

---

# REVIEW OF THE PROCESS FOR DESIGN, DEVELOPMENT, TESTING, APPLICATION, REAL-TIME USE, AND REMOVAL OF SECURITY CONSTRAINTS

Review undertaken as part of UTS Settlement Agreement reference  
EGR285

A report to Transpower New Zealand Limited as System Operator

Prepared by:

Elliston Power Consultants Limited

Unit 23, 43-53 Nairn Street

Wellington

Tel: (021) 681 688

Email: [ellpow@xtra.co.nz](mailto:ellpow@xtra.co.nz)

April 2006

---

---

## Contents

1.0 Executive Summary .....	3
2.0 Compliance Findings .....	6
3.0 Terms of Reference.....	11
4.0 Background .....	11
5.0 Review Process .....	12
6.0 Documentation reviewed .....	12
7.0 Personnel interviewed .....	13
8.0 Outline of EGR Requirements relating to Security Constraints.....	14
9.0 Review of Main Documented Procedures related to Security Constraints and Interviews with Staff .....	16
9.1 Constraint Design, Development and Testing .....	16
9.1.1 Document 327 Security Constraint Development and Review Process.....	16
9.1.2 Document 326 Security Constraint Development Methodology .....	25
9.1.3 Document 325 Security Constraints Database Operating Procedure .....	26
9.2 Security Constraints Application and Removal including for Outages.....	29
9.2.1 Document 237 Assess and Confirm Plant Requests Workflow .....	29
9.2.2 Document 243 Week Ahead Process Flow Overview .....	33
9.2.3 Document 242 Week Ahead MDE Entry.....	33
9.3 Security Constraints Use including checking.....	34
9.3.1 Document 239 Day Ahead Grid Plan Check.....	34
9.3.2 Document 541 Security Coordinator Day Ahead Check Process .....	35
9.3.3 Document 373 System Management .....	36
9.3.4 Document 527 Amending constraints in real time.....	37
9.3.5 Document 553 Re-rating of constraints in real time .....	37
9.3.6 Document 585 Real time MDE updates for Grid Owner Offer Changes .....	38
9.4 Notifications .....	39
9.4.1 Document 342 Issuing a Customer Advice Notice .....	39
9.4.2 Document 506 Distribution of Notices.....	39
10.0 Conclusions and Recommendations .....	40
11.0 Appendix .....	41

---

---

## Introduction

A review was undertaken of the process for the design, development, testing, application, real time use, and removal of security constraints. The review was undertaken as part of the UTS Settlement Agreement [reference EGR285].

This report records the outcome of that review.

## 1.0 Executive Summary

By and large, the processes seem reasonable and consistent with the requirements of the EGRs. A number of the procedures reviewed have some outdated and inaccurate information. Interviews with staff show that the processes are largely adhered to, but the review showed that staff members take steps to ensure the EGRs are complied with where the procedures themselves have gaps or are duplicated. This means that the written processes need to be brought in line with actual practice.

On the issue of consistency of application and reproducibility, there are some areas where there is a degree of staff discretion. Although these are documented so that consistency in application can be achieved, different staff may in reality show different judgement. This could lead to different outcomes for the same set of circumstances.

There are a number of areas where the application, modification and removal of constraints is problematic.

Firstly, the constraints database is designed to not be linked to the operational plans, such as the Gridplan that is produced a day ahead of real time. The importing of a constraint from the database into the operational plans is a manual process. Once imported, any change to the constraint within the database is not picked up by the operational plan. Also, any change to a constraint in MDE (the Market Data Entry tool) will not be reflected in the constraints database. This mismatch in terms of what is updated and what isn't may result in a constraint being thought to have been modified, but which is not in the database.

Secondly, the constraints are not "time stamped". Their application and removal are manual processes. This leaves another possible avenue for applying constraints which are no longer valid, or applying constraints that are not yet valid. In addition, where a constraint is to be applied for a number of days, or where a constraint that has been applied is to be removed, a manual entry is made in each day for which the constraints is to be applied or removed. So for example, where a constraint is to be applied for 30 days, 30 manual entries have to be made, and likewise if the constraint is to be removed after application. This leaves a significant opportunity for errors and omissions. These errors and omissions may result in the System Operator breaching the EGRs.

---

---

Thirdly, when a constraint is to be made in-active, there is no date entry for when this becomes effective other than at the point in time when the "in-activate" button is pushed on the constraints tool. As things stand, the existing software does not allow a constraint that is currently being applied in MDE to be de-activated. If an assessment shows that the constraint should be made inactive, this step cannot be taken until the constraint is no longer applied in MDE. There needs to be some way of not having to remind staff to do a task in some point in the future, and to allow staff to apply use-from and use-by dates to constraints at the time of assessment.

As far as compliance with the EGRs, it is noted that the procedures are written from an "operations" point of view, whereas the EGRs are mainly written from an "outcomes" point of view. It would be useful to prepare a flowchart that matches the various processes to the appropriate rules within the EGRs, showing exactly what rules each process complies with.

In addition, there are a large number of written procedures, some of which included instructions on how to undertake a particular process. There are also processes which are similar to each other, but resulting in two separate procedures/documents. The written procedures are stored in different directories of the computer system, with staff in some areas having access to some directories and not others.

From an external reviewer's viewpoint it is preferable to simplify the written processes by separating what needs to be done (process) from how it should be done (procedures). The benefits would be to make the process requirements more explicit and aid compliance, as well as making audit more straightforward. Any staff unfamiliar with how to undertake a required process step can refer to a more detailed procedure document.

Finally, to ensure consistency and reproducibility of process, the remaining discretionary steps should be reviewed and removed unless there is a good reason to allow discretion, except for those steps that require expert or professional judgement on the part of the staff member.

In terms of the original error, a review of the incident report showed that the constraint which caused the UTS was being removed by two different staff members, one removing the constraint from some days and the other from other days. No procedure has been identified to explain why the constraint removal process would involve multiple persons depending on how many days ahead the constraint was to be removed. (This has since been documented in document 553 – *Handling of Re-rating Constraints in Real Time.*)

Under the settlement agreement, paragraph 4(e) notes that the System Operator has reviewed its process for the removal of permanent constraints and has made a number of operational improvements as a result, namely:

- All instructions from the Security Co-ordinator to other System Operator personnel to change a constraint or other SPD input are now formally logged;
-

- 
- Any verbal instruction from the Security Co-ordinator to other System Operator personnel is followed by an email confirmation, to mirror other operational processes.

Further, paragraph 5 of the settlement agreement ensures that whenever the System Operator identifies a binding constraint is creating infeasible schedule prices in the dispatch schedule, it will, when reasonable, attempt to revise or remove the constraint in real time. This process is covered by existing instructions on changing constraints in real time. It is unclear why this was not done in the particular instance above.

With the formal logging of all instructions, and the following up with email, one would expect that the same situation will not arise again. It is unclear from the procedures reviewed why the person who initiates the removal of a constraint for some days would not then ensure the constraint is removed for all relevant days.

There is also some discussion about whether it could have been foreseen that the constraint would not have achieved its objectives.

Although the constraint development process includes a range of generation and load scenarios, it does not include a requirement to include the likely behaviour of market participants, and it is debateable whether it should. Therefore, it can be envisaged that in general, some constraints may not achieve what was intended. Whether someone should have foreseen that the particular constraint resulting in the UTS on 24 April 2004 was likely to work or not is unclear. When it became clear that the constraint was not working as intended, the constraint removal process did not go smoothly.

Since the incident on 24 April 2004, there has been one other incident where a superseded constraint has been applied. In this case, a superseded summer constraint was not made inactive and was applied some months in the future, in the following summer period. If constraints were able to have some form of expiry date beyond that which they cannot be used, this will make it more difficult to inadvertently apply superseded constraints, or leave them in when they should have been removed.

---

---

## 2.0 Compliance Findings

Rule reference	Compliance Findings
----------------	---------------------

<p>Rule 2.1 of Section II of Part C</p> <p>2. Principal performance obligations of the system operator (PPOs)</p> <p>The principal performance obligations of the system operator are to:</p> <p>2.1 Avoid cascade failure</p> <p>Act as a reasonable and prudent system operator with the objective of dispatching assets made available in a manner which avoids the cascade failure of assets resulting in the loss of demand and arising from:</p> <p>2.1.1 Frequency or voltage</p> <p>Frequency or voltage excursions; or</p> <p>2.1.2 Imbalances</p> <p>Supply and demand imbalances.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>How rule is met:</p> <p>In relation to security constraints, the derivation and application of permanent and other security constraints have the purpose of minimising the risk of asset overload or cascade failure in the transmission network during a contingency – refer document 326 <i>Security Constraint Development Methodology</i>. Therefore all processes relating to security constraints will have as a fundamental objective the achievement of this rule.</p> </div>	<p><b>Fully met</b></p>
--	-------------------------

<p><b>15.1 and 15.2*</b> For a contingent event and for extended contingent events (in relation to asset capability and stability only):</p> <ul style="list-style-type: none"> <li>▪ No asset will exceed its stated capability</li> <li>▪ Grid voltage will be within a specified range</li> <li>▪ Voltage stability of power system is maintained</li> </ul> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>How rule is met:</p> <p>Document 327 Security Constraint Development and Review Process: processes and responsibilities for initiating, developing, documenting, notifying and implementing security constraints in the SPD model, including various analysis of asset capability under contingency and post-event voltages</p> <p>Document 326 Security Constraint Development Methodology: process to identify whether assets will be operating within their capabilities and to develop constraints to address any problems identified</p> <p>Document 325 Security Constraints Database Operating Procedure: procedures for adding/viewing/modifying constraints</p> <p>Document 237 Assess and Confirm Plant Requests Workflow: contingency analysis completed to ensure sufficient network capability for plant outage requests</p> </div>	<p><b>Fully met</b></p>
--	-------------------------

\* Unless otherwise stated, these refer to clauses in the Policy Statement in schedule C4 of the Electricity Governance Rules and Regulations.

