retirement of requirement R2</u>	

A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003-1
3. **Purpose:** Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.
4. **Applicability:**
 - 4.1. Within the text of Standard CIP-003, “Responsible Entity” shall mean:
 - 4.1.1 Reliability Coordinator.
 - 4.1.2 Balancing Authority.
 - 4.1.3 Interchange Authority.
 - 4.1.4 Transmission Service Provider.
 - 4.1.5 Transmission Owner.
 - 4.1.6 Transmission Operator.
 - 4.1.7 Generator Owner.
 - 4.1.8 Generator Operator.
 - 4.1.9 Load Serving Entity.
 - 4.1.10 NERC.
 - 4.1.11 Regional Reliability Organizations.
 - 4.2. The following are exempt from Standard CIP-003:
 - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
 - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
 - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.
5. **Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-003:

- R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management’s commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:
 - R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
 - R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

- R1.3.** Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.
- R2.** Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
 - R2.1.** The senior manager shall be identified by name, title, business phone, business address, and date of designation.
 - R2.2.** Changes to the senior manager must be documented within thirty calendar days of the effective date.
 - R2.3.** The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.
- R3.** Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).
 - R3.1.** Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).
 - R3.2.** Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.
 - R3.3.** Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.
- R4.** Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
 - R4.1.** The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.
 - R4.2.** The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
 - R4.3.** The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.
- R5.** Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
 - R5.1.** The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
 - R5.1.1.** Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.
 - R5.1.2.** The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

- R5.2.** The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
- R5.3.** The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.
- R6.** Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-003:

- M1.** Documentation of the Responsible Entity's cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.
- M2.** Documentation of the assignment of, and changes to, the Responsible Entity's leadership as specified in Requirement R2.
- M3.** Documentation of the Responsible Entity's exceptions, as specified in Requirement R3.
- M4.** Documentation of the Responsible Entity's information protection program as specified in Requirement R4.
- M5.** The access control documentation as specified in Requirement R5.
- M6.** The Responsible Entity's change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

- 1.1.1** Regional Reliability Organizations for Responsible Entities.
- 1.1.2** NERC for Regional Reliability Organization.
- 1.1.3** Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

- 1.3.1** The Responsible Entity shall keep all documentation and records from the previous full calendar year.
- 1.3.2** The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

- 1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

- 1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.

2. Levels of Noncompliance

2.1. Level 1:

- 2.1.1 Changes to the designation of senior manager were not documented in accordance with Requirement R2.2; or,
- 2.1.2 Exceptions from the cyber security policy have not been documented within thirty calendar days of the approval of the exception; or,
- 2.1.3 An information protection program to identify and classify information and the processes to protect information associated with Critical Cyber Assets has not been assessed in the previous full calendar year.

2.2. Level 2:

- 2.2.1 A cyber security policy exists, but has not been reviewed within the previous full calendar year; or,
- 2.2.2 Exceptions to policy are not documented or authorized by the senior manager or delegate(s); or,
- 2.2.3 Access privileges to the information related to Critical Cyber Assets have not been reviewed within the previous full calendar year; or,
- 2.2.4 The list of designated personnel responsible to authorize access to the information related to Critical Cyber Assets has not been reviewed within the previous full calendar year.

2.3. Level 3:

- 2.3.1 A senior manager has not been identified in accordance with Requirement R2.1; or,
- 2.3.2 The list of designated personnel responsible to authorize logical or physical access to protected information associated with Critical Cyber Assets does not exist; or,
- 2.3.3 No changes to hardware and software components of Critical Cyber Assets have been documented in accordance with Requirement R6.

2.4. Level 4:

- 2.4.1 No cyber security policy exists; or,
- 2.4.2 No identification and classification program for protecting information associated with Critical Cyber Assets exists; or,
- 2.4.3 No documented change control and configuration management process exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

Standard CIP-003-1 — Cyber Security — Security Management Controls

Appendix QC-CIP-003-1 Provisions specific to the standard CIP-003-1 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003-1
3. **Purpose:** No specific provision
4. **Applicability:**
 - Functions**
 - 4.1. No specific provision
 - Facilities**
 - No specific provision
 - Exemptions**
 - 4.2. The following are exempt from Standard CIP-003:
 - 4.2.1 No specific provision
 - 4.2.2 No specific provision
 - 4.2.3 No specific provision
 - 4.2.4 Entities identified in the Register of Entities that have no Critical Assets.
5. **Effective Date:**
 - 5.1. Adoption of the standard by the Régie de l'énergie: October 30, 2013
 - 5.2. Adoption of the appendix by the Régie de l'énergie: ~~October 30~~Month xx, 2013x
 - 5.3. Effective date of the standard and its appendix in Québec: Month xx 201x

B. Requirements

~~No specific provision~~Retirement of requirements R1.2, R3, R3.1, R3.2, R3.3 and R4.2.

C. Measures

~~No specific provision~~Retirement of measures M1 and M3.

D. Compliance

1. **Compliance Monitoring Process**
 - 1.1. **Compliance Monitoring Responsibility**
 - 1.1.1 The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.
 - 1.1.2 No specific provision
 - 1.1.3 No specific provision

1.2. Compliance Monitoring Period and Reset Time Frame

No specific provision

1.3. Data Retention

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Levels of Non-Compliance

No specific provision

E. Regional Differences

No specific provision

Revision History

Revision	Adoption Date	Action	Change Tracking
0	July 25, 2012	New appendix (decision D-2012-091)	New
1	October 30, 2013	<ul style="list-style-type: none"> Removed "Responsible" from section 4.2.4 Use of a new template Capitalized the term "Register of Entities" 	Revised
<u>2</u>	<u>Month xx, 201x</u>	<ul style="list-style-type: none"> <u>Retirement of requirements R1.2, R3, R3.1, R3.2, R3.3 and R4.2, and associated measures</u> <u>Modification of the adoption date of the appendix</u> 	<u>Revised</u>

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-1
3. **Purpose:** Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.
4. **Applicability**
 - 4.1. Within the text of Standard CIP-005, “Responsible Entity” shall mean:
 - 4.1.1 Reliability Coordinator.
 - 4.1.2 Balancing Authority.
 - 4.1.3 Interchange Authority.
 - 4.1.4 Transmission Service Provider.
 - 4.1.5 Transmission Owner.
 - 4.1.6 Transmission Operator.
 - 4.1.7 Generator Owner.
 - 4.1.8 Generator Operator.
 - 4.1.9 Load Serving Entity.
 - 4.1.10 NERC.
 - 4.1.11 Regional Reliability Organizations.
 - 4.2. The following are exempt from Standard CIP-005:
 - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
 - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
 - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.
5. **Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-005:

