



Operations Division

PR-OC-203 Analyse Security Implications and Mitigate Violations

This Procedure is part of the Outages and Constraints (OC) process within Transpower and forms part of the System Operator function. The document can be found in the [Operational Documentation Library](#)

Document Status: **Issued**

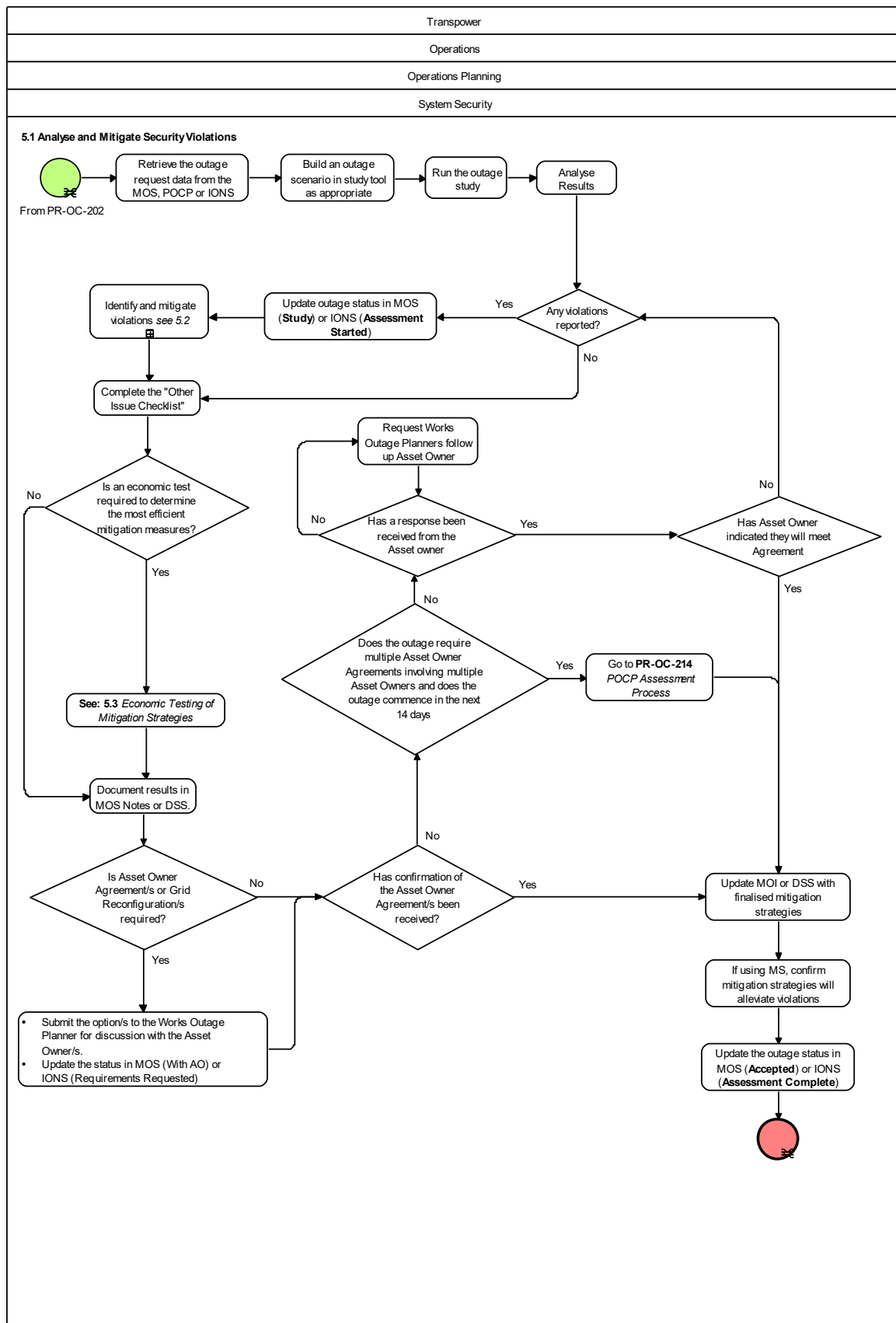
Published Date: **19/03/2026**

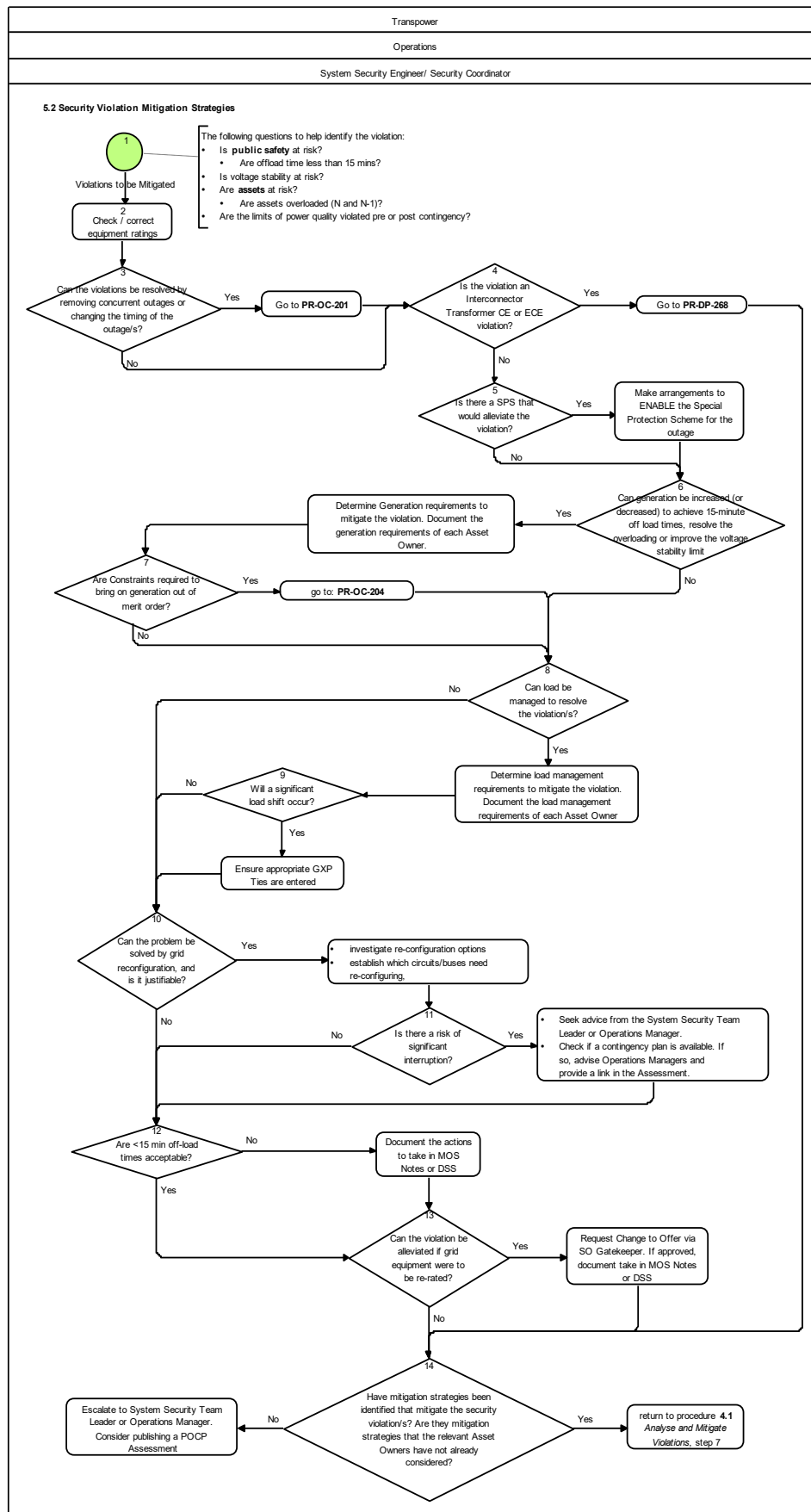
Table of Contents

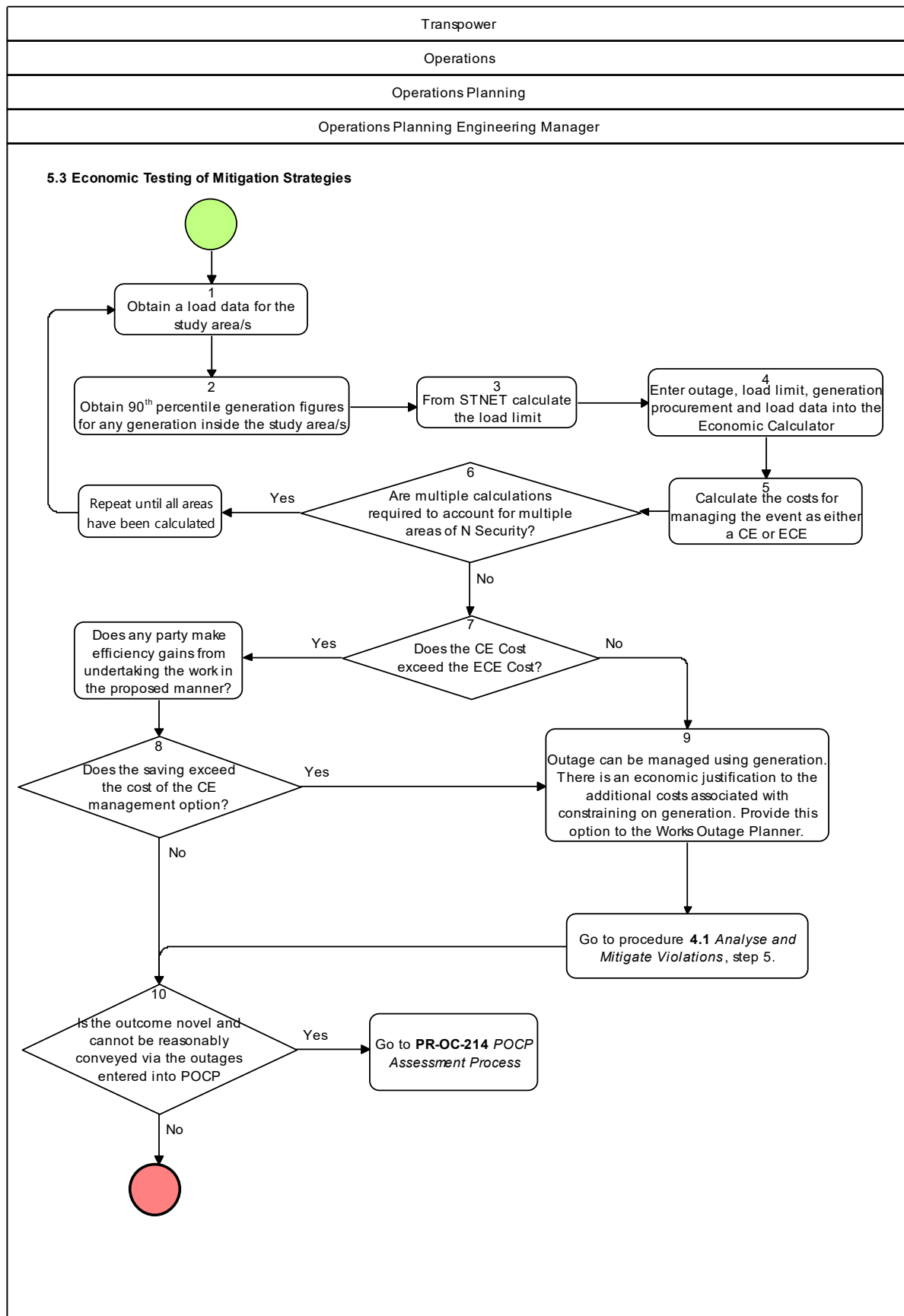
1	Procedure Summary Diagrams	2
2	Purpose & Policy.....	5
3	Security Analysis Background and Requirements	7
4	Related Procedure/Processes	9
5	Procedures	10
5.1	Identify and Mitigate Security Violations.....	10
5.2	Security Violation Mitigation Strategies.....	12
5.3	Economic Testing of Mitigation Strategies	14
6	Appendix	16
6.1	Security Report Checklist.....	16
6.2	Other Issues Checklist.....	20
6.3	Developing Mitigations Options	27
7	Document Information	34
7.1	Copyright Information.....	34
7.2	Document Feedback	34
7.3	Revision History	34
7.4	Metadata.....	35



1 Procedure Summary Diagrams









2 Purpose & Policy

Purpose and Objectives

This procedure describes the methodology of mitigating security and market issues that can occur as a result of an outage. It describes the following:

- how to **identify** security/market violations
- how to assess the **impact** of those violations
- identify **options** and means to **mitigate** those violations,
- analysing and mitigating all **other** outage related security implications.

The objective of this procedure is to identify the means of mitigation and then subsequently **modify** the case **inputs** to ensure a secure planning and production schedule.

External Policy/ Rules / Regulations

The 'Code'

Policy Statement

Related Internal Policies, Processes and Procedures

The Operations Division's operational procedures are located in the Volt DM.

Operational Documentation (Published)

- [PR-OC-200 Outage Assessment Overview](#)
- [PR-OC-201 Perform a Preliminary Outage Assessment](#)
- [PR-OC-202 Prepare and Modify Inputs to the Planning Schedule](#)
- [PR-OC-204 Security Constraints Process](#)
- [PR-OC-211 Create a Basecase](#)
- [PR-OC-214 Publish a Planned Outage Co-ordination Procedure \(POCP\) Assessment](#)
- [PR-OC-216 Assess a Reclose Block \(RCB\) Request](#)
- [PR-OC-230 Manage SFT-created Constraints](#)
- [PR-SH-001 Operational Management of Permanent System Splits](#)
- [PR-SH-217 Issue Notices](#)
- [PR-SH-221 Assess the Production Schedules and Mitigate Violations](#)
- [PR-DP-268 Operational Management of Interconnector Risk](#)
- [PR-DP-212 Manage an Island Following an Unplanned Event](#)
- [PR-DP-235 Manage Grid and Supply Voltage](#)
- [GL-OP-1024 Outage Planning Process](#)
- [GL-SH-011 Bus Configuration Guideline](#)
- [SP-SH-002 Policy on Single End Fed Operation of Transmission Circuits](#)
- [TI-DP-026 Generator MVAR Capabilities Dispensations](#)

Operational Registers

- [RS-EA-001 GO Special Offer Register](#)
- [RS-EA-000 Register of Manual Constraints](#)

Controlled Documents

Transpower Outage Planning Policy

Refer to 'related procedure/processes' chart.

**Definitions**

Descriptions of acronyms and non-standard or uncommon words specific to this document. (delete section if not required)

Definition	Description
DSS	Detailed Security Study Used to document outage information where multiple scenarios are modelled and multiple options are available to resolve a security violation. A DSS is used for non-routine or complex project outages where information is required further out from real-time (>10 weeks).
Dispatchable generation	Generation available physically or contractually to respond to changes in system demand or to respond to transmission security constraints.
TP	Trading period
CRE	Competition-Reliability-Efficiency objective of the EA is "to promote competition in, reliable supply of, and the efficient operation of, the electricity industry for the long-term benefit of consumers"



3 Security Analysis Background and Requirements

Priorities

Operations Planning Engineers and Security Coordinators deal with a number of issues when performing a security assessment. The following describes each issue in order of priority:

1. Public safety: Sagging of overhead transmission circuits endangers the people in the area by violating minimum safety clearances. Sagging is caused by overloading lines.
2. Compliance with the 'Code' and the Policy Statement, including the System Operator's CRE objective
3. Risks to assets: Assets are at risk if the operational limits ratings are exceeded. These can consist of
 - Voltage stability. Ensuring operating parameters are kept below the VS margin.
 - Voltage issues. The voltages need to be kept within the specified Quality Limits in steady state and following all credible contingencies. If it is not possible to maintain the pre and post contingent voltages within the specified limits, need to obtain specific agreement from the Grid Owner and Connected Parties.
