~~ELECTRICITY INDUSTRY ACT~~

~~ELECTRICITY INDUSTRY (WHOLESALE ELECTRICITY MARKET) REGULATIONS 2004~~

~~WHOLESALE ELECTRICITY MARKET RULES~~

~~Power System Operation Procedure:~~

~~Power System Security~~

~~1. VERSION HISTORY~~

~~21 SEPTEMBER 2006~~ WEM RULES

POWER SYSTEM OPERATION PROCEDURE: POWER SYSTEM SECURITY

~~01 February 2009~~

~~Balancing Market Commencement Day~~	~~Replacement of the Procedure resulting from Procedure Change Proposal PPCL0022~~

TABLE OF CONTENTS

~~2. RELATIONSHIP WITH MARKET RULES~~

PREPARED BY: System Management (WA)

DOCUMENT REF:

VERSION: 3.0

EFFECTIVE DATE: TBC 2019

STATUS: DRAFT FOR CONSULTATION

Approved for distribution and use by:

APPROVED BY:

TITLE:

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	TBC 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

~~2.1.1.~~1.1.1. This Power System Operation Procedure (PSOP): Power System Security (Procedure) has been developed in accordance with~~, and should be read in conjunction with,~~ clause 3.2.7 of the Wholesale Electricity Market Rules (~~Market~~WEM Rules).

~~2.1.2.~~1.1.2. References to particular ~~Market~~WEM Rules within ~~the~~this Procedure in bold and square brackets **[~~MR~~Clause XX]** are ~~current as of the Balancing Market Commencement Day. These references are~~ included for convenience only~~,~~ and are not part of this ~~procedure~~Procedure.

1.2. ~~This Procedure is subservient to the Market Rules.~~ Interpretation

1.2.1. In ~~the event of conflict between~~this Procedure:

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

~~(a)~~(b) to the extent that this Procedure ~~and~~is inconsistent with the ~~Market~~WEM Rules ~~or any other document, the order of precedence is as set out in the Market~~, the WEM Rules ~~[MR 1.5.2]~~prevail to the extent of the inconsistency;

~~1. This Procedure may include explanatory text, including quotations from the Market Rules. Such explanatory text is for information only, does not form part of the Procedure, and is italicised and contained in a rectangular box.~~

~~2. A word or phrase defined in the Electricity Industry Act 2004, or in the Regulations or Market Rules made under that Act, has the same meaning when used in this Procedure.~~

~~3.RELATED DOCUMENTS~~

~~1. This Procedure is related to, and should be read in conjunction with, the following documents:~~

~~a. SWIS Technical Rules and Operating Standards;~~

~~b. PSOP: Dispatch;~~

~~c. PSOP: Ancillary Services;~~

~~d. PSOP: Communications and Control Systems;.~~

~~e. PSOP: Facility Outages; and~~

~~f. PSOP: Commissioning and Testing.~~

~~4.COMMENCEMENT~~

(c) ~~1. This Procedure replacement has effect from~~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

unless the ~~Balancing Market Commencement Day.~~

~~1 SCOPE~~

~~1. This Procedure has been developed in accordance with clause 3.2.7 of the Market Rules and documents the process to be followed by:~~

(e) context requires otherwise, references to AEMO include AEMO in its System Management ~~in maintaining~~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 ~~and System Management in~~must follow when determining Security Limits and maintaining Security Limit information~~;~~ [Clause 3.2.7(b)];

(c) ~~System Management in~~ AEMO must follow when establishing and modifying the Technical Envelope~~;~~ [Clause 3.2.7(c)]; and

~~a. System Management~~AEMO must follow to ~~enable it to operate~~ensure the SWIS operates according to the Technical Envelope applicable to each SWIS Operating State~~.~~

~~2. The Procedure details the processes that take place each Scheduling Day and Trading Day, outside the balancing horizon, inside the balancing horizon and in real time to ensure that the power system is managed within the Dispatch Criteria at all times.~~

~~3. This Procedure covers all equipment and Facilities forming part of the power system and subject to direction by System Management, including Scheduled Generators, Non-Scheduled Generators, Demand-Side Programmes, Dispatchable Loads and Networks.~~