- R1.** Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
 - R1.1.** Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
 - R1.2.** For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

- R1.3.** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
- R1.4.** Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.
- R1.5.** Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.
- R1.6.** The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.
- R2.** Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
 - R2.1.** These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
 - R2.2.** At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
 - R2.3.** The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).
 - R2.4.** Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
 - R2.5.** The required documentation shall, at least, identify and describe:
 - R2.5.1.** The processes for access request and authorization.
 - R2.5.2.** The authentication methods.
 - R2.5.3.** The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.
 - R2.5.4.** The controls used to secure dial-up accessible connections.
 - R2.6.** Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.
- R3.** Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

- R3.1.** For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.
- R3.2.** Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.
- R4.** Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
 - R4.1.** A document identifying the vulnerability assessment process;
 - R4.2.** A review to verify that only ports and services required for operations at these access points are enabled;
 - R4.3.** The discovery of all access points to the Electronic Security Perimeter;
 - R4.4.** A review of controls for default accounts, passwords, and network management community strings; and,
 - R4.5.** Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.
- R5.** Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.
 - R5.1.** The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
 - R5.2.** The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
 - R5.3.** The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-005. Responsible entities may document controls either individually or by specified applicable grouping.

- M1.** Documents about the Electronic Security Perimeter as specified in Requirement R1.
- M2.** Documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.
- M3.** Documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.
- M4.** Documentation of the Responsible Entity's annual vulnerability assessment as specified in Requirement R4.
- M5.** Access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless longer retention is required pursuant to Standard CIP-008, Requirement R2.

1.3.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005 from the previous full calendar year.

1.3.3 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 All document(s) identified in CIP-005 exist, but have not been updated within ninety calendar days of any changes as required; or,

2.1.2 Access to less than 15% of electronic security perimeters is not controlled, monitored; and logged;

2.1.3 Document(s) exist confirming that only necessary network ports and services have been enabled, but no record documenting annual reviews exists; or,

2.1.4 At least one, but not all, of the Electronic Security Perimeter vulnerability assessment items has been performed in the last full calendar year.

2.2. Level 2:

2.2.1 All document(s) identified in CIP-005 but have not been updated or reviewed in the previous full calendar year as required; or,

2.2.2 Access to between 15% and 25% of electronic security perimeters is not controlled, monitored; and logged; or,

2.2.3 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed in the previous full calendar year.

2.3. Level 3:

- 2.3.1** A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Cyber Assets not within the defined Electronic Security Perimeter(s); or,
 - 2.3.2** One or more identified non-critical Cyber Assets is within the Electronic Security Perimeter(s) but not documented; or,
 - 2.3.3** Electronic access controls document(s) exist, but one or more access points have not been identified; or
 - 2.3.4** Electronic access controls document(s) do not identify or describe access controls for one or more access points; or,
 - 2.3.5** Electronic Access Monitoring:
 - 2.3.5.1** Access to between 26% and 50% of Electronic Security Perimeters is not controlled, monitored; and logged; or,
 - 2.3.5.2** Access logs exist, but have not been reviewed within the past ninety calendar days; or,
 - 2.3.6** Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than two full calendar years.
- 2.4. Level 4:**
- 2.4.1** No documented Electronic Security Perimeter exists; or,
 - 2.4.2** No records of access exist; or,
 - 2.4.3** 51% or more Electronic Security Perimeters are not controlled, monitored, and logged; or,
 - 2.4.4** Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than three full calendar years; or,
 - 2.4.5** No documented vulnerability assessment of the Electronic Security Perimeter(s) process exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-1

3. **Purpose:** No specific provision

4. **Applicability:**

Functions

4.1. No specific provision

Facilities

No specific provision

Exemptions

4.2. The following are exempt from Standard CIP-005:

4.2.1 No specific provision

4.2.2 No specific provision

4.2.3 No specific provision

4.2.4 Entities identified in the Register of Entities that have no Critical Assets.

5. **Effective Date:**

5.1. Adoption of the standard by the Régie de l'énergie: October 30, 2013

5.2. Adoption of the appendix by the Régie de l'énergie: ~~October 30~~Month xx, 2013x

5.3. Effective date of the standard and its appendix in Québec: Month xx 201x

B. Requirements

~~No specific provision~~Retirement of requirement R2.6.

C. Measures

No specific provision

D. Compliance

1. **Compliance Monitoring Process**

1.1. **Compliance Monitoring Responsibility**

1.1.1 The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.1.2 No specific provision

1.1.3 No specific provision

1.2. Compliance Monitoring Period and Reset Time Frame

No specific provision

1.3. Data Retention

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Levels of Non-Compliance

No specific provision

E. Regional Differences

No specific provision

Revision History

Revision	Adoption Date	Action	Change Tracking
0	July 25, 2012	New appendix (decision D-2012-091)	New
1	October 30 2013	<ul style="list-style-type: none">Removed "Responsible" from section 4.2.4Use of a new templateCapitalized the term "Register of Entities"	Revised
<u>2</u>	<u>Month xx, 201x</u>	<ul style="list-style-type: none"><u>Retirement of requirement R2.6</u><u>Modification of the adoption date of the appendix</u>	<u>Revised</u>

A. Introduction

1. **Title:** Cyber Security — Systems Security Management
2. **Number:** CIP-007-1
3. **Purpose:** Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.
4. **Applicability:**
 - 4.1. Within the text of Standard CIP-007, “Responsible Entity” shall mean:
 - 4.1.1 Reliability Coordinator.
 - 4.1.2 Balancing Authority.
 - 4.1.3 Interchange Authority.
 - 4.1.4 Transmission Service Provider.
 - 4.1.5 Transmission Owner.
 - 4.1.6 Transmission Operator.
 - 4.1.7 Generator Owner.
 - 4.1.8 Generator Operator.
 - 4.1.9 Load Serving Entity.
 - 4.1.10 NERC.
 - 4.1.11 Regional Reliability Organizations.
 - 4.2. The following are exempt from Standard CIP-007:
 - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
 - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
 - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.
5. **Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):

- R1.** Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

- R1.1.** The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.
- R1.2.** The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.
- R1.3.** The Responsible Entity shall document test results.
- R2.** Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
 - R2.1.** The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
 - R2.2.** The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
 - R2.3.** In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.
- R3.** Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
 - R3.1.** The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
 - R3.2.** The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.
- R4.** Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
 - R4.1.** The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.
 - R4.2.** The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures.
- R5.** Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
 - R5.1.** The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.

