Security and Reliability Council

Supply-side reliability – credible event data

21 August 2012

Information only

Note: This paper has been prepared for the purpose of SRC discussions. Content should not be interpreted as representing the views or policy of the Electricity Authority.

1 The SRC has requested a dashboard of reliability data

1.1.1 At its meeting on 10 May 2012 the Security and Reliability Council (SRC) requested the secretariat provide a 'dashboard' of security of supply and reliability measures for its consideration, together with a paper discussing the Authority's interest in reliability in context of its statutory objective and the boundaries with other jurisdictions such as the Commerce Commission. Rather than attempting to 're-package' data and information generated by other parties, the secretariat has invited both Transpower and the Commerce Commission to present relevant information to the SRC at this meeting.

1.1.2 The focus of both of these parties is generally at the consumer-end of the electricity supply chain, i.e. in measures such as supply interruptions. Reliability issues on the supply-side of the electricity system do not generally manifest themselves as supply interruptions, as system redundancy and system operations will generally ensure that supply is maintained (i.e. the availability of parallel transmission circuits and the provision of ancillary services).

1.1.3 The scale and frequency of supply-side reliability events has implications for consumers, through the cost of providing the necessary system redundancy, ancillary services, etc. The system operator collects relevant data for use in the development of the credible event policy that is described in the Policy Statement (that is incorporated into the Code by reference).

2 The system operator's security policy review provides a source of supply-side reliability data

2.1.1 The Policy Statement sets out the policies and means that are considered appropriate for the system operator to observe in meeting its Principal Performance Obligations (PPOs), subject to its acting as a reasonable and prudent operator.

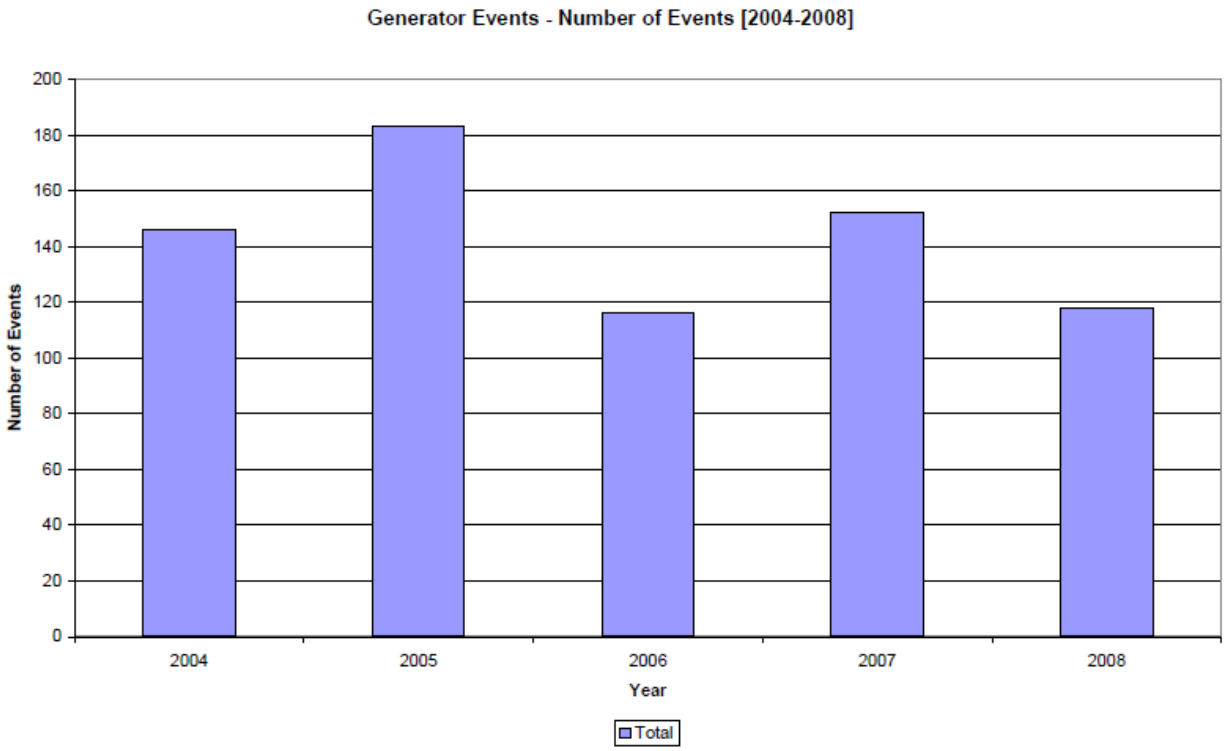
2.1.2 The first chapter of the Policy Statement, the Security Policy, includes the identification of the potential credible events that may result in cascade failure, due to these events causing quality and/or power flow outcomes that exceed asset capabilities. These events include the loss of generating units, transmission circuits, a pole of the HVDC link and various other events. Having identified these events, the system operator assesses their likely incidence, the means and costs of mitigating the consequences and, subsequently, identifies the possibility for the events to be managed. Management of these events includes the use of tools such as reserves, constraints and automatic load shedding (i.e. AUFLS).

