Security and Reliability Council

22 July 2016 incident at Manapouri power station

Event summary, root causes and remedial actions

28 March 2017

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

1 The purpose of this paper is for Meridian to present to the SRC on an incident at the Manapouri power station on 22 July 2016

1.1 The Security and Reliability Council (SRC) functions under the Electricity Industry Act 2010 include providing advice to the Electricity Authority (Authority) on the security and reliability of the power system.

1.2 The Manapouri power station unexpectedly ramped down from 750 MW to 400 MW on 22 July 2016. Meridian offered to present to the SRC on the event, its root causes, contributing factors and remedial actions. The Chair of the SRC accepted this offer.

1.3 Therefore, the purpose of this paper is for Meridian to present its finding to the SRC and for the SRC to consider whether it should provide any advice in relation to this event or events of this kind.

2 Actual and potential consequences of the incident

2.1 Slides five and six of Meridian's presentation include a summary of the power system response. In particular:

a) South Island frequency dropped to 49.46 Hz

b) Clutha increased by ~60 MW

c) Waitaki block increased by ~90 MW

d) HVDC northward flow decreased by ~120 MW.

2.2 Had Meridian's generation controller not manually intervened to arrest Manapouri's ramp-down, system frequency would have fallen further. In addition to the 'swiss cheese slices' shown (which represent Meridian's barriers) on slide seven of Meridian's presentation, there were at least three remaining risk controls (system operator barriers) preventing a nationwide blackout:

a) generation governors are programmed with a permanent 4% droop setting, which means that before frequency could reach 48 Hz (4% droop from 50 Hz), the governors would have been ramping generation output to 100%

b) automatic under-frequency load shedding (AUFLS) would have tripped (two 16% blocks of load at 47.5 Hz and 45.5Hz in the South Island) to reduce load and increase system frequency

c) HVDC controls would have acted to prevent a North Island blackout by separating the islands in the event South Island blackout could not be prevented.

2.3 In addition to the above controls, if the incident were to occur today, there is another control that now exists. The establishment of a national market for instantaneous reserve means that North Island interruptible load would trip at 49.25 Hz (as happened recently in the 2 March 2017 South Island AUFLS trip).

2.3.1 [Correction] At the SRC meeting on 28 March 2017, it was noted by a member that reserve sharing was already in place at the time of the incident and therefore the national market for instantaneous reserves will not be a new control for future events. Reserves were being shared using the HVDC frequency keeping controls. It was also noted that the reserve sharing arrangement did work and mitigated the effect of the event.

2.4 One consequence of the incident not mentioned in the Meridian presentation relates to over-frequency arming[1] at the time of the incident being enabled on two of the six Manapouri units. This was temporarily disabled on both units for approximately nine minutes to facilitate increasing Manapouri back to setpoint. In principle, this was a slight reduction in security compared to the level of over-frequency arming that the system operator had deemed appropriate to procure. In practice, the low HVDC transfer and low frequency at the time meant that there was almost certainly no actual security issue.

3 Questions for the SRC to consider

3.1 Meridian's presentation is attached to this cover paper. Representatives from Meridian will attend the SRC's meeting to present and respond to the SRC's questions.

3.2 There are venues for companies to share lessons relating to health and safety matters. StayLive's 'Process Safety Industry Group' subgroup enables its members to learn from each other and to improve safety outcomes.[2]

3.3 The SRC secretariat is not aware of any equivalent forum for either the operational lessons in the electricity industry, or risk management generically. SRC members may wish to consider whether such a function is desirable and would be of net benefit. Pertinent to this question is:

a) whether distributors can effectively share lessons via the Electricity Networks Association

b) whether the New Zealand branch of the International Council on Large Electric Systems (CIGRE) or the Electricity Engineers' Association might provide suitable forums for such lesson-sharing by industry participants

c) that the Authority's Market Monitoring team conducts reviews of power system events (such as the Penrose incident previously considered by the SRC)

d) that the Authority's Compliance team publish some case studies (with the consent of the relevant parties) where there are compliance lessons for other industry participants

e) that the system operator has made a commitment to publishing reporting into a selection of power system events (such as AUFLS events)

f) that the SRC does review a small number of highly significant incidents, though it appears to be an inefficient use of the SRC's time to perform this function in any broader capacity.