~~2 ASSESSMENT OF POWER SYSTEM SECURITY~~

~~*Maintenance of power system security essentially means taking all required actions to ensure that the Dispatch Criteria are satisfied at all times. Since some actions must be taken in advance, assessing power system security must be done not only in real time but also on a forward-looking basis.*~~

~~2.1 ASSESSMENT OF POWER SYSTEM SECURITY~~

~~1. System Management must use assessments of power system security as the basis for deciding what actions to take, permit, mandate or prohibit in respect of the operation of the power system.~~

~~2. System Management may, as a result of a power system security assessment, do any one or more of the following:~~

a. ~~Issue Dispatch Advisory notices in relation to an actual or forecast change in Operating State; or~~

b. ~~Issue Dispatch Advisory notices in relation to technical constraints; or~~

c. ~~Issue Dispatch Instructions and Dispatch Orders consistent with its powers under the prevailing Operating State; or~~

d. ~~Cancel or recall Planned Outages (Facility and Network) consistent with its powers under the prevailing Operating State; or~~

e. Issue Operating Instructions consistent with the contract, or Market Rules provisions, to which those instructions relate; or

f. Disconnect, or direct the disconnection of, Facilities consistent with its powers under the prevailing Operating State; or

g. Direct Facilities to change reactive power output as required for voltage control.

For the following sections 2.1, 2.2 and 2.3 System Management may need to amend the criteria for forecast load and forecast intermittent generation to ensure that a consistent approach is taken in dealing with forecast uncertainty in each of the timeframes (pre-dispatch outside the Balancing Horizon, pre-dispatch within the Balancing Horizon and dispatch in Real-Time within the current interval)

2.2 ASSESSMENT OUTSIDE THE BALANCING HORIZON

1. System Management must base its assessment of power system security for any future time outside the current Balancing Horizon on the adequacy of generation and SWIS network capacity to meet forecast load, ancillary services and ready reserve requirements within the Technical Envelope, assuming:

   a. Generation and network availability in accordance with the latest approved outage plans and Forced Outage notifications, and

   b. System load level based on its SEDM forecast for the mean system load plus two standard deviations, or its Metrix forecast for the mean system load plus two standard deviations, or its load forecast applied to clause 3.19.6(a) of the Market Rules, whichever is applicable, and

   c. Intermittent generation at the mean forecast level, and at the mean forecast level minus two standard deviations, and

   d. n-1 level of contingency for all credible network contingency events, and

   e. n-2 level of contingency for the transmission network, applicable for system load up to 80% of peak, and

   f. Full coverage of all Ancillary Services is maintained, including any additional quantities required to support approved commissioning and testing activities, and

   g. Any additional constraints System Management is required to manage are appropriately dealt with.

A requirement for n-1 for generation contingencies is not included in part d, since the ancillary services standard for spinning reserve establishes this.

Part g envisages management of fuel during gas supply emergencies.

2.3 ASSESSMENT WITHIN THE BALANCING HORIZON

1. System Management must base its assessment of power system security for any future time outside the current Trading Interval but within the current Balancing Horizon on the adequacy of generation capacity and SWIS network capacity to meet forecast load, ancillary services and ready reserve requirements within the Technical Envelope, assuming:
   a. Network availability in accordance with the latest approved Outage Plans and Forced Outage notifications, and
   b. Generation availability and ramp rate limits in accordance with the latest Forecast BMO and Forced Outage notifications, and
   c. n-1 level of contingency for all credible network contingency events, and
   d. n-2 level of contingency for the transmission network, applicable for system load up to 80% of peak, and
   e. Three scenarios, representing the mean forecasts of load and any non-scheduled generation, plus one standard deviation load forecast combined with minus one standard deviation of any non-scheduled generation forecast, and minus one standard deviation load forecast combined with plus one standard deviation of any non-scheduled generation forecasts, and
   f. Full coverage of all Ancillary Services is maintained, including any additional quantities required to support approved commissioning and testing activities, and
   g. Any additional constraints System Management is required to manage are appropriately dealt with, including but not limited to Market Generator runback and load trip schemes.