2.1.3 The Security Policy requires the system operator to review the identification, assessment and assignment of potential credible risks not less than once in each five year period. The most recent review was concluded in 2009. With the next review not due until 2014, the most recent information available is from that 2009 report. The data from that review, that looked at events over the period 2004-2008, is presented in this paper as an indication of the extent and frequency of supply-side issues.[1]

[1] The review and related data analysis is available at http://www.systemoperator.co.nz/n2531.html

3 Generator events

Figure 1: Recorded generator events 2004 – 2008



3.1.1 Relevant statistics include:

Average annual outage rate: 143 events per year (144 for 1995-2000)

Of which:	27.2 events/year >100 MW
And:	14 events/year >200 MW (about 10% of the total)
And:	11 events/year involve multiple units

Average MW loss: ≈ 70 MW

3.1.2 The interruptions were shared amongst the different fuel/technology types, with hydro representing about 30% of the total, gas and thermal at roughly the same level of events as the previous review period and the frequency for technologies such as geothermal and wind starting to increase as the installed capacity increased.

3.1.3 Generator outages caused frequency to move outside the normal control band about 17 times per year on average.

4 HVDC events

4.1.1 At the start of 2008 the operation of pole 1 of the HVDC link was changed significantly. Half of pole 1 was placed permanently out of service and the remaining half pole 1 was only made available for limited operation under certain, critical situations. Pole 1 was recently taken out of

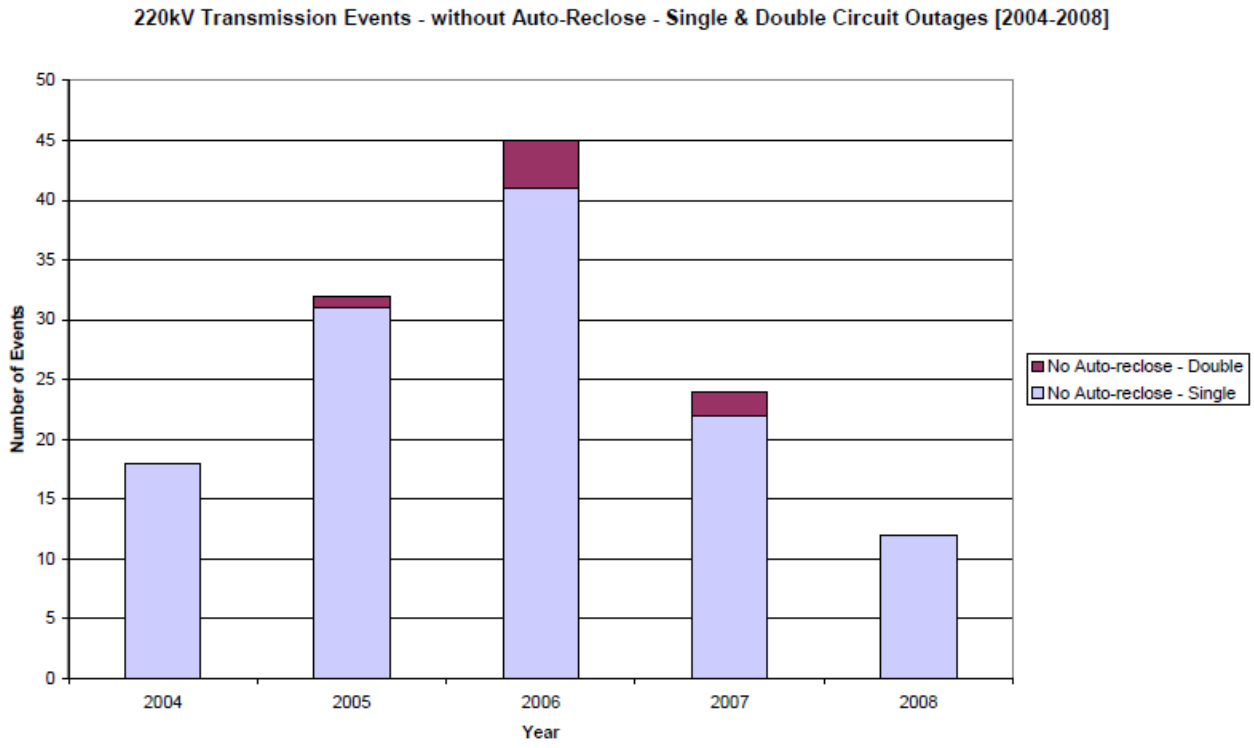
service completely in preparation for the commissioning of the new pole 3. As a result, the HVDC event data presents limited useful insight into potential future event rates.