3.4 The SRC may wish to consider the following questions.

Q1.	What questions, if any, does the SRC wish to ask of Meridian's representatives?
Q2.	Does the SRC have any concerns with current industry arrangements for sharing lessons (not health and safety) from operating in the electricity industry?
Q3.	What further information, if any, does the SRC wish to have provided to it by the secretariat?
Q4.	What advice, if any, does the SRC wish to provide to the Authority?

[1] Over-frequency arming is an ancillary service procured by the system operator. Generators providing over-frequency arming must reduce output in the event that system frequency rises to 53-54 Hz.

[2] StayLive members include Contact Energy, Genesis Energy, Meridian Energy, Mighty River Power, Pioneer Energy and Trustpower. Source: http://www.energyawards.co.nz/finalist/2016/health-and-safety-initiative-of-the-year/staylive

Manapouri Ramp Down Incident

Overview of event and remedial actions

Chris Ewers – February 2017

Outline

On the 22nd July 2016 while some corrective maintenance was being undertaken on a low voltage distribution board, Manapouri (MAN) generation unexpectedly ramped down from its dispatched level of approximately 750 MW to 400 MW.

Manapouri Power Station is a critical component of the Southland region and the South Island.

This paper discusses:

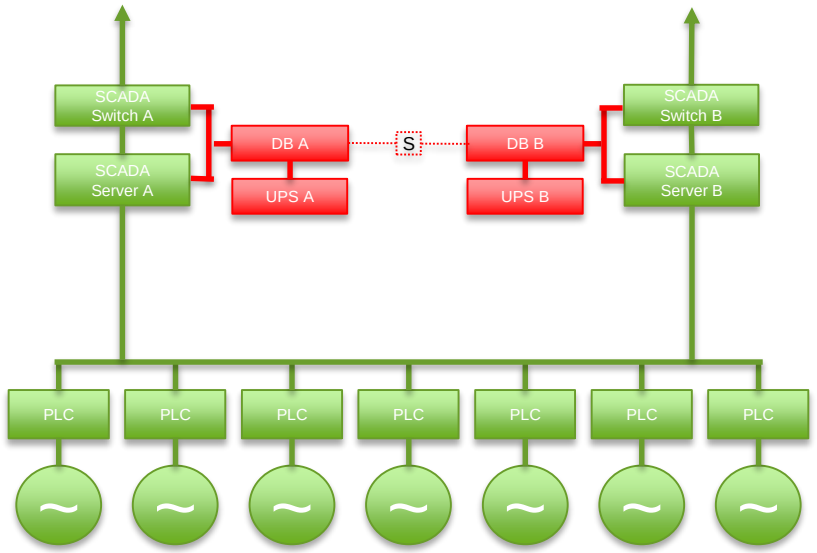
1. Summary of Manapouri control system and its importance in the system
2. How 350 MW of generation was unexpectedly lost
3. Root causes and contributing factors
4. Remedial actions and improvements

Manapouri Power Station Control

MAN consists of 7 x 130 MW generating units controlled by a pair of station SCADA servers.

Each server has its own uninterruptable power supply (UPS), distribution board (DB) and a network switch that connects to the remote Meridian Control Centre. The server pair operate so that one is on 'duty' and the other on 'standby'.

The corrective maintenance work scheduled on 22 July was to remove a redundant switch "S" that connected the two DB's[1].



1. This switch allowed both DB's to be connected, to allow for one UPS to be taken out for maintenance while retaining both server pairs in service. A move to separate unitised power supplies required this functionality to be removed. The switch had been "tagged out of service" in the meantime to avoid operation.

MAN Ramp Down Incident

MAN was generating 750MW. Server B was in 'duty' and Server A was on standby.