 - Equipment loading. Equipment needs to be operated within loading limits and short-term ratings to prevent damage.
4. Compliance with temporary restrictions on the operation of the plant (as normally described in the SO temporary instructions).
5. Compliance with Local Quality Agreements. Refer to document RS-EA-001.
6. Impact on operation of the protection.

Contingent Events (CE)

Are contingencies where the impact, probability of occurrence and estimated cost and benefits of mitigation are considered to justify implementing policies that are intended to be incorporated into the scheduling and dispatch processes pre-event.

For contingent events, the system operator must endeavour to schedule and dispatch sufficient reserves to provide asset redundancy, maintain the levels of quality defined in the Security Policy, and plan to avoid post-event unplanned demand shedding, taking into account any other agreed control measures (for example special protection schemes and automatic under voltage load shedding schemes) advised to and agreed by the system operator.

The following contingencies are regarded as a contingent risk and are modelled as such in EMS SCADA:

- Transmission circuits
- The loss of a single generating unit.
- The loss of an HVDC Pole
- The loss of reactive injections
- The loss of certain interconnecting transformers (Refer to PR-DP-268 for further details)

**Extended
Contingent
Events (ECE)**

Are contingencies for which the impact, probability, cost and benefits are not considered to justify the controls required to totally avoid demand shedding or maintain the same quality limits defined for contingent events.

For extended contingent events, the system operator must plan to maintain the levels of quality defined in clause 17.2 of the Security Policy through a combination of AUFLS, the provision of reserves, asset redundancy, demand shedding, and acceptance of greater quality disturbances than for contingent events, taking into account any other agreed control measures (for example special protection schemes and automatic under voltage load shedding schemes) advised to and agreed by the system operator. These control measures do not preclude the system operator taking action before an extended contingent event occurs, such as network reconfiguration, but do preclude the system operator changing any price responsive schedule, non-response schedule and dispatch schedule by applying constraints that may dispatch off Dispatchable Demand (DD) or result in generation being dispatched out of merit order.

The following contingencies are regarded as extended contingent risks and are modelled as such in EMS SCADA:

- The sudden loss of the HVDC bi-pole
- The loss of certain interconnecting transformers (Refer to PR-DP-268 for further details)
- The loss of certain 220 kV, 110 kV or 66 kV busbars

Quality Limits

The Quality Limits defined in the Policy Statement must be met. This involves keeping frequency, voltage and equipment loading within defined limits to ensure system stability.

For a contingent event, the system operator plans to achieve the following quality conditions during and after the occurrence of a contingent event:

- No asset will exceed its stated load carrying, thermal or voltage capability.
- Grid voltage will be within the range set out in the Code or Wider Voltage Agreement (WVA), or where required by Local Quality Agreements (LQA) for higher levels of quality, the quality targets of such agreements will be met.
- No demand is interrupted other than contracted reserves and/or interruptible load contracted or pre-arranged to be interrupted.
- Voltage stability of the power system is maintained.

For extended contingent events, the system operator plans to achieve the following quality conditions during and after the occurrence of an extended contingent event:

- No asset will exceed its stated load carrying or thermal capability.
- Voltage stability of the power system is maintained.
- Target grid voltages will be within the range set out in the Code
- Other grid voltages may be outside the range set out in the Code. Where this is the case the system operator will respond to return these voltages to within the limits as soon as practicable.

For some outages, it may not be possible to maintain the pre and post contingent voltages within the range specified above. Where the range will be outside an LQA, an Asset Owner Agreement with the Connected Party will be required. Where the range will be outside a WVA or Code Limit, specific agreement from Grid Compliance is required. The ability of Grid Compliance to agree or disagree with the SO request will depend on how the voltage outside the range impacts asset operation and/or capability.