It is envisaged that assessment within the balancing horizon will be based on examination of a security-constrained dispatch plan for the power system, for each of the three scenarios referred to in e. above. Dispatch Advisory notices would be generated for:

-Breaches of constraints identified in the dispatch solution, some of which would correspond to forecast changes in Operating State,

-Dispatches that substantially violate certain standing data limitations such as minimum generation, minimum up / down times, startup times

-Facilities whose output changes from zero to non-zero, or vice versa, between the three scenarios referred to in step 2.3.(e). above.

2.4 REAL-TIME ASSESSMENT

1. System Management must assess power system security for the current

~~Trading Interval on the ability to meet the forecast system load, based on:~~

a. Generation availability and ramp rate limits according to the BMO, unless advised otherwise by a Market Participant, and

b. Which Facilities are currently committed, or are able to be committed, within the Trading Interval, and

c. System Management's current forecasts of load and Non-Scheduled Generation, and

d. The impact of automatic schemes in place to manage network, generation and other SWIS system constraints, and

e. The adequacy of Ancillary Services for the prevailing conditions, and

f. System Management's current ability to communicate with those Facilities and/or control them directly.

3 MANAGEMENT OF POWER SYSTEM OPERATING STATE

Each Operating State has a defined set of conditions, one or more of which must be met before the system can be placed in that state. System Management's powers and discretion increase as the Operating State is escalated.

The conditions for each of the Operating States are specified in the Market Rules

3.1 FORECASTING CHANGES IN OPERATING STATE

1. If System Management forecasts that the power system Operating State may need to change in the future, then System Management must as soon as practicable issue a Dispatch Advisory notice to inform the market of that fact.

2. System Management must deem that the power system Operating State needs to be escalated in the future ("forecast a change in Operating State") if, and only if, all of the following conditions are satisfied:

   a. The power system is forecast to meet one or more of the conditions for the escalated Operating State in some time period in the future, but not in the immediately preceding period, and

   b. System Management is able to take actions that would result in the conditions referred to in step 3.1.2(a) being alleviated, and

(d) System Management's powers under the escalated Operating State would permit it to take the actions referred to in step [Clause 3.1.2 (b), but its powers under the currently prevailing Operating State would not permit it to do so, and 2.7(d)].

   c. The actions referred to in step 3.1.2(b) can be taken, and would have effect, prior to the start of the relevant time period.

In plain language, if System Management can foresee something adverse occurring that it requires increased powers to deal with, but time remains for the market to

~~*correct the problem, it will advise the market that "the Operating State is forecast to escalate" but will take no direct action to intervene at this time*~~

~~3. System Management must deem that the power system Operating State may be de-escalated in the future ("forecast a change in Operating State") if the power system is forecast to meet none of the conditions for the prevailing Operating State in the applicable time period and is not required to remain in the prevailing Operating State pursuant to step 3.1.2 above for any subsequent time periods.~~

~~3.2 CHANGING OPERATING STATE~~

~~1. If System Management deems it necessary to change the power system Operating State, then System Management must as soon as practicable issue a Dispatch Advisory notice to inform the market of that fact.~~

~~2. System Management must escalate the power system Operating State if the power system currently meets one or more of the conditions for the escalated Operating State~~

~~3. System Management must escalate the power system Operating State if all of the following conditions are satisfied:~~

~~a. The power system is forecast to meet one or more of the conditions for the escalated Operating State in some time period in the future, and~~

1.3.2. ~~System Management's powers under the escalated Operating State would permit it to take the actions to address the conditions referred to in Part a~~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.
Network Limits	As described in step 2.1.3.
Non-Credible Contingency	A Contingency not classified as a Credible Contingency.

Term	Definition
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

Reference	Title	Location
SO-OP_WA_3805	IMS Interface Market Procedure	AEMO Website
N/A	PSOP: Facility Outages	AEMO Website
N/A	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].

