WEM RULES

POWER SYSTEM OPERATION PROCEDURE: POWER SYSTEM SECURITY

PREPARED BY:	System Management (WA)
DOCUMENT REF:	SO_OP_WA_3808
VERSION:	3.0
EFFECTIVE DATE:	1 July 2019
STATUS:	FINAL

Approved for distribution and use by:

APPROVED BY:	Cameron Parrotte
TITLE:	Executive General Manager, Western Australia

VERSION RELEASE HISTORY

Version	Effective Date	Summary of Changes
1.0	21 September 2006	21 September 2006 Market Procedure for Power System Security at Market Start
2.0	01 February 2009	Amendments to the Procedure resulting from Procedure Change PPCL0002
3.0	Balancing Market Commencement Day	Amendments to the Procedure resulting from Procedure Change PPCL0022
4.0	1 July 2019	Amendments to the Procedure resulting from Procedure Change AEPC_2019_08

CONTENTS

TABLES

1. PROCEDURE OVERVIEW

1.1. Relationship with the Wholesale Electricity Market Rules

1.1.1. This Power System Operation Procedure (PSOP): Power System Security (Procedure) has been developed in accordance with clause 3.2.7 of the Wholesale Electricity Market Rules (WEM Rules).

1.1.2. References to particular WEM Rules within this Procedure in bold and square brackets **[Clause XX]** are included for convenience only and are not part of this Procedure.

1.2. Interpretation

1.2.1. In this Procedure:

(a) terms that are capitalised, but not defined, have the meaning given in the WEM Rules;

(b) to the extent that this Procedure is inconsistent with the WEM Rules, the WEM Rules prevail to the extent of the inconsistency;

(c) a reference to the WEM Rules, or Market Procedures, includes any associated forms required or contemplated by the WEM Rules or Market Procedures;

(d) words expressed in the singular include the plural and vice versa; and

(e) unless the context requires otherwise, references to AEMO include AEMO in its System Management capacity.

1.3. Purpose and application of this Procedure

1.3.1. The purpose of this Procedure is to describe the processes that:

(a) AEMO must follow to maintain Equipment Limit information **[Clause 3.2.7(a)]**;

(b) AEMO and Network Operators must follow when determining Security Limits and maintaining Security Limit information **[Clause 3.2.7(b)]**;

(c) AEMO must follow when establishing and modifying the Technical Envelope **[Clause 3.2.7(c)]**; and

(d) AEMO must follow to ensure the SWIS operates according to the Technical Envelope applicable to each SWIS Operating State **[Clause 3.2.7(d)]**.

1.3.2. This Procedure may also include guidelines describing matters AEMO will take into account when determining the SWIS Operating State **[Clauses 3.3.3, 3.4.9 and 3.5.11]**.

1.3.3. In addition, the defined terms in Table 1 have the meanings given.

Table 1 Defined Terms

Term	Definition
Contingency	An event that affects the power system in a way that would be likely to result in the failure or sudden removal of a Facility or network equipment from operation.
Credible Contingency	A Contingency that AEMO has determined is reasonably likely to occur.
Facility Limits	As described in step 2.1.1.

Term	Definition
Network Limits	As described in step 2.1.3.
Non-Credible Contingency	A Contingency not classified as a Credible Contingency.
Power System Security	As defined in the WEM Rules is the ability of the SWIS to withstand sudden disturbances, including the failure of generation, transmission and distribution equipment and secondary equipment.

1.4. Associated documents

1.4.1. The following documents in Table 2 below (available on the Market Web Site) provide background information to this Procedure:

Table 2 Associated documents

Term	Definition	Location
SO-OP_WA_3805	IMS Interface Market Procedure	AEMO Website
SO-OP_WA_3804	PSOP: Facility Outages	AEMO Website
SO-OP_WA_3802	PSOP: Communications and Control Systems	AEMO Website
SO_OP_WA_3803	PSOP: Dispatch	AEMO Website
SO_OP_WA_3807	PSOP: Network Modelling Data	AEMO Website
N/A	Technical Rules for the South West interconnected network	ERA Website

2. FACILITY LIMITS AND SECURITY LIMITS

2.1. Facility Limits

2.1.1. Facility Limits are Equipment Limits (only applicable to non-Network Facilities) and Network Limits used to determine the Technical Envelope.