- R5.1.1.** The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.
 - R5.1.2.** The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.
 - R5.1.3.** The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.
- R5.2.** The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
 - R5.2.1.** The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.
 - R5.2.2.** The Responsible Entity shall identify those individuals with access to shared accounts.
 - R5.2.3.** Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
- R5.3.** At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:
 - R5.3.1.** Each password shall be a minimum of six characters.
 - R5.3.2.** Each password shall consist of a combination of alpha, numeric, and “special” characters.
 - R5.3.3.** Each password shall be changed at least annually, or more frequently based on risk.
- R6.** Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
 - R6.1.** The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
 - R6.2.** The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
 - R6.3.** The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
 - R6.4.** The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
 - R6.5.** The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

- R7.** Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
- R7.1.** Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
- R7.2.** Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
- R7.3.** The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.
- R8.** Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
- R8.1.** A document identifying the vulnerability assessment process;
- R8.2.** A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;
- R8.3.** A review of controls for default accounts; and,
- R8.4.** Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.
- R9.** Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-007:

- M1.** Documentation of the Responsible Entity's security test procedures as specified in Requirement R1.
- M2.** Documentation as specified in Requirement R2.
- M3.** Documentation and records of the Responsible Entity's security patch management program, as specified in Requirement R3.
- M4.** Documentation and records of the Responsible Entity's malicious software prevention program as specified in Requirement R4.
- M5.** Documentation and records of the Responsible Entity's account management program as specified in Requirement R5.
- M6.** Documentation and records of the Responsible Entity's security status monitoring program as specified in Requirement R6.
- M7.** Documentation and records of the Responsible Entity's program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.
- M8.** Documentation and records of the Responsible Entity's annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

- M9.** Documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The Responsible Entity shall retain security-related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008 Requirement R2.

1.3.3 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information.

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 System security controls are in place, but fail to document one of the measures (M1-M9) of Standard CIP-007; or

2.1.2 One of the documents required in Standard CIP-007 has not been reviewed in the previous full calendar year as specified by Requirement R9; or,

2.1.3 One of the documented system security controls has not been updated within ninety calendar days of a change as specified by Requirement R9; or,

2.1.4 Any one of:

- Authorization rights and access privileges have not been reviewed during the previous full calendar year; or,
- A gap exists in any one log of system events related to cyber security of greater than seven calendar days; or,
- Security patches and upgrades have not been assessed for applicability within thirty calendar days of availability.

2.2. Level 2:

2.2.1 System security controls are in place, but fail to document up to two of the measures (M1-M9) of Standard CIP-007; or,

2.2.2 Two occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.3. Level 3:

2.3.1 System security controls are in place, but fail to document up to three of the measures (M1-M9) of Standard CIP-007; or,

2.3.2 Three occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.4. Level 4:

2.4.1 System security controls are in place, but fail to document four or more of the measures (M1-M9) of Standard CIP-007; or,

2.4.2 Four occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.4.3 No logs exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** Cyber Security — Systems Security Management

2. **Number:** CIP-007-1

3. **Purpose:** No specific provision

4. **Applicability:**

Functions

4.1. No specific provision

Facilities

No specific provision

Exemptions

4.2. The following are exempt from Standard CIP-007:

4.2.1 No specific provision

4.2.2 No specific provision

4.2.3 No specific provision

4.2.4 Entities identified in the Register of Entities that have no Critical Assets.

5. **Effective Date:**

5.1. Adoption of the standard by the Régie de l'énergie: October 30, 2013

5.2. Adoption of the appendix by the Régie de l'énergie: ~~October 30~~Month xx, 2013x

5.3. Effective date of the standard and its appendix in Québec: Month xx 201x

B. Requirements

~~No specific provision~~Retirement of requirement R7.3.

C. Measures

No specific provision

D. Compliance

1. **Compliance Monitoring Process**

1.1. **Compliance Monitoring Responsibility**

1.1.1 The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.1.2 No specific provision

1.1.3 No specific provision

1.2. Compliance Monitoring Period and Reset Time Frame

No specific provision

1.3. Data Retention

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Levels of Non-Compliance

No specific provision

E. Regional Differences

No specific provision

Revision History

Revision	Adoption Date	Action	Change Tracking
0	July 25, 2012	New appendix (decision D-2012-091)	New
1	October 30, 2013	<ul style="list-style-type: none">Removed "Responsible" from section 4.2.4Use of a new templateCapitalized the term "Register of Entities"	Revised
<u>2</u>	<u>Month xx, 201x</u>	<ul style="list-style-type: none"><u>Retirement of requirement R7.3</u><u>Modification of the adoption date of the appendix</u>	

A. Introduction

1. **Title:** Coordination of Plans For New Generation, Transmission, and End-User Facilities
2. **Number:** FAC-002-1
3. **Purpose:** To avoid adverse impacts on reliability, Generator Owners and Transmission Owners and electricity end-users must meet facility connection and performance requirements.
4. **Applicability:**
 - 4.1. Generator Owner
 - 4.2. Transmission Owner
 - 4.3. Distribution Provider
 - 4.4. Load-Serving Entity
 - 4.5. Transmission Planner
 - 4.6. Planning Authority
5. **(Proposed) Effective Date:** The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

B. Requirements

- R1. The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:
 - 1.1. Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.
 - 1.2. Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.
 - 1.3. Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.
 - 1.4. Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance under both normal and contingency conditions in accordance with Reliability Standards TPL-001-0, TPL-002-0, and TPL-003-0.
 - 1.5. Documentation that the assessment included study assumptions, system performance, alternatives considered, and jointly coordinated recommendations.
- R2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional

Reliability Organization(s) and NERC on request (within 30 calendar days). (Retirement approved by FERC effective January 21, 2014.)

C. Measures

- M1.** The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider's documentation of its assessment of the reliability impacts of new facilities shall address all items in Reliability Standard FAC-002-0_R1.
- M2.** The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each have evidence of its assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems is retained and provided to other entities in accordance with Reliability Standard FAC-002-0_R2. (Retirement approved by FERC effective January 21, 2014.)

D. Compliance**1. Compliance Monitoring Process****1.1. Compliance Enforcement Authority**

Regional Entity.

1.2. Compliance Monitoring Period and Reset Timeframe

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

Evidence of the assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems: Three years.

1.5. Additional Compliance Information

None

2. Violation Severity Levels (no changes)**E. Regional Differences**

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	January 13, 2006	Removed duplication of "Regional Reliability Organizations(s).	Errata
1	August 5, 2010	Modified to address Order No. 693 Directives	Revised.

