A scientific contextualisation and methodology for analysing cascade generation failures in power systems

M Viljoen

orcid.org/ 0009-0008-09517-6450

Thesis accepted in fulfilment of the requirements for the degree
Doctor of Philosophy in Electrical Engineering at the
North-West University

Promoter:	Prof JA de Kock
Graduation:	June 2025

Abstract

Electrical power systems form the key infrastructure that underpins the health, stability, and general prosperity of modern societies. However, the stability and reliability of such power systems are not absolute, and vulnerabilities expose them to disruptions that, in turn, threaten to disrupt the very societies they serve.

Electrical power systems are among the largest physical systems created by mankind, consisting of various constituent parts like power lines, substations, municipal distribution systems, and end-user customers. One of the most important components of any electrical power system is power stations – vast assets comprising intricate systems and processes that function in a coordinated fashion to generate electricity. When a power station is compromised, it threatens the stability and integrity of the electrical power system in which it is embedded.

Disruption of power generation facilities (like power stations) constitutes a specific subset of adverse events that require in-depth understanding to manage and mitigate effectively. Such an understanding needs to be derived by investigating and analysing the events that caused the disruption.

As a distinctly separate subset of adverse events in the diverse suite of undesirable societal disruption events, power station disruption events internationally suffer from an absence of a uniform methodology for investigation and analysis. This is particularly surprising given the ever-increasing number of large-scale power system disruption events that affect millions of people every year across the globe.

This study provides an overview of the engineering endeavour that is electricity generation, its evolution, and its disruption. It explores the inherent vice of all power stations, namely interdependencies and co-dependencies, to provide a context for the problem of power system disruption.

The international landscape of large-scale generation disruption events is explored, and shortcomings are identified. The historical perspective for the systematic and deliberate evolution of electrical power systems and power stations is presented as a contextual foundation. Developing the context further, many of the systems found within power stations are explored, and their deficiencies are highlighted through suitable case studies and examples, both locally and internationally.

Ultimately, a methodology is developed whereby cascade disruption events of power generation facilities can be appraised for analysis, recording, ranking and evaluating such events. For the development to be undertaken, various factors are identified that erode the integrity of an electrical power system during a disruption.

Metrics are developed to assess an event's impact and severity, using suitable integrity erosion factors as inputs.

Finally, a framework for collating event data and information is provided to aid in systematically recording and archiving event information.

List of Publications that Emanated from this Research

International academic and industry institutions play an important role in furthering the understanding and application of pertinent knowledge and sharing experience pertaining to the electricity supply industry. During the course of conducting this research, various articles were presented and subsequently published, outlined below.

a *Cascade Disruption of Generation – Using Adversity for Learning & Improvement*, published in the 2011 IEEE Eurocon.

b *Cascade Disruption of Generation – A Special Focus on African Grid Vulnerabilities*, published in the 2011 IEEE Africon.

c *Cascade Disruption of Generation: The Hidden Gift of Failure*, published in the 2012 IEEE PowerAfrica.

d *Exploiting Cascade Failure for the Calibration of Planning Assumptions & Operational Improvement*, published in the CIGRE Proceedings 2019.

e *Determining Vulnerability Parameters for Power Generation Fleets to Adverse Environmental Conditions*, published in the CIGRE Proceedings 2021.

Keywords

Cascade failure; power system disruption; aberrant behaviour; power station evolution; disruption event progression; power system integrity erosion; system commonality; multiple contingency disruption event.

Preface and Acknowledgements

The need for this research became evident towards the end of the history timeline of large electrical power systems when large utilities dominated the electricity supply industry. Most Western countries had already adopted liberalised models for power supply and embraced the concept of independent power producers – both conventional and so-called clean electricity sources. The abolition of conventional, monolithic models for electricity supply ushered in the age of grid-tied inverter-based power generation and a wide variety of smart technologies with the promise of ever-greater economic efficiencies and operational flexibility.

However, these macro changes permeated power systems with significant undesirable side effects and have, as yet, failed to definitively prove the macro benefits upon which the transformation was predicated.

One such area where undesirable side effects are particularly pervasive is the large-scale power system disruptions that escalated significantly since the start of the 21st century. With a career spent in the field of cascade disruption events in the realm of power generation, the absence of industry focus on such a significant aspect of power system performance grew ever more concerning.

Realising the international lack of recognition and industry attention to this subject matter, seeded an analytic curiosity towards better understanding – ultimately culminating in a proposal for dedicated research.