Document 243 Week Ahead Process Flow Overview: process to confirm plant requests, outages and constraints are entered into Market Data Entry

Document 242 Week Ahead MDE Entry: Ensures constraint bundles are entered into Market Data Entry

Document 239 Day Ahead Grid Plan Check: process to ensure that the Grid Plan is accurate and reflects what is in the MDE. All entries are checked.

Document 541 Security Coordinator Day Ahead Check Process: separate check process carried out by SC (Security Coordinator) in parallel with the checks carried out under document 239 (above)

Document 527 Amending Constraints in Real Time: procedure to adjust constraints in MDE to ensure that the SPD model output is a closer match to real time operation

Document 553 Re-rating of Constraints in Real Time: procedure to adjust SPD constraints in real time where the constraint is linked to a branch re-rating associated with outages

Document 585 Real Time MDE Updates for Grid Owner Offer Changes: analysis of new offer is carried out by Operation Planning Engineers as well as SC, checking whether asset capabilities and voltage stability requirements are exceeded. Where violations occur, permanent security constraints are developed and applied

---

**17** System Operator to Apply Permanent Security Constraints to the Scheduling Pricing and Dispatch (SPD) software model for expected normal range of dispatch scenarios with all transmission assets available by: **Fully met**

- 17.1** Identifying contingent and stability events that ... may ... result in the need for security constraints
- 17.2** Analysing a range of transmission, generation and power flow scenarios
- 17.3** Designing and applying security constraints to maintain post-event stability; short-term overloads, and allow time for re-dispatching generation or demand shedding to maintain operation within ...transmission capability

How rule is met:

Same as for 15.1 and 15.2 above

---

**18** System Operator to Apply Temporary Security Constraints to the Scheduling Pricing and Dispatch (SPD) software model for expected range of dispatch scenarios when assets are temporarily unavailable or asset capability is temporarily changed as notified by asset owners. Temporary security constraints will be: **Fully met**

- 18.1** Determined by identifying possible contingent and stability events that ... may ... result in the need for security constraints:
- During outage coordination and commissioning planning.
  - During the scheduling period and in real time.
- 18.2** Applied to ..... maintain post-event stability; short-term overloads, and allow time for re-dispatching generation or demand shedding to maintain operation within ... transmission capability
- 18.3** Applied ... for a defined period of asset unavailability or changed asset capability  
.....

## How rule is met:

Same as for 15.1 and 15.2 above, but in particular:

Document 237 Assess and Confirm Plant Requests Workflow: contingency analysis completed to ensure sufficient network capability for plant outage requests

Document 527 Amending Constraints in Real Time: procedure to adjust constraints in MDE to ensure that the SPD model output is a closer match to real time operation

Document 553 Re-rating of Constraints in Real Time: procedure to adjust SPD constraints in real time where the constraint is linked to a branch re-rating associated with outages

Document 585 Real Time MDE Updates for Grid Owner Offer Changes: analysis of new offer is carried out by Operation Planning Engineers as well as SC, checking whether asset capabilities and voltage stability requirements are exceeded.

Where violations occur, permanent security constraints are developed and applied

- 19** When circumstances require a constraint is to be applied or modified at short notice the initial constraint design be conservative to maintain security. This may also apply for the initial application of a permanent constraint. The System Operator will use reasonable endeavours to refine any constraint for accuracy and as operational experience permits.

**Partially met:**  
compliance is indeterminate on first half of clause

## How rule is met:

Document 327 Security Constraint Development and Review Process: Outlines that Operational Planning Engineers are responsible for reviewing the post real time performance of constraints and doing any fine-tuning to ensure they meet their objectives

- 20** The System Operator will:
- 20.1** Advise participants of permanent constraints two weeks prior to ... implementation, including brief summary of constraint design ...
- 20.2** At time of assessment, advise any asset outage constraints that will apply for planned outages through the Planned Outage Coordination process.
- 20.3** List all asset outage constraints on the System Operator's website including some prescribed details
- 20.4** Notify participants when a constraint has been applied or modified pursuant to clause 19 and the System Operator identifies the giving of such notification will assist it meet the PPOs
- 20.5** Correctly apply all constraints described in clauses 17, 18 and 19 to the SPD model.

**Partially met:**  
unclear if 20.2 is met; clarification of procedures required

## How rule is met:

Document 327 Security Constraint Development and Review Process: notification requirements are set out, including procedure for listing all asset outage constraints on Transpower's website. Document needs updating as notification of permanent constraints is "4 hours" in one part of document and "two weeks" in the overview section of same document

Document 342 Issuing a Customer Advice Notice: This document outlines the types of information covered in a CAN, who the CANs should be issued under and procedures for issuing CANs

Document 506 Distribution of Notices: procedure setting out the required distribution of various types of notices, and the make-up and maintenance of distribution lists, including those applicable to CANs, but excludes the distribution of block constraint notices

Document 243 Week Ahead Process Flow Overview: procedure includes the issuing of market notices, but does not specify that at time of assessment, any asset outage constraints are to be advised. The advice is sent a week ahead.

A number of checks are included to ensure constraints are correctly applied: Document 243 Week Ahead Process Flow Overview; Document 242 Week Ahead MDE Entry; Document 239 Day Ahead Grid Plan Check and Document 541 Security Coordinator Day Ahead Check Process.

<p><b>64</b> To carry out the security assessment, the System Operator will:</p>	<p><b>Partially met:</b></p>
<p><b>64.1</b> Produce a Security Schedule independent from the Pre-dispatch Schedule [by some specified time].</p>	<p>clarification required -</p>
<p><b>64.2</b> Perform further security assessments during the schedule period if [circumstances change]. A new security schedule will be produced at least four times per day.</p>	<p>procedure for meeting</p>
<p><b>64.3</b> Use .. inputs ... including security constraints derived by the system operator...</p>	<p>64.8 not explicit in</p>
<p><b>64.4</b> Update the current security schedule for each trading period with any changes .... and ... adjustments to meet the dispatch objective for each trading period. .....</p>	<p>document- tation</p>
<p><b>64.7</b> Assess power flows to identify and assess possible transmission security restrictions, capacity restrictions, or voltage conditions on the grid.</p>	
<p><b>64.8</b> Identify stability conditions on the grid.</p>	
<p><b>64.9</b> Identify and apply security constraints, where necessary, to constrain subsequent schedules and dispatch.....</p>	

How rule is met:

In addition to documents on deriving the security constraints (as above):

Document 373 System Management: procedure setting out the steps for producing Security Dispatch Schedules at least four times a day

Document 527 Amending constraints in real time: procedure for adjusting security constraints when triggered by a number of tests and queries

Document 553 Re-rating of constraints in real time: as a result of outage being postponed or cancelled mid-outage or being brought back early

Document 585 Real Time MDE updates for Grid Owner Offer Changes: response to Grid Owner Offer changes which require modifications to asset outage constraints in MDE in real time

---

**65** Each Pre-Dispatch Schedule will .... include: **Fully met**

**65.1** Security constraints entered by the system operator .... The security constraints will be the most recent, derived from security assessment processes prior to and during real time.

.....

How rule is met:

Document 373 System Management: document notes that the PDS is produced and published automatically every 2 hours starting with the 13:00 PDS

In addition, with the MDE being modified in real time through documents 527 Amending constraints in real time, 553 Re-rating of constraints in real time, and 585 Real time MDE updates for Grid Owner Offer Changes, the MDE being used to produce the PDS will result in the most recent security constraints.

---

**66** .... the system operator will .... adjust a dispatch schedule, where ... required, to include: **Fully met**

**66.1** The most recent security constraints identified from the security assessment processes, including any refinements made under clause 19 of the Security Policy in Section C4.

.....

How rule is met:

As above: with the real time modifications to constraints in MDE, the Dispatch Schedule would pick up the most recent security constraints identified from security assessment processes.

---

**67** To continually meet the dispatch objective during a trading period, .... the system operator will adjust the current dispatch schedule to: **Fully met**

**67.1** Produce a new dispatch schedule during the current trading period to incorporate:

.....

- security constraints required to meet the dispatch objective

How rule is met:

As above

---

....

**69** As part of the inputs specified in the rules, each SDPO will .... include: **Fully met**

**69.1** Security constraints entered by the system operator up until the time that the schedule commenced solving.

.....

How rule is met:

As above

---

---

### 3.0 Terms of Reference

The objectives of the review are to:

- Confirm the processes for the design, application, use and removal of constraints are consistent with:
  - Clause 15.1 and 15.2 of the Policy Statement in schedule C4 (in relation to asset capability and stability)
  - Clauses 17 – 20 of the Policy Statement in schedule C4
  - Clauses 64, 65, 66, 67 and 69 of the Policy Statement in schedule C4
  - Rule 2.1 of section II of Part C of the Rules
- Confirm the System Operator applies a consistent and reproducible practice consistent with its stated processes
- Confirm the system operator has made adequate changes to address the original cause of the error
- Determine any process improvements or additions

The scope does not include the constraint design methodology, which was audited in 2004.

The review was limited to security constraints in particular. However, the findings may be applicable to other constraint types.

### 4.0 Background

On or about 22 April 2004, SPD contained a security constraint what was meant to have been removed, but was not. The industry had previously been notified that the constraint had been removed. The constraint bound in trading period 36 (17:30 – 17:59), the result of which was that a number of nodes experienced high prices, and one node experienced negative prices. A market participant reported a potential undesirable trading situation (UTS) to the Electricity Commission. The Commission subsequently found that a UTS did indeed exist for that trading period. In the investigations and discussions that followed, it was identified that the issue of major concern to market participants relates to the development, application, notification and removal of permanent security constraints. A settlement agreement, the “UTS Settlement Agreement” [reference EGR285], was concluded, a provision of which was that the System Operator was to commission an audit of its processes for the design, development, testing and application of constraints, and its processes for removing constraints.