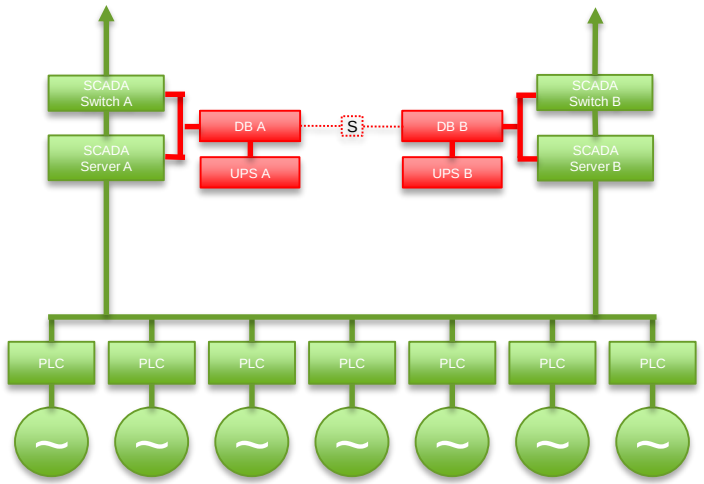
Original work-plan was to remove the switch while live. Upon commencement of work, it was deemed safer to undertake the work with the panels containing the DB's de-energised.

This change in work practice should have triggered a new change control process, however this was not undertaken.

UPS B was powered down first, causing Server B to power down and Server A to assume 'duty'.

The wires for the switch were removed from DB B and then UPS B supply was restored. Server B automatically rebooted on power up, saw that Server A had control, and then awaited for a manual operator action to initialise a 'hot standby'[2] process to return Server B to 'standby'. This action was not undertaken[3].

UPS A was then powered down to remove the remaining set of switch wires. Server A powers down and SCADA control (both local and remote) to MAN are interrupted[4]. The generating units remain generating under PLC[5] control on their last set point.



2. The 'hot standby' process synchronises current status data from the 'duty' server to the 'standby' server, such as current dispatched station MW setpoint.

3. Thus Sever B is neither 'duty' or 'standby' – essentially it doesn't have a role at all.

4. Since Server B had not previously been put into 'standby', it did not assume the 'duty' role when power was lost to Server A.

5. A PLC is a form of industrial computer. Each unit at MAN has a PLC as the first point of control.

MAN Ramp Down Incident

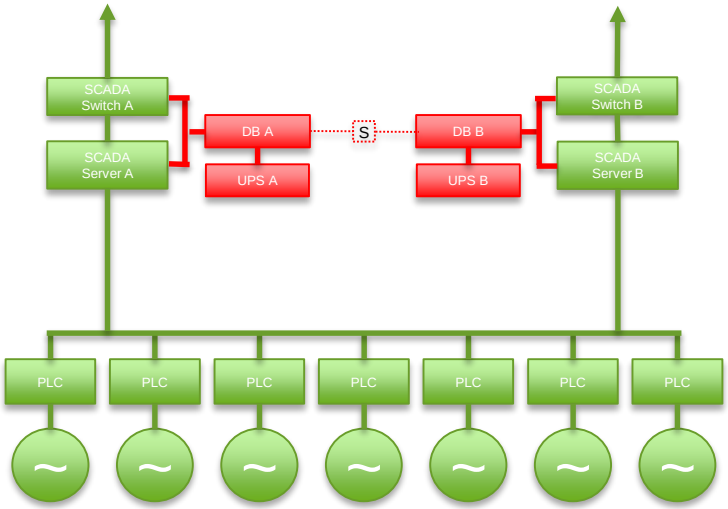
UPS A was then reenergised and the SCADA Server A rebooted. Upon coming online, Server A did not see a primary server online, and therefore assumed that it was in a 'cold reboot' scenario.

Server A then assumed 'duty' and loaded default values – including a station setpoint of 0 MW. The software then allocated this set point out to the generator units and the plant begins ramping down from 750 MW.

The 0 MW default value issue within SCADA was known by some but not all Meridian's staff. The SCADA switch A also rebooted after being reenergised and came online after Server A. Once the switch came online, visibility of MAN was restored to the Meridian Control Centre.

Meridian's Generation Controller saw the MAN indications and noticed the output dropping. He reissued a new setpoint which arrested the fall in output to approximately 400 MW. This started to return the station output towards 750 MW.

Full output is returned to 750 MW some minutes later. South Island system frequency dipped to 49.46 Hz.