It is necessary to acknowledge Eskom, the power utility of South Africa, for its unwavering support of this research and for granting access to proprietary information, without which the research effort would have been impossible.

Table of Contents

Abbreviations, Definitions and Units

Abbreviations

AGC	Automatic Generation Control
AC	Alternating Current
A.D.	Anno Domini
AVR	Automatic Voltage Regulator
CCGT	Combined Cycle Gas Turbine
CME	Coronal Mass Ejection
COMELEC	Comité Maghrébin de l'Electricité (Maghreb Electricity Committee)
COMESA	Common Market for Eastern and Southern Africa
CPU	Central Processing Unit
CT	Current Transformer
C&I	Control and Instrumentation
DC	Direct Current
DCS	Distributed Control System
DMP	Demand Market Participation
DRC	Democratic Republic of Congo
EAC	East African Community
EL1	Emergency Level 1
EMI	Electromagnetic Interference
EOD	Electrical Operating Desk
GX	Generation
H_2	Molecular hydrogen gas
HMI	Human Machine Interface (historic MMI – Man Machine Interface)
HP	High Pressure
HV	High Voltage
HVDC	High Voltage Direct Current

IED	Intelligent Electronic Device
I/O	Input / Output (typically in terms of electronic equipment)
IP	Intermediate Pressure (used in reference to steam turbines)
IP	International Protection rating as defined in IEC 60529 [173]
IPP	Independent Power Producer
IPS	Interconnected Power System
LAN	Local Area Network
LP	Low Pressure
LV	Low Voltage
MCR	Maximum Continuous Rating
MUD	Multiple Unit Disruption
MUT	Multiple Unit Trip
MV	Medium Voltage
NER	National Electricity Regulator
NERSA	National Energy Regulator of South Africa
OEM	Original Equipment Manufacturer
OPCR	Outside Plant Control Room
PLC	Programmable Logic Controller
PV	Photovoltaic
QOS	Quality of Supply
RoCoF	Rate of Change of Frequency
SA	South Africa
SADC	Southern African Development Community
SAGC	South African Grid Code
SAPP	Southern African Power Pool
SCADA	Supervisory Control and Data Acquisition
SVC	Static var Compensator
TSO	Transmission System Operator

TX	Transmission
UFLS	Underfrequency Load Shedding
UPS	Uninterruptible Power Supply
USA	United States of America
VFP	Victoria Falls Power Company Limited
VSD	Variable Speed Drive
VT	Voltage Transformer
WAP	Wide Area Network
ZESA	Zimbabwe Electricity Supply Authority

Definitions

alive	Energised in an electrical context.
auxiliaries	Equipment (components and systems) that directly supports and enables a larger goal to be achieved, e.g., the production of electricity.
cascade	A chain reaction of events – each having been caused by a previous event but also serving as a trigger for the next event, e.g., the toppling downfall of a row of dominos.
co-dependence	Being mutually reliant upon an external function or production commodity.
C&I	Control and instrumentation are secondary systems that enable the automation, control, monitoring and protection of primary and auxiliary systems and processes – normally implemented through electronic, digital or pneumatic technologies.
blackout	An abnormal event that has such severity as to cause the grid to destabilise to an extent that results in the cessation of all power delivery on a largescale, affecting many people simultaneously – major cities, large regions, entire countries or even across national borders.
black-start	To restore the power system to within normal operating conditions following a blackout.
dead	Not energised in an electrical context.
disruption	An abnormal event that caused the normal operational envelope to be exceeded.
disruptor	An event or condition that causes a deviation from the normal steady state.
EL1	***E****mergency* ***L****evel* ***1*** is a state of unit operation when the unit generates a greater quantity of power than what it is designed for, exceeding the MCR of the unit but without exceeding the safety margins of any of the installed plant and equipment comprising the unit.
electricity	The commercial commodity that is based on the science of the electrical charge of subatomic particles, exchanged through dedicated