This report is the result of that audit.

---

---

## 5.0 Review Process

The following steps were taken in the review:

- Clarification of terms of reference, identification of review resources including documentation to be reviewed, timing, and personnel to be interviewed
- Review documented procedures and identify if these are consistent with EGR rule requirements
- Conduct interviews with personnel identified earlier and obtain further documentation of processes
- Review documented procedures for content and consistency of process
- Undertake on-site verification to confirm compliance with each process
- Confirm if the System Operator applied a consistent and reproducible practice consistent with its stated processes
- Confirm if, for the particular instance of the UTS in reference EGR285, the system operator has made adequate changes to address the original cause of the error
- Determine any gaps and recommend process improvements or additions

## 6.0 Documentation reviewed

(listed here in numerical order, but the review does not follow this order)

### Constraint design

Doc 325 – **Security Constraints Database Operating Procedure** (59 pp) (includes ACI Process States flowchart)

Doc 326 – **Security Constraints Development Methodology** (21 pp)

Doc 327 – **Security Constraints Development and Review Process** (41 pp)

Doc 329 – **Testing Security Constraints Using Esched** (20 pp) (how to test a constraint using Esched)

### Constraint Application (including notification)

Doc 237 – **Assess and confirm requests workflow** (9 pp)

Doc 242 – **Week ahead MDE entry** (5 pp)

Doc 243 – **Week ahead process flow overview** (9 pp)

Doc 327 – as above

Doc 480 – **Constraint Bundling** (4 pp) (how to build constraint bundles)

### Constraint Use (Real time) including day ahead checking

Doc 239 – **Day ahead Grid Plan check** (6 pp)

Doc 373 – **System Management** (9 pp)

Doc 480 – as above

Doc 527 – **Amending Constraints in Real Time** (6 pp)

---

---

Doc 541 – **Security Co-ordinator Day Ahead Check Process** (5 pp)

Doc 553 – **Handling of Re-Rating Constraints in Real Time** (9 pp)

Doc 585 – **Real Time MDE Updates for GO Offer Changes** (10pp)

#### Constraint Removal

Doc 325 – as above

Doc 327 – as above

#### Notifications

Doc 342 – **Issuing a Customer Advice Notice** (10 pp)

Doc 506 – **Distribution of Notices** (14 pp)

SI 50 – **System Operator Notices Overview** (16 pp)

#### Approvals and Logs

Doc 454 – **Logging of Events in MELT** (8 pp)

Checklist – **Security Constraint Review/Approval Checklist** (1 pp)

#### Background Information and Event Reports

Doc 548 – **Security Constraints Naming Conventions** (10 pp) (how to name constraints)

Doc 598 – **Determining Conductor Thermal Characteristics for use in Constraints Development** (6 pp) (how to find thermal ratings)

Selection of **National Grid Plans** (produced daily by Operations Planning)

Event report - **TGA\_TRK\_1\_S\_P Group Constraint Issue, Saturday 24 April 2004 (Breach reference EGR201)**, Event reference 179

Internal memorandum – example of constraints applied after they had been superseded

## 7.0 Personnel interviewed

Interviews were held with the following staff members:

- Angela Houston, Operations Planning Team Leader
- Derrick Westenra, Market Services Manager
- Phillip Pigeon, Operations Planning Engineer
- Mark Gilchrist, System Coordinator

A brief discussion was also held with Dave Harper, Security Coordinator.

---

---

## 8.0 Outline of EGR Requirements relating to Security Constraints

(Clauses refer to Policy Statement in schedule C4, unless otherwise stated)(Relevant EGRs rules are provided in the appendices)

Rule 2.1 of Section II of Part C	<p>This rule specifies that one of the Principal Performance Obligations of the System Operator (SO) is that the SO is to act as a reasonable and prudent operator with the objective of dispatching assets in a manner that cascade failure of assets resulting in the loss of demand is to be avoided, arising from frequency and voltage excursions or supply and demand imbalances.</p> <p>This is an overriding objective, and the practical outcome of this objective in relation to security constraints is to ensure that where security constraint(s) can be applied, the absence of which may lead to the above circumstances, the SO is required by this rule to ensure that such security constraints are indeed applied.</p>
Clauses 15.1 and 15.2	<p>These sub-clauses relate to quality levels the SO plans to achieve for contingent and extended contingent events. During contingent events and extended contingent events, asset capability is not to be exceeded, the prescribed grid voltage range is to be maintained by the SO, voltage stability is to be maintained, and certain matters relating to frequency are to be observed.</p>
Clause 17	<p>This clause states that the SO will apply permanent security constraints to SPD with a process of identifying system scenarios, designing appropriate constraints to manage these scenarios, and applying these constraints to SPD in order to ensure the system maintains a certain level of post event integrity.</p>
Clause 18	<p>This clause states that, when assets are temporarily unavailable or when asset capability is temporarily changed as notified by asset owners, the SO will apply temporary security constraints (including asset outage constraints) to SPD with a process of identifying system scenarios during outage planning, commissioning planning, within the scheduling period as well as in real time, and applying any temporary constraints identified which will ensure the system meets certain levels of post event integrity.</p> <p>These constraints are applied with a defined period.</p>
Clause 19	<p>This clause states that when circumstances require a constraint to be applied or modified at short notice, the initial design needs to be conservative, to maintain security, allowing for the SO to use reasonable endeavours to refine the constraint for accuracy and as experience permits.</p>
Clause 20	<p>This clause primarily relates to notification of constraints by the SO. The requirements are notification of permanent security constraints at a defined time before they are applied, including certain information to be supplied; assessment of asset outage constraints required in relation to temporary changes in asset capability and at the time of assessment, advise appropriate parties of these; provide a list of all asset outage constraints available for use on the SO's website including certain prescribed details; notification when constraints have been applied or modified at short notice but only if such notification to participants will</p> <hr/>

---

help the system operator meet its PPOs.

The clause also requires that all constraints be applied accurately to the SPD model.

- Clause 64 This clause requires the SO to prepare a security assessment for the Schedule Period by producing a Security Schedule independently from the Pre-Dispatch Schedule, concurrently with its first production at 13:00, covering the same period as the Pre-Dispatch Schedule. Further security assessments are to be carried out during the Schedule Period based on circumstances, but in any case the Security Schedule is to be produced at least four times a day.
- In addition to inputs described in rule 1.3.2 of schedule G6 of part G, the security assessment will include security constraints derived by the SO, up until the time that the Security Schedule commenced solving.
- There are other requirements in this clause not related to security constraints.
- As part of the security assessment, there are also requirements to assess power flows to identify and assess possible transmission security restrictions, or voltage conditions on the grid, and to identify stability conditions on the grid. The security assessment is required to identify and apply [further] security constraints, where necessary to constrain subsequent schedules and dispatch.
- Clause 65 This clause requires that each Pre-Dispatch Schedule is to include Security Constraints entered by the SO, up until the time that the schedule commenced solving. The security constraints are required to be the most recent, derived from security assessment processes prior to and during real time.
- Clause 66 This clause requires the Dispatch Schedule to include Security Constraints entered by the SO, up until the time that the schedule commenced solving. The security constraints are required to be the most recent, derived from security assessment processes prior to and during real time.
- Clause 67 In order to meet the Dispatch Objective during the Trading Period, this clause requires that the SO adjusts the Dispatch Schedule during the current trading period to produce a new Dispatch Schedule by incorporating, among other things, security constraints required to meet the dispatch objective.
- The system operators' Dispatch Objective is to maximise for each half hour the gross economic benefits to all purchasers of electricity at the grid exit points, less the cost of supplying the electricity at the grid injection points and the cost of ancillary services purchased by the system operator, subject primarily to the capability and availability of the system, achieving the principal performance obligations, and certain requirements for restoration.
- Clause 69 This clause requires that each Schedule of Dispatch Prices and Quantities (SDPQ) is to include security constraints entered by the SO up until the time that the schedule commenced solving.
-

---

## 9.0 Review of Main Documented Procedures related to Security Constraints and Interviews with Staff

Preamble:

Security constraints are constraints placed by the system operator in SPD to ensure that it meets its Principle Performance Obligations and various requirements under the EGRs, to enable the system operator to achieve certain quality conditions and limits during and following the occurrence of contingent events and extended contingent events as specified in the EGRs. They are applied pursuant to various requirements of the EGRs.

One of the Principal Performance Obligations of the SO is that the SO is to act as a reasonable and prudent operator with the objective of dispatching assets in a manner that avoids the cascade failure of assets resulting in the loss of demand and arising from either frequency and voltage excursions, or supply and demand imbalances (Rule 2.1 of Section II of Part C).

The system operator's Dispatch Objective is to maximise for each half hour the gross economic benefits to all purchasers of electricity at the grid exit points, less the cost of supplying the electricity at the grid injection points and the cost of ancillary services purchased by the system operator, subject primarily to the capability and availability of the system, achieving the principal performance obligations, and certain requirements for restoration.

### 9.1 Constraint Design, Development and Testing

#### 9.1.1 Document 327 Security Constraint Development and Review Process

This document sets out the processes and responsibilities for initiating, developing, documenting, notifying and implementing transmission security constraints in the SPD model.

It covers the management of system voltage and stability.

A large number of change notification processes are noted for a large number of circumstances which result in a requirement to make changes to constraints, such as a change in transmission capacity or impedance, a change in generation capacity, a change of load or load growth, a change of operational configuration, grid outages, a change to SPD model, and violations in real time operations.

Compliance

Rule 2.1 of Part C Section II; clauses 15.1 and 15.2; 17, 18 (except for removal of constraints (18.3); 19 (partial) and clause 20.3, 20.4, 20.5. Clause 20.1: clarification required on notice period.