4.1.2 The average event rate for pole 2 over the 5 year review period was 2.6 events per year, with 2 "other" events (loss of a condenser or filter bank, line fault or MCB fault). This was down slightly on the previous review period.

5 Transmission line events

5.1.1 The primary focus of the analysis was on 220 kV circuits (that represent the core of the transmission network). Most of these circuits have auto-reclose facilities, that look to restore operation automatically in the event of a fault. Where this is successful the only noticeable impact on service might be a voltage flicker. Where the auto-reclose is unsuccessful, remote switching or maintenance attention is required to return the circuit to service. On average 60% of the outages resulted in successful auto-reclose.

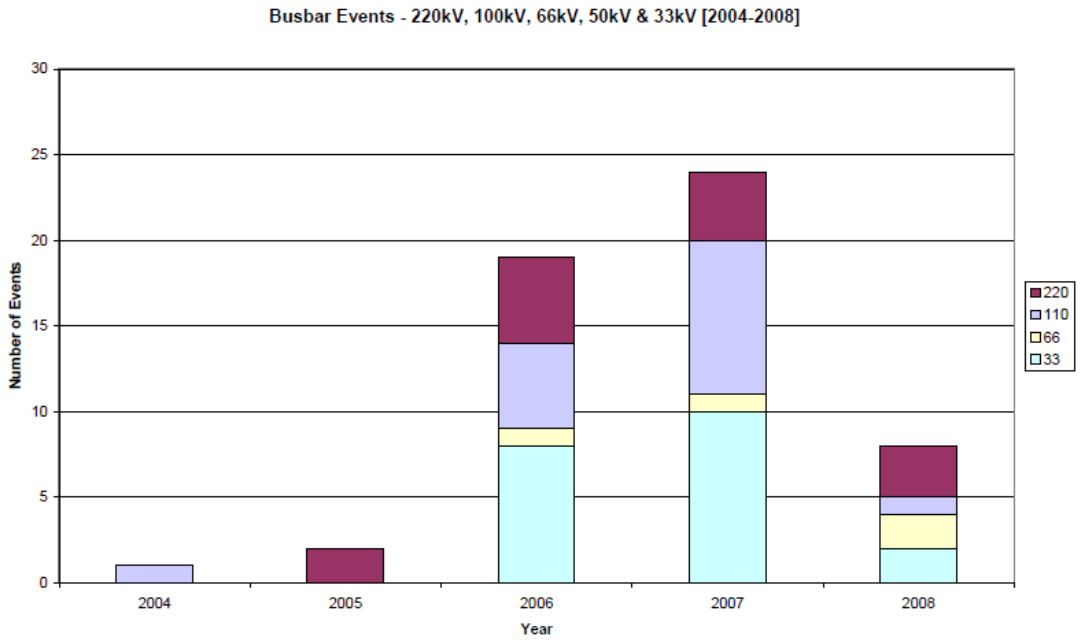
Figure 2: Recorded 220 kV transmission events - without auto-reclose action – single and double circuit outages 2004-2008



5.1.2 The average number of interruptions (25 per year for single circuits, 1.4 for double circuits and zero for multiple circuits) were similar to those from the previous review period.