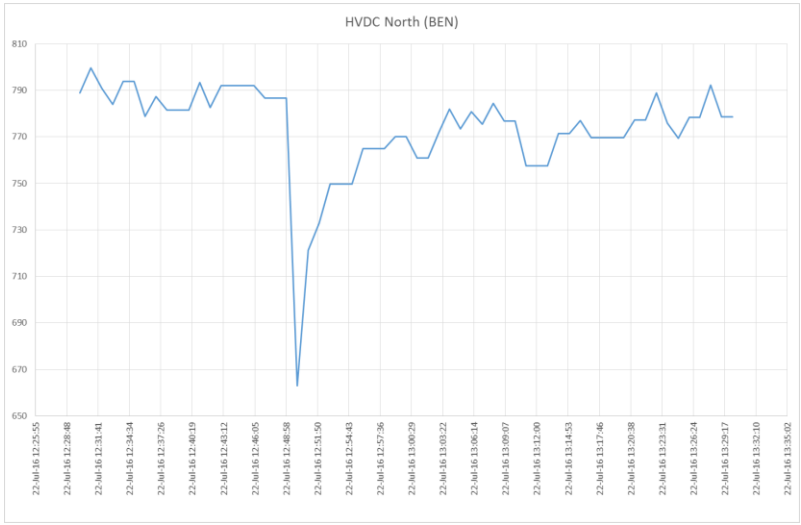
MAN Ramp Down Incident – System Response

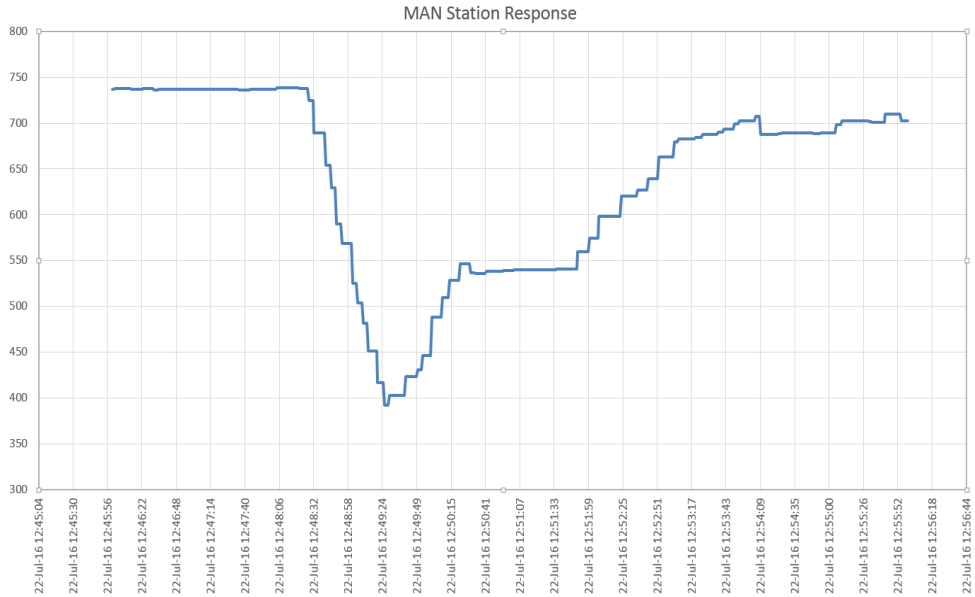
South Island demand was approximately 1780 MW. HVDC was transferring approximately 790 MW to the North Island

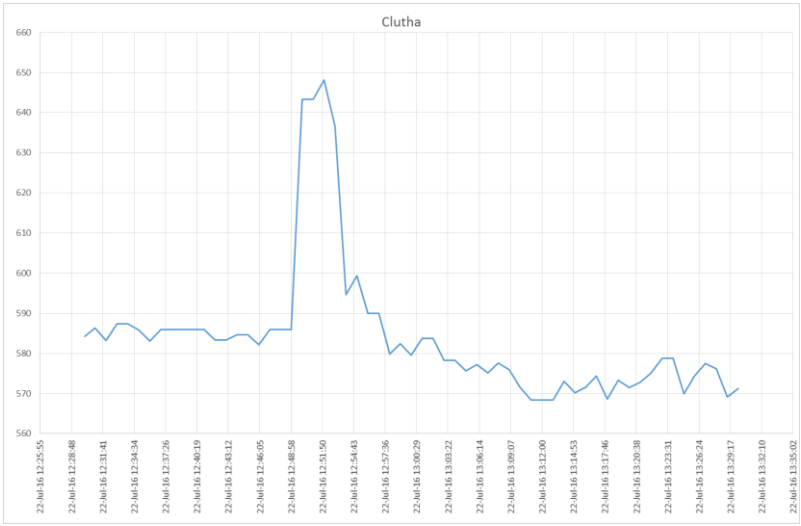
Manapouri generation ramped down at 1 MW/sec for each of the six units generating. 350 MW over one minute.

