Meeting Date: 2 March 2022

# Emergency Preparedness and business continuity planning

Security and Reliability Council

This paper provides a report from the system operator on their approach to emergency preparedness and business continuity planning, providing the opportunity for discussion and advice on areas of future focus.

**Note:** This paper has been prepared for the purpose of the Security and Reliability Council. Content should not be interpreted as representing the views or policy of the Electricity Authority.

# 1. Purpose and Executive Summary

1.1. The purpose of this paper is to provide the SRC with information about the system operator's approach to emergency management preparedness and business continuity planning, including rolling outages, system restoration and black start.

1.2. The information is presented to the SRC to assist in its role to advise the Authority on matters of security and reliability of supply and system operator performance, including areas for potential development.

1.3. Emergency management is the process of preparing for, mitigating, responding to and recovering from an emergency. Emergency management is a dynamic process. Planning, though critical, is not the only component. Training, conducting drills, testing equipment and coordinating activities with the community and other bodies are other important functions.

1.4. As noted in the system operator's paper in Appendix A, the SRC has previously received information at its Q1 2021 meeting on 'management of short-term system risk[1]', including ancillary services and event identification and classification. The system operator's paper builds on that paper.

1.5. This paper discusses the principles underpinning the system operator's approach and outlines the plans in place to meet those principles. The paper also covers collaboration with industry and what they've learned from it. The business continuity planning section talks about threat identification and the measures in place to provide the appropriate level of assurance.

1.6. This paper, together with a presentation from NEMA, an independent report from MartinJenkins, and information about communication plans from the Authority and system operator, inform the SRC's theme of resilience of the system to sudden unexpected shocks.

## Recommendations from the 9 August event reports

1.7. Note that this paper presents the current emergency preparedness and business continuity planning approach and may not include any changes or improvements as a result of various report recommendations from the 9 August event.

[1] https://www.ea.govt.nz/assets/dms-assets/28/SRC13-Management-of-short-term-system-risk-includes-credible-event-review- and-ancillary-services.pdf

# 2. What is emergency preparedness and emergency management?

2.1. An emergency is:

*"an unplanned event that can cause death or significant injuries to employees or the public, or that can disrupt a business or its operation, cause physical or environmental damage or threaten the organisation's financial standing or public image."*[2]

2.2. Emergency preparedness across the industry is driven primarily by the Civil Defence and Emergency Management Act 2002 (CDEM Act). This requires agencies to have resilience and emergency planning as part of their business.

2.3. Emergencies can strike an organisation in many different ways. The underlying events that cause emergencies can be classified as set out in Table 1 below.

**Table 1: Classification and examples of emergencies**

| Natural events | Technological events | Human events |
|---|---|---|
| Drought | Hazardous material release | Economic |
| Snow/ice/hail | Transportation accident | Terrorism |
| Windstorm/Tropical Storm | Power/utility failure | Hostage situations |
| Hurricane/Typhoon | Radiological accident | Enemy attack |
| Tornado | Fuel/resource shortage | Mass hysteria |
| Lightning storm | Business interruption | General strike |
| Extreme heat/cold | Communication interruption | Sabotage |
| Earthquake/land shift | Explosion/fire | Civil unrest |
| Dust/sand storm | Building/structure collapse | Arson |
| Fire | Extreme air pollution | |
| Tsunami | Dam/stockbank failure | |
| Biological, eg influenza | Strike | |
| Flood/wind-driven water | Financial collapse | |
| Volcanic eruption | | |
| Landslide/mudslide | | |
| Geomagnetic storms | | |

[2] Alexander A. (2003) Towards the development of standards in emergency management training and education,Disaster prevention and Management 12(2), 113-123

2.4 The phased activities involved in emergency preparedness and emergency management can be categorised as follows:

2.4.1. **Risk Reduction**: Preparing to handle an emergency:

2.4.1.1. includes any activities that prevent an emergency, reduce the chance of an emergency happening.

2.4.1.2. involves actions taken to protect lives and property.

2.4.1.3. compliance with regulation like the Building Code and the ResourceManagement Act are also examples of emergencypreparedness.