Standard FAC-002-1 — Coordination of Plans for New Facilities

		contained in paragraph 693. Adopted by the NERC Board of Trustees.	
1	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
1	November 21, 2013	R2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

Appendix QC-FAC-002-1
Provisions specific to the standard FAC-002-1 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

- 1. Title:** Coordination of Plans For New Generation, Transmission, and End-User Facilities
- 2. Number:** FAC-002-1
- 3. Purpose:** No specific provision
- 4. Applicability:** No specific provision
- 5. Effective Date:**
 - 5.1.** Adoption of the standard by the Régie: Month xx, 201x
 - 5.2.** Adoption of the appendix by the Régie: Month xx, 201x
 - 5.3.** Effective date of the standard and its appendix in Québec: Month xx, 201x

B. Requirements

- R1.** No specific provision
- R1.1.** No specific provision
- R1.2.** No specific provision
- R1.3.** No specific provision
- R1.4.** Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance under both normal and contingency conditions in accordance with Reliability Standards TPL-001-0.1, TPL-002-0.b, and TPL-003-0.a. For facilities that are not par of the Bulk Power System, compliance with standards TPL-001-0.1, TPL-002-0.b and TPL-003-0.a is not required.
- R1.5.** No specific provision
- R2.** ~~No specific provision~~ Requirement retired.

C. Measures

Specific provision applicable to measures M1 and M2: the reference to standard FAC-002-0 is replaced by the reference to standard FAC-002-1.

Retirement of measure M2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.

1.2. Compliance Monitoring Period and Reset Timeframe

No specific provision

1.3. Compliance Monitoring and Enforcement Processes

No specific provision

1.4. Data Retention

No specific provision

1.5. Additional Compliance Information

No specific provision

Appendix QC-FAC-002-1
Provisions specific to the standard FAC-002-1 applicable in Québec

2. Violation Severity Levels

Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The responsible entity failed to include in its assessment one of the subcomponents (R1.1 to R1.5).	The responsible entity failed to include in its assessment two of the subcomponents (R1.1 to R1.5).	The responsible entity failed to include in its assessment three of the subcomponents (R1.1 to R1.5).	The responsible entity failed to include in its assessment four of the subcomponents (R1.1 to R1.5).
R1.1.	N/A	N/A	N/A	N/A
R1.2.	N/A	N/A	N/A	N/A
R1.3.	N/A	N/A	N/A	N/A
R1.4.	N/A	N/A	N/A	N/A
R1.5.	N/A	N/A	N/A	N/A
R2. (Requirement retired)	The responsible entity provided the documentation more than 30 calendar days, but less than or equal to 40 calendar days, after a request.	The responsible entity provided the documentation more than 40 calendar days, but less than or equal to 50 calendar days, after a request.	The responsible entity provided the documentation more than 50 calendar days, but less than or equal to 60 calendar days, after a request.	The responsible entity provided the documentation more than 60 calendar days after a request or was unable to provide the documentation for the required three-year period.

Standard FAC-002-1 — Coordination of Plans for New Facilities

Appendix QC-FAC-002-1

Provisions specific to the standard FAC-002-1 applicable in Québec

E. Regional Differences

No specific provision

Revision History

Revision	Adoption Date	Action	Change Tracking
0	Month xx, 201x	New appendix	New

A. Introduction

- 1. Title:** System Operating Limits Methodology for the Planning Horizon
- 2. Number:** FAC-010-2.1
- 3. Purpose:** To ensure that System Operating Limits (SOLs) used in the reliable planning of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.
- 4. Applicability**
 - 4.1. Planning Authority**
- 5. Effective Date:** April 19, 2010

B. Requirements

- R1.** The Planning Authority shall have a documented SOL Methodology for use in developing SOLs within its Planning Authority Area. This SOL Methodology shall:
 - R1.1.** Be applicable for developing SOLs used in the planning horizon.
 - R1.2.** State that SOLs shall not exceed associated Facility Ratings.
 - R1.3.** Include a description of how to identify the subset of SOLs that qualify as IROLs.
- R2.** The Planning Authority's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:
 - R2.1.** In the pre-contingency state and with all Facilities in service, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect expected system conditions and shall reflect changes to system topology such as Facility outages.
 - R2.2.** Following the single Contingencies¹ identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.
 - R2.2.1.** Single line to ground or three-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.
 - R2.2.2.** Loss of any generator, line, transformer, or shunt device without a Fault.
 - R2.2.3.** Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.
 - R2.3.** Starting with all Facilities in service, the system's response to a single Contingency, may include any of the following:
 - 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 R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.

- R2.3.2.** System reconfiguration through manual or automatic control or protection actions.
 - 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.
 - R2.5.** Starting with all Facilities in service and following any of the multiple Contingencies identified in Reliability Standard TPL-003 the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.
 - R2.6.** In determining the system's response to any of the multiple Contingencies, identified in Reliability Standard TPL-003, in addition to the actions identified in R2.3.1 and R2.3.2, the following shall be acceptable:
 - R2.6.1.** Planned or 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) electric power Transfers.
- R3.** The Planning Authority's methodology for determining SOLs, shall 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 Planning Authority Area as well as the critical modeling details from other Planning Authority Areas that would impact the Facility or Facilities under study).
 - R3.2.** Selection of applicable Contingencies.
 - R3.3.** Level of detail of system models used to determine SOLs.
 - R3.4.** Allowed uses of Special Protection Systems or Remedial Action Plans.
 - R3.5.** Anticipated transmission system configuration, generation dispatch and Load level.
 - R3.6.** Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_v .
- R4.** The Planning Authority shall issue its SOL Methodology, and any change to that methodology, to all of the following prior to the effectiveness of the change:
 - R4.1.** Each adjacent Planning Authority and each Planning Authority that indicated it has a reliability-related need for the methodology.
 - R4.2.** Each Reliability Coordinator and Transmission Operator that operates any portion of the Planning Authority's Planning Authority Area.
 - R4.3.** Each Transmission Planner that works in the Planning Authority's Planning Authority Area.
- R5.** If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why. (Retirement approved by FERC effective January 21, 2014.)

C. Measures

- M1.** The Planning Authority's SOL Methodology shall address all of the items listed in Requirement 1 through Requirement 3.

- M2.** The Planning Authority shall have evidence it issued its SOL Methodology and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.

If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Planning Authority that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5. (Retirement approved by FERC effective January 21, 2014.)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Planning Authority shall self-certify its compliance to the Compliance Monitor at least once every three years. New Planning Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

1.3. Data Retention

The Planning Authority shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years.~~ In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. (Deleted text retired-Retirement approved by FERC effective January 21, 2014.)

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Planning Authority shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology.

Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses.
(Retirement approved by FERC effective January 21, 2014.)

1.4.2 Superseded portions of its SOL Methodology that had been made within the past 12 months.

1.4.3 Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.

2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)

2.1. Level 1: There shall be a level one non-compliance if either of the following conditions exists:

2.1.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.