2.1.2. An Equipment Limit means any limit on the operation of a Facility's equipment that is provided as Standing Data for the Facility [Clause 3.2.1].

2.1.3. Network Limits are limit information relating to Network equipment, which includes, but is not limited to, the following information provided to AEMO by a Network Operator in accordance with the PSOP: Network Modelling Data:

(a) Transmission circuit limits;

(b) Overload ratings; and

(c) Fault ratings.

2.1.4. The Network Operator must provide information relating to each Network Limit including but not limited to:

(a) equipment covered by the limit, or areas of the SWIS where the limit applies;

(b) the conditions of the Network for which the limit applies;

(c) the times during which the limit applies or is active; and

(d) specific restrictions that apply to the equipment affected by the limit sufficient for AEMO to manage the limit operationally.

2.1.5. Facility Limits may vary for different conditions including, but not limited to, season, time of day and temperature.

2.2. Security Limits

2.2.1. Security Limits represent any static and dynamic technical limits on the operation of the SWIS as a whole, or a region of the SWIS, necessary to maintain Power System Security, including but not limited to:

(a) any limit on power transfer between different areas of the SWIS;

(b) pre and post contingent circuit loadings that are limited by the thermal rating of network elements;

(c) fault levels that are limited by short circuit rating of network elements;

(d) voltage and rotor angle stability limits (in accordance with the standards set out in the Technical Rules);

(e) short-term and long-term voltage recovery limits (in accordance with the standards set out in the Technical Rules);

(f) pre and post contingent steady state voltage limits (in accordance with the standards set out in the Technical Rules);

(g) oscillatory rotor angle stability limits (in accordance with the standards set out in the Technical Rules);

(h) an asset or equipment issue that requires it to be operated in a specific way to avoid damage or harm which may include information to be used in preference to a specific Facility Limit in particular circumstances;

(i) scenarios where facilities are unable to be controlled or managed in order to maintain SWIS Operating Standards (e.g. generator islanding scenarios with no isochronous control capability or no automated disconnection protection);

(j) any special protection schemes advised by a Network Operator including run-back schemes; and

(k) security constraints provided by the Network Operator in accordance with the PSOP: Network Modelling Data.

2.2.2. Security Limits:

(a) must take into account normal operation of the SWIS and operation under outage conditions; and

(b) may apply in specific conditions or for a specified period.

2.2.3. Network Operators must:

(a) determine all applicable Security Limits **[Clauses 3.2.4 and 3.2.7(b)]**; and

(b) provide those Security Limits to AEMO in accordance with the PSOP: Network Modelling Data, the IMS Interface Market Procedure and the PSOP: Communications and Control Systems.

2.2.4. The Network Operator must provide information relating to each Security Limit including but not limited to:

(a) equipment covered by the limit, or areas of the SWIS where the limit applies;

(b) the conditions of the Network for which the limit applies

(c) the times during which the limit applies or is active; and

(d) specific restrictions that apply to the equipment affected by the limit, sufficient for AEMO to manage the limit operationally.

2.3. Maintaining Facility Limits

2.3.1. AEMO maintains Facility Limits and Security Limits by [Clauses 3.2.7(a) and 3.2.7(b)]:

(a) obtaining Equipment Limit information, Network Limit information and Security Limit information;

(b) recording Equipment Limit information [Clause 3.2.2], Network Limit information and Security Limit information; and

(c) reviewing and updating Equipment Limit information, Network Limit information and Security Limit information as appropriate.

2.3.2. Where AEMO has reason to believe that a Facility Limit or Security Limit is incorrect, AEMO:

(a) must request an updated Facility Limit or Security Limit from the relevant Market Participant or Network Operator; and

(b) may, using the best available information, determine a new Facility Limit or Security Limit until the Market Participant or Network Operator provides a replacement [Clause 3.2.7(b)].

3. TECHNICAL ENVELOPE AND OPERATING STATES

3.1. The Technical Envelope and Its Application

3.1.1. The Technical Envelope represents the limits within which the SWIS can be operated in each SWIS Operating State [Clause 3.2.5].