2.4.2. **Readiness (to respond)**: Means actions taken before an emergency occurs designed to influence how to respond to an emergency:

2.4.2.1. identifying hazards, quantifying risks and developing an overall framework

2.4.2.2. plans to save lives and to help response and rescue operations

2.4.2.3. exercises/drills are undertaken to prepare

2.4.3. **Response**: Response is safely putting your preparedness plans intoaction during an emergency, such as:

2.4.3.1. seeking shelter, shutting off gas valves, boarding windows

2.4.3.2. first response, saving lives, supporting community, securing against further damage

2.4.3.3. assessing impact and coordinating resources

2.4.3.4. establishing a basis for recovery

2.4.4. **Recovery**: Activities that take place after an emergency, such as:

2.4.4.1. taking actions to return to a normal or even safer situation

2.4.4.2. learning lessons and adapting risk reduction and readiness activities accordingly

2.4.4.3. making plans for who will do what and how will it be paid for.

2.5. Pre-emergency activities (risk reduction and readiness) are collectively referred to as emergency preparedness.

2.6. Activities during and after an emergency (response and recovery) are collectively referred to as emergency management.

## The New Zealand Co-ordinated Incident Management System (CIMS)

2.7. CIMS is an agreed method of incident management to be employed by emergency responders for efficient incident management in New Zealand.

CIMS is mandated through the CDEM Act for essential services (fire, ambulance, police). When distributors interact with essential services during an emergency, it will follow the CIMS protocols.

2.8. CIMS provides a set of management rules that is common to all emergency service providers. This means that when different emergency services need to work together on an incident or disaster, they already share a standardised management structure, a standardized set of management principles, and a standardized system of information management.

## CDEM Act

2.9. Key criteria for assessing compliance with the CDEM Act requires that:

2.9.1. Emergency management framework and specific plans are in place to provide minimum disruption to the lifeline utility

2.9.2. Emergency management plans need to be current, periodically tested and subject to a meaningful review process

2.9.3. Post-event performance reviews need to take place with lessons fed back into risk reduction and readiness plans.

# 3. Questions for the SRC to consider

3.1 The SRC may wish to consider the following questions.

**Q1. The SRC may want to ask the system operator:**

- **how the recommendations from the 9August event link to their emergency preparedness and business continuity planning, and**
- **what changes does the system operator expect to make to their emergency preparedness and business continuity planning as a response to the 9 August event report recommendations?**

**Q2. Does the SRC require further information at this stage?**

**Q3. What advice, if any, does the SRC wish to provide to the Authority at this stage?**

# Appendix A: System operator paper – Emergency Preparedness and Business Continuity Planning

TRANSPOWER

Security and Reliability Council Paper

| | |
|---|---|
| Meeting date: | 2 March 2022 |
| Author: | Matt Copland<br>SO Power Systems Manager |

# Emergency preparedness and business continuity planning

## 1 Purpose

The purpose of this paper is to outline for the Security and Reliability Council (SRC) members the System Operators' approach to emergency preparedness and business continuity planning and provide the opportunity for discussion.

This paper builds on the 2 February 2021 SRC paper 'System Operator management of short-term system risk' which discussed ancillary services procured to manage credible events, and the process we utilise to identify and classify those events in accordance with the Policy Statement.

## 2 Emergency Preparedness

Being prepared to respond to emergencies (incidents) on the power system is a key accountability of the System Operator. Failure to effectively respond to incidents has the potential to impact end consumers and erode our reputation and social license to operate.

We train in and utilise the Coordinated Incident Management System (CIMS) to respond to incidents. This structured incident management approach allows for our response to be integrated with other Transpower responses, but also on a national level with other organisations such as Civil Defense and Fire Emergency New Zealand should this be required to facilitate a safe recovery. CIMS is also utilised for business continuity responses as outlined in Section 3 below.

In order to be prepared we have developed plans and principles to guide our response to incidents, such as the loss of supply to a region, splitting of an electrical island, blackout of an island, or the need for rolling outages due to a security of supply event. We practice these responses as part of ongoing training and are looking to improve how we practice with industry.

Lessons from power system incidents that have occurred both here in New Zealand and overseas are sought out with an objective of mitigating or improving our response to similar future events should they occur.

Further details on the above points are outlined in the sections below.

## 2.1 Emergency response principles and plans in place

The System Operator has restoration principles and plans in place to guide our people in how to respond to different types of events.

### 2.1.1 Restoration principles

Contingency plans outline how to restore the power system after a total island-wide or regional outage. We have documented principles to guide us in the development and execution of a contingency (restoration) plan, including:

- restoration priorities – public safety, risk of damage to assets, stabilising the system, restoring the system, and recovery to normal operation
- dispatching – guidance on approaches including the use of discretion
- load pickup – how much load can be safely restored at each point of the response to maintain system stability
- effects of loss of power supply on asset and generation operation – understanding what is likely to be impacted and therefore not available for the response
- indications and remote control – understanding what is likely to be impacted and therefore not available for the response.