- 2.1.2** No evidence of responses to a recipient's comments on the SOL Methodology.
(Retirement approved by FERC effective January 21, 2014.)
- 2.2. Level 2:** The SOL Methodology did not include a requirement to address all of the elements in R2.1 through R2.3 and E1.
- 2.3. Level 3:** There shall be a level three non-compliance if any of the following conditions exists:
 - 2.3.1** The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.
 - 2.3.2** The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.
 - 2.3.3** The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.
- 2.4. Level 4:** The SOL Methodology was not issued to all required entities in accordance with R4

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

3. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.2	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.3.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.1. OR The Planning Authority has no documented SOL Methodology for use in developing SOLs within its Planning Authority Area.
R2	The Planning Authority's SOL Methodology is missing one requirement as described in R2.1, R2.2, R2.3, R2.4, R2.5, or R2.6.	The Planning Authority's SOL Methodology is missing two requirements as described in R2.1, R2.2, R2.3, R2.4, R2.5, or R2.6	The Planning Authority's SOL Methodology is missing three requirements as described in R2.1, R2.2, R2.3, R2.4, R2.5, or R2.6.	The Planning Authority's SOL Methodology is missing four or more requirements as described in R2.1, R2.2-, R2.3, R2.4, R2.5, or R2.6
R3	The Planning Authority has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that is missing a description of four or more of the following: R3.1 through R3.6.
R4	One or both of the following: The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	One of the following: The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR	One of the following: The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR	One of the following: The Planning Authority failed to issue its SOL Methodology and changes to that methodology to more than three of the required entities. The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

Requirement	Lower	Moderate	High	Severe
		<p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change.</p> <p>OR</p> <p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>provided 90 calendar days or more after the effectiveness of the change.</p> <p>OR</p> <p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change.</p> <p>OR</p> <p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change.</p> <p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but four of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>
R5 (Retirement)	The Planning Authority received documented technical comments on its SOL Methodology and	The Planning Authority received documented technical comments on its SOL Methodology and	The Planning Authority received documented technical comments on its SOL Methodology and	The Planning Authority received documented technical comments on its SOL Methodology and

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

Requirement	Lower	Moderate	High	Severe
approved by FERC effective January 21, 2014.)	provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Planning Authority's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	provided a complete response in a time period that was 90 calendar days or longer. OR The Planning Authority's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.

E. Regional Differences

- 1.** The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:
 - 1.1.** As governed by the requirements of R2.5 and R2.6, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:
 - 1.1.1** Simultaneous permanent phase to ground Faults on different phases of each of two 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 towers at each station, then this condition is an acceptable risk and therefore can be excluded.
 - 1.1.2** A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7
 - 1.1.3** Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.
 - 1.1.4** The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.
 - 1.1.5** A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.
 - 1.1.6** A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-010.
 - 1.1.7** The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.
 - 1.2.** SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:
 - 1.2.1** All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.
 - 1.2.2** Cascading does not occur.
 - 1.2.3** Uncontrolled separation of the system does not occur.
 - 1.2.4** The system demonstrates transient, dynamic and voltage stability.
 - 1.2.5** 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) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.
 - 1.2.6** Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

- 1.2.7** To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.
- 1.3.** SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:
- 1.3.1** Cascading does not occur.
- 1.4.** The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
1	November 1, 2006	Fixed typo. Removed the word “each” from the 1 st sentence of section D.1.3, Data Retention.	01/11/07
2	June 24, 2008	Adopted by Board of Trustees; FERC Order 705	Revised
2		Changed the effective date to July 1, 2008 Changed “Cascading Outage” to “Cascading” Replaced Levels of Non-compliance with Violation Severity Levels	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2.1	November 5, 2009	Adopted by the Board of Trustees — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	April 19, 2010	FERC Approved — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	February 7, 2013	R5 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

2.1	November 21, 2013	R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	
2.1	February 24, 2014	Updated VSLs based on June 24, 2013 approval.	

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

Appendix QC-FAC-010-2.1

Provisions specific to the standard FAC-010-2.1 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** System Operating Limits Methodology for the Planning Horizon

2. **Number:** FAC-010-2.1

3. **Purpose:** No specific provision

4. **Applicability:**

Functions

No specific provision

Facilities

This standard only applies to the facilities of the Main Transmission System (RTP)

5. **Effective Date:**

5.1. Adoption of the standard by the Régie de l'énergie: Month xx, 201x

5.2. Adoption of the appendix by the Régie de l'énergie: Month xx, 201x

5.3. Effective date of the standard and its appendix in Québec: Month xx, -201x

B. Requirements

~~No specific provision~~ Retirement of requirement R5 and its associated elements.

C. Measures

~~No specific provision~~ Retirement of measure M3 and its associated elements.

D. Compliance

1. **Compliance Monitoring Process**

1.1. **Compliance Monitoring Responsibility**

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. **Compliance Monitoring Period and Reset Time Frame**

No specific provision

1.3. **Data Retention**

No specific provision

1.4. **Additional Compliance Information**

No specific provision

2. **Levels of Non-Compliance for Western Interconnection**

No specific provision

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

Appendix QC-FAC-010-2.1

Provisions specific to the standard FAC-010-2.1 applicable in Québec

3. Violation Severity Levels

No specific provision

E. Regional Differences

No specific provision

Revision History

Revision	Adoption Date	Action	Change Tracking
0	Month xx, 201x	New appendix	New

A. Introduction

1. **Title:** System Operating Limits Methodology for the Operations Horizon
2. **Number:** FAC-011-2
3. **Purpose:** To ensure that System Operating Limits (SOLs) used in the reliable operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.
4. **Applicability**
 - 4.1. Reliability Coordinator
5. **Effective Date:** April 29, 2009

B. Requirements

- R1.** The Reliability Coordinator shall have a documented methodology for use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:
 - R1.1.** Be applicable for developing SOLs used in the operations horizon.
 - R1.2.** State that SOLs shall not exceed associated Facility Ratings.
 - R1.3.** Include a description of how to identify the subset of SOLs that qualify as IROLs.
- R2.** The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:
 - R2.1.** In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect current or expected system conditions and shall reflect changes to system topology such as Facility outages.
 - R2.2.** Following the single Contingencies¹ identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.
 - R2.2.1.** Single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.
 - R2.2.2.** Loss of any generator, line, transformer, or shunt device without a Fault.
 - 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 shall 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 R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be 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
 - R2.3.3.** System reconfiguration through manual or automatic control or protection actions.
 - 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 Reliability Coordinator's methodology for determining SOLs, shall 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 Reliability Coordinator 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 (provided by the Planning Authority in accordance with FAC-014 Requirement 6) are applicable for use in the operating horizon given the actual or expected system conditions.
 - R3.3.1.** This process shall 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 SOLs.
 - R3.5.** Allowed uses of Special Protection Systems or Remedial Action Plans.
 - R3.6.** Anticipated transmission system configuration, generation dispatch and Load level
 - R3.7.** Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_v .
- R4.** The Reliability Coordinator shall issue its SOL Methodology and any changes to that methodology, prior to the effectiveness 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 Reliability Coordinator's Reliability Coordinator Area.
 - R4.3.** Each Transmission Operator that operates in the Reliability Coordinator Area.
- R5.** If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why. (Retirement approved by FERC effective January 21, 2014.)