3.1.2. AEMO must establish and modify the Technical Envelope for each SWIS Operating State [Clause 3.2.6].

3.1.3. In establishing and modifying the Technical Envelope, AEMO must take into account the matters specified in clause 3.2.5 of the WEM Rules as well as [Clause 3.2.7(c)]:

(a) In a Normal Operating State:

(i) For Scheduled Generators and Non-Scheduled Generators:

(A) When dispatching Out of Merit in accordance with clause 7.6.1C(c) of the WEM Rules, respect all Normal Operating State Facility Limits applicable for the relevant Trading Interval; and

(B) When dispatching in merit (or Out of Merit to the next Facility in the BMO) as required by clauses 7.6.1C(a) and 7.6.1C(b) of the WEM Rules, respect all Equipment Limits but only to the extent those limits

are not inconsistent with the dispatch of Facilities that, but for the Equipment Limits, would be dispatched under clause 7.6.1C of the WEM Rules **[Clause 3.2.5(a)]**;

(ii) For all other Facilities, respect all Normal Operating State Facility Limits;

(iii) Respect the Ready Reserve Standard, including where the Ready Reserve Standard is relaxed in accordance with clause 3.18.11A(c) of the WEM Rules;

(iv) Respect all Normal Operating State Security Limits relevant for the Trading Interval **[Clause 3.2.5(b)]**;

(v) Respect all Ancillary Service Requirements and Ancillary Service standards [Clause 3.2.5(d)].

(b) In a High Risk Operating State:

(i) Where provided, respect all High Risk Operating State Facility Limits **[Clause 3.4.2(a)]**;

(ii) Respect the overload capacity limits of Scheduled Generators **[Clause 3.4.3(c)]**;

(iii) Where provided, respect all High Risk Operating State Security Limits **[Clause 3.2.5(b)]**;

(c) In an Emergency Operating State:

(i) Where provided, respect all Emergency Operating State Facility Limits **[Clause 3.5.4]**;

(ii) Respect the overload capacity limits of Scheduled Generators **[Clause 3.5.5(b)]**; and

(iii) Where provided, respect all Emergency Operating State Security Limits **[Clause 3.5.4]**.

3.2. Management of SWIS Operating States

3.2.1. At all times AEMO must classify which Contingencies are Credible Contingencies.

3.2.2. AEMO may re-classify a Non-Credible Contingency as a Credible Contingency, and:

(a) must record that re-classification; and

(b) where relevant, must notify impacted Network Operators and Market Participants.

3.2.3. The following clauses in the WEM Rules specify the actions AEMO must or may take in:

(a) A Normal Operating State: clause 3.3.2;

(b) A High Risk Operating State: clauses 3.4.3 and 3.4.4; and

(c) An Emergency Operating State: clause 3.5.5.

3.2.4. The SWIS is in a High Risk Operating State when actions, other than those allowed under step 3.2.3(a), must be implemented immediately by AEMO to manage a Credible Contingency and one of the circumstances outlined in clause 3.4.1 of the WEM Rules exists or is likely to exist in the specified timeframes **[Clause 3.4.1]**.

3.2.5. The SWIS is in an Emergency Operating State when actions other than those allowed under steps 3.2.3(a) and 3.2.3(b) must be implemented immediately by AEMO to

manage a Credible Contingency and one of the circumstances outlined in clause 3.5.1 of the WEM Rules exists or is likely to exist in the specified timeframes **[Clause 3.5.1]**.

3.2.6. AEMO must ensure the SWIS operates according to the Technical Envelope applicable to each SWIS Operating State **[Clause 3.2.7(d)]** by:

(a) determining whether the power system is capable of maintaining operation within the Technical Envelope of the current Operating State, following any Credible Contingency;

(b) taking actions specified in step 3.2.3 for the current Operating State to maintain or return to a Normal Operating State **[Clauses 3.4.5 and 3.5.6]**; and

(c) ensuring that no actions are taken that in its opinion would be reasonably likely to lead to:

(i) a High Risk Operating State **[Clause 3.3.2(e)]** or an Emergency Operating State **[Clause 3.5.3]** if in a Normal Operating State; and

(ii) an Emergency Operating State **[Clause 3.5.3]** if in a High Risk Operating State.