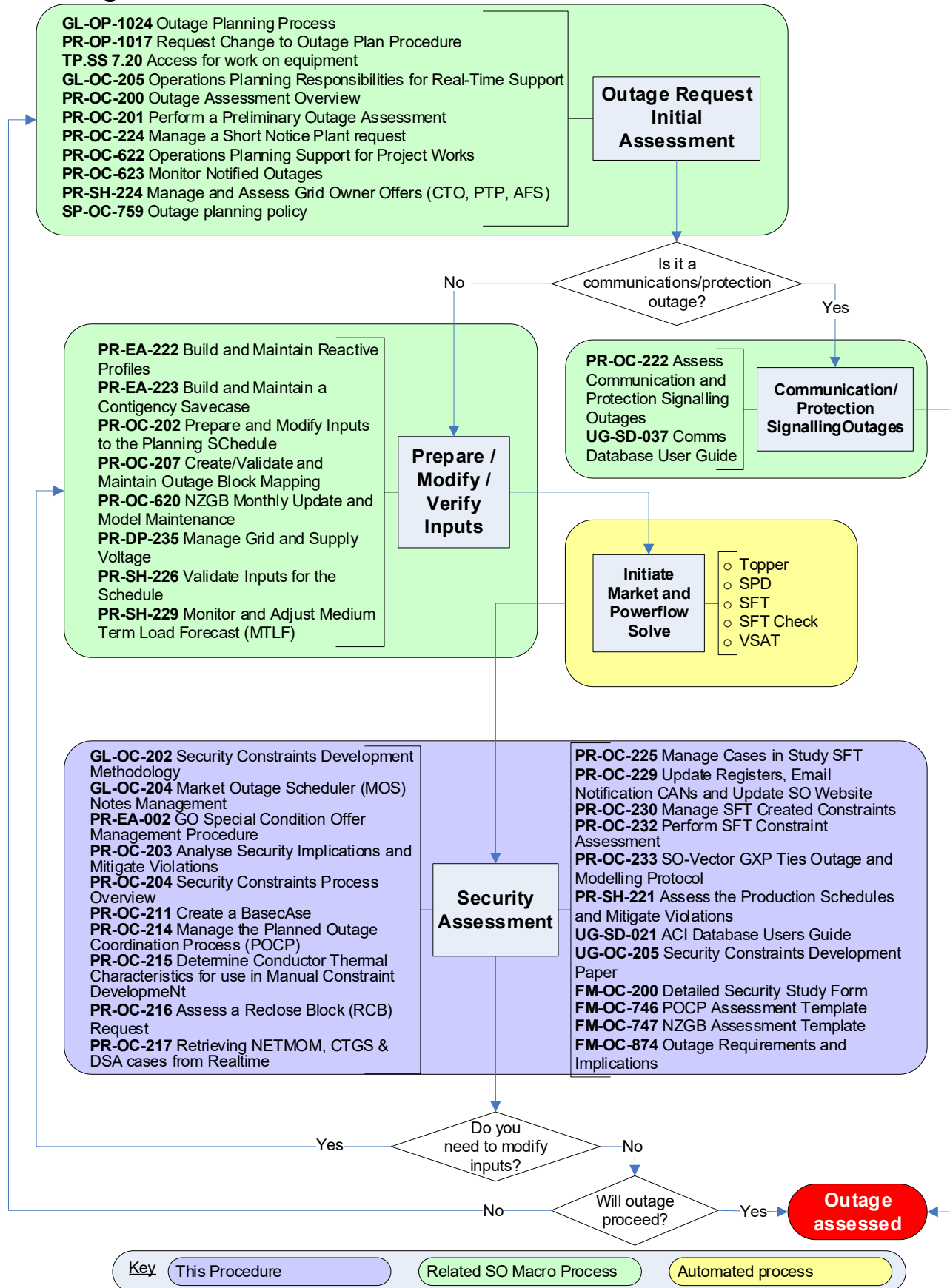
The guideline on how to manage voltage levels on the grid and LV buses for steady state and post contingent situations during an outage is given in PR-DP-235 Manage Grid and Supply Voltage.

The majority of GXPs are covered by the Code limits with LQAs and WVAs applying only to selected locations as listed in RS-EA-001 GO Special Condition Offer Register.



4 Related Procedure/Processes

Outage Assessment Process Documents





5 Procedures

5.1 Identify and Mitigate Security Violations

Inputs

Outage requests arrive via POCP, IONS, MOS

Outputs

Security violations and implications (if any) identified and mitigated.

- Options are developed
- Results documented in MOS notes or a DSS
- Relevant information sent to Asset Owner/s
- Inputs into the planning schedule are entered or modified

See: PR-OC-200 Outage Assessment – Overview for more detail on outputs.

Responsibilities

Operations Planning Engineer up until two business days prior to outage
Security Coordinator in real-time.

Instructions

Step	Action						
1	Retrieve the outage request data from the MOS, POCP or IONS						
2	Build an outage scenario in study tool (EMS and/or MS and Study SFT) as appropriate ▪ Refer to PR-OC-211 Create a Basecase ▪ Refer to PR-OC-202 for MS and Study SFT Studies						
3	Run the outage study.						
4	Analyse Results ▪ Analyse Basecase Violations (EMS) ▪ Analyse STCA Violations (EMS) ▪ Analyse Voltage Stability Results (EMS) ▪ Analyse Security Report and complete <i>6.1 Security Report Checklist</i> (MS)						
5	Are violations reported? <table border="1"> <tr> <th>If</th><th>Then</th></tr> <tr> <td>Yes</td><td> ▪ update outage status in MOS (Study) or IONS (Assessment Started) ▪ continue with step 6. </td></tr> <tr> <td>No</td><td>Go to step 7</td></tr> </table>	If	Then	Yes	▪ update outage status in MOS (Study) or IONS (Assessment Started) ▪ continue with step 6.	No	Go to step 7
If	Then						
Yes	▪ update outage status in MOS (Study) or IONS (Assessment Started) ▪ continue with step 6.						
No	Go to step 7						
6	Identify and mitigate the violations. See: 5.2 Security Violation Mitigation Strategies.						
7	Complete the Other Issues Checklist See: 6.2 Other Issues Checklist.						



Step	Action						
8	Is an economic test required to determine the most efficient mitigation measures? An economic test is required in instances where: ▪ Unrelated or separable concurrent outages result in the application of security constraints; or ▪ An asset owner has notified an outage at short notice that will result in the application of security constraints; and ▪ A grid re-configuration is available that mitigates the security violation and removes or reduces the need for constraints <table border="1"> <tr> <th>If</th><th>Then</th></tr> <tr> <td>Yes</td><td>See: 5.3 Economic Testing of Mitigation Strategies.</td></tr> <tr> <td>No</td><td>Go to step 9.</td></tr> </table>	If	Then	Yes	See: 5.3 Economic Testing of Mitigation Strategies.	No	Go to step 9.
If	Then						
Yes	See: 5.3 Economic Testing of Mitigation Strategies.						
No	Go to step 9.						
9	Document the results and mitigation options in MOS Notes, or Outage Requirements & Implications (ORI) or the Detailed Security Study (DSS).						
10	Is Asset Owner Agreement/s or Grid Reconfiguration/s required? <table border="1"> <tr> <th>If</th><th>Then</th></tr> <tr> <td>Yes</td><td>Continue with step 11</td></tr> <tr> <td>No</td><td>Go to step 12.</td></tr> </table>	If	Then	Yes	Continue with step 11	No	Go to step 12.
If	Then						
Yes	Continue with step 11						
No	Go to step 12.						
11	▪ Submit the option/s to the Outage Planners for discussion with the Asset Owner/s. See: GL-OP-1024 Outage Planning Process ▪ Update the status in MOS (With AO) or IONS (Requirements Requested)						
12	Has confirmation of the Asset Owner Agreement/s been received? <table border="1"> <tr> <th>If</th><th>Then</th></tr> <tr> <td>Yes</td><td>Go to step 14</td></tr> <tr> <td>No</td><td>Continue with step 13.</td></tr> </table>	If	Then	Yes	Go to step 14	No	Continue with step 13.
If	Then						
Yes	Go to step 14						
No	Continue with step 13.						
13	Does the outage require multiple Asset Owner Agreements involving multiple Asset Owners and does the outage commence in the next 14 days? <table border="1"> <tr> <th>If</th><th>Then</th></tr> <tr> <td>Yes</td><td>Go to PR-OC-214 Publish a Planned Outage Co-ordination Procedure (POCP) Assessment</td></tr> <tr> <td>No</td><td>No response has been received – Request Outage Planners follow-up Asset Owner. Asset Owner has indicated they will not meet Agreement – Return to step 5.</td></tr> </table>	If	Then	Yes	Go to PR-OC-214 Publish a Planned Outage Co-ordination Procedure (POCP) Assessment	No	No response has been received – Request Outage Planners follow-up Asset Owner. Asset Owner has indicated they will not meet Agreement – Return to step 5.
If	Then						
Yes	Go to PR-OC-214 Publish a Planned Outage Co-ordination Procedure (POCP) Assessment						
No	No response has been received – Request Outage Planners follow-up Asset Owner. Asset Owner has indicated they will not meet Agreement – Return to step 5.						
14	Update MOI or DSS with finalised mitigation strategies: ▪ Add/Modify/Identify Overrides ▪ Add/Modify/Identify EMS/Market Modelling changes ▪ Add/Modify/Identify SFT or Manual Constraints ▪ Request/Modify Asset Owner Agreements						
15	If using MS, confirm mitigation strategies will alleviate violations. See: PR-OC-202 Prepare and Modify Inputs to the Planning Schedule, 4.2 Prepare / Modify and Check Accuracy of Inputs for the Outage Planning Schedule (OPS) cases Re-run the Case.						