C. Measures

- M1.** The Reliability Coordinator's SOL Methodology shall address all of the items listed in Requirement 1 through Requirement 3.
- M2.** The Reliability Coordinator shall have evidence it issued its SOL Methodology, and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.
- M3.** If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Reliability Coordinator that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5. (Retirement approved by FERC effective January 21, 2014.)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Reliability Coordinator shall self-certify its compliance to the Compliance Monitor at least once every three years. New Reliability Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

1.3. Data Retention

The Reliability Coordinator shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years.~~ In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. (Deleted text retired-Retirement approved by FERC effective January 21, 2014.)

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Reliability Coordinator shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology.

1.4.2 Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses.
(Retirement approved by FERC effective January 21, 2014.)

- 1.4.3** Superseded portions of its SOL Methodology that had been made within the past 12 months.
 - 1.4.4** Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.
- 2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)**
 - 2.1. Level 1:** There shall be a level one non-compliance if either of the following conditions exists:
 - 2.1.1** The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.
 - 2.1.2** No evidence of responses to a recipient's comments on the SOL Methodology (Retirement approved by FERC effective January 21, 2014.)
 - 2.2. Level 2:** The SOL Methodology did not include a requirement to address all of the elements in R3.1, R3.2, R3.4 through R3.7 and E1.
 - 2.3. Level 3:** There shall be a level three non-compliance if any of the following conditions exists:
 - 2.3.1** The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.
 - 2.3.2** The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.
 - 2.3.3** The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.1, R3.2, R3.4 through R3.7.
 - 2.4. Level 4:** The SOL Methodology was not issued to all required entities in accordance with R4.

3. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.2	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.3.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.1. OR The Reliability Coordinator has no documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area.
R2	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance following single contingencies, but does not require that SOLs are set to meet BES performance in the pre-contingency state. (R2.1)	Not applicable.	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state, but does not require that SOLs are set to meet BES performance following single contingencies. (R2.2 – R2.4)	The Reliability Coordinator's SOL Methodology does not require that SOLs are set to meet BES performance in the pre-contingency state and does not require that SOLs are set to meet BES performance following single contingencies. (R2.1 through R2.4)
R3	The Reliability Coordinator's SOL Methodology includes a description for all but one of the following: R3.1 through R3.7.	The Reliability Coordinator's SOL Methodology includes a description for all but two of the following: R3.1 through R3.7.	The Reliability Coordinator's SOL Methodology includes a description for all but three of the following: R3.1 through R3.7.	The Reliability Coordinator's SOL Methodology is missing a description of four or more of the following: R3.1 through R3.7.
R3.6	N/A	N/A	N/A	N/A
R4	The Reliability Coordinator failed to issue its SOL Methodology and/or one or more changes to that methodology to one of the required entities specified in R4.1, R4.2, and R4.3.	The Reliability Coordinator failed to issue its SOL Methodology and/or one or more changes to that methodology to two of the required entities specified in R4.1, R4.2, and R4.3.	The Reliability Coordinator failed to issue its SOL Methodology and/or one or more changes to that methodology to three of the required entities specified in R4.1, R4.2, and R4.3.	The Reliability Coordinator failed to issue its SOL Methodology and/or one or more changes to that methodology to four or more of the required entities specified in R4.1, R4.2, and R4.3

Requirement	Lower	Moderate	High	Severe
	<p>OR</p> <p>For a change in methodology, the changed methodology was provided to one or more of the required entities before the effectiveness of the change, but was provided to all the required entities no more than 10 calendar days after the effectiveness of the change.</p>	<p>OR</p> <p>For a change in methodology, the changed methodology was provided to one or more of the required entities more than 10 calendar days after the effectiveness of the change, but less than or equal to 20 days after the effectiveness of the change.</p>	<p>OR</p> <p>For a change in methodology, the changed methodology was provided to one or more of the required entities more than 20 calendar days after the effectiveness of the change, but less than or equal to 30 days after the effectiveness of the change.</p>	<p>OR</p> <p>For a change in methodology, the changed methodology was provided to one or more of the required entities more than 30 calendar days after the effectiveness of the change.</p>
<p>R5 (Retirement approved by FERC effective January 21, 2014.)</p>	<p>The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.</p>	<p>The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.</p>	<p>The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days.</p> <p>OR</p> <p>The Reliability Coordinator's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.</p>	<p>The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer.</p> <p>OR</p> <p>The Reliability Coordinator's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.</p>

Regional Differences

- 1.** The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:
 - 1.1.** As governed by the requirements of R3.3, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:
 - 1.1.1** Simultaneous permanent phase to ground Faults on different phases of each of two 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 towers at each station, then this condition is an acceptable risk and therefore can be excluded.
 - 1.1.2** A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7
 - 1.1.3** Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.
 - 1.1.4** The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.
 - 1.1.5** A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.
 - 1.1.6** A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-011.
 - 1.1.7** The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.
 - 1.2.** SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:
 - 1.2.1** All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.
 - 1.2.2** Cascading does not occur.
 - 1.2.3** Uncontrolled separation of the system does not occur.
 - 1.2.4** The system demonstrates transient, dynamic and voltage stability.
 - 1.2.5** 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) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.
 - 1.2.6** Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

- 1.2.7** To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.
- 1.3.** SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:
- 1.3.1** Cascading does not occur.
- 1.4.** The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
2		Changed the effective date to October 1, 2008 Changed “Cascading Outage” to “Cascading” Replaced Levels of Non-compliance with Violation Severity Levels Corrected footnote 1 to reference FAC-011 rather than FAC-010	Revised
2	June 24, 2008	Adopted by Board of Trustees: FERC Order 705	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2	February 7, 2013	R5 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
2	November 21, 2013	R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	
2	February 24, 2014	Updated VSLs based on June 24, 2013 approval.	

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** System Operating Limits Methodology for the Operations Horizon

2. **Number:** FAC-011-2

3. **Purpose:** No specific provision

4. **Applicability:**

Functions

No specific provision

Facilities

This standard only applies to the facilities of the Main Transmission System (RTP).