---

---

When one of these triggers or inputs is received, the Operations Planning Engineer (OPE) performs a security assessment through power flow, contingency analysis or dynamic stability analysis for possible and likely worst generation scenarios. The OPE also performs loading scenarios for the affected area for both summer and winter ratings. These are to identify possible steady state loading violations or unmanageable single contingent events. All likely worst case scenarios are considered.

Where a power flow solution shows unmanageable contingencies, this highlights the areas that need to be managed by security constraints. The dynamic and voltage stability issues are identified by a tool called "VSAT" (Voltage Stability Analysis Tool). In addition to system studies, flags for action also arise from unmanageable contingencies in scheduling and real time operations as well as infeasibilities in SPD caused by security constraints.

If constraints are required, the constraints database (ACI, asset capability information) is used to identify all existing constraints with the affected SPD branches. Where no existing constraints are identified, new constraints are created in the ACI database.

The constraints are either permanent - relating to the 'normal' grid configuration when all transmission capacity is available, or outage constraints - where these are constraints as a result of equipment outages, both forced and planned.

Where an existing constraint is identified, it is checked for validity, using power flow for confirmation as necessary.

If changes to the constraint are required, or for new constraints, whether the constraint needs to be tested in SPD or not is determined. This is by reference to whether the constraint is to be applied in an area with non-conforming loads, or commercially or politically sensitive loads.

If the modified or new constraint does not require testing in SPD, approval by another OPE is sought at this stage.

If the modified or new constraint requires testing in SPD, the procedure for fine-tuning or testing constraint is then used (document 329 Testing Security Constraints Using Esched). If the results from the SPD testing are acceptable, approval for the constraint by another OPE is sought.

Once approved, whether changes are required to MDE constraints or to SPD security branch limits is then determined. If the constraints are to be entered as MDE equation constraints, the constraints are released to MDE upon approval above.

If a change to SPD security branch limits is required, a number of processes are specified for doing this, with Market Services having the responsibility for changes to the SPD Security Branch Limits, and Operations Planning having the

---

---

responsibility for updating circuit ratings. The OPE does however review all changes made by Market Services and verifies the entry in SPD has been made as per requested. The constraints database is updated once changes to SPD have been made. Some further steps are provided where a constraint is required in a bundle. Notification requirements are then specified.

Responsibilities:

The procedure notes that Operation Planning Engineers (OPEs) are responsible for:

- identifying requirements of security constraints through the Equipment Ratings Change Notification process
- general power system or outage assessment studies
- developing security constraints in a timely manner
- updating and managing the contents of the ACI constraint database
- notification of internal and external stakeholders of changes to existing constraints or creation of new constraints
- reviewing the post real time performance of constraints and doing any fine-tuning to ensure that they meet their objectives.

The procedure notes that it is the responsibility of Market Services Analysts to identify affected security constraints in MDE and SPD as a result of SPD branch changes and notify OPEs of this, as well as to arrange update of security branch limits in the SPD model in a timely manner. The process for doing this is outlined in 295 Changing SPD Corporate Data - Asset Capability Information Changes.

The Operations Planning Team Leader (OPTL) ensures the process outlined in the document is followed, as well as reviewing and approving security constraints to be entered into SPD. The Operations Planning Manager ensures staff follow this process, and is the party accountable to TP management for this process.

Notifications:

Notification processes are then followed to notify parties of permanent constraints only, and the weekly list of constraints on Transpower's website is updated. The instruction for notification then outlines that at least 4 hours is to be allowed for from notification to the application of permanent constraints. The EGRs state that permanent constraints require a 2

The process document specifies two different dates for notifying permanent constraints. The document needs updating.

---

week notification period.

On-site verification for these processes looked at an example of a PROMS outage request, and following through a number of pages which showed the various steps in the process for assessing such requests in order to identify whether security constraints will be required in the particular circumstance.

Also viewed were powerflow modelling outcomes showing unsolved contingencies, unmanageable contingencies, harmful contingencies and potentially harmful contingencies.

Clarifications, identification of gaps and recommended actions:

- 1 The notifications outlined show two different time periods for notification of permanent constraints
  
- 2 The document lists the inputs and triggers that result in a change to transmission security constraints. The required change in constraints may be a result of changes in transmission capacity or impedance, change in generation capacity, change in load or load growth, change of operation configuration, grid outages, changes to the SPD model, and violations in real time operation.  
  
 Transpower staff have noted that in addition to these triggers, in practice Operations Planning review all constraints that Market Services identify being affected in MDE and SPD (i.e. always perform step 3B1 in document on this trigger). This is shown in one of the flow charts in the document, and the party responsible for doing this is also clearly specified, but this step itself is not included in the main text of the process document.

Transpower Comments:

327 Document update required – we outline the 2 week notification period in the Overview section on p8 - p32 step 2 should be amended to take out reference to 4 hours.  
  
 [Transpower identified this issue and notes that document 327 needs to be updated to better reflect this].

Document Procedure Changes

Document Procedure Changes

3	<p>The validation of existing constraints entails a number of checks to be made of whether the SPD constraints are referring to the current SPD branches at all times. What is the flag that the SPD constraints are not referring to the current SPD branch? Although a process is noted for how to determine the SPD branches and flow direction, there are so many branches that it is unclear what would draw the OPEs attention that a branch is in fact incorrect or not the current one.</p>	<p>When undertaking the peer review/approval process the SPD branches included in the constraint equations are checked for correctness – this is usually a check to see that the correct section of a circuit is in the equation, rather than the name is correct. ACI synchronises with SPD daily to ensure SPD branch names are current. An SPD branch would only be not current if it was a brand new one that has not been loaded into SPD yet, in which case it can be created in ACI and then over-ridden by the new one once it is created in SPD. All others SPD branches are time-stamped and their names do not change. 327 Document update required to explain this.</p>	<p>Document Procedure Changes</p>
4	<p>The process of “Identifying SPD Branches for Underlying Circuits” is provided at the end of the document. It notes that the circuit rating spreadsheet and the SPD drawing are only updated once a fortnight and the changes to either may not be synchronised. What is the barrier preventing these basic information documents from being continually up to date and showing non-contradictory information?</p>	<p>Documentation is not correct in the Synchronising changes section. SPD branches do not change very often due to use of time-stamping, and the tools/SPD drawing is updated on an as-required basis. 327 Document update required.</p>	
5	<p>It is also unclear why the SPD drawings may not reflect the actual grid, with future changes being allowed to be incorporated into the spreadsheet or drawings while not yet commissioned. Within this review, a number of processes would be improved through the use of time-stamping of various documents. In this instance, a drawing that will become obsolete should have a “valid to” date, and a drawing or circuit rating spreadsheet that</p>	<p>The SPD diagram is maintained as current on the intranet – hence there is only ever one (current) version available for reference. Agree with comments with respect to having one source of ratings information which is the role of ACI. The GO is currently working on a number of ACI fixes to improve handover of ratings information to the SO.</p>	<p>General Process Improvement</p>

reflects a future scenario should have a “valid from” date, and the clocks on the IT system should be used to flag whether something is currently applicable or not. The current process requires a manual check with a particular designated OPE staff member and a MSA staff member to check what is current or valid, etc. What if that staff member is unavailable? It is not reasonable to have databases that are not accurate or current.

6

7 The testing of constraints in SPD is not always carried out, with the guidelines specifically mentioning testing in the circumstance of non-conforming loads and commercially or politically sensitive loads. Is there a concern or time issue with testing all constraints in SPD? This would remove a subjective decision from OPEs which is outside their area of expertise (for example, in determining whether a load is considered commercially or politically sensitive or not). Commercially sensitive to whom – a lines company, a retailer, a generator, no-one important?

It is not feasible to test all constraints in ESCHEd – this requires Market Services to do, and is not set up to provide realistic data, so results are often inconclusive. 327 Document update required to change wording of commercially or politically sensitive loads.

327 wording needs to be updated to reflect that new ‘type’ or ‘class’ of constraints are to be tested in esched prior to going into production e.g.: recently used voltage stability constraint used for UNI security). There is little value in testing conventional permanent and outage constraints due to the number of constraints involved and the unsuitability of the test platform (esched), however new ‘types’ of constraint (e.g. mixed integer constraints) are rigorously tested to ensure they deliver the right outcome.

Document Procedure Changes

8 Where a constraint has been changed, it has to be approved by a second OPE. Should the constraint actually be approved by a more senior staff member rather than a peer?

Currently the approval is done by a team leader, but peer review by a peer OPE is possible. These OPEs should have sufficient knowledge of the process requirements to carry this out.