### 2.1.2 Restoration plans

The System Operator presently maintains 15 restoration plans which cover regions across New Zealand that have the potential to be disconnected from the main power system due to the failure of grid assets, as well as the situation where two separate electrical islands are created e.g. the South Island gets split in two electrical islands as was the case on the 2 March 2017.

We train our people in the use of these plans as outlined in Section 2.2 below, and each plan is reviewed on a cyclic basis as part of our controlled document management.

A list of active restoration plans is contained in Appendix 1.

### 2.1.3 Black start plans

We contract two generators in each island that are designated to restart the power system in the event that the power system collapses. In preparation to undertake a black start we maintain restoration plans for both the North and South Islands.

We ensure black start generators and plans perform as expected by regular testing, both with physical tests performed with the Grid Owner and Asset Owners, and through simulated testing as part of competency training for our National Coordination Centre (NCC) operators.

A list of active black start plans is contained in Appendix 1.

### 2.1.4 Rolling outage plans

In accordance with the Code, we have prepared and published the System Operator rolling outage plan on our website. This plan provides for the management and co-ordination of planned rolling outages as an emergency measure during energy shortages e.g. an extreme dry winter scenario.

Rolling outages are planned network outages which avoid unplanned grid outages, save energy as a last resort during a security of supply emergency, are used for immediate or developing events, are

triggered by the System Operator when there is a supply shortage (when unplanned outages are likely), and are implemented by distributors and direct connects.

Distributor and direct connect rolling outage plans must be kept up to date and updated plans must be sent to the System Operator for approval. Rolling outage plans must be re-submitted to the System Operator for approval not later than two years after they were last approved. The list of approved rolling outage plans can be found on our website. We are aware that some participant's rolling outage plans are overdue and we have agreed plans in place to bring them up to date.

To further lift our preparedness, in first quarter of 2022 we are planning on running a rolling outage exercise, focusing on hand-overs and operational communications between the System Operator, distributors and direct connects. Depending on the situation with COVID-19, this exercise may be postponed.

## 2.2 Training

For the controls above to be fully effective, our people need to understand how they are enacted through our tools and processes when required. To that end our NCCs maintain emergency preparedness through regular training in a simulator environment. Each NCC coordinator completes at least two four-day sessions in our control room simulator per year, experiencing simulated events that are designed to challenge and grow their skillsets and maintain competency with tools and familiarity with processes for managing power system incidents.

Simulated events range from scenarios that may be straight forward and we have plans in place for, but are still relatively rare in occurrence (such as under-frequency events, HVDC outages, restoring a faulted section of the grid), to high impact, low probability (HILP) events that stretch the teams to deal with complex and unusual scenarios where specific response plans do not exist and coordinators need to go back to basic principles (recent examples: a river flooding event that collapsed multiple South Island circuits, a major volcanic event that split the North Island into two electrical islands). "Soft skills" training forms an important element of all simulated events. In addition to tools and processes competencies, teams are expected to demonstrate capabilities in teamwork, leadership, communications and problem solving.

## 2.3 Practicing with industry

Over the years we have undertaken various Grid Restoration workshops with industry participants around the country, allowing us to test restoration and black start plans in a desk top exercise that simulates a restoration of the power system post-incident. Not only do these workshops provide lessons and improvements, they also provide us and participants the chance to work through a scenario that if it occurred would be highly stressful and complex. This controlled environment allows us to test the plans without the pressure of reality and provide all parties with the opportunity to ask questions, create a coordinated understanding across and within the various organisations, and create familiarity with processes.

As part of our response to lift our performance post the 9 August 2021 demand management incident, we will be establishing and publishing a calendar of exercises which will simulate a range of different types of incidents, helping to enable us to build better shared industry understanding of emergency response including communication and processes. The first such exercise is being planned for the end of May 2022.

## 2.4 Learning from operational incidents

Through our event investigation and significant incident reporting processes, we take the opportunity to learn from operational incidents that occur on the system. These include both significant incidents such as the 2017 South Island AUFLS incident, and the 9 August 2021 generation shortfall incident, through to less significant incidents such as the temporary loss of asset indications, asset trippings or undesirable asset or system performance.