5. **Effective Date:**

5.1. Adoption of the standard by the Régie de l'énergie: Month xx, 201x

5.2. Adoption of the appendix by the Régie de l'énergie: Month xx, 201x

5.3. Effective date of the standard and its appendix in Québec: Month xx, 201x

B. Requirements

~~No specific provision~~ Retirement of requirement R5 and its associated elements.

C. Measures

~~No specific provision~~ Retirement of measure M3 and its associated elements.

D. Compliance

1. **Compliance Monitoring Process**

1.1. **Compliance Monitoring Responsibility**

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. **Compliance Monitoring Period and Reset Time Frame**

No specific provision

1.3. **Data Retention**

No specific provision

1.4. **Additional Compliance Information**

No specific provision

2. **Levels of Non-Compliance**

No specific provision

3. Violation Severity Levels

All occurrences of the term “BES” are replaced by “RTP”.

E. Regional Differences

No specific provision

Revision History

Revision	Adoption Date	Action	Change Tracking
0	Month xx, 201x	New appendix	New

A. Introduction

1. **Title:** Coordination of Real-time Activities Between Reliability Coordinators
2. **Number:** IRO-016-1
3. **Purpose:** To ensure that each Reliability Coordinator's operations are coordinated such that they will not have an Adverse Reliability Impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations.
4. **Applicability**
 - 4.1. Reliability Coordinator
5. **Effective Date:** November 1, 2006

B. Requirements

- R1. The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.
 - R1.1. If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.
 - R1.2. If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).
 - R1.2.1. If time permits, this re-evaluation shall be done before taking corrective actions.
 - R1.2.2. If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.
 - R1.3. If the involved Reliability Coordinators cannot agree on the solution, the more conservative solution shall be implemented.
- R2. The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.

(Retirement approved by FERC effective January 21, 2014.)

C. Measures

- M1. For each event that requires Reliability Coordinator-to-Reliability Coordinator coordination, each involved Reliability Coordinator shall have evidence (operator logs or other data sources) of the actions taken for either the event or for the disagreement on the problem or for both.

D. Compliance

1. **Compliance Monitoring Process**
 - 1.1. **Compliance Monitoring Responsibility**

Regional Reliability Organization
 - 1.2. **Compliance Monitoring Period and Reset Time Frame**

The performance reset period shall be one calendar year.

1.3. Data Retention

The Reliability Coordinator shall keep auditable evidence for a rolling 12 months. In addition, entities found non-compliant shall keep information related to the non-compliance until it has been found compliant. The Compliance Monitor shall keep compliance data for a minimum of three years or until the Reliability Coordinator has achieved full compliance, whichever is longer.

1.4. Additional Compliance Information

The Reliability Coordinator shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor shall use a scheduled on-site review at least once every three years. The Compliance Monitor shall conduct an investigation upon a complaint that is received within 30 days of an alleged infraction's discovery date. The Compliance Monitor shall complete the investigation and report back to all involved Reliability Coordinators (the Reliability Coordinator that complained as well as the Reliability Coordinator that was investigated) within 45 days after the start of the investigation. As part of an audit or investigation, the Compliance Monitor shall interview other Reliability Coordinators within the Interconnection and verify that the Reliability Coordinator being audited or investigated has been coordinating actions to prevent or resolve potential, expected, or actual problems that adversely impact the Interconnection.

The Reliability Coordinator shall have the following available for its Compliance Monitor to inspect during a scheduled, on-site review or within five working days of a request as part of an investigation upon complaint:

- 1.4.1 Evidence (operator log or other data source) to show coordination with other Reliability Coordinators.

2. Levels of Non-Compliance

- 2.1. **Level 1:** For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did coordinate, but did not have evidence that it coordinated with other Reliability Coordinators.
- 2.2. **Level 2:** Not applicable.
- 2.3. **Level 3:** Not applicable.
- 2.4. **Level 4:** For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did not coordinate with other Reliability Coordinators.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	August 10, 2005	<ol style="list-style-type: none"> 1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Hyphenated "30-day" and "Reliability Coordinator-to-Reliability Coordinator" when used as adjective. 	01/20/06

		<ul style="list-style-type: none"> 3. Changed standard header to be consistent with standard “Title.” 4. Added “periods” to items where appropriate. 5. Initial capped heading “Definitions of Terms Used in Standard.” 6. Changed “Timeframe” to “Time Frame” in item D, 1.2. 7. Lower cased all words that are not “defined” terms — drafting team, and self-certification. 8. Changed apostrophes to “smart” symbols. 9. Removed comma after word “condition” in item R.1.1. 10. Added comma after word “expected” in item 1.4, last sentence. 11. Removed extra spaces between words where appropriate. 	
1	February 7, 2006	Adopted by NERC Board of Trustees	
1	March 16, 2007	Approved by FERC	
1	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
1	November 21, 2013	R2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

Appendix QC-IRO-016-1
Provisions specific to the standard IRO-016-1 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

- 1. Title:** Coordination of Real-time Activities Between Reliability Coordinators
- 2. Number:** IRO-016-1
- 3. Purpose:** No specific provision
- 4. Applicability:** No specific provision
- 5. Effective Date:**
 - 5.1.** Adoption of the standard by the Régie de l'énergie: ~~October~~ Month xx30, 201x3
 - 5.2.** Adoption of the appendix by the Régie de l'énergie: Month~~October~~ xx30, 201x3
 - 5.3.** Effective date of the standard and its appendix in Québec: ~~April~~ Month x1, 201x5

B. Requirements

~~No specific provision~~ Retirement of requirement R2.

C. Measures

No specific provision

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Compliance Monitoring Period and Reset Time Frame

No specific provision

1.3. Data Retention

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Levels of Non-Compliance

No specific provision

E. Regional Differences

No specific provision

Standard IRO-016-1 — Coordination of Real-time Activities Between Reliability Coordinators

Appendix QC-IRO-016-1
Provisions specific to the standard IRO-016-1 applicable in Québec

Revision History

Revision	Adoption Date	Action	Change Tracking
0	October 30, 2013	New appendix	New
<u>1</u>	<u>Month xx, 201x</u>	<ul style="list-style-type: none">• <u>Modification of adoption dates</u>• <u>Retirement of requirement R2</u>	

A. Introduction

1. **Title:** Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program.
2. **Number:** PRC-010-0
3. **Purpose:** Provide System preservation measures in an attempt to prevent system voltage collapse or voltage instability by implementing an Undervoltage Load Shedding (UVLS) program.
4. **Applicability:**
 - 4.1. Load-Serving Entity that operates a UVLS program
 - 4.2. Transmission Owner that owns a UVLS program
 - 4.3. Transmission Operator that operates a UVLS program
 - 4.4. Distribution Provider that owns or operates a UVLS program
5. **Effective Date:** April 1, 2005

B. Requirements

- R1.** The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program. This assessment shall be conducted with the associated Transmission Planner(s) and Planning Authority(ies).
 - R1.1.** This assessment shall include, but is not limited to:
 - R1.1.1.** Coordination of the UVLS programs with other protection and control systems in the Region and with other Regional Reliability Organizations, as appropriate.
 - R1.1.2.** Simulations that demonstrate that the UVLS programs performance is consistent with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-0.
 - R1.1.3.** A review of the voltage set points and timing.
- R2.** The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days). (Retirement approved by FERC effective January 21, 2014.)