N/A

N/A

N/A

9	It is unclear from the documented procedure the difference between a SPD security limit and an MDE equation constraint.	An SPD security limit is reflected by a branch constraint in MDE. An equation constraint contains more than one SPD branch. 327 Document update required to make this distinction.	Document Procedure Changes	
10	Under stages 9 to 12, where a SPD Branch security limit is required to be changed, the OPE responsible for updating the Circuit Rating spreadsheet is advised. It is unclear who advises this person.	The OPE (after consultation with team leader) who determines the need to change the SPD limit.	Document Procedure Changes	
11	The process then notes that when the constraint has been reviewed and approved (by whom is not specified)...	327 document update required – this approval is by the team leader		General Process Improvement
12	(cont) ... the delegated Market Services Analyst managing the SPD model is then advised (by whom is not specified).	327 document update required - by the OPE following this process		General Process Improvement
13	At this stage, the constraint database is updated to include the security branch limit once changes to SPD security constraints have been made. Can the constraints database be modified within the same step as the changes to the SPD security constraints, so that there is no opportunity for error/misalignment between the constraints database and the SPD security constraints?	Not really, it has to be done independently in ACI		General Process Improvement
14	General comment: the constraints database should be the location of all information relating to constraints, but there are a number of instances where the constraint database does not reflect actual constraints.	There is a mismatch between constraints in ACI and MDE that we are currently addressing with a query that is run on a regular basis to compare the content of MDE and ACI	Process Issue	

<p>15 There are a number of references to documents such as 'Refer to the Word file called "342 Issuing a Customer Advice Notice" stored in \\wnfs1\GOS_doc\System_Management\notices for more information'. A recommendation is that all instructions should be placed in one common location, not spread throughout the IT system. This will ensure no duplication, easier management and control, and that latest versions of documents are the only ones on the system.</p>	<p>327 document update required - the document reference should be updated to the DMS folder, where all of our documentation now resides</p>	<p>Document Procedure Changes</p>	
<p>16 The constraints to be notified are extracted from the constraints database. There is a place for entering the "Schedule From Date" for new constraints. However, this entry is purely for information purposes only – any dates entered in here are not automatically picked up by any process. This means that although a "schedule from" date is entered here, the constraint is actually scheduled by a Hamilton OPE manually, and any information in this entry may or may not reflect what is actually scheduled. The issue here is that the document gives the impression of something being done, when in fact there is no certainty that the action is actually being taken.</p>	<p>Need to differentiate here between constraints that are going to be used in the short-term, i.e. new permanent constraints and those for upcoming outages, as opposed to ones that are being revised as a result of a ratings change, etc. If they are the latter, they are not going to be scheduled in the near future, and hence we use generic comments such as 'schedule during the next xxx_xxx summer outage'</p>		<p>General Process Improvement</p>
<p>17 An instruction is then provided to create an email of the notification. There is a further step which requires the sender of the email to file then file the sent email in a new folder called "Outlook/Operations Planning Mailbox/Constraints Advice". This step should not be manual. This is necessary to ensure ease of audit and tracking. All such constraints advice should be automatically logged and not require a secondary step, given the</p>			

---

possible significant effects of permanent constraints on the whole market.

18 There is also an instruction for notifying the Internet Administrator to update the SMS CAN website when a CAN is issued for, among other things, changes to permanent security constraints. This notification is a manual process, whereas it should be automated so that CANs relating to changes to permanent security constraints are always notified to the internet administrator, or even more appropriately, as the technology allows, automatically posted on the internet when issued.

19 These intermediary manual steps (outlined in the preceding paragraphs) should not be part of the process, as they require no expert input, but the opposite – they are trivial actions which are relatively easy to accidentally omit on the part of the operator. As these intermediary steps are always taken, this is an area for automation to remove the prospect of human error.

20 Clarification required: the references in “External policy/rules and regulations” are incorrect and need to be updated, and “Internal policies and guidelines” contain reference to a document that no longer exists – Standing Instruction 51: “Communication and Documentation of Outage Security Issues”. Also, “Standing Instruction 50: Issuing Security Notices” is now called by another name.

327 Document update required

General Process Improvement

General Process Improvement

Document Procedure Changes

---

21 Clarification required: In the "Responsibility" section, the table shows that OPEs are responsible for notifying both internal and external stakeholders of changes to existing constraints or creation of new constraints, but the text says that Security Coordinators should be issuing CANs for all constraints. The responsibility for the issuing of CANs should be clarified, so that only one party is responsible.

327 Document update required – OPEs contribute to the notification process by identifying when CANs are required to be issued for constraints, and drafting CANs for permanent constraints. The Security Coordinator always sends them out

Document Procedure Changes

**9.1.2 Document 326 Security Constraint Development Methodology**

This procedure sets out the process for developing security constraint equations to manage grid equipment and circuits to their:

- steady state continuous maximum limits, and
- contingency short term ratings.

The document does not cover managing system voltage and stability.

The document notes that:

"All possible contingencies must be identified, suitable constraints developed and incorporated into the SPD model ahead of real time." ("Overview" section of paper, under heading "Identifying contingencies")

The SO uses an operational database to run power flows ahead of real time and during real time to model the system's operation, using the STNET/STCA (study-time network / contingency analysis) and RTNET/RTCA (real time network / contingency analysis) applications.

The model outputs reveal whether assets will be operating within their capabilities or not, as well as resulting voltages at all nodes within the Transpower system. The program also identifies contingent events that will result in asset capabilities and voltage stability requirements being exceeded.

Compliance

Compliance with Rule 2.1 of Part C Section II, and clause 15.1 and 15.2 insofar as asset capability is concerned.

Clauses 17 and 18 are partially covered as to identification of system scenarios and the designing of the required constraints.

In summary, for a particular pre-event circuit loading, a post event circuit loading is determined. If this post event loading will cause the particular conductor to reach its sag limit in less than 15 minutes, then the pre-event circuit loading must be constrained back. The pre- and post-event loadings are calculated by reference to load distribution factors between circuits, to determine what the increase in circuit loading for a particular transmission circuit would be if it has to share the load of a line that tripped out.

It is noted that a primary assumption in this document is that the equations are calculated to give the System Operator a 15-minute window to implement any other actions to manage a contingency. This means that the security constraints being developed are to ensure compliance with clause 15.1 and 15.2 in the first 15 minutes after a contingent event. Other remedial actions by the System Operator may or may not be required to ensure continued compliance outside of this period, but at least the System Operator has a reasonable time (15 minutes) to implement these actions.

Clarifications, identification of gaps and recommended actions:

Transpower Comments:

22 It is unclear what happens if the circuit rating is limited by the static limit or static protection settings, and what this means for the development on constraints, as the document outlines how to determine the constraints equations under the circumstance where the circuits are limited by their thermal limits as their limiting factors, not their static limits or protection setting limits.

The documentation has been recently updated to be more explicit about static component constraints.

N/A

N/A

N/A

**9.1.3 Document 325 Security Constraints Database Operating Procedure**

Compliance

This document sets out the procedures for adding/viewing/modifying constraints.

Compliance with Rule 2.1 of Part C Section II, and clause 15.1 and 15.2, 17 and 18.

Operations Planning use the ACI database. This database is found in the ACI application. The database records details of all transmission security constraints that are planned or have been applied in the SPD model.

The key point to note is that the constraints database is not a real time operational database. Constraints that are modified in the database may take up to a week before they are applied in SPD. Any changes in MDE will not be reflected

in the constraints database.

There is a review process that requests approval for a constraint or bundle, and then allows the reviewer to accept or reject it as appropriate.

File transfer is able to be used for constraint information to be published on the Transpower website.

Although constraints can be inactivated in MDE when superseded, there is an issue that where a constraint has been applied in MDE, the constraints database does not allow the constraint to be superseded.

An Operations Planning Engineer has write-access to the constraints database, but a Security Co-ordinator only has read-access. However, a Security Co-ordinator has access to MDE to modify a constraint which is in MDE.

On-site verification of this included viewing a sample of constraints which are to be superseded, the spreadsheet outputs showing what is being superseded and the replacement constraints, reviewer checklist, extraction of these constraints into a spreadsheet, the importing of the spreadsheet into an email for notification.

Clarifications, identification of gaps and recommended actions:

- 23 When a constraint or constraint bundle is created, the constraints database will allow more than one object with the same description, but MDE will not allow this. What is the practical effect of two objects having the same description? If the effect is likely to have a market effect, then the constraints database needs to be modified so that when a new object is entered, it cannot share the same description as another object. At present, there is an instruction specifying that the same name should not be used, but the software would accept it, which leaves room for human error.

Transpower Comments:

There is a rule in ACI that rejects any record to be added which has the same name of a constraint or bundle that exists. An error arises, and so the user is forced to use a different name. So this is consistent with MDE. 325 document update required to explain this.

*[Reviewer response to Transpower: if the explanation above is saying that no two names can be the same in the ACI database as the ACI software will NOT accept this, then a document update is required.*

*If to the contrary, that is, the ACI software will accept the duplicated name (as currently documented), then a change in the software will need to be investigated.]*

Process Issue or	Document Procedure Changes

24	<p>The instructions for cloning an object states that automatic superseding of a constraint can be achieved by ticking the “supersede cloned constraint” box – does this automatic superseding of constraints prevent them from being applied in future?</p>	<p>Yes, they become inactive in MDE so cannot be applied. They can be reactivated again in ACI if required to be applied again at a later time. 325 document update required to explain this</p>	<p>Document Procedure Changes</p>
25	<p>When the cloning process is used to automatically supersede constraints, if the old constraint is scheduled in MDE it will not be deactivated, even though it may be superseded in ACI at this stage. (Page 39 of 5, bottom of page). If the intent of the developer is to ensure that the constraint is no longer able to be used, this objective will not be met, as long as the old constraint remains scheduled in MDE.</p>	<p>We have asked for an IT change to prevent this happening</p>	<p>Process Issue</p>
26	<p>If the constraint is no longer scheduled in MDE, will it then be unable to be applied again?</p> <p>As in the item above, if the constraint remains active and available for use, despite the intent that it should become inactive once the scheduling in MDE has ceased, then a reminder or some flag needs to be implemented to ensure staff are alerted to this, to ensure the constraint is not re-applied inadvertently.</p>	<p>No, it still remains active and available for use again if required. It only is unable to be applied again once it is superseded / inactivated.</p>	<p>General Process Improvement</p>
27	<p>It is noted that when SPD branches are created in ACI, they are only valid for 14 days. The same branch name needs to be created in SPD for it to be active after this. Is there a process for informing someone that a new SPD branch needs to be created in SPD itself?</p>	<p>Yes, the equipment ratings change and commissioning processes inform Market Services of any need for new SPD branches. With time-stamping of SPD branches this does not happen very often. 325 document update required to explain this</p>	<p>Document Procedure Changes</p>

28 The procedure for Modifying Constraints and Constraint Bundles needs further explanation:

a. Why is it possible to change the RHS of a constraint, even though it notes in step 2 of page 40 that "...no other information will be updated in MDE after the constraint is created, particularly not the constraint equation. If the equation needs to be changed, the constraint will have to be superseded and another created. This restriction is in place to ensure the integrity of current and past scheduled constraints."?