Other generator governor response and HVDC response[6] during the MAN ramp down involved:

- Clutha increased ~ 60 MW
- Waitaki Block increased ~ 90 MW
- HVDC ramped back ~ 120 MW



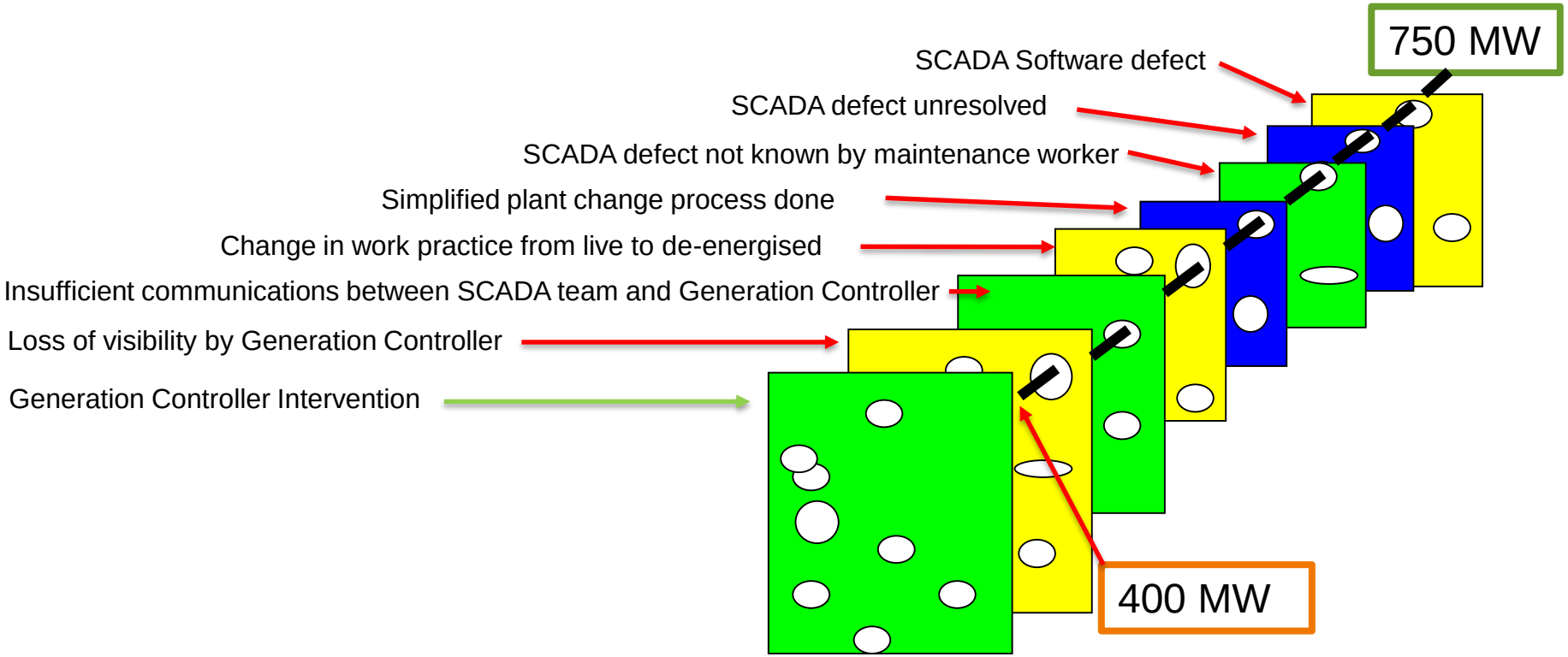




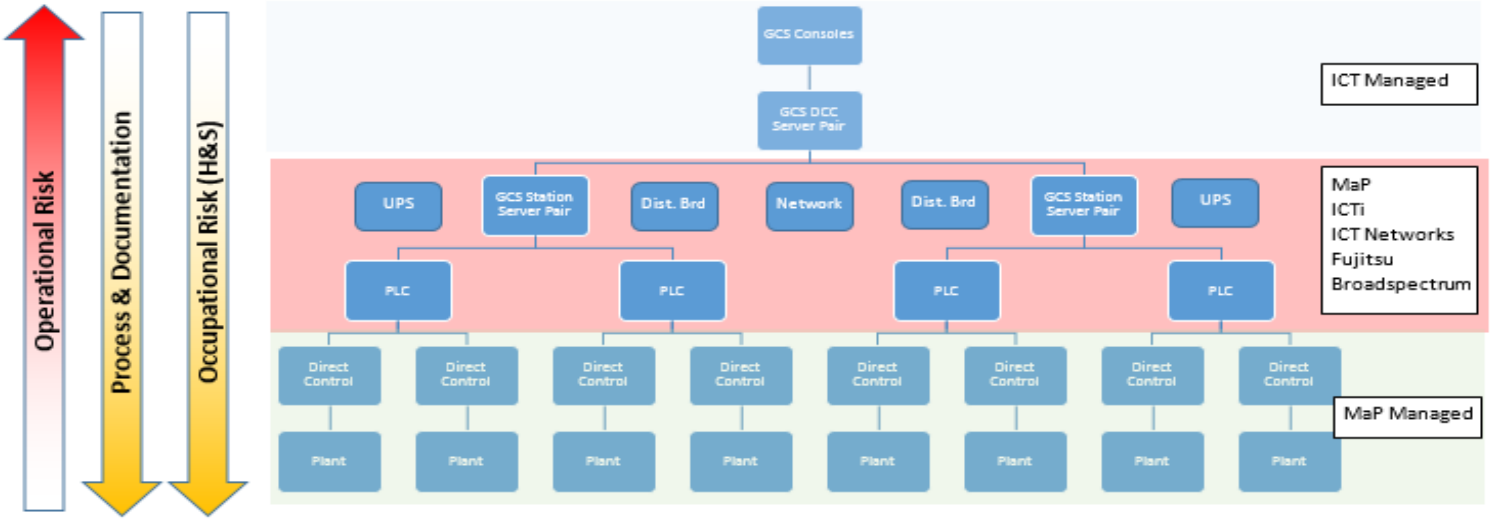
6 Source: 1 minute SCADA data published via EM6

Root Causes and Contributing Factors

The James Reason Swiss Cheese model, likens organisational defences against failure to a series of slices of randomly holed Swiss Cheese. The holes in the cheese slices represent individual weakness in the defence barriers. The system as a whole produces failures when the holes in all the slices align.



High level findings



Meridian's process and procedures have been focused on gear that can hurt people physically. Occupational safety and health systems, processes, procedures and culture are strong and have been an ongoing focus for a number of years.

However operational system level risks are greater with equipment that generally doesn't carry a risk of physical harm (IT and SCADA systems). Systems, processes, procedures and culture need to receive a strong focus, similar to occupational health and safety.

Meridian has a number of boundaries and interfaces where ICT services connect with large generation plant. Coordination and collaboration are an essential part of ensuring good plant and process safety outcomes.

Remedial Actions and Improvements

Meridian undertook an internal review, and engaged DuPont to review the incident. The detailed recommendations are :

- *Implement a change to SCADA to ensure that the ramp down event cannot reoccur through the same mechanism.*
- *Review all outstanding SCADA defects and present a prioritised set of corrective actions*
- *Review the current corporate risk appetite to "process safety/operational risk" events.*
- *Design and rollout risk evaluation check as part of the job planning process*
- *Review corrective maintenance work orders to ensure classification is appropriate*
- *Review alarms and recommend changes to avoid "alarm flooding" for generation controllers*
- *Start a programme of "culture change" by raising awareness of the event and the company response to improve its plant safety similar to Meridian's approach to occupational health and safety*

Actions underway

- Governance Group made up of the Chief Executive, GM Markets and Production, ICT and HR. The terms of reference includes recommendations from the DuPont review combined with internal investigation outcomes and existing process safety work that has been underway over the last 18 months.
- A SCADA ramp down defect patch has been implemented to avoid a recurrence of a similar event at any Meridian generation site.
- All outstanding SCADA defects will be reviewed and change recommendations made by the end of April 2017.
- Communication of the findings presented to all levels of the business as well as opportunities to engage people in improving process safety culture and performance.
- A SCADA alarm management project is underway. This will rationalise the current alarm levels to reduce nuisance alarms and provide generator controllers with improved decision making information.