Incidents are logged in a register, assigned to an investigator, and tracked through the investigation process. Any breaches of the Code identified are feed into our compliance framework managed by the SO Compliance & Impartiality manager. Corrective actions are recorded in a separate register and tracked through to completion. Live reporting of investigations and actions is provided to all managers weekly, with more detailed reporting provided to Senior Leadership monthly. Investigatorsand action owners also receive weekly reminders of outstanding items to address. As part of the closure process, the investigator shares findings at a weekly meeting of subject matter experts from across the Operations division, further helping to embed any lessons.

Not only do we look at New Zealand incidents, but we also monitor for and look at international incidents taking into consideration New Zealand's context to determine any relevant lessons.

Incidents provide us the opportunity for lessons to be identified, shared and improvements made to mitigate a future reoccurrence and lift our future response.

# 3 Business Continuity Planning

We recognise that the System Operator service plays a vital role in operating one of New Zealand's most critical infrastructure systems. The failure of this service would negatively impact electricity consumers, industry participants and Transpower's reputation. Through business continuity planning we identify potential threats to our people, facilities and tools that could impact our ability to sustain this service. We have put in place mitigations and plans to respond should such a threat eventuate.

To ensure our preparations are robust and reliable, we undertake assurance through scheduled testing and simulation. These simulations test the ability of our responses to be applied to a variety of scenarios in a consistent and structured way.

Threats of national significance such as a pandemic, major earthquake or tsunami are events that we cannot prevent. Therefore, we must be prepared through our business continuity planning to respond to such a threat in ways that allows us to recover to full operation as soon as possible given the vital importance our service plays in New Zealand. To this end, we prepare and train our staff in the Coordinated Incident Management System (CIMS). This structured incident management approach allows for our response to be integrated on a national level with other government agencies to facilitate a safe recovery.

The following table (Table 1) outlines three high level threats to our ability to sustain the System Operator service. For each we show the preparations/responses and assurance activities put in place through our business continuity planning to manage these threats. More detailed information on different threats, preparations/response and assurance activities is provided later in this paper.

Table 1 High Level Threats

| Threat | Preparation / Response | Assurance |
|---|---|---|
| **Loss of people** | Proactive skill-based recruiting; responsive people management; succession identification and planning; cross-role skill training; pandemic response plan | Annual skill gap and needs analysis; active staff management; three-monthly performance agreement discussions; development plans |
| **Loss of facilities** | Critical site redundancy and resilience; virtual control centre; working from home technology | Weekly inter-site fail-over testing; weekly stand-alone dispatch testing; monthly generator testing; three-monthly primary data centre switch over |
| **Loss of tools** | Critical IST site redundancy and resilience; back up communications; support service agreements based on service criticality | Weekly supervisory control and data acquisition (SCADA) and Market System performance testing; weekly satellite phone checks; monthly cyber security testing, cyber security audits and control testing; |

Our responses are informed by understanding what functions we perform as part of the System Operator service. We have undertaken a process of assessing and categorising these functions for criticality. This criticality is expressed as the maximum tolerable outage (MTO) for each function before it impacts our business continuity, as outlined in Table 2 below. We prepare our responses by understanding the priority of those functions that have the highest criticality.

Table 2 Maximum Tolerable Outage (MTO) categories

| Maximum Tolerable Outage (MTO) | | Description |
|---|---|---|
| **Tier 1** | < 1 hour | Core Functions – managing or supporting System Operator<br>Priority focus of the Incident Management Team is to coordinate the response and recovery of these functions<br>*Examples: Realtime scheduling and dispatch* |
| **Tier 2** | > 1 hour to 1 day | Various functions that support the Core Functions.<br>Key stakeholder and financial management functions are covered.<br>*Examples: Outage assessment, ancillary services processing* |
| **Tier 3** | > 1 day | Supporting functions with a lower criticality.<br>*Examples: Supporting final pricing, commissioning & testing, training* |

## 3.1 Identified Threats

Our ability to provide the service relies on ensuring we have the resources to operate effectively and have in place preparations to respond to threats to those resources. The following section outlines a selection of the existing threats to our people, facilities and tools that could impact on our ability to deliver the service.

### 3.1.1 To our people

Our most important resource is our people. A threat to this resource must be managed and controls put in place to prevent the impacts affecting the service we provide. The following table (Table 3) identifies a selection of the threats which could impact on the capability of our people.