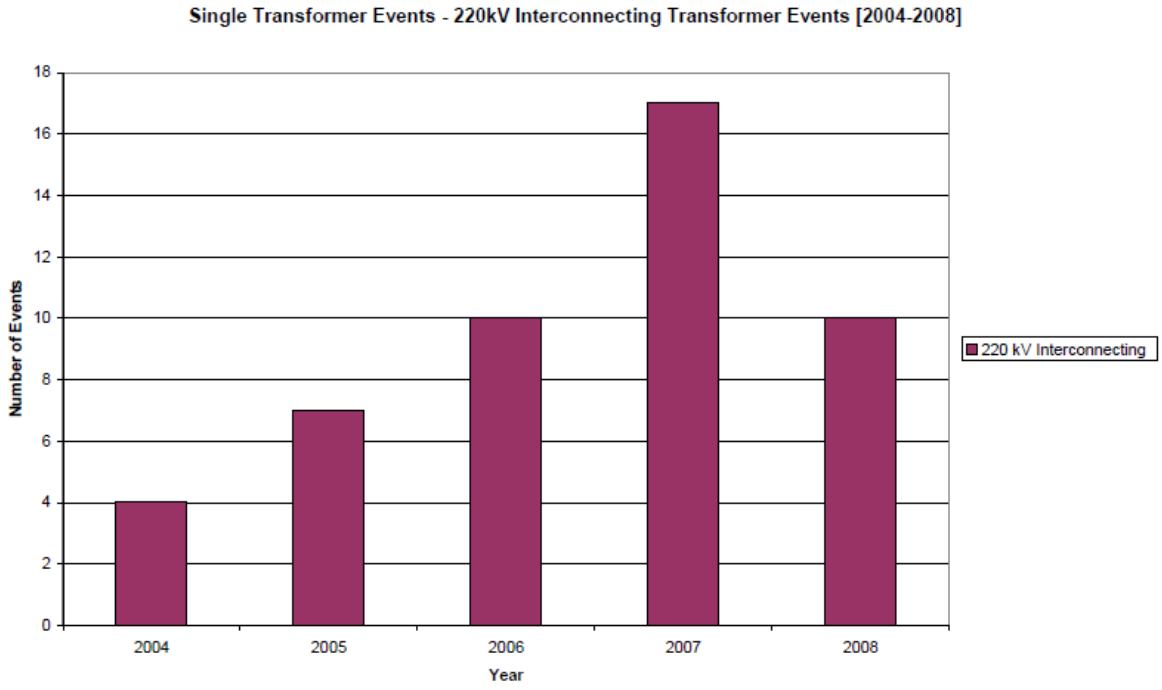
6 Other events

Figure 3: Busbar events – 220 kV, 100 kV, 66 kV, 50 kV & 33 kV – 2004-2008



6.1.1 There was an average of 11 busbar events (across all voltage levels) per year, with an average duration of 9.1 hours. 6 of the 11 events would be expected to occur on the 220 kV or 110 kV busbars. The previous review showed an average of 10 events per year, though did not distinguish between voltage levels. 90% of events lasted less than 8 hours, with 5% greater than 24 hours.

Figure 4: Recorded 220 kV interconnecting transformer events – 2004-2008



6.1.2 There was an average of 10 220 kV interconnecting transformer events per year, with an average duration of 52.3 hours. 92% of events lasted less than 48 hours.

6.1.3 The loss of a 220 kV interconnecting transformer or an individual 220 kV busbar, 110 kV busbar or 66 kV busbar connected to the core grid has been considered have been reviewed for potential inclusion in the Security Policy as extended contingent events (ECE, i.e. an event requiring the use of automatic load shedding). The system operator has concluded "*no additional controls are required to treat these potential events as an ECE with all circuits in service i.e., the system is designed to be capable of sustaining such faults without asset or load security concern. The only exceptions to this is the potential loss of the Manapouri busbar which, due to the recent addition of two wind farms in the South Island that do not meet frequency asset owner performance obligations, will require generation at such wind farms to be constrained at times of low load.*"[2]

7 Credible event risk summary

7.1.1 The collected data was summarised into a table ranking the various events in terms of their "event risk factor" (number of events divided by the number of elements in that risk set). The most significant of these are presented below:

Credible event i.e. loss of…	No. elements in set	No. events per year	Event risk factor
HVDC half pole	2	20	10
HVDC pole	2	7	3.5
Single generating unit	<234	132	0.56
Reactive plant	<134	49	0.37
HVDC bipole	1	<0.5	<0.5
Single 220 kV circuit (no auto-reclose)	142	25	0.18
220 kV interconnecting transformer	105	10	0.095
Multiple generating units	<117	11	0.094
110 kV interconnecting transformer	10	<0.5	0.05

[2] http://www.systemoperator.co.nz/security-management#cs-1876931