	technologies to predominantly trade energy between market participants – packaged with reliability services to enhance the economic value of the product.
Eskom	The main electricity supplier of South Africa, exists as a parastatal, having evolved from the Afrikaans and English acronyms Evkom (Elektrisiteitsvoorsieningskommissie) and Escom (Electricity Supply Commission) respectively, which was the South African Electricity Supply Commission, which in turn came fourth after acquiring the Victoria Falls Power Company Limited (VFP).
generation	a. The process of converting energy specifically into electricity. b. A technological manifestation shared amongst plants developed during a specific era. c. The collective noun that signifies a collective concept of various (or all) producers of electricity.
grid	A system that interconnects many suppliers and consumers of electricity – with multiple nodes and possible paths through which electricity can reach those connected to it.
grid code	A official regulatory set of rules that governs access to the power system by producers and consumers and ensures fair access to all participants.
interdependence	Being mutually reliant upon one another for specific functions or production commodities.
islanding	When a generating unit separates from the power system in such a way that the process of electricity generation is not shut down or interrupted – allowing the unit to be reconnected to the power system without delay.
min-gen	The minimum level at which a generating unit can operate in a stable condition without requiring additional fuel support.
multiple unit trip	More than one generating unit disconnecting from the grid in reaction to the same initiating event (trigger).
outside plant	All plant for systems that are common between the units – also known as *common plant* or *balance of plant*.

peaking	A form of power generation that can readily and within a relatively short space of time, be brought into service from a standby state (or readily returned to standby from an operational state).
plant	An encompassing set of equipment and systems that are individually or collectively intended to fulfil a specific function – normally forming part of a larger system or process.
power station	A collective set of power-generating units that share the same geographic location.
power system	A vast superstructure that interconnects consumers and producers of electricity through network and grid topologies – operated collectively for the mutual benefit of the participants.
process	A compound arrangement of various associated systems and equipment that collectively achieves an overall goal. Often used in relation to the conversion of energy.
resilience	The ability of a power system to continue to fulfil its function or a power station to continue operation without a cessation in power generation, when disruptions occur.
set	A generator with its prime mover and all requisite auxiliary equipment and systems that would allow for electricity generation when the prime mover is set in motion. The energy source required to set the prime mover in motion is excluded. Also, gen-set or generator-set.
shaft train	A set of various rotating masses that are mechanically linked together and rotate together, to collectively convert mechanical energy into electricity or vice versa – whilst storing angular momentum while in operation.
six-pack	A power station consisting of six generating units – the median utility power station configuration in South Africa.
system	An arrangement of components and equipment that collectively produce a desired function – typically having specific inputs and outputs.

trigger	A precursory event that sets a subsequent series of events in motion that collectively develops, in a cascade fashion, into a large-scale disruption event (also initiating event).
trip	The rapid and automated action, to switch out, interrupt(s) or disconnect processes and equipment – thereby temporarily withdrawing it from operation. It is normally implemented when entering an operational state that threatens to damage the plant or otherwise cause human harm.
turbo-generator	The total assembly of turbine stages together with the generator and its rotating exciter stages that function collectively on a single shaft train to generate electricity. Also known as the *turbine centre line*.
unit	A set of associated equipment that are embedded into a power station and collectively convert energy into electricity, functioning as an entity that is connected to the grid as an electricity production element.

Units

dB	decibel, the expression of a ratio of one physical quantity to another value on a logarithmic scale
GW	gigawatt, a unit of power [10^9 W]
GW·h	gigawatt-hour, a unit of electrical energy [10^9 W·h]
GW·s	gigawatt-second, a unit of electrical energy [10^9 W·s]
h	hour, unit of time [3 600 s]
horsepower	unit of power [745,7 W]
Hz	hertz, a unit of frequency [s^{-1}]
J	joule, a unit of energy
kA	kilo-ampère [10^3 A]
kg	kilogram, a unit of mass [10^3 g]
kg·m^2	kilogram metre squared, a unit for the moment of inertia
km	kilometre, a unit of distance [10^3 m]
kV	kilovolt, a unit of electrical potential difference [10^3 V]
kW	kilowatt, a unit of power [10^3 W]
kW·h	kilowatt-hour, a unit of electrical energy [10^3 W·h]
m	metre, a unit of distance
mHz	millihertz, a unit of frequency [10^{-3} Hz]
MJ·kg^{-1}	megajoule per kilogram, a unit to express the energy content of a fuel
MPa	megapascal, a unit of pressure [10^6 Pa]
m·s^{-1}	metre per second, velocity
MW	megawatt, a unit of power [10^6 W]
MW·h	megawatt-hour, a unit of electrical energy [10^6 W·h]
MW·s	megawatt-second, a unit of electrical energy
nT	nanotesla [10^{-9} T]
rad·s^{-1}	radians per second, used to express angular speed
r.p.m.	revolutions per minute, used to express rotational speed

s	second, a unit of time
TW	terawatt, a unit of power [10^{12} W]
TW·h	terawatt-hour, a unit of electrical energy [10^{12} W·h]
W	watt, a unit of power [J·s^{-1}]
W·h	watt-hour, a unit of electrical energy
W·s	watt-seconds, a unit of electrical energy [J]