If the RHS of the constraint is found to be too low or too high when it is applied in real time (i.e. the contingency violations used in the constraint design are not corresponding to the off-load time / equipment limit violations coming up in real time), it may be appropriate to adjust the RHS of the constraint. This is to ensure the constraint will not over or under constraint flows, and is usually due to a different voltage profile / reactive power flows used in the planning case. We refer to the equation as the LHS of the constraint, and this is what should not be changed at all once the constraint is available in MDE. 325 document update required to explain this

Document Procedure Changes

b. Why is it possible to change a constraint bundle and have no effect on past or current scheduled bundles? (Para 1 of page 41)?

Bundles are time-stamped in MDE. Retrospective changes to scheduled bundles are only made in specific circumstances (to resolve pricing infeasibilities) in order to preserve the integrity of historical data.

N/A

N/A

N/A

## 9.2 Security Constraints Application and Removal including for Outages

### 9.2.1 Document 237 Assess and Confirm Plant Requests Workflow

Plant requests are assessed up to 4 weeks leading up to the outage (purpose statement).

Maintenance contractors raise operational request for outage; an outage window is created, a plant request is created in PROMS containing specific details of the outage and the request is submitted to OPEs for approval. The Regional Operator searches daily on PROMS for lodged plant requests and submits PSOs (switching operations) to OPE for approval. OPEs

Compliance

Compliance with clauses 15.1 and 15.2, 17 and 18.

It is not immediately apparent that this process

---

then complete security assessment. For most requests a powerflow is completed to resolve potential loading and voltage issues. The document allows an experienced planning engineer to omit this step if the outage is known to have no load or voltage issues. The document notes that this is the exception rather than the rule. (Discretionary step)

A contingency analysis is completed to ensure sufficient network capacity.

The OPE is then to consider the risk implications (Step 8). The document is silent on what risks are acceptable or what risks are not. If the risks are acceptable, the plant (outage) request is approved by the OPE. (see Step 13)

If not, a discussion takes place between field services and the OPE, outlining options field services may have to take in order to get the plant outage request approved (Step 10). Options may include rescheduling of the outage or procuring additional generation commitments. The process may include discussing options with customers (Step 11). The plant request may have to be re-lodged (Step 11) or cancelled (Step 12), if no means can be found of addressing unacceptable risks.

Step 13 specifies that the OPE is responsible for updating the PROMS plant request status to "Approved". The plant requests may be approved conditionally, and the OPE dictates whether a request is confirmed conditionally or returned to field services for pre-requisite agreement to specified conditions.

Step 14 notes that it is the responsibility of OPEs to monitor PROMS for short notice requests, which is anything coming in less than 6 weeks from the start of the month.

Step 15 notes that Market Notices are to be indicated in the Security Schedule, but does not show who is responsible for this, or what consequential step follows this.

Step 16 notes that when a plant request is approved, it is added to the Grid Plan for the relevant day.

Step 17 then specifies that it is the OPEs responsibility to enter the outage into MDE at Week Ahead Check, that is, MDE is updated 7 days prior to outage commencement date.

A number of additional resources for completing security risk assessment are listed.

---

achieves compliance with clause 20.2, where a notification at the time of assessment is stipulated

Clarifications, identification of gaps and recommended actions:

Transpower Comments:

29 Step 14 notes that it is the responsibility of OPEs to monitor PROMS for short notice requests, which is anything coming in less than 6 weeks from the start of the month. This is in conflict with the purpose statement of this document, which states "Plant requests are assessed up to 4 weeks leading up to the outage".

237 Document update required

Document Procedure Changes

30 Step 15 notes that Market Notices are to be indicated in the Security Schedule, but does not show who is responsible for this, or what consequential step follows this.

237 Document update required - Responsibility needs to be added to document – OPE.

Document Procedure Changes

31 Step 17 specifies that it is the OPEs responsibility to enter the outage into MDE at Week Ahead Check, that is, MDE is updated 7 days prior to outage commencement date. The Flowchart that is part of document 237 notes that approved plant requests are to be entered into MDE by "10th". It is unclear how step 17 and the flowchart fit together.

237 Document update required – remove 10<sup>th</sup> in flow diagram, should be 7 days ahead

Document Procedure Changes

32 In addition, if the assessment was made 6 weeks prior to start of the month, then the entry into MDE may be up to 9 weeks later. From a process point of view, it may be simpler to carry out the two steps sequentially, that is, assess outage then enter into MDE for the future dates required, rather than having the two steps several weeks apart and then having to have a reminder to do something at some later date.

General Process Improvement

a. Can the entry be made in MDE at time of assessment?

Yes, week ahead check would pick this up.

N/A

N/A

N/A

	<p>If not, what is the flag for the OPE to remember to enter the outage into MDE? Is this carried out in the week ahead MDE data entry?</p>				
	<p>b. That procedure notes that "the Gridplan contains all MDE requirements except those that have simple PROMS to MDE relationships". What happens to these MDE requirements that is not in the relevant Gridplan?</p>	237 Document update required		Document Procedure Changes	
	<p>c. Also, is the OPE staff member who ensures that the approved request is entered into MDE the same staff member as that who did the approval? What is the process for ensuring that the MDE entry is made?</p>	<p>This is covered in the week-ahead and day-ahead checks, and is usually undertaken by a different OPE</p>	N/A	N/A	N/A
33	<p>Step 18 notes that it is the OPEs responsibility to change the outage request in PROMS from "lodged" to "approved". This has already been done in step 13.</p>	237 Document update required		Document Procedure Changes	
34	<p>A number of additional resources for completing security risk assessment are listed. Within this list, it is noted that "Transformer (Network Planning) and Circuit Ratings (Operations Planning) spreadsheets" are to be used, but which in future are to be replaced by the ACI (Asset Capability Information) tool. However, the processes outlined in the documents on the subject of developing constraints (which is within the ACI tool) specifically notes that Circuit Ratings are to be referred to in developing constraints. These two instructions are circular in nature and need to be clarified.</p>	<p>ACI does provide rating information on assets, but the tool is still not providing accurate information to the SO yet, so we are still relying on the use of the Circuit Ratings Spreadsheet. 237 Document update required to explain this further</p>		Document Procedure Changes	

---

35	The security risk assessment is completed when the outage is assessed. What are the processes for completing security risk assessments closer to real time, in accordance with clause 64?	This is covered by doc 541 Security Coordinator Day Ahead Check Process which ensures that all plant requests are in the grid plan and line up with MDE entries, and that any short notice requests or forced outages are included.	N/A	N/A	N/A
----	---	---	-----	-----	-----

**9.2.2 Document 243 Week Ahead Process Flow Overview**

Compliance

Overview of main process steps. This document outlines a process to ensure that all plant requests for the week ahead are confirmed, the grid plan is checked, and outages and constraints are entered into MDE, market notices are issued, as well as a contingency plan if necessary. The Gridplan is completed as an output of this process flow. The flowchart in the document shows that the Gridplan is “released” as the final step in the flowchart.

Compliance with clauses 15.1 and 15.2, 17, 18 and 20.3, 20.4, 20.5.

Clarifications, identification of gaps and recommended actions:

Transpower Comments:

36 The flowchart in the document shows that the Gridplan is “released” as the final step in the flowchart. In the day ahead grid plan check document 239, as grid plan is not “handed over” to the SC until the day before.

- a. Does “handed over” mean the same as released?
- b. What is the actual event that makes a gridplan become operational, as against simply a document that can be modified at will?

Yes  
Once the Security Coordinator receives it, it is operational. The Coordinator can still make changes to it once they ‘own’ it.

N/A N/A N/A

**9.2.3 Document 242 Week Ahead MDE Entry**

Compliance

This document is the main document for entering constraint bundles into MDE. The Gridplan is the starting document. Document 239 is effectively the procedure for undertaking step 17 in document 237.

Compliance with clauses 15.1 and 15.2, 17, 18 and 20.4, 20.5.

Clarifications, identification of gaps and recommended actions:

Transpower Comments:

- 37 The week ahead spreadsheet named in Step 6 does not line up with the name of the sheet in document 239.
- 38 It is unclear in step 15 that this is the step where the requirement for CANs should be indicated.
- 39 In document 243, step 11 is to issue market notices. Although the document outlines a process that is the OPEs responsibility and the OP Manager’s accountability, step 11 is the responsibility of the NCC Security Coordinator. This is confusing.
- 40 What is the flag to show the SC that a CAN is needed, and for the SC to issue the CAN 6 days before, as outlined in Step 11? Or is step 15 of document 237 the step that flags to the SC a CAN is required for an outage?

242 document update required to change it to GRIDPLANSMMDAYDD\_DD.XLS

237 Document update required – need for CANs is indicated in the Grid Plan and also in the Market Notice Monitoring Spreadsheet  
(\nipub\opsplanner\market\_notice\_monitoring\_ss\market\_notice\_monitoring.xls). The Security Coordinator checks this spreadsheet daily and confirms in the s/s when the notice is issued

242 Document update required

See comments in 37 above – 242 document update required to show current process

Document Procedure Changes

Document Procedure Changes

Document Procedure Changes

Document Procedure Changes

**9.3 Security Constraints Use including checking**

**9.3.1 Document 239 Day Ahead Grid Plan Check**

Whereas document 237 notes that the OPEs are responsible for ensuring any approved outage request is entered into MDE a week ahead, in the day ahead check, the OPEs and the Operations Planning Manager are respectively responsible and accountable to ensure that the next day’s Grid Plan is accurate and complete. The day ahead checks include multi-

Compliance

Compliance with clauses 15.1 and 15.2, 17, 18 and 20.5.

days ahead for weekends and public holidays for when there are no planners present. The Plan check is to be completed by 12:00 for handover at 13:00 to the SC. The procedure outlined is very prescriptive.

Further checks are specified in the procedure, to ensure that the Grid Plan reflects what is in the MDE correctly. The checks that are to be performed are clearly stated, and an entry that is checked is marked "ent" to ensure checks have been carried out. This process seems to ensure that all entries are indeed checked.