Table 3 Threats to our people

| Threat | Preparation / Response | Assurance |
|---|---|---|
| **Widespread Illness / COVID-19** | Cross-role skill training; working from home technologies; COVID-19 pandemic response plan (includes vaccination and testing policy, additional Health &Safety protocols to safeguard control room staff) | Health & Safety audits |
| **Aging workforce** | Succession identification and planning | Annual skill gap and needs analysis (9-box talent matrix, critical people, critical roles) |
| **Lack of skilled staff** | Succession identification and planning; proactive skill-based recruiting; targeted training and development | Annual skill gap and needs analysis (9-box talent matrix, critical people, critical roles); three-monthly performance agreement discussions; development plans |
| **Lengthy training requirement** | Succession identification and planning; proactive skill-based recruiting; dedicated training function | Annual skill gap and needs analysis (9-box talent matrix, critical people, critical roles); three-monthly performance agreement discussions; six-monthly performance testing / training of critical skills staff |
| **Single points of failure (knowledge or skills)** | Cross-role skill training; succession planning | Annual skill gap and needs analysis (9-box talent matrix, critical people, critical roles); three-monthly performance agreement discussions |

### 3.1.2 To our facilities

We have redundancy and resilience across our business facilities. Our key facilities are the two National Co-ordination Centres and the two Data Centres. All four facilities are located separately to mitigate the likelihood that a threat at one location impacts on any other.

All facilities have active site management to ensure they can operate 24 hours a day, 365 days a year. Each facility has its own regularly tested UPS (Uninterruptible Power Supply) battery system and on-site, regularly tested generator.

The following table (Table 4) identifies a selection of the threats which could impact on our facilities.

Table 4 Summary of threats to our facilities

| Threat | Preparation / Response | Assurance |
|---|---|---|
| **Loss of facility** | Critical site redundancy and resilience; virtual control centre; working from home technology | Weekly inter-site fail-over testing; weekly stand-alone dispatch (SAD) testing; control room simulation testing; annual CIMS simulation exercises |
| **Power Supply loss** | UPS battery systems, on-site diesel generators | Regular scheduled testing of facilities services |
| **Transport Infrastructure failures** | Working from home technology | Technology review and testing |
| **Failure or compromise of security systems** | Working from home technology; facility service agreements | Security audits; annual CIMS simulation exercise |
| **Sabotage or terrorist threat** | Security systems; critical site redundancy and resilience; virtual control centre; working from home technology | Security audits; weekly inter-site fail-over testing; weekly stand-alone dispatch (SAD) testing; control room simulation testing; annual CIMS simulation exercises |
| **Natural disaster, earthquake, tsunami, flood, hurricane, tropical storm, bush fire** | Critical site redundancy and resilience; virtual control centre; working from home technology; 0800 WHAT TO DO (Transpower's internal communications helpline) | Weekly inter-site fail-over testing; weekly stand-alone dispatch (SAD) testing; control room simulation testing; annual CIMS simulation exercises |

### 3.1.3 To our tools

The System Operator service relies heavily on the performance of our and other industry providers' tools. These primarily are the SCADA system, the Scheduling Pricing and Dispatch (SPD) tool and the Reserve Management Tool (RMT). These tools are necessary for the continued operation of the power system and market. A failure in any of these tools directly impacts our performance and potentially our ability to provide the System Operator service.

The following table (Table 5) identifies examples of the threats which could impact on our tools.

Table 5 Summary of threats to our tools

| Threat | Preparation / Response | Assurance |
|---|---|---|
| **Loss of tools** | Critical IST site redundancy and resilience; support service agreements based on service criticality | Weekly SCADA and market system performance testing; monthly cyber security testing, cyber security audits and control testing |
| **Loss of Market System functionality** | Critical IST site redundancy and resilience; support service agreements based on service criticality; stand-alone dispatch (SAD) | Weekly SAD testing; control room simulation testing; annual CIMS simulation exercises |
| **Breach of system security** | Software updates and patching processes; international system knowledge base; industry groups membership; secure market system; SAD | Weekly SCADA and market system performance testing; monthly cyber security testing, cyber security audits and control testing |
| **Loss of communication and information paths (e.g. SCADA)** | Critical IST site redundancy and resilience; support service agreements based on service criticality; alternative email and communication paths such as satellite phones | Weekly SAD testing; weekly backup communication testing; control room simulation testing; annual CIMS simulation exercises |

Expanding on the key controls for two of the most serious high impact low probability threats:

- Loss of Market System functionality – The National Coordination Centre (NCC) control rooms have a laptop dedicated to taking a snapshot of the system every 30 minutes. This snapshot is used for Stand Alone Dispatch (SAD). SAD is not connected to our normal networks and if the Market System and networks are unavailable, we have a snapshot of the system and associated schedules to dispatch the system from. As time goes on the schedules degrade in accuracy since there are no inputs updating the view. However, this does allow us to operate the system for up to 36 hours using offers from participants. The more up to date and forward-looking the offers from participants are, the longer SAD's schedules can be relied on. We use SAD on a regular basis when we transfer primary control from one data centre to another, we also test the snapshot capture on a weekly basis to ensure it is working as expected.
- Loss of communication and information paths (e.g. SCADA) – SCADA has built in resilience. It has multiple communication paths through which the data it provides can be received. If the situation impacted those multiple paths, we have in the past worked with the Grid Owner to ensure people are sent to substations or important sites (HVDC) to pass on instructions and relay necessary indications. We maintain with the Grid Owner a prioristised list of substations and important sites to man should this situation occur in order to streamline the response.

## 3.2 Maintenance, assurance and improvement

We prepare to respond to threats we have identified. We check to make sure what we have prepared is appropriate and will work when called on. The processes for review and assurance of our plans and preparations are embedded into our normal business as usual activities.

The safety of our people is paramount with six-monthly fire drills and evacuation procedures being tested across random dates and times to ensure our people understand what to do. Access to audited civil defense supplies and grab bags are provided for our people's welfare during a prolonged event. We have also recently introduced a Transpower COVID-19 policy requiring all staff and visitors to our sites to be fully vaccinated. We have developed extensive pandemic response plans since the arrival of COVID-19, with a focus of safeguarding our control room teams, which includes bubble rosters, separate rooms for coordinators at each site, and contactless handovers. We are in the process of developing our approach to rapid antigen testing as well as procuring testing supplies in light of the Omicron variant situation and changing government settings.

Our facilities team regularly check the functions of our backup power supplies and fire systems and well as security access. All of these are reported on to governance functions, and improvement opportunities are actively pursued.

As part of maintaining our knowledge base for business continuity planning, we undertake annual BCP exercises along with six-monthly training sessions for our control room staff. These are focused on upskilling and the testing of knowledge using our simulator and desk-based event scenario exercises.

The performance of our critical tools is constantly reviewed and reported on. Weekly failovers from one control room to another, as well as three-monthly from one data centre to another. This allows for testing of the hardware, familiarity for staff, and assurance that the process works as expected. We rely on many of the IST functions being performed for us by third parties, though we are actively involved in the testing and fully informed of the outcomes from these activities.

Learning identified from the above activities are discussed and feed back into our processes and business continuity planning as appropriate.

# Appendix 1 Emergency response plans

## Appendix 1.1 Restoration plans

PR-CP-011 Bay of Plenty 220kV Contingency Plan
PR-CP-012 Hawkes Bay via 220kV Contingency Plan
PR-CP-013 Hawkes Bay via 110kV Contingency Plan
PR-CP-016 Wellington Region Contingency Plan
PR-CP-017 Auckland 220-110kV Contingency Plan
PR-CP-018 Otago Southland 110kV Contingency Plan
PR-CP-021 Nelson-Marlborough-Buller Contingency Plan
PR-CP-025 HAM and Waikato 110kV Contingency Plan
PR-CP-047 Canterbury Contingency Plan
PR-CP-049 North Auckland and Northland via 220kV Contingency Plan
PR-CP-638 Northland Region Contingency Plan via 110kV
PR-CP-772 TKA Dead Bus Contingency Plan
PR-CP-876 Taranaki Contingency Plan
PR-CP-879 Bunnythorpe 110kV Contingency Plan
PR-DP-200 Manage IL Events
PR-DP-212 Manage an Island Following an Unplanned Event
PR-DP-231 Manage a System Event (including a Grid Emergency)
PR-DP-252 Manage Geomagnetic Induced Currents
PR-DP-254 Manage AUFLS Event
PR-DP-257 Manage Demand
PR-DP-260 Gas Critical Contingency Management
PR-DP-262 Manage Energy Systems Tools Failures using Backup Tools
PR-DP-264 Manage Insufficient Generation Offers and Reserve Deficits
PR-DP-341 Manage a National SCADA_EMS Failure
PR-DP-599 Manage a Potential Electrical Island
PR-DP-899 Tsunami Risk Management

## Appendix 1.2 Black start plans

PR-CP-015 North Island Black Start Contingency Plan
PR-CP-091 South Island Black Start (MAN) Contingency Plan
PR-CP-092 South Island Black Start (CYD) Contingency Plan
PR-CP-578 South Island Black Start (AVI) Contingency Plan