List of Symbols

G	The magnitude of an event [dB]
P	Power [W, MW, GW, TW]
P_{IPS}	Total power carried in the power system [MW, GW, TW]
P_{event}	Total power lost during an event [MW, GW]
R	Dynamic restitution
f	Network frequency [Hz]
t	Lapsed time [s, min]
f_N	Nominal network frequency [Hz]
f_{min}	Minimum network frequency resulting from the event [Hz]
$t\|_{f_N}$	The time at which the network frequency recovered to f_N [min]
t_0	The specific time when the event initiated
Γ	Gamma probability density
α, β	Gamma function parameters
μ	Gamma probability density mean
P_1, P_2, P_3, P_4	Various pressure values
ε	Erosion rate
V	Gas velocity [m·s^{-1}]
a, α	Material constants (for wear calculations)
$\angle$Ж	Event angle [°]
E	Energy [MW·h]
P^3	Cubic power [MW^3]
Q	Reactive power [var]
J	Moment of inertia [kg·m^2]
m	Mass [kg]
L	Angular momentum [kg·m^2·s^{-1}]

ω	Angular speed [rad·s^{-1}]
N	Rotational speed [r.p.m]
E_k	Kinetic energy [J, MW·s, GW·s, TW·s]
H	Inertia constant
T	Number of shaft trains in a power system
Э	Erosion in power system integrity
Э(t)	Erosion trajectory (piecewise function)
Я	Restoration of power system integrity
Я(t)	Restoration trajectory (piecewise function)
Ɛ	Event progression
Ɛ(t)	Event trajectory (piecewise function)
Ƨ	Event severity
F_1 to F_6	Erosion factors
$\overline{q}$	Progression vector
A	Area
b, h	Breadth, height

1. Introduction

Electricity is the pillar. As an enabler of quality of life and industrial output, it rivals every other technology. From vital life support in the practice of medicine to the information backbone on which society grows increasingly dependent, the basics of domestic living and even the luxuries of entertainment and recreation – electricity powers and sustains human development. Its prominence continues to expand as it displaces alternative and rival energy options.

Due to the significant role that electricity plays in everyday life, it is desirable (if not essential) to ensure the reliability and affordability of this paramount commodity. The entire value chain of a resource such as electricity is exceptionally complex, and its reliability could be compromised at various steps in the process of manufacture, transport, and distribution, not even reaching the consumer. Electricity is a vital commodity required in every sphere of human welfare – the absence thereof not merely erodes human welfare but compromises the security and safety of communities and destabilises social structures.

Globally, much focus and effort are dedicated to the reliability of power systems – striving to attain the utopian goal of eradicating the very possibility of a power system blackout.

In this initial chapter, a basic introduction will orient the reader to the subject matter covered in subsequent sections.

1.1 Large-Scale Power Interruption

A significant failure within the electricity supply system must happen for a major power interruption or blackout to occur. The interconnected power system (IPS) is the all-encompassing system through which electrical power is channelled from producers to consumers. Typically, the main structure comprising an interconnected power system is the power grid, which consists of the transmission system and distribution networks through which the consumers and power producers are interconnected. The power grid is typically designed and operated with some redundancy. In the South African case, the (n-1) philosophy is used as the default design basis in the transmission system, although exceptions to this rule do exist in some instances. There are also specific requirements for designing the transmission system connection to a power station (and more onerously to nuclear power stations) that provide additional redundancy [1].

The so-called power station is the most fundamental power-producing building block in an IPS. A power station is an amalgamated collection of equipment that is managed together to convert energy into electricity, after which it is made available to the local transmission (or sometimes distribution) system. A power station may consist of a single set of electricity-generating equipment or several sets. In South Africa, it is typical for a power station to consist of multiple generating sets – six sets being the median in 2023.

Although it is theoretically possible for a significant grid failure to cause a large-scale power interruption to an entire community, it is seldom seen to occur without a significant loss in generated power, which normally manifests through the disconnection of generation capacity from the interconnected power system. All major blackouts occurred due to the disconnection of many generating sets – normally at many different power stations.