Clarifications, identification of gaps and recommended actions:

Transpower Comments:

41 It is understood that part of this process can be automated to some degree, as one staff member has done using the macros facility in the spreadsheet programme. If the process can be automated to remove human error, or to remove a manual step that requires no expert judgements, then this new procedure should be formally checked, documented and incorporated.

239 Document/process update required to incorporate macros in spreadsheet

Document Procedure Changes

**9.3.2 Document 541 Security Coordinator Day Ahead Check Process**

The OPEs run a check process under procedure 239, and the SC runs a day ahead check process using this document. On site verification included viewing a number of gridplans (which are handed over to the SC from OP at 13:00 on the previous day).

Compliance  
Compliance with clauses 15.1 and 15.2, 17, 18 and 20.5.

Clarifications, identification of gaps and recommended actions:

Transpower Comments:

42 The OPEs run a check on the accuracy of the Grid Plan prior to handing it over to the SC by 13:00 for the next day. But while this check is being done, the same Grid plan is also being checked by the SC. This means that there is a possibility that the Grid Plan being checked is not the Grid Plan that is will be handed over, and any earlier checks by the SC is redundant.

The Security Coordinator begins checking the grid plan prior to handover so that they have enough information available to them to perform the 13:00 security schedule. Any changes made by the OPE will be picked up by the Security Coordinator after the grid plan is handed over, and then incorporated into further security checks and schedules. 541 document update required to make this explicit.

Document Procedure Changes

**9.3.3 Document 373 System Management**

This document outlines the process/procedure for completing the Security Dispatch Schedules (SDS) and issuing notices as necessary. The Security Dispatch Schedule is produced every 6 hours starting with the 13:00 SDS or more frequently under some specified circumstances, with all 12 steps in the process being repeated at each of these times.

The inputs used include a generation comparison check between the latest Pre-dispatch schedule (PDS) produced with the previous PDS, the output of the Security Coordinator Day Ahead Check Process (document 541), reserve data, and tomorrow’s load forecast for each area (compared with same day previous week). The Security Dispatch Schedule is then run and checked for any issues arising.

Binding constraints and status discrepancies are also checked using the Constraints Visualisation tool Branch overview. If these discrepancies exist, the constraints and times are checked to see if they are correctly entered into MDE.

Abnormally high/low prices and location factors are checked using the Constraints Visualisation tool Location Factor overview. Other checks are made not related to security constraints.

Power flow analysis and contingency analysis are then carried out for 4 specific times (13:00, 19:00, 01:00 and 07:00). Power flow analysis is carried out and checked for voltage violations and steady states branch (overload) violations. Contingency analysis is carried out to identify violations and check that plan(s) are in place to manage these. Security checks are also carried out for zone 1/3/GZ9. Notices are then issued if necessary.

Clarifications, identification of gaps and recommended actions:

Transpower Comments:

43 The procedure does not specifically state that stability analysis is carried out.

Stability analysis is carried out using VSAT as part of the contingency analysis checking procedure. Though this may not be implicitly stated, it is referred to in various instructions for managing voltage stability e.g. GZ9/Z3 Security Management.

Stability analysis to be included in process documentation.

Compliance

Complies with 64.1, 64.2, 64.3, 64.4, 64.7 and 65.

Procedure does not specifically satisfy 64.8: stability analysis needs to be documented

Document Procedure Changes

### 9.3.4 Document 527 Amending constraints in real time

A procedure is provided to amend the SPD model output to closer match real time operation to provide better management of system security and to enable economic dispatch. Various triggers are mentioned that would indicate a mismatch, to allow a decision to be made of whether adjustments to SPD should be made. The two main triggers identified are real time contingency analysis (refer document 373) violations that were not binding in the schedules, and vice versa. Other triggers include external query regarding price separation/infeasibilities in the Pre-Dispatch Schedule as well as internal query.

The System Coordinator can adjust the constraints in MDE, checking to ensure it is working properly by running short term Security Dispatch Schedule and powerflow as necessary for the Trading periods concerned.

Changes to the constraint are required to be logged in MELT and a CAN is issued advising of a change to any constraint.

On site verification included viewing the constraints visualisation tool which identifies potential problems which may result in a requirement to modify constraints in real time. Such modification was not required at the time of the on site visit.

Compliance

Complies with clauses 15.1 and 15.2, 17, 18, 64.4, 64.7, 64.9, 65, 66, 67 and 69.1

### 9.3.5 Document 553 Re-rating of constraints in real time

Several very similar procedures are outlined for four different cases of re-rating in real time.

The process requires that details of change are logged in MELT and a change or cancellation notice is issued to Operations Planners and Market Services.

Compliance

Complies with clauses 15.1 and 15.2, 17, 18, 64.3, 64.4, 64.9, 65, 66.1, 67 and 69.1

#### Clarifications, identification of gaps and recommended actions:

#### Transpower Comments:

- 44 These procedures may be able to be simplified down to one set of equations given their similarity.
- 45 Nonetheless, from the procedures, it is unclear what the checks on this process are.

General  
Process  
Improve-  
ment  
General  
Process  
Improve-  
ment

**9.3.6 Document 585 Real time MDE updates for Grid Owner Offer Changes**

The GO is able to make changes to offer at any time as long as notification requirements in the EGRs are met. Security constraints are not to be altered retrospectively. Security constraints will not be altered for the current trading period unless system security is at risk. Analysis of the new offer is carried out using SCADA / EMS applications e.g. Powerflow, Real-time Contingency Analysis and Voltage Stability Analysis Tool. The model outputs are analysed by Operation Planning Engineers as well as the System Co-ordinator, checking where asset capabilities and voltage stability requirements are exceeded.

Where violations occur, permanent security constraints are developed and applied.

Compliance

Complies with clauses 15.1 and 15.2, 17, 18, 64, 65, 66, 67 and 69

Clarifications, identification of gaps and recommended actions:

Transpower Comments:

46 Failure to notify whether returning to service earlier or later previously notified will result in a report of potential breach in MELT. How is this policy policed? Can someone inadvertently omit to notify the potential breach? If so, some step which will prevent such omissions should be implemented.

This is "policed" by the Security Coordinator in real-time following document 585 - Realtime MDE Updates for GO Offers Changes and does rely on the Coordinator to e-mail Market Services to advise of a potential breach. Where equipment is returned earlier/later then the Coordinator would be alerted to the discrepancy by CV and Alarm Monitor.

47 Failure to notify a change to an outage notice: the heading "late return" needs to be deleted from page 6 of 10 as this heading is incorrect.

General Process Improvement

Document Procedure Changes

---

## 9.4 Notifications

### 9.4.1 Document 342 Issuing a Customer Advice Notice

This document outlines the types of information covered in a CAN, who the CANs should be issued under and procedures for issuing CANs. CANs are used to comply with the issuing of notices under EGR Part C Schedule C4, for advising permanent security constraints and their removal or revision, outage constraints for planned outages, and modifications to any constraints or the application of a new constraint.

Complies with 20.1, 20.4

When a CAN issued using the Market Reporting Tool (MRT), it is automatically filed electronically. When a CAN is issued from Outlook, the sender files it electronically via a separate manual step, to a particular specified location.

On site verification included viewing the email template for a CAN, including a number of distribution lists.

### 9.4.2 Document 506 Distribution of Notices

This procedure sets out the required distribution of various types of notices, and the make-up and maintenance of distribution lists, including those applicable to CANs, but excludes the distribution of block constraint notices.

Complies with 20.1, 20.4

---

## 10.0 Conclusions and Recommendations

The main findings of the review are that System Operator generally complies with the EGRs. The System Operator achieves this with a large number of processes and procedures. A number of the procedures reviewed have some outdated and inaccurate information. Interviews with staff show that the processes are largely adhered to, but the review showed that staff members take steps to ensure the EGRs are complied with where the procedures themselves have gaps or are duplicated. With the large number of processes and procedures, the risk of non-compliance is always present. Therefore, the recommendations below are largely related to process improvements.

General recommendation:

- A. This review recommends that the System Operator go through the findings in section 9 and address the documentation, process improvement and process issues raised.

The specific recommendations are:

- B. Process control documents need to be up-to-date, simple and relevant, otherwise there may be a temptation to ignore them. When a process is to be reviewed, it is recommended that it should be simplified by separating what needs to be done (process) from how it should be done (procedures).
- C. It would be useful to prepare a flowchart that matches the various processes to the appropriate rules within the EGRs, showing exactly what rules each process complies with.
- D. To ensure consistency and reproducibility of process, the remaining discretionary steps should be reviewed and removed unless there is a good reason to allow discretion, except for those steps that require expert or professional judgement on the part of the staff member.
- E. In the particular instance regarding week ahead MDE entries, the procedure is very prescriptive, possibly indicating that there is an intention that staff are to follow it explicitly. The question here is to what degree of a procedure is to be adhered to, or should the procedure be a given the status of a guideline only. When a process is to be reviewed, some thought should be given as to whether the level of prescription is warranted.
- F. The application of security constraints into MDE is labour intensive and presents a large number of opportunities for error. A means to reduce this opportunity needs to be investigated, including process automation where practical.
- G. If constraints were able to have some form of expiry date beyond that which they cannot be used, this will make it more difficult to inadvertently apply superseded constraints, or leave them in when they should have been removed.
- H. The issue where a constraint that is to be made inactive but cannot because it has been applied in MDE needs to be resolved.
- I. The lack of linking between the constraints database and operational plans has its advantages, but a notification or flag that the constraint in an operational plan does not line up with its counterpart in the ACI database may be beneficial.