Step	Action
16	Update the outage status in MOS (Accepted) or IONS (Assessment Complete)

5.2 Security Violation Mitigation Strategies

Inputs	Security violations identified from outage study
Outputs	Security violations and implications (if any) identified and mitigated. Results documented in MOS Notes, or an ORI or a DSS Inputs into the daily planning schedule identified
Responsibilities	Operations Planning Engineer up until two business days prior to outage Security Coordinator in real-time
Guideline	Note: As you work through these steps. Document the actions to take or the possible options in MOS Notes or DSS. Refer to Appendix 6.3 for more detailed information
Instructions	

Step	Action						
1	In 5.1 Analyse and Mitigate Violations, step 5, these are the questions that help you identify the violation: ▪ Is public safety at risk? ○ Are offload time less than 15 mins? ▪ Is voltage stability at risk? ▪ Are assets at risk? ○ Are assets overloaded (N and N-1)? ▪ Are the limits of power quality violated pre or post contingency? If the answer to any of the above is 'Yes', work through the Violation Mitigation Strategies below. Note for some outages, more than one mitigation strategy will be required and there may be a choice of different mitigation strategies to mitigate a single violation.						
2	Check equipment ratings and correct them if necessary.						
3	Can the violations be resolved by removing concurrent outages or changing the timing of the outage/s? <table border="1"> <tr> <th>If</th><th>Then</th></tr> <tr> <td>Yes</td><td>Go to PR-OC-201 Preliminary Outage Assessment. Continue to step 4.</td></tr> <tr> <td>No</td><td>Continue with step 4.</td></tr> </table>	If	Then	Yes	Go to PR-OC-201 Preliminary Outage Assessment . Continue to step 4.	No	Continue with step 4.
If	Then						
Yes	Go to PR-OC-201 Preliminary Outage Assessment . Continue to step 4.						
No	Continue with step 4.						
4	Is the violation an Interconnector Transformer CE or ECE violation? <table border="1"> <tr> <th>If</th><th>Then</th></tr> <tr> <td>Yes</td><td> ▪ Go to PR-DP-268 Operational Management of Interconnector Risk. ▪ Continue to step 14 </td></tr> <tr> <td>No</td><td>Continue to step 5.</td></tr> </table>	If	Then	Yes	▪ Go to PR-DP-268 Operational Management of Interconnector Risk. ▪ Continue to step 14	No	Continue to step 5.
If	Then						
Yes	▪ Go to PR-DP-268 Operational Management of Interconnector Risk. ▪ Continue to step 14						
No	Continue to step 5.						



Step	Action						
5	Is there a Special Protection Scheme that would alleviate the violation?						
	Refer to RS-EA-001 Special Offer Register						
	<table><tr><th>If</th><th>Then</th></tr><tr><td>Yes</td><td>Make arrangements to ENABLE the Special Protection Scheme for the outage. Continue to step 6</td></tr><tr><td>No</td><td>Continue to step 6.</td></tr></table>	If	Then	Yes	Make arrangements to ENABLE the Special Protection Scheme for the outage. Continue to step 6	No	Continue to step 6.
	If	Then					
Yes	Make arrangements to ENABLE the Special Protection Scheme for the outage. Continue to step 6						
No	Continue to step 6.						
6	Can generation be increased (or decreased) to achieve 15-minute off load times, resolve the overloading or improve the voltage stability limit?						
	<table><tr><th>If</th><th>Then</th></tr><tr><td>Yes</td><td>Continue with step 7</td></tr><tr><td>No</td><td>Go to step 8</td></tr></table>	If	Then	Yes	Continue with step 7	No	Go to step 8
	If	Then					
	Yes	Continue with step 7					
No	Go to step 8						
7	Determine Generation requirements to mitigate the violation. Document the generation requirements of each Asset Owner.						
	Are Constraints required to bring on generation out of merit order?						
	<table><tr><th>If</th><th>Then</th></tr><tr><td>Yes</td><td> - Go to: PR-OC-204 Security Constraints Process - Continue to step 8. </td></tr><tr><td>No</td><td>Continue with step 8</td></tr></table>	If	Then	Yes	- Go to: PR-OC-204 Security Constraints Process - Continue to step 8.	No	Continue with step 8
	If	Then					
Yes	- Go to: PR-OC-204 Security Constraints Process - Continue to step 8.						
No	Continue with step 8						
8	Can load be managed to resolve the violation/s?						
	<table><tr><th>If</th><th>Then</th></tr><tr><td>Yes</td><td>Continue with step 9</td></tr><tr><td>No</td><td>Go to step 10</td></tr></table>	If	Then	Yes	Continue with step 9	No	Go to step 10
	If	Then					
	Yes	Continue with step 9					
No	Go to step 10						
9	Determine load management requirements to mitigate the violation. Document the load management requirements of each Asset Owner.						
	Will a significant load shift occur?						
	<table><tr><th>If</th><th>Then</th></tr><tr><td>Yes</td><td> - Ensure appropriate GXP Ties are entered, and - Continue with step 10. </td></tr><tr><td>No</td><td>Continue with step 10.</td></tr></table>	If	Then	Yes	- Ensure appropriate GXP Ties are entered, and - Continue with step 10.	No	Continue with step 10.
	If	Then					
Yes	- Ensure appropriate GXP Ties are entered, and - Continue with step 10.						
No	Continue with step 10.						
10	Can the problem be solved by grid reconfiguration, and is it justifiable?						
	<table><tr><th>If</th><th>Then</th></tr><tr><td>Yes</td><td> - Investigate re-configuration options. - Establish which circuits/buses need re-configuring, and - Go to step 11. </td></tr><tr><td>No</td><td>continue with step 12.</td></tr></table>	If	Then	Yes	- Investigate re-configuration options. - Establish which circuits/buses need re-configuring, and - Go to step 11.	No	continue with step 12.
	If	Then					
	Yes	- Investigate re-configuration options. - Establish which circuits/buses need re-configuring, and - Go to step 11.					
No	continue with step 12.						



Step	Action						
11	Is there a risk of significant interruption?						
	<table><tr><th>If</th><th>Then</th></tr><tr><td>Yes</td><td> ▪ Seek advice from the System Security Team Leader or Operations Manager. ▪ Check if a contingency plan is available. If so, advise Operations Managers and provide a link in the Assessment. </td></tr><tr><td>No</td><td>Continue with step 12.</td></tr></table>	If	Then	Yes	▪ Seek advice from the System Security Team Leader or Operations Manager. ▪ Check if a contingency plan is available. If so, advise Operations Managers and provide a link in the Assessment.	No	Continue with step 12.
	If	Then					
	Yes	▪ Seek advice from the System Security Team Leader or Operations Manager. ▪ Check if a contingency plan is available. If so, advise Operations Managers and provide a link in the Assessment.					
No	Continue with step 12.						
12	Are <15 min off-load times acceptable? See: item Offload times, in section 6.3.						
	<table><tr><th>If</th><th>Then</th></tr><tr><td>Yes</td><td>Document the actions to take in MOS Notes or DSS. Continue to step 13</td></tr><tr><td>No</td><td>Continue with step 13.</td></tr></table>	If	Then	Yes	Document the actions to take in MOS Notes or DSS. Continue to step 13	No	Continue with step 13.
	If	Then					
	Yes	Document the actions to take in MOS Notes or DSS. Continue to step 13					
No	Continue with step 13.						
13	Can the violation be alleviated if grid equipment were to be re-rated? See: item Request Re-Rated Equipment, in section 6.3.						
	<table><tr><th>If</th><th>Then</th></tr><tr><td>Yes</td><td>Request Change to Offer via SO Gatekeeper. If approved, document take in MOS Notes or DSS. Continue to step 14</td></tr><tr><td>No</td><td>Continue with step 14.</td></tr></table>	If	Then	Yes	Request Change to Offer via SO Gatekeeper. If approved, document take in MOS Notes or DSS. Continue to step 14	No	Continue with step 14.
	If	Then					
	Yes	Request Change to Offer via SO Gatekeeper. If approved, document take in MOS Notes or DSS. Continue to step 14					
No	Continue with step 14.						
14	Have mitigation strategies been identified that mitigate the security violation/s? Are they mitigation strategies that the relevant Asset Owners have not already considered?						
	<table><tr><th>If</th><th>Then</th></tr><tr><td>Yes</td><td>return to procedure 4.1 Analyse and Mitigate Violations, step 7.</td></tr><tr><td>No</td><td>Escalate to System Security Team Leader or Operations Manager. Consider publishing a POCP Assessment. If required, go to PR-OC-214 POCP Assessment Process.</td></tr></table>	If	Then	Yes	return to procedure 4.1 Analyse and Mitigate Violations , step 7.	No	Escalate to System Security Team Leader or Operations Manager. Consider publishing a POCP Assessment. If required, go to PR-OC-214 POCP Assessment Process .
	If	Then					
	Yes	return to procedure 4.1 Analyse and Mitigate Violations , step 7.					
No	Escalate to System Security Team Leader or Operations Manager. Consider publishing a POCP Assessment. If required, go to PR-OC-214 POCP Assessment Process .						

5.3 Economic Testing of Mitigation Strategies

Inputs	Multiple violations mitigation strategies identified from outage study
Outputs	Most cost-effective mitigation strategy identified for implementation Results documented in MOS Notes or a DSS
Responsibilities	Operations Planning Engineer up until two business days prior to outage
Guideline	An economic test is generally going to be required when the mitigation options available vary greatly. One option will generally involve constraining on significant generation or utilising significant load management while the other will place the load on N Security. The test is designed to compare the costs of constraining on generation against to economic costs of a loss of supply or any net benefit received by an Asset Owner.
Instructions	