1.2 Power Stations

To understand the role that power stations may play in large-scale blackouts, the internal structure of a power station, at least at a conceptual level, needs to be understood. The internal configuration of a power station is the key to comprehending the issues about the reliability of the process through which electricity is produced.

A power station is a facility where electricity is converted into electricity from a primary energy source. To achieve the required conversion, various processes need to take place in a coordinated fashion, requiring auxiliary equipment to function on an ongoing basis. Therefore, an interruption in the energy conversion process automatically results in an interruption in the generation of electricity.

Normally, plant and equipment used to produce electric power at a power station are divided into various generating sets or units. Different generating units are designed to operate independently from one another, and a failure of one would normally not affect the operation of the others.

In addition to the generating units, a power station also has plant and equipment that are common or shared among the generating units, for example, the water treatment plant for purifying raw (river) water into water suitable for process use. Therefore, the generating units cannot be regarded as entirely independent from one another since they are individually interdependent on certain common systems. This implies that, in the event of a major disruption of a common system, the individual generating units may suffer consequential failure as a cascading result emanating from the failure of the common plant.

Similarly, all the generating units of a power station connect individually to the transmission grid through a dedicated interface known as the high voltage yard (HV yard). This HV yard is merely a dedicated substation designed to accommodate the energy from a power station into the local network or grid. However, since the HV yard is typically a single electric node that joins all the generating units of a power station together, a disruption of the node itself may cause a consequential disruption of the generating units that form part of the power station – once again emphasising that the generating units are not entirely independent, but susceptible to common mode failure.

1.3 Hypothesis

The hypothesis on which this study is based, consists of more than one focal point that collectively guides the body of work that will subsequently be undertaken.

Hypothesis: *There exists an inherent reluctance (and subsequent void) to analyse generation disruptions and evaluate their contribution to large scale power system disruption events, which stems from:*

a. The absence of suitable methods and techniques to aid in the quantification of large scale power disruption events in holistic terms, including power generation.

b. The underlying nature of disruption event data that are prone to be incomplete with a large degree of uncertainty.

c. *Portability requirements in recognising that methodologies need to transcend geographic and temporal separation between events, requiring to remain applicable regardless of the specific power system attributes wherein the event has manifested.*

1.4 Research Aims and Objectives

The research that is hereby undertaken sets out to achieve the following:

a. Provide a comprehensive contextualisation of the field of large scale cascade disruption events in power systems and the role that the disruption of generation resources play therein.

b. Provide specific context of power generation from a historic and evolutionary perspective to enable thorough understanding of its role within power system disruption events.

c. Present case study examples, where available, for actual cascade disruption events of generation for purposes of illustration.

d. Develop a methodology for the analysis of large scale cascade disruption events in power systems, with the following objectives.

   - Enabling the severity of events to be determined, allowing their ranking and comparison.
   - Achieve sufficient portability of developed methods to allow for their application across geographic and temporal boundaries.
   - Ensuring sufficient robustness of the methods to allow for analysis of events to continue despite omissions and uncertainty within the data of the event record.

1.5 Research Scope

The scope of the research being undertaken encompasses all large scale power disruption events of interconnected power systems – specifically those where power generation played a technically significant role.

In specific, the research aims at the ultimate quantification of the extent and severity of events as quantitative metrics for event comparison and ranking.

1.6 Exclusions and Delimitations

In order to focus the research, certain limitations are excluded from its scope, including:

a. Power system disruptions in non-interconnected scenarios.

b. Disruption events affecting generation only, with no technically significant effects on the power system.

c. Evaluation of plant or equipment damage *per se*, except in as far as it affected or contributed to the disruption event.

d. Energy market impacts and monetary production losses.

e. Political and socio-economic effects stemming from the disruption event.

f. Consequential impacts resulting from disruption events, e.g. deployment of police, unrest, economic losses in commercial sectors, adverse civilian impacts, etc.

1.7 Remarks

Since large-scale disruptions of the power generation base, embedded within a power system, often serve as a precursor to a power system blackout, the first chapter introduced these two concepts as a starting point. In the following section, the author will provide the necessary background as a context for the material content body of this endeavour.

2. Background and Context

The preceding section introduced the concept of a power station as a fundamental building block in a power system. Also, the concept of a power system blackout was introduced as a disruption event that adversely affects vast communities of people and detracts from a society's goals and attaining prosperity.

In this next section, the development of an electric power system, as well as the development of power stations, will be explored to ultimately serve as the foundation of the subsequent sections following later.