~~b.~~ Network Limits are limit information relating to Network equipment, which includes, but ~~its powers under the currently prevailing Operating State would not permit it to do so, and~~

~~c. Any further delay would result in the actions to address the conditions referred to in Part a not being able to be taken, or not being able to have effect, prior to the start of the relevant time period.~~

~~*At the point SM can no longer wait for the market to correct an issue, it will escalate the Operating State to give itself the powers to deal with the issue directly.*~~

~~4. System Management must de-escalate the Operating State if the power system does not currently meet any of the conditions for the prevailing Operating State and~~ is not ~~required~~limited to ~~remain in,~~ the ~~prevailing Operating State pursuant~~following information provided to ~~step 3.2.2 above.~~

~~4 MANAGEMENT OF THE TECHNICAL ENVELOPE~~

~~*System Management has an obligation to operate the power system "within the Technical Envelope"* ***[MR 3.2.8]****. System Management characterise the Technical Envelope as a* ***dynamic set of constraints.*** *Some of the constraints describing the Technical Envelope are a function of the Operating State.*~~

The constraints comprising the Technical Envelope are derived from standing data equipment limits, ancillary services standards, network operating standards (and exceptions to them), and security constraints.

Some of the Technical Envelope constraints (relating to equipment limits, for example) will be able to be watched through the pre-dispatch. Others (e.g. voltage) won't be able to be watched in the Dispatch Planning Tool, but may be examined in other systems (e.g. TSM).

4.1 TECHNICAL ENVELOPE

1. System Management must set the Technical Envelope as permissively as possible within the requirements of the Market Rules.
2. The Technical Envelope is established and maintainedAEMO by System Management by organising elements of:
   a. Standing Data provided by Market Participants, and
   b. Operating Standards such as Frequency and Voltage Limits specified in the Technical Rules, and
   c. Ancillary Services Standards specified in the Market Rules **[MR 3.10]**, and
   d. Security Constraints provided by Network Operators in consultation with System Management,

   In combinations that allow the widest range of dispatch solutions.
3. System Management must manage the power system to ensure operation within the Technical Envelope at all times, by
   a. Maintaining definitions of the constraints that comprise the Technical Envelope, and
   b. Keeping current the data that quantifies the constraints, and
   c. Operating the power system within the constraints.
4. In a Normal Operating State, the conditions set out in the Technical Rules apply to the Technical Envelope.
5. In a High Risk Operating State or Emergency Operating State:
   a. the frequency for a multiple contingency event; and
   b. the emergency condition voltage level,

   apply as specified in the Technical Rules.
6. The Technical Envelope must take into account the circumstances of a potential High Risk Operating State or Emergency Operating State and System Management's powers as set out in the Market Rules **[MR 3.4 and 3.5]**.

4.1.1.2.1.3. ~~System Management must operate the SWIS~~ Network Operator in accordance with the ~~Technical Envelope applicable to each operating state~~PSOP: Network Modelling Data:

7. ~~As System Management's Technical Envelope is based on elements of the Technical Rules, modifications to the Technical Rules may also modify the Technical Envelope, in so far as they are relevant.~~

8. ~~System Management must as soon as practicable modify the applicable Technical Envelope when changes to the elements and constraints outlined in step 4.1 occur.~~

(a) ~~Equipment~~Transmission circuit limits;

~~***[MR 3.2.1]** states that:*~~

~~*"An equipment limit means any limit on the operation of a Facility's equipment that is provided as Standing Data for the Facility to System Management by the IMO in accordance with clause 2.34.1(b)."*~~

9. ~~Equipment Limit information must include all Standing Data thermal ratings for generator and network equipment that form the SWIS, and any other elements of Standing Data that are relevant to the capability of the equipment to operate at a particular level of output.~~

10. ~~The IMO must provide the Standing Data for a Facility and any revisions of the Standing Data to System Management as soon as practicable.~~

11. ~~In setting Equipment Limits, System Management must have regard to any additional information that it becomes aware of, including but not limited to notification by the operator of the equipment of a full or partial de-rating.~~

~~*Where there are changes to the commissioning status of generation or transmission facilities or equipment, the boundaries of the Technical Envelope will be dynamically updated in System Management's systems. System Management will also update the network and generator topology accordingly.*~~