Step	Action
------	--------



Step	Action						
1	Obtain a load data for the study area/s. The load data may need to be broken down further if any grid reconfigurations will create multiple areas of N Security. Each area of N Security will need its own calculation performed.						
2	Obtain 90 th percentile generation figures for any generation inside the study area/s. Wind generation is to be set to zero MW.						
3	From STNET calculate the load limit (i.e maximum permissible load into the area before violations occur). This should include the contribution of the 90 th percentile generation. If the calculation is for an N Security area only, and no generation is required, set the load limit to a value greater than the actual load.						
4	Enter outage, load limit, generation procurement and load data into the Economic Calculator (FM-OC-XXX). Refer to User Guide for information on how to specifically use the Economic Calculator.						
5	Calculate the costs for managing the event as either a CE or ECE.						
6	Are multiple calculations required to account for multiple areas of N Security? <table border="1"> <tr> <th>If</th><th>Then</th></tr> <tr> <td>Yes</td><td>Return to step 1 and repeat until all areas have been calculated. Summate total costs for all areas to obtain total CE and ECE Costs.</td></tr> <tr> <td>No</td><td>Continue to step 7</td></tr> </table>	If	Then	Yes	Return to step 1 and repeat until all areas have been calculated. Summate total costs for all areas to obtain total CE and ECE Costs.	No	Continue to step 7
If	Then						
Yes	Return to step 1 and repeat until all areas have been calculated. Summate total costs for all areas to obtain total CE and ECE Costs.						
No	Continue to step 7						
7	Does the CE Cost exceed the ECE Cost? <table border="1"> <tr> <th>If</th><th>Then</th></tr> <tr> <td>Yes</td><td>Go to step 8</td></tr> <tr> <td>No</td><td>Continue to step 9.</td></tr> </table>	If	Then	Yes	Go to step 8	No	Continue to step 9.
If	Then						
Yes	Go to step 8						
No	Continue to step 9.						
8	Does any party make efficiency gains from undertaking the work in the proposed manner? For example the Grid Owner makes a \$30,000 saving from taking a double circuit outage to be able to paint both sides of a transmission tower at once. However, it is this additional circuit outage that requires generation support. Does the saving exceed the cost of the CE management option? <table border="1"> <tr> <th>If</th><th>Then</th></tr> <tr> <td>Yes</td><td>CE management is justified. Continue to step 9</td></tr> <tr> <td>No</td><td>CE management is not justified. Continue to step 10</td></tr> </table>	If	Then	Yes	CE management is justified. Continue to step 9	No	CE management is not justified. Continue to step 10
If	Then						
Yes	CE management is justified. Continue to step 9						
No	CE management is not justified. Continue to step 10						
9	Outage can be managed using generation. There is an economic justification to the additional costs associated with constraining on generation. Provide this option to the Outage Planners. Return to procedure 4.1 Analyse and Mitigate Violations , step 5.						
10	Outage cannot be managed using generation. There is an economic justification to putting load on N Security. Provide this option to the Outage Planners. Is the outcome novel and cannot be reasonably conveyed via the outages entered into POCP? <table border="1"> <tr> <th>If</th><th>Then</th></tr> <tr> <td>Yes</td><td>Go to PR-OC-214 POCP Assessment Process</td></tr> <tr> <td>No</td><td>End process.</td></tr> </table>	If	Then	Yes	Go to PR-OC-214 POCP Assessment Process	No	End process.
If	Then						
Yes	Go to PR-OC-214 POCP Assessment Process						
No	End process.						



6 Appendix

6.1 Security Report Checklist

 TRANSPOWER	Security Analysis and Mitigation Strategies – Security Report Checklist.
Use of Checklist:	This checklist is used as part of the Security Analysis and Mitigation Strategies process PR-OC-203. It is used to check the violations report and should be used as a prompt.

Section 1 Outage Information

Prepared by:	
Outage (s):	
Date of outage:	Date of Assessment:

Section 2 Violations Report Checklist

☐	SFT Off
	Check and mitigate (where appropriate):
☐	the case has solved.
☐	SPD (offered grid).
☐	SFT Check topology (actual grid).
☐	schedule totals and energy balance
☐	HVDC configuration
☐	cleared generation
☐	SFTCheck Violations (base case and contingency results)
☐	contingency results
☐	schedule scarcity prices
☐	constraint outputs (from SFT) refer to PR-OC-230
☐	constraint outputs (from SFT Check - advisory in CSV file)
☐	Identify if further analysis is required.

See: 6.1 Section 3 Further Information for detailed notes on checks above.



Section 3 Further Information

Check the case was solved	Use the message log or OPS Case Control display. Status of case should be "solved".
Check SPD/SFT topology (offered grid or market model)	Using the market topology display if required or Study SFT, check for 'OMW' flows on branch's that are on outage (schedule outputs, branch outputs). If any branch has flow (that shouldn't) then check outage block mapping. SPD may need to model an unusual grid configuration. The 'force close breaker' list may need adjusting to ensure accurate modelling. Market Services may also need to create a zero impedance branch to help with the modelling issue. A zero impedance branch is considered to be a circuit with no resistance, and therefore no transmission loss. A zero impedance branch may need to be created and added to the outage block mapping. Check the SPD diagram to see what breakers, etc are modelled (e.g. OTA has a lot of switchgear modelled) and advise Market Services if there may be a change required at least two weeks in advance.
Check SFTCheck topology (actual grid)	Check base case results. Check for discrepancies on the forced close breaker exception list. This list will identify any 'force closed breaker' that is 'opened' in the 'actual grid' Check this is consistent with your outages. Use: Schedule Results: SFTCheck Summary StudySFT to visualise topology
Check Schedule totals and energy balance	Check Schedule summary: ▪ NIPs ▪ SIPs Are totals reasonable/ appropriate for season, trading periods? Check schedule totals: - Shortfall - Residual - Max. constraint price - DC transfer Is the difference between offered and cleared generation > largest available generating unit MW? (will usually be HLY 5) Energy Offered and Energy Cleared 400 MW total for NZ, not just by island If not, investigate offers and compare against POCP availability if required Use: Schedule Results: Schedule Summary Schedule Results: Schedule Outputs: Schedule Totals
Check HVDC configuration	Do you have enough HVDC scheduled for the scenario you are checking against. If not then use the HVDC transfer constraints to 'transfer' you want to check for
Check cleared generation	Is this the scenario that you want to study the outage case? If not apply Market Node constraints and re run case. Alternatively create a new case (via batching if required) and apply case level Market Node constraints to create the new scenario. Refer to PR-OC-202.

**Check SFTCheck Violations**

Using Schedule Results: SFTCheck Violations

Using the various tabs check and mitigate the various violations as appropriate.

These violations are the same as Network Basecase Violations and Contingency Solution Results in EMS.

- Branch Outputs:
 - sort by flow % of Limit
- Basecase Results:
 - Voltage
 - Static
 - Target voltage
 - Unmanageable / Unsolved
 - Harmfuls
 - CA Flows

Individual trading periods may need to be exported to Study SFT for mitigation options –

- Voltage plane management
- Transformer tap positions
- Load agreements
- System reconfigurations
- CAs – load or generation agreements may be required
- Constraints may be required.

Check Scarcity and Infeasibilities.

Check Schedule results: Schedule Outputs: Scarcity and Infeasibilities.

If you have a scarcity price, you may have one of the following issues:

- A constraint binding with no generation available to fulfil the constraint
- A branch overload
- Unsupplied load at a PNode (due to an outage of equipment to supply the PNode)

Use:

Schedule Results: Security Report

Schedule Outputs: Constraint outputs

Schedule Outputs: Branch outputs

Check that the branch re-ratings are correct against the NETMOM. These are applied as overrides.

Use: Schedule Inputs: overrides

Check if the load forecast is realistic, does it need to be adjusted down?

Use:

Schedule Inputs: Load Forecast <14 days

Schedule Studies: LTLF >14 days

If the ratings and load forecast are OK, you need to ensure enough generation is scheduled. A generation availability agreement may be required.

If generation is not available then load management will be required.

Check constraint outputs.

Check for any binding or near binding constraints. Instances of these will indicate potential security issues or the potential to have deficit generation. Generation availability agreements may be required.

You must determine if a constraint is pulling back or bringing on generation.

If the constraint is not binding but you have an un-manageable you should check the reactive profiles and/or how the constraint is built.



<i>Check constraint outputs from SFT Check</i>	SFT check advices on constraints on the actual grid. Compare the SFTCheck constraint with the SFT constraint. This comparison will help in determining the validity and accuracy of SFT constraints, refer to PR-OC-230 Manage SFT-Created Constraints section 4.3 Validate an SFT Constraint and 4.5 Check SFT Constraint Accuracy.
<i>Identify if further analysis is required.</i>	If further analysis is required then export results into SFT Study or EMS.



6.2 Other Issues Checklist

 TRANSPOWER		Security Analysis and Mitigation Strategies – Other Issues Checklist.
Use of Checklist:	This checklist is used as part of the Security Analysis and Mitigation Strategies process PR-OC-203. It is used to check other issues that are not identified in the violations report and should be used as a prompt.	

Section 1 Outage Information

Prepared by:			
Outage (s) :			
Date of outage:		Date of Assessment:	

Section 2 Other Issues Checklist

	Check and mitigate (where appropriate):
☐	▪ for switching issues
☐	▪ for implications of outage overruns
☐	▪ supply transformer implications
☐	▪ for implications of RCB's
☐	▪ Check for load shifting
☐	▪ if EMS/Source changes required
☐	▪ protection implications
☐	▪ Special Protection Schemes
☐	▪ Communications outage implications
☐	▪ RTU implications
☐	▪ IT& T implications
☐	▪ for Islanding of generation
☐	▪ Bus Configurations ○ Splitting of Buses for EMS ○ Abnormal Bus Configurations ○ Loss of VT Voltage Reference
☐	▪ for circuits that become single fed due to outages
☐	▪ for GXP ties
☐	▪ for phase angle issues

See: 6.2 Section 3 Further Information for detailed notes on checks above.