C. Measures

- M1.** Each Transmission Owner's and Distribution Provider's UVLS program shall include the elements identified in Reliability Standard PRC-010-0_R1.
- M2.** Each Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall have evidence it provided documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC as specified in Reliability Standard PRC-010-0_R2. (Retirement approved by FERC effective January 21, 2014.)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Compliance Monitor: Regional Reliability Organizations. Each Regional Reliability Organization shall report compliance and violations to NERC via the NERC Compliance Reporting process.

1.2. Compliance Monitoring Period and Reset Timeframe

Assessments every five years or as required by System changes.

Current assessment on request (30 calendar days.)

1.3. Data Retention

None specified.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: An assessment of the UVLS program did not address one of the three requirements listed in Reliability Standard PRC-010-0_R1.1 or an assessment of the UVLS program was not provided.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	February 8, 2005	Adopted by NERC Board of Trustees	
0	March 16, 2007	Approved by FERC	
0	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
0	November 21, 2013	R2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program.
2. **Number:** PRC-010-0
3. **Purpose:** No specific provision
4. **Applicability:** No specific provision
5. **Effective Date:**
 - 5.1. Adoption of the standard by the Régie de l'énergie: Month xx 201x
 - 5.2. Adoption of the appendix by the Régie de l'énergie: Month xx 201x
 - 5.3. Effective date of the standard and its appendix in Québec: Month xx 201x

B. Requirements

~~No specific provision~~ Retirement of requirement R2.

C. Measures

~~No specific provision~~ Retirement of measure M2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.

1.2. Compliance Monitoring Period and Reset Timeframe

No specific provision

1.3. Data Retention

No specific provision

1.4. Additional Compliance Information

No specific provision

2. Levels of Non-Compliance

No specific provision

E. Regional Differences

No specific provision

Revision History

Revision	Adoption Date	Action	Change Tracking
0	Month xx, 201x	New appendix	New

A. Introduction

1. **Title:** Under-Voltage Load Shedding Program Performance
2. **Number:** PRC-022-1
3. **Purpose:** Ensure that Under Voltage Load Shedding (UVLS) programs perform as intended to mitigate the risk of voltage collapse or voltage instability in the Bulk Electric System (BES).
4. **Applicability**
 - 4.1. Transmission Operator that operates a UVLS program.
 - 4.2. Distribution Provider that operates a UVLS program.
 - 4.3. Load-Serving Entity that operates a UVLS program.
5. **Effective Date:** May 1, 2006

B. Requirements

- R1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:
 - R1.1. A description of the event including initiating conditions.
 - R1.2. A review of the UVLS set points and tripping times.
 - R1.3. A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.
 - R1.4. A summary of the findings.
 - R1.5. For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.
- R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request. (Retirement approved by FERC effective January 21, 2014.)

C. Measures

- M1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have documentation of its analysis of UVLS operations and Misoperations in accordance with Requirement 1.1 through 1.5.
- M2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have evidence that it provided documentation of its analysis of UVLS program performance within 90 calendar days of a request by the Regional Reliability Organization. (Retirement approved by FERC effective January 21, 2014.)

D. Compliance

1. Compliance Monitoring Process
 - 1.1. **Compliance Monitoring Responsibility**

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Data Retention

Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall retain documentation of its analyses of UVLS operations and Misoperations for two years. The Compliance Monitor shall retain any audit data for three years.

1.4. Additional Compliance Information

Transmission Operator, Load-Serving Entity, and Distribution Provider shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Documentation of the analysis of UVLS performance was provided but did not include one of the five requirements in R1.

2.3. Level 3: Documentation of the analysis of UVLS performance was provided but did not include two or more of the five requirements in R1.

2.4. Level 4: Documentation of the analysis of UVLS performance was not provided.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	December 1, 2005	1. Removed comma after 2004 in “Development Steps Completed,” #1. 2. Changed incorrect use of certain hyphens (-) to “en dash” (—) and “em dash (—).” 3. Lower cased the word “region,” “board,” and “regional” throughout document where appropriate. 4. Added or removed “periods” where appropriate. 5. Changed “Timeframe” to “Time Frame” in item D, 1.2.	January 20, 2006
1	February 7, 2006	Adopted by the NERC Board of Trustees	
1	March 16, 2007	Approved by FERC	
1	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending	

Standard PRC-022-1 — Under-Voltage Load Shedding Program Performance

		applicable regulatory approval.	
1	November 21, 2013	R2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

Standard PRC-022-1 — Under-Voltage Load Shedding Program Performance

Appendix QC-PRC-022-1

Provisions specific to the standard PRC-022-1 applicable in Québec

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of its appendix must be read together for the purposes of understanding and interpretation. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** Under-Voltage Load Shedding Program Performance
2. **Number:** PRC-022-1
3. **Purpose:** No specific provision
4. **Applicability:** No specific provision
5. **Effective Date:**
 - 5.1. Adoption of the standard by the Régie de l'énergie: Month xx 201x
 - 5.2. Adoption of the appendix by the Régie de l'énergie: Month xx 201x
 - 5.3. Effective date of the standard and its appendix in Québec: Month xx 201x

B. Requirements

~~No specific provision~~ Retirement of requirement R2.

C. Measures

~~No specific provision~~ Retirement of measure M2.

D. Compliance

1. **Compliance Monitoring Process**
 - 1.1. **Compliance Monitoring Responsibility**

The Régie de l'énergie is responsible, in Québec, for compliance monitoring with respect to the reliability standard and its appendix that it adopts.
 - 1.2. **Compliance Monitoring Period and Reset Time Frame**

No specific provision
 - 1.3. **Data Retention**

No specific provision
 - 1.4. **Additional Compliance Information**

No specific provision
2. **Levels of Non-Compliance**

No specific provision

E. Regional Differences

No specific provision

Standard PRC-022-1 — Under-Voltage Load Shedding Program Performance

Appendix QC-PRC-022-1

Provisions specific to the standard PRC-022-1 applicable in Québec

Revision History

Revision	Adoption Date	Action	Change Tracking
0	Month xx, 201x	New appendix	New