12. ~~System Management must deem the Balancing Merit Order (BMO) and Forecast Balancing Merit Order (Forecast BMO) information provided to it by the IMO to have precedence over Standing Data Equipment Limits when establishing the Technical Envelope in accordance with the following criteria:~~

    a. ~~The maximum generation capability of a Balancing Facility must be taken to be the sum of its quantities in its the BMO ; and~~

    b. ~~The minimum stable generation capability of a Balancing Facility must be taken to be its first (lowest placed) tranche in the BMO ; and~~

    c. ~~The maximum ramp rate capability of a Balancing Facility must be taken to be the Facility's Ramp Rate Limit provided by the IMO with the BMO;~~

~~*Step 4.2.4 above relates to **[MR 3.2.5 (a)]** which states:*~~

~~and~~

"The Technical Envelope represents the limits within which the SWIS can be

operated in each SWIS Operating State. In establishing and modifying the Technical

(a) respect all Equipment Limits but only to the extent those limits are not inconsistent with the dispatch of Balancing Facilities that, but for the Equipment

13. System Management must maintain a list of all Equipment Limits on equipment for which it has operating authority, and must ensure that, where Equipment Limits are managed using System Management's SCADA and other monitoring systems, the SCADA database and other system data bases are updated as required to reflect the current Equipment Limits.

Where necessary, System Management will review and update plant ratings on a monthly basis using semi-automated data comparison procedures.

14. System Management must arrange for the SCADA system to monitor, as applicable, the voltage, current, real power flow and/or reactive power flow within each item of equipment or Facility for which Equipment Limits are provided, for which it has operating authority.

15. Plant rating limits must be incorporated into System Management's equipment ratings database and the SCADA system which triggers alarms in the System Management System Operations Control Centre ('SOCC') when limits are breached for which it has operating authority.

16. System Management must update the SCADA database with any new Equipment Limit prior to the limit data becoming operational.

17. Where System Management becomes aware that a generator Standing Data is inaccurate or may become inaccurate in the future, System Management must notify IMO of this as soon as practicable and update any associated EquipmentLimits.

4.2 SECURITY LIMITS

The definition of a Security Limit is specified in the Market Rules ***[MR 3.2.3].***

"A Security Limit means any technical limit on the operation of the SWIS as a whole, or on a region of the SWIS, necessary to maintain Power System Security, including both static and dynamic limits, and including limits to allow for and to manage contingencies."

~~1. System Management must establish a list of the equipment for which Network Operators must provide and maintain Security Limits.~~

~~2. Each Network Operator must determine the Security Limits applicable to its Network.~~

~~3. A Network Operator must consult with System Management in determining any Security Limits applicable to its Network.~~

(b) ~~A~~ Overload ratings; and

(c) Fault ratings.

~~4.1.2.~~2.1.4. The Network Operator must ~~notify System Management of the Security Limits applicable to its~~ provide information relating to each Network ~~and must provide System Management with updated Security Limits where a revision has been required.~~Limit including but not limited to:

(a) ~~The~~ 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 ~~must be those~~

~~4. Security Limits represent any static and dynamic~~ technical ~~requirements and standards in the Technical Rules that represent constraints~~limits on the operation of the SWIS~~, imposed for the purpose of managing electricity quality and security.~~

~~5. The Security Limits include:~~

~~a. SWIS Operating Standards that stipulate maximum and minimum voltage and frequency conditions for the overall SWIS network; and~~

~~4.1.3.~~2.2.1. ~~voltage and other limits that apply to~~ as a whole, or a region of the SWIS ~~network, and are specified by a Network Operator.~~, necessary to maintain Power System Security, including but not limited to:

~~6. System Management must maintain a list of all Security Limits provided by Network Operators that represents actual or potential constraints on the transfer of energy across the SWIS network, in System Management's systems and review the currency of these from time to time.~~

(a) ~~When 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 ~~has not provided sufficient Security,~~in accordance with the PSOP: Network ~~or Equipment Limit information, System Management must operate the SWIS network according to its best estimate of the Security or Equipment Limits based on prior~~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~~, or~~ 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 ~~it possesses~~, 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 ~~is~~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 ~~to similar equipment elsewhere~~, 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

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