**Section 3 Further Information**

Check for switching issues	If the NGOC is required to step into a Bus (and remove additional equipment not identified in IONS) they must submit a PSO. The PSO is required to identify that switching operation. The System Security Engineer must assess and accept all PSO's. For complex outages and grid configuration changes, request the switching sequence from the NGOC and check to ensure security can be maintained throughout the sequence.
Implication of outage overruns	When assessing outages the impact of any outage overrun must be considered. This is especially important for outages undertaken during PM trough periods when the outage could run over into the PM peak or instances where the outage would cross into a different ratings period, with lower equipment ratings. Also important to assess possible implications on other planned work in the region due to outage overruns.
Supply Transformers Implications	Maintaining the loading of supply transformers is managed in real-time by the NGOC. The System Security Engineer will only specify load management of a supply transformer if: ▪ The high load is causing voltage issues or overloading elsewhere on the grid. ▪ There is unequal load sharing of the remaining in-service supply transformers on a split HV bus, causing one to overload before their combined rating is exceeded. ▪ A contingency of a core grid asset causes a supply transformer to overload or causes excessively low voltage to the connected party.
RCB Implications	Where the issue of an RCB on a transmission circuit will have an impact on the system security then a RCB is not to be issued. The assessment document is to document any circuits where RCB's are not to be granted. Refer to PR-OC-216 for situations where RCB's should not be approved.
Check for Load Shifting	Load shifting will occur via a GXP Tie. Overrides are applied in the Market System (associated with the GXP Tie) to model any load transfer greater than 1MW. The use of overrides to model load transfers may cause potential problems with the Bus Load Participation Factors (BLPFs) used in scheduling (WDS, NRSL, NRSS, PRSL and PRSS). The Market Group Team requires notification (by email to Market.operations@transpower.co.nz) of instances where this may be the case. Ideally such notification would be at least two to three days prior to the load shifts/outage to allow Market Group to assess the potential for this load shift/outage to cause problems. Situations that may trigger the need to consult with Market Group include: ▪ Instances where the load shift will be for longer than seven days ▪ Instances where there are multiple load shifts to or from a single GXP ▪ Instances where there was a load shift to or from a GXP in the week prior
Check for EMS changes required	EMS changes are required generally as a result of the following: ▪ New commissioning. ▪ VSAT DSA case changes. ▪ Activation of contingencies and/or contingency groups. ▪ Changes to the CTGS database that can only be done via an IT solution. Seek advice from System Security Manager or Senior Engineers if required and document changes required in the assessment. Real-time may need to update RTNET

**Check Protection Implications**

If it is believed that an outage may have protection implications then:

1. Check previous outage advice
2. If no advice can be found and there are still concerns or previous advice is dated or suspect then set the outage window in IONS to 'protection requested'. If less than 6 weeks out, contact the protection engineer and let them know you have requested some advice

For CB Fail and Bus zone protection outages – No RCBs are to be issued on the transmission circuits connecting to the effected bus.

Special Protection Schemes

To check for special protection schemes that the outage may impact on refer to RS-EA-001 GO Special Offer register. Also check MOS Notes to view current special protection schemes that have been implemented for concurrent outages.

Check communication outage implications

The impact of communications outages on the security of the grid is assessed.

Check RTU implications

Concurrent RTU outages may not occur as per the "RTU dependencies spreadsheet".

This spreadsheet has been developed by ITS Real Time Support as RTNET will not solve with various concurrent RTU outages.

The spreadsheet is located in

<https://transpowernz.sharepoint.com/sites/it053/Planner%20Tools/Forms/AllItems.aspx> and should also be used by the Outage Planners prior to submitting outages. Details for using the spreadsheet can be found under the Instructions tab.

Check IT& T implications

The impact of IT & T outages is assessed by the Operations Managers.

The outages (with RFC reference no.) are documented in MOS Notes as a calendar note.

Check for Islanding of generation

In some situations a contingent event will result in islanding of load and generation. Operations Planning Engineers do not plan for successful islands to be established post-contingency, but do identify when generation will be available in the island to help manage the situation.

Market Insights Team and Real-time need to know at least 1 week in advance of any outage that may island any generators or buses, so that they can ensure their SPD and real-time processes will operate properly. There may be pricing implications that result.

Real-time will manage any unplanned island as per PR-DP-212.

Check bus configurations**General**

While Transpower does not consider bus faults as a credible event, bus outages at a substation fitted with bus zone protection decrease system security for the following reasons:

- The number of transmission circuits and generation connected to the remaining in-service bus zone(s) will be increased (if circuits are switched over to them from the bus being removed by the outage), multiplying the disruption to the system in the event of a bus tripping.
- During the reconfiguration of the bus for the outage human error increases the risk of an inadvertent bus zone tripping.
- During a bus outage personnel and machinery will be working in the switchyard at a time of reduced bus security.

Where an outage increases the number of circuits connected to a 220 kV or 110 kV bus zone (compared with the normal configuration) measures shall be undertaken to alleviate the risk. During complex bus outages, Operations Planning Engineers should consult with the Grid Outage Planners to ensure security risk is adequately considered in the final grid configuration selected by the Grid Outage Planner.



One of the outcomes of the SI AUFLS event on the 2nd March 2017, proposed to:

"Improve current outage planning processes to include a risk-based approach that assess requests for outage of protection equipment to identify maintenance or project outages activities that have a high system impact, including the impact of other concurrent planned outages"

Identified protection outage blocks that involve increased risk and significant impact are Bus Zones, CB Fail and Special Protection Scheme outage blocks. There are some Bus Zone or CB Fail schemes that have duplicate protection and this will be indicated in the outage block.

For all the Bus Zone, CB Fail and Special Protection Scheme outage blocks, identified as causing an increased risk or significant impact, additional information has been included in the outage block in IONS.

As an Example of CYD_220BZ Outage:

Under Protection Information section of this Outage Block:

An outage of this BZ/CBF system has been identified as presenting a significant risk of a regional or wide-area impact in the event of a genuine bus fault or human-error incident.

The four 220 kV transmission circuits and four 120 MW generators are connected at CYD 220 kV bus. South to North power flow in South Island is mainly via CYD and simultaneous tripping of the 220 kV circuits connected to CYD 220 kV buses could cause high supply and generation loss.

External CB Fail Timers (VTT14) on all of 220 kV CBs. ITrip(CB Fail)Send & Rec on CYD-TWZ 1 & 2 circuits. (ITrip Rec at TWZ should be disabled for CB Fail testing on these circuits). MFAC 34 high impedance Bus Zone schemes are installed in Bus A, B & C.

The Service Provider should be engaged early for situational awareness and informed of the need for increased rigour in planning & preparation.

For information on measures that can be undertaken to manage the risk associated with bus outages refer to: GL-SH-011 Bus Configuration Guideline.

Abnormal bus configurations

Bus section and bus coupler outages may reduce the number of connections between buses at a substation. Planning for the removal of equipment (particularly at breaker and a half stations) that involves a bus coupling needs to fully consider the ramifications of a contingent event removing another bus coupling. This consideration needs to consider whether steady state and N-1 voltage, frequency, loading and stability can still be managed to within the obligations set out in the 'Code'.

The following steady-state and post-contingent issues can occur:

- Overloading of transmission circuits. For example in April 2005 a CYD-CML-TWZ 1 outage concurrent with TWZ CB2432 resulted in 2 of the 3 TWZ bus couplings being removed. A contingency on either BEN-TWZ 1 or TKB-TWZ 1 would have removed the remaining TWZ bus coupling leaving a coupling though the OHA bus, or through OHB and OHC and BEN. During the outage, RTCA reported an overload of OHA-TWZ 2 for a contingency on TKB-TWZ 1 as post-contingency flow from OHB was being fed up the TWZ A bus to OHA, through OHA, and then back to the TWZ B bus. In this instance the violation was able to be resolved by issuing a Dispatcher Security Constraint. The system stability risk was also unknown, as a CYD-TWZ 2 to ISL-TIM-TWZ 1 through circuit would have been formed.
- Uneven loading of the supply transformers due to different circuit impedances in the supply path to the individual transformers. Even if uneven loading is not an issue at peak loads then an assessment should be undertaken at trough loads as when the load decreases the resulting network impedance change will allow increased power transfer via the supply transformers. To resolve this issue may require load management at the substation or removal of one of the transformers.
- Backfeeds via the supply transformers. If this is found to be occurring then it is necessary to ensure that either the supply transformers are fitted with backfeed protection or where it is not fitted one of the transformers must be removed pre-contingent. Removal may require load management to ensure that the remaining unit is not overloaded. The substation relay and instrument diagrams may provide an indication of whether backfeed



protection is fitted. If there is any doubt then a protection engineer must be consulted.

- PLEASE NOTE: it is unacceptable to use an unknown distribution network as a planned back feed to supplying Transpower grid, pre or post contingently unless prior permission obtained by the distribution network. This is due to the unknown capability, condition and integrity of that network.
 - HAY 110 kV bus has a normally open point (DIS 37). When assessing outages, it is important to consider closing this to ensure the 110kV bus remains solid. There are some outages when this is not possible therefore the final configuration of a split bus should be closely checked for security.
-

Loss of VT voltage reference

When a bus is split or an outage occurs that removes a bus VT it is necessary to confirm that this does not cause any in service protection relay to lose its VT reference.

If a relay will lose its voltage reference then remove the effected protection relay from service by selecting its test switch to test.

Check circuits which become single fed due to outages

Introduction

This section should be read in conjunction with document SP-SH-002.

Circuits which become sole feeds due to outages

If a single substation or multiple substations in a section of the grid supplied via single transmission circuit then it is necessary to:

- Switch on Continuous Signal Receive (CSR) where it is installed on the in-feeding end. Switching on CSR will counteract the loss of in-feed from the open end of the circuit by ensuring a fast clearance by the protection at the in-feeding end. If CSR needs to be applied on-site by a technician then a protection engineer shall be consulted.
 - Check if auto reclose is installed on the transmission circuit, and to determine if this should be disabled for the duration of the outage. Disable the auto reclose:
 1. Whenever CSR is switched.
 2. Where a trip/auto reclose operation puts at risk a weak power system or will stress a thermal generator through the loss and sudden restoration of a block of load (40-50 MW). An example is an outage that puts BRY on N-security.
 3. Where the auto reclose will re-liven transformers with a connected load greater than 50% of the transformer rating.
 4. Where the existence of large motors is known or suspected at industrial sites connected to the circuit. This is because synchronous motors will act to delay the system collapse. Known substations with large motors connected are Kawerau, Kinleith, Whirinaki, Glenbrook and Bream Bay.
 - Consider the impact of the loss of load on the grid frequency and voltage due to the loss of grid connection. While the stable post-contingent voltage can be determined by removing the load on N-security it is not currently possible to model the transient voltage. The frequency can be modelled by undertaking a drop load simulation in RMT. At present the Operations Planning Engineers do not undertake any evaluation of the impact of the loss of load on voltage and frequency. However where a large amount of load (> 300 MW) is at risk then serious consideration should be given to moving the outage to a period which will reduce the amount of load at risk and mitigate the impact of loss of supply on industrial users. HAM-OHW1 and HAM-WKM1 circuit outages are examples of outages which put a large amount of load on N-security.
 - Consider if the single fed circuit will constrain generation. Either as the frequency keeping station or will limits the reserves that the station can offer.
-

**If generation is connected to a single infeed**

The risk with generation connected to a circuit fitted with auto reclose is that the generator protection settings may allow the generators to hang on for longer than the auto reclose dead time. This would allow the grid to reclose on an unsynchronised machine, with resulting damage to the machine as it attempts to come into step with the grid.