## 11.0 Appendix

The above-mentioned clauses from the EGRs are presented below. The references to the Policy Statement in schedule C4 are as follows:

### Security Policy

#### RISK MANAGEMENT POLICIES

##### Quality Limits Associated with Events

- 15.1 For a **contingent event**, the **system operator** plans to achieve the following quality conditions and limits during and following the occurrence of a **contingent event**:
- No **asset** will exceed its stated capability.
  - Subject to clause 30, **grid** voltage will be within the range set out in rule 3.1.1 of section III of Part C.
  - No demand is interrupted other than contracted **reserves** and/or **interruptible load** contracted or pre-arranged to be interrupted.
  - Frequency in either **island** will not drop below 48Hz or rise above 52Hz in the North Island or 55Hz in the South Island.
  - Frequency in either **island** will be restored to within 50 Hz +/-0.75Hz within 1 minute.
  - Frequency **reserves** will be restored within 30 minutes.
  - Voltage stability of the power system is maintained.
  - Where required by agreements for higher levels of quality, rule 6 of section II of part C or rule 2.1 of section II of part I, the quality targets of such agreements will be met.
- 15.2 For **extended contingent events**, the **system operator** plans to achieve the following quality conditions and limits during and following the occurrence of an **extended contingent event**:
- No **asset** will exceed its stated capability.
  - Voltage stability of the power system is maintained.
  - Subject to clause 30, **grid** voltage will be within the range set out in rule 3.1.1 of section III of Part C.
  - **AUFLS** may be used.
  - Disconnected **demand** will be restored as soon as practicable.
  - Frequency in either **island** will be restored to within the normal band as soon as possible.

#### SECURITY MANAGEMENT

##### Security Constraints

17. The **system operator** will apply **permanent security constraints** to the **Scheduling Pricing and Dispatch (SPD)** software model for what it considers to be an expected normal range of **dispatch** scenarios and for situations with all transmission **assets** available by:

- 17.1 Identifying the **contingent events** and **stability events** that the **system operator** considers may reasonably result in the need for **security constraints**.
- 17.2 Analysing a range of transmission, generation, and power flow scenarios.
- 17.3 Designing and applying **security constraints** to the **SPD** model intended to:
- Maintain post-event operation within stability limits.
  - Maintain operation within the stated short term transmission capability (as advised by **grid owners**) after a **contingent event**.
  - Allow sufficient time after a **contingent event** to allow for re-dispatch of generation or **demand shedding** to maintain operation within advised transmission capability.
18. In addition to the above, the **system operator** will apply **temporary security constraints** (including **asset outage constraints**) to the **SPD** model to allow for **contingent events** and **stability events** for what it considers to be an expected range of dispatch scenarios when **assets** are temporarily unavailable or **asset** capability is temporarily changed as notified by **asset owners** to the **system operator**. **Temporary security constraints** will be:
- 18.1 Determined by identifying possible **contingent events** and **stability events** the **system operator** considers may reasonably result in the need for **security constraints** at the following stages:
- During outage coordination and commissioning planning.
  - During the **scheduling period** and in real time.
- 18.2 Applied to the **SPD** model to:
- Maintain post-event operation within stability limits.
  - Maintain operation within the stated short term transmission capability (as advised by **grid owners**) after a **contingent event**.
  - Provide sufficient time after a **contingent event** or **stability event** to allow for re-dispatch of generation or **demand shedding** to maintain operation within advised transmission capability.
- 18.3 Applied to the **SPD** model for a defined period of **asset** unavailability or changed **asset** capability and are intended to maintain scheduled and dispatched security.
19. When circumstances require a **constraint** to be applied or modified at short notice the initial **constraint** design be conservative, to maintain security. This may also apply for the initial application of a permanent **constraint**. The **system operator** will use reasonable endeavours to refine any **constraint** for accuracy and as operational experience permits.
20. The **system operator** will:
- 20.1 **Advise participants** of new **permanent security constraints** two weeks prior to the implementation of a new **permanent security constraint**. The advice given will include a brief summary of the constraint design, sufficient for **participants** to assess the effect of the constraint.

- 20.2 At the time of assessment, **advise** any **asset outage constraints** that will apply for planned outages through the **Planned Outage Coordination Process**.
- 20.3 List all **asset outage constraints** available to the **system operator** on the **system operator's** website. The list will include details of constraint design and their effects.
- 20.4 Notify **participants** when a **constraint** has been applied or modified pursuant to clause 19 and the **system operator** identifies the giving of such notification will assist it meet the **PPOs**.
- 20.5 Correctly apply all **constraints** described in clauses 17, 18 and 19 to the **SPD** model.

.....

Clauses 64, 65, 66, 67 and 69 of the Policy Statement in schedule C4 are as follows:

## Dispatch Policy

Dispatch Policy & Process Statement

The Scheduling Process

Security Assessment

63. [Not discussed in this audit]
64. To carry out the security assessment, the **system operator** will:
- 64.1 Produce a Security Schedule independently from the **Pre-Dispatch Schedule**, but concurrently with its first production at 13:00, which covers the same period as the concurrent **Pre-Dispatch Schedule**.
- 64.2 Perform further security assessments during the **schedule period** if there have been any significant changes to the generation and/or load profiles. A new security schedule will be produced at least four times per day.
- 64.3 Use the inputs described in rule 1.3.2 of schedule G6 of part G. As part of these inputs, the **system operator** will include:
- **Security constraints** derived by the **system operator**, up until the time that the Security Schedule commenced solving.
  - The reserve requirements in the form of the most recent reserve information, for each **trading period**, calculated up until the time that the Security Schedule commenced solving.
- 64.4 Update the current Security Schedule for each **trading period** with any changes received from **participants**, latest reserve requirements, and any further adjustments to meet the **dispatch objective** for each **trading period**.
- 64.5 Calculate the reserve requirements in the current **trading period** for the following **trading period**. These changes are included as the latest changes in each schedule.
- 64.6 Produce a **demand** profile for the **schedule period** for each **grid exit point** determined by the matters including:
- Regional weather forecast information.

- Non-standard **demand** profiles (from **purchaser bid** information).
  - Historical **demand** information based on time of the day, day of the week, and time of the year.
  - **Fixed load distribution factors** determined by the **system operator** for all **grid exit points** and reviewed weekly. The fixed load distribution factors will be applied to each **grid exit point** except where the **system operator** believes the fixed load distribution factors for a **grid exit point** may be materially inaccurate in which event the **system operator** may include the **demand** bids for such **grid exit point**.
- 64.7 Assess power flows to identify and assess possible transmission security restrictions, capacity restrictions, or voltage conditions on the **grid**.
- 64.8 Identify stability conditions on the **grid**.
- 64.9 Identify and apply **security constraints**, where necessary, to constrain subsequent schedules and **dispatch**.
- 64.10 Identify where shortfalls in standby reserves exist by:
- Checking that there are sufficient uncleared energy and **reserve offers** to provide for a second **contingent event**.
  - Checking that there are sufficient energy **offers** in each **island** for a frequency keeper to provide the required **frequency keeping** band.

#### **Pre-Dispatch Schedule (PDS)**

65. Each **Pre-Dispatch Schedule** will, in addition to complying with the requirements of Schedule G6 of part G, include:
- 65.1 **Security constraints** entered by the **system operator**, up until the time that the schedule commenced solving. The **security constraints** will be the most recent, derived from the security assessment processes prior to and during real time.
- 65.2 The reserve requirements in the form of the most recent reserve information, for each **trading period**, calculated up until the time that the schedule commenced solving.

#### **Dispatch Schedule**

66. Pursuant to rule 4.1 of section III of part G, the **system operator** will, in addition to complying with the requirements of Schedule G6 of part G, adjust a **dispatch schedule**, where adjustment is required, to include:
- 66.1 The most recent **security constraints** identified from the security assessment processes, including any refinements made under clause 19 of the Security Policy in Schedule C4.
- 66.2 Any bona fide reductions notified under rules 3.18 or 6.15 of section II of part G.
- 66.3 Changes notified by **generators**, **purchasers**, and **ancillary service agents** during a **trading period**.
- 66.4 The most recent reserve information received by the **system operator** at the beginning of each **trading period**.

67. To continually meet the **dispatch objective** during a **trading period**, the **system operator** will adjust the current **dispatch schedule** to:
- 67.1 Produce a new **dispatch schedule** during the current **trading period** to incorporate:
- The **frequency keeping** generation relative to the **frequency keeping** capability.
  - The anticipated **demand** change in the near future.
  - **Dynamic load distribution factors** for all **grid exit points**, but only once the **system operator** has developed and implemented the **software** necessary to incorporate such **dynamic load distribution factors** (and provided that if, after implementation, the software is unavailable for any reason, the **system operator** may, during the period of unavailability, use the last available **fixed load distribution factor** or factors determined taking into account the matters listed in clause 64.6).
  - Observed variation in **generating** plant ramp from the calculated ramp and expected 'make-up' of this in the next **trading period(s)**.
  - **Security constraints** required to meet the **dispatch objective**.

#### **Schedule of Dispatch Prices and Quantities (SDPQ)**

68. [Not discussed in this audit]
69. As part of the inputs specified in the **rules**, each SDPQ will, in addition to complying with the requirements of Schedule G6 of part G, include:
- 69.1 **Security constraints** entered by the **system operator** up until the time that the schedule commenced solving.
- 69.2 The reserve requirements in the form of the most recent reserve information, for each **trading period**, calculated up until the time that the schedule commenced solving.

Rule 2.1 of section II of Part C of the Rules is as follows:

#### **Section II The principal performance obligations of the system operator (PPOs)**

##### **2. Principal performance obligations of the system operator**

The **principal performance obligations** of the **system operator** are to:

###### **2.1 Avoid cascade failure**

Act as a **reasonable and prudent system operator** with the objective of **dispatching assets** made available in a manner which avoids the cascade failure of **assets** resulting in the loss of **demand** and arising from:

###### **2.1.1 Frequency or voltage**

Frequency or voltage excursions; or

###### **2.1.2 Imbalances**

Supply and demand imbalances.

.....