The following requirements apply irrespective of whether the generation is embedded or directly connected to the grid:

- If the circuit is fitted with synch-check and the auto reclose on/off control **can be** performed by remote control then the auto reclose **may be left enabled**.
- If the circuit is fitted with synch-check and the auto reclose on/off control **cannot** be performed by remote control then the auto reclose **shall be disabled**.
- If the circuit is not fitted with synch-check then the auto reclose shall be disabled if the generation connected to the circuit exceeds one third of the total load connected to the circuit. This needs to be checked.

Special cases:

- RDF-WRK and WRK-WHI have a single-pole auto reclose scheme with synch-check. These auto reclose schemes can be left on unless special conditions, such as live line work require it disabled.
- MAN split bus scenario where auto reclose will need to be disabled from all in-service MAN circuits (refer to document PR-DP-253).

Check for GXP ties.**General**

Parallel connection of grid exit points is frequently undertaken to enable equipment maintenance without disruption of supply, re-configuration to improve network operation or to facilitate restoration of supply to customers after a network fault. There are typically two distinct types of parallel connection:

- A parallel connection between two radial feeders where both feeders are supplied from the same GXP.
- A parallel connection between GXP supply buses where the system impedance between the two buses includes enough impedance to potentially cause voltage differences (angular and /or magnitude) between the two buses. This can have a serious impact on the operation of the power system and grid assets.

Assessing the Impact

Assessing the impact of GXP ties shall be undertaken in accordance with the "Guideline for Parallel Grid Exit Point Connection". This document also lists GXPs where ties are frequently performed.

Operations Planning Engineers and Security Coordinators are required to assess GXP Ties from a system security perspective in accordance with **5.1 Identify and Mitigate Security Violations**.

The procedure for distributors notifying the system operator of their intention to tie GXP is documented in "Process for Assessment of Parallel Grid Exit Point Applications".

Both documents are available on the Transpower website on the following page

<https://www.transpower.co.nz/system-operator/information-industry/asset-owner-requirements/paralleling-gxps>

**Check for phase angle issues.**

Phase angle issues To confirm that system stability will be maintained, it is necessary for certain outages that the phase angle difference between certain locations remains within a specified limit.

Locations where the difference between the bus phase angles must be within specified limits are listed in the following table.

Phase angle issues				
Between		Maximum difference (degrees)	Outages which can increase the phase angle difference	Managed by
Station 1	Station 2			
Benmore 220 kV bus	Roxburgh 220 kV bus	19	CYD-ROX	Power System Small Signal Stability Studies Outage stability constraint (not yet developed)

Instructions – measure phase angle

Follow these steps to measure the phase angle.

Step	Action
1	Go to the Network Bus Summary screen. The path is as follows: Analysis Displays→Network Components→Network Bus Summary
2	From this screen obtain the bus angle for the two locations being compared.
3	Calculate the difference between the two.



6.3 Developing Mitigations Options

Options for Mitigation of Security Violations

Operations Planning Engineers and Security Coordinators may have several options to mitigate any identified security violations. Managing an outage or combination of outages could require a combination of these mitigation strategies. Outage Planners need to decide which option is the most realistic or achievable from their perspective. They may also discuss the mitigation strategies with the relevant industry participants to understand their perspective.

The following table describes each option and in priority.

Priority	Option	Description
1	Reschedule Outages	Conflicting or inappropriately timed outages may be requested to be rescheduled. Refer to PR-OC-201.
2	Special Protection Schemes (SPS)	Special Protection Schemes (as per to current Offer) may be utilised to resolve security violations. Refer to RS-EA-001 Special Offer Register.
3	Security Constraints (Manual or SFT)	Constraints may be used to limit power flows through circuits and prevent overloading of equipment or manage voltage stability. This maintains reasonable reserve transmission capacity to allow for contingent events and to meet Quality Limits.
4	Generation Availability	If satisfying constraint requirements or as a stand-alone strategy then an availability agreement is required.
5	Load Management	Establishing load management details and communicating this to the Asset Owners
6	Changing grid configuration	Reconfiguring the grid, by closing or opening system splits to mitigate violations. These can be conditional if possible. May result in connected parties being on N Security.
7	Re-Rate Equipment	Requesting the Grid Owner re-rate equipment to provide additional capacity into an area. This includes changes to 15 minute offload times.

Note: The above options are to be applied in accordance with the classification of the assets involved (CE, ECE, Other) as determined by the Credible Event Review.

The following documents can provide assistance with understanding issues associated with a particular outage and possible solutions to problems:

- Historical MOS Notes
- Historical DSS's
- **'Introduction to GZ**. These documents are located in The Volt DM >> Operations >> Operation Power System >> Manage Outages and Constraints >> Outage Planning >> Technical Library [click here](#)
- Standing instructions
- System Security Forecast (SSF).

Reactive plant

Adjust the level of reactive support. Where condensers/capacitors/SVCs are required to be in service, it is necessary to ensure that they will be available for the outage.

Adjust the voltage profile

Raise or lower the voltage profile in the affected area by

- adjusting the voltage set-point at generators,
- tapping interconnecting transformers, and
- adjusting the voltage set-point on reactive plant (i.e. ISL SVC).

**Tap supply transformers**

Tap supply transformers to alleviate low or high steady-state or post-contingent voltages at a specific GXP.

When off-load transformers are tapped up:

- It is necessary to ensure that to ensure that voltages higher than the specified upper limit do not occur during trough periods.
- That circulating currents will not cause the MVA rating of the transformers to be exceeded while they are on different taps during the tapping operation.
- Total station load will not exceed the rating of the remaining in-service unit during adjustment of the tap. If the rating is being exceeded then the tapping may have to be changed to a time period when the load will be below the rating.
- If a Tap change is required on a supply transformer send a tap change request to the Grid **Operation** Planner via an instruction in the market system as well as an email/phone call if planning close to real-time.

Special Protection Schemes**RAS Common Information**

In the Market System the RAS application allows Special Protection Schemes to be modelled more realistically and increases the accuracy of the SFT constraints or removes the need for a constraint at all.

SFT Check performs a contingency analysis on the final SPD schedule against the actual grid and reports any violations. The RAS application is designed to minimise the security violations reported, given the constraints created are more accurate or are no longer needed.

RAS Operation

SFT will create a constraint based on the MCR, if all of the following are true:

- an element is part of an available RASMOM trigger
- the post CA flow is greater than the Maximum Continuous Rating (MCR)
- the last stage equals "Only", "Sole" or "Last"

Note: the Maximum Continuous Rating (MCR) is the Load shed value.

Market System Modelling

RAS definition status changes are applied in the Market System as an override

Security Constraints**Identify need for security constraints**

Constraints may be used to limit power flows through circuits and prevent overloading of equipment or manage voltage stability. This maintains reasonable reserve transmission capacity to allow for contingent events and to meet Quality Limits

It is up to the System Security Engineer to recognise the need for constraints.

SFT Constraints

Where possible SFT Security Constraints should be used.

Manual Constraints

A complete list of Manual Constraints is available. Refer to RS-EA-000 Manual Constraints Register. If required for a specific outage of outage combination, new Manual Constraints can be created. Refer to PR-OC-204 Security Constraints Process Overview.

Manual Constraints are applied in the Market System as an override. If an outage will cross multiple ratings periods, constraints for all relevant ratings periods must be applied. The Market System is able to correctly schedule the constraint based on the equations temperature attributes.

***When not to
use security
constraints***

Constraints are not to be applied:

- Where a constraint will become infeasible due to no generation being available to fulfil the constraint. This may occur when the only generation available to fulfil the constraint is on outage (as notified to the system operator) or when a grid owner outage or grid configuration removes the pathway for generation to alleviate the violation (FHL-TUI-1 outage prevents TUI generation from alleviating a FHL-RDF-1 or 2 tripping from overloading the remaining circuit)
- In certain circumstances where an economic test identifies that the use of constraints to bring on generation is not the most economical solution.

In both these situations generation and load management agreements should be used to manage the situation.

**Generation Availability and Load Management****Generation**

Request sufficient generation. Confirmation is required that sufficient generation will be available.

For outage assessments, wind generation is never considered to be available. 90th Percentile Generation may be considered as a reasonable generation assumption (subject to checking there are no planned generation outages).

The table below shows the confirmation required for various types of generation requirements.

A generation availability agreement means that the requested generation is '*available to be dispatched*'. Ensure that the availability agreement is specific in terms of whether it is required for the entire duration of the outage or peaks only and is documented as such.

Generation Availability Agreement Scenarios				
Scenario	Constraint	No. of generator traders in the area	Example	Requirement
Generation is required to satisfy load or voltage issues	A constraint is not suitable	One	Embedded Generation, Co-Gen Plant ALD, NGA, KIN, GLN, KMI et al.	Check POCP for sufficient plant availability Seek a generation availability agreement with the generator for the amount of required generation.
	A constraint is suitable and will be applied	One	Trustpower	Check POCP for sufficient plant availability Seek a generation availability agreement with the generator for the amount of generation necessary to satisfy the constraint.
		Multiple	Genesis and Contact	Check POCP for sufficient plant availability Seek a generation availability agreement with the generators for the amount of generation necessary to satisfy the constraint. Distribute generation across Traders. If required, publish a System Operator Outage Security Assessments on POCP.
A certain number of machines is required to raise the steady-state or post-contingent voltages in the region	May or may not be suitable	One or multiple traders	ROX 110 kV for GZ14 110 kV outages. COL for GZ12 outages.	Seek a generation availability agreement for the number of machines required to maintain the required voltage plane.
Generation and load management is required from multiple parties	A constraint is suitable and will be applied	Multiple	Outages of 220 kV circuits into Zone 3 or Zone 1	Seek a generation availability and load agreements with the generators and connected parties for the amount of generation and load management necessary to satisfy the constraint. Distribute equitably across traders and connected parties. If required, publish a System Operator Outage Security Assessments on POCP.

**Notification of Availability**

The Operations Planning expect that in response to the generation availability request:

- >1 week out – Written confirmation from Outage Planners that this agreement has been obtained. This confirmation could be via e-mail or sign-off on a DSS.
- <1 day out – Schedules indicate an offer of the requested generation.

Note: If doubts are raised about the Mvar capability of generators modelled in EMS SCADA document TI-DP-026 should be consulted.

Load Management

This can involve management of load at individual substations, across numerous substations or an entire Grid Zone or Zone or movement of loads between substations.

Where widespread load management is required across a Grid Zone or a Zone then the overall load management value must to be broken down by distributor (which assists Outage Planners to reach agreement with distributors).

Be aware that the network company to meet the load management requirements may move load to another GXP which could create additional problems.

Reference: For a list of substations by distributor refer to document PR-SH-217 .

Grid Reconfiguration**Reconfiguration**

Implement a system reconfiguration to prevent circuits overloading. Examples include:

- Creating a temporary system split. This may put some parts of the grid on N-security. For information on System Splits, see **System Splits** below.
- Closing or moving a permanent system split. For example closing the STU split for an AVI WTK 1 or LIV WTK 1 outage. For information on existing permanent system splits refer to Document PR-SH-001 Operational Management of Permanent System Splits.
- Selecting transmission circuits to a different bus to resolve issues due to a bus section outage.

If a system split is less than 8 hours in duration it is acceptable to open a circuit at the circuit breaker. For split of longer duration then the circuit must be opened at a disconnecter. This may require a site visit as disconnectors cannot normally be controlled via the SCADA. Refer to document SP-SH-002 for further information on the risks of opening a circuit at the circuit breaker.

Where a system split takes place at transformer, then it is normal to create the split on the low voltage side and leave the transformer energised from the stronger high voltage side. This will ensure sufficient fault current to operate the protection. An example is a West Coast split on the West Coast at DOB T12 by opening CB152 on the 66 kV side while leaving the transformer energised from the 110 kV side.

Where it is necessary to insert a system split, creating it by open ending one end of a circuit reduces the switching time.

System Splits

System Splits may be conditional. The aim of conditional splits is to help balance N-1 security for the connected parties against system security. This means that are added or removed in real-time on an as required basis. System Splits should be specified as follows:

Option 1:

System Split matches the outage start and ends times as the system split is required for the outage duration. An OPE will be requested to be entered into IONS to reflect this. These splits are not conditional. The connected parties will be on N Security for the outage duration.

Option 2:

System split is required during certain periods of an outage (i.e during peak loads). An OPE will be requested to be entered into IONS to reflect this, with the Operations Planning Engineer indicating the times the split is believed required. The start and ends times may be varied (or the split cancelled) in real-time based upon actual system conditions by the Security Coordinator. The Operations Planning Engineer indicates this requirement to the Grid

**Operations** Planners and Outage Planners**Open ending a transmission circuit**

Where there is a low voltage issue then opening only a circuit at only one end can be used as a means of providing reactive support and so raise the voltage at the closed end. Before undertaking this option then consider the following:

- Are there any protection issues?
- Is the circuit subject to a lot of line faults which (as a result of it remaining in service open-ended) would increase the risk of a protection operation?

Refer to document SP-SH-002 for guidance.

Request Re-Rated Equipment**Voltage agreements**

Where the steady-state or post-contingent voltage will be outside of the 'Code', then a voltage agreement may be arranged via Outage Planners. This voltage agreement must confirm that:

- The loading on any grid asset will not be exceeded.
- The grid protection will still be able to operate.
- The network company is agreeable.

In many areas a wider voltage agreement may already exist. Refer to Document RS-EA-001 for a list of applicable substations and their limits.

Offload Times

On overhead transmission circuits where the restriction on post-contingent energy transfer is determined by the overhead conductor rating and not a static component, an off-load time of at least 15 minutes is required. Offload time is defined as the length of time taken for a conductor to sag from its pre-contingent height to its minimum design clearance from the ground.

Fifteen minutes gives the Security Co-ordinator enough time to:

- Ascertain what the event is and its cause.
- Understand its implications.
- Determine the course of action to take and to relieve the situation by:
 - Ramping up or down any required generation (if available).
 - Requesting manual load shedding by connected parties.
 - Manually removing equipment via SCADA (if required).

Shorter off-load times may be applied in the following situations.

Off-load time (minutes)	Criteria
10 to 15	Customer(s) has provided in writing a plan to shed or shift load. Agreed immediate action will be taken by the network company on request by the System Operator. The NGOC will have delegated authority to act on the SO behalf
5 to 10	EMS SCADA is set up to manually trip the network company's agreed loads. In response to the SCADA alarm the Security Coordinator manually trips feeders until overloading is eliminated.
3 to 5	EMS SCADA is set up to automatically trip the network company's agreed loads. The Grid Owner installs a hardwired protection grade inter-trip

All of the above are subject to written sign-off from the Operations Manager and Grid Owner.

If <15min off-load times are used:



SFT Off: new manual constraints may need developing

SFT On: the off-load time will require an override on its monitored element pair

AUVLS

Automatic Under Voltage Load Shedding (AUVLS) is currently only active at the HOR, WGN and HWA substation (previously schemes were installed in the upper South Island to manage Zone 3, Grid Zone 9 & Grid Zone 12 Voltage stability).

Note that although at present USI AUVLS scheme is withdrawn by the Grid Owner, the purpose of these schemes was to enable the System Operator to reduce the normal voltage stability operating margin and run closer to N-1 voltage stability limit and so make further use of the existing installed transmission capability. Automatic under-voltage load shedding (AUVLS) relays do not disable feeder used for the AUFLS scheme as defined in the 'Code'.

Following a contingent event that results in an under-voltage situation, to avoid a voltage collapse situation, the relays will start tripping selected feeders.

The load armed for AUVLS is twice the margin to allow for the possibility of feeders not tripping, feeder outages etc.

Monitoring and availability of AUVLS is usually managed by the NGOC.

Important Note: *The AUVLS can only be used by the System Operator if it has been offered by the Grid Owner.*



7 Document Information

7.1 Copyright Information

COPYRIGHT © 2026 TRANSPOWER NEW ZEALAND LIMITED. ALL RIGHTS RESERVED.

This document is protected by copyright vested in Transpower New Zealand Limited ("Transpower"). No part of the document may be reproduced or transmitted in any form by any means including, without limitation, electronic, photocopying, recording or otherwise, without the prior written permission of Transpower. No information embodied in the documents which is not already in the public domain shall be communicated in any manner whatsoever to any third party without the prior written consent of Transpower.

Any breach of the above obligations may be restrained by legal proceedings seeking remedies including injunctions, damages and costs.

7.2 Document Feedback

If you find an error in this document or wish to provide feedback about any improvements please submit feedback [here](#) or use the QR code.



7.3 Revision History

Link to document review survey <https://forms.office.com/r/sYbiNMKMwY>

SharePoint Revision	Date	Change	Section
7.0	3/10/19	Changes made due to the outcome of the SI AUFLS event on the 2 nd March 2017 investigation resulting in additional bus configuration checks.	
8.0	27/07/20	Updated bus configuration section information on the HAY 110 kV bus.	
9.0	21/3/2022	Cyclic review reissued no change	
10	28/10/2022	RTP3 Project Update: - Changed Infeasibility price to schedule scarcity prices. - Check Schedule results: Schedule Outputs: Infeasibility Outputs – Changed to "Check Scarcity and Infeasibilities" and updated the wording of the content to match this.	Page 16 Page 18
11	13/12/2023	BAU Update: Outage Assessment process document diagram updated, related procedure list updated with link. This change was actioned due to feedback being raised on the document. No change to next revision date. [TN]	
12	27/6/2024	Cyclic Review: Removed reference to SP-DP-003 and PR-OC-222, updated links, updated System splits specification, minor update to back-feeding. And other minor updates.	Page 5 Page 23 Page 32/33 Page 25
13	19/03/2026	Cyclic Review: Minor update	Page 11, 25, 26, 28, 34



7.4 Metadata

Document ID Information

Document ID number:	PR-OC-0203
Document Title:	PR-OC-203 Analyse Security Implications and Mitigate Violations
Document Type:	Procedure
SharePoint Version:	V13
Document Status:	Issued
Severity of Consequences:	Moderate
Frequency of use	Daily
Level of Risk:	High

DMS Structure

Macro-Process:	Outages and Constraints (OC)		
Process:			
Process Hierarchy:	<u>L1</u> : 02 Scheduling	<u>L2</u> : 03 Manage Outages and Constraints	
	<u>L3</u> : 03-03 Perform Security Assessment	<u>L4</u> : [Business Model L4]	
Document Complexity Rating (days)	21 days		

Document Control

Business Group Owner:	Operations Planning Engineering		
Prepared by (Writer/Reviewer):	Ahmad Faizan		
Peer Reviewer	[Peer Reviewer]		
Approved by (Owner 1):	Mark Gilchrist		
Approved by (Owner 2):	Click or tap here to enter text.		
Approved by (Owner 3):	Click or tap here to enter text.		
Published Date: <i>(only changed by Doc Administrator)</i>	19/03/2026		
Update Type:	Cyclic Review		
Next Review Date:	19/09/2027		
Review Period:	18 Months		
Primary User Group(s):	NCC, Ops Planning		
Secondary User Group(s):	Click or tap here to enter text.		
Hardcopy Kept in:	string;#RT Security===Schedules		
To be published on TP Web site	false	Web Area:	N/A