2.1 Historic Overview – The South African Case Study

The focus of this study is general and generic and does not depend on the power system's specifics. However, an understanding of certain concepts and principles is required as a foundation for later sections, and to that end, a specific example, the South African power system, was selected as a case study.

Being one of the power systems that has remained under utility control for an extended duration (more so than many others), the ease with which information can be collected has proven to be a major benefit. Also, the South African power system had a relatively rapid development spurred on by mining and industrial development – necessitating high reliability from the outset, making it an ideal example for this study.

This section will explore the South African system as an archetype of power systems in general.

2.1.1 South African Electric Power Industry Progression

Electricity was introduced into South Africa early in its technological life cycle. Following the invention of the electric lamp by Thomas Edison in 1879, the first commercial lighting installation was on the steamship Columbia, consisting of 115 lights. As early as 1 September 1882, Kimberley became the first town, anywhere, where an electrical installation provided street illumination. Although the lighting achievement in Kimberley remains one of the most astounding historical facts about South Africa, it is often overlooked that the power for the lights had to be generated somewhere. The source for the Kimberley streetlights was the Kimberley Power Station of the Cape Electric Light and Telephone Company – the first power station in Africa, initially consisting of four 70 horsepower belt-driven dynamos. This achievement at Kimberley occurred three days before the commissioning of the “world’s first commercial power station”, the Pearl Street Generating Station in New York City, on 4 September 1882 [2].

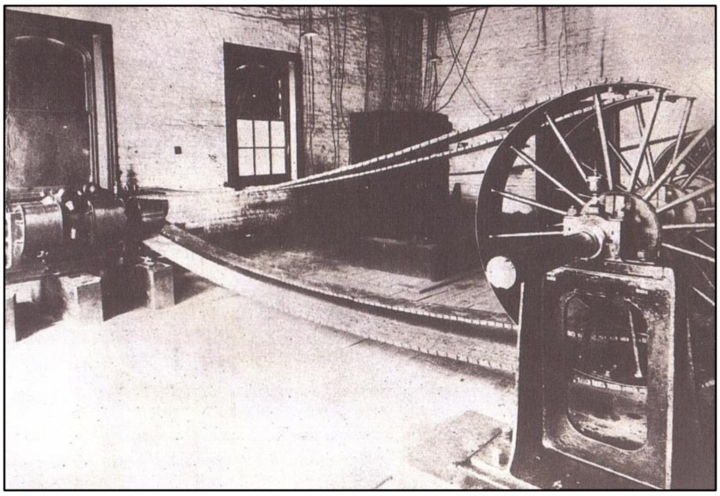


Figure 1: The Kimberley Power Station (1882) – the first power station in Africa [2]

Various South African cities and towns received electrical installations in the years following the Kimberley event, primarily for lighting. And, with the lighting installations, power stations had to be built and commissioned. At first, all the power stations were operated under the auspices of towns and municipalities or private owners for personal use. Initially, small dynamos were erected near the locations where electricity was required, but the realisation that central power stations would be more economical and reliable soon became the norm. The first central power station in South Africa came into operation in the Cape Colony in 1891 – the Table Bay Harbour Electric Light Works [2].

Figure 2: The Table Bay Harbour Electric Light Works – the first central power station in SA [2]

The Table Bay Harbour Electric Light Works consisted of a 150 kW steam engine-driven dynamo powered by two coal boilers. It was used to power the Public Library, the Royal

Observatory, various Houses of Parliament, the Old Somerset Hospital, the Cape Town Railway Station, the "New" Post and Telegraph Office, and the Grand Hotel [2].

However, the industrial development in South Africa stemmed from mining, with the discovery of diamonds at Kimberley in 1866 and gold at Johannesburg in 1886. To provide sufficient energy for the mining endeavours, firewood was initially used, a scarce resource in the interior of South Africa that had to be hauled from coastal regions at a significant cost. With the discovery of rich coal reserves in the Orange Free State Republic in 1876 and in the Transvaal Republic in 1887, coal rapidly displaced wood to fuel the stationary steam engines that were employed for driving the mining-related industries and the railway infrastructure that were soon to link the Cape Colony with Johannesburg and later Delagoa Bay (Maputo) [2].

Kimberley was the first town to have electric street lighting on 1 September 1882. However, before this event, an experimental use of electric light was undertaken in Kimberley in August 1881 in the mining industry with a 300-candlepower arc lamp – hailed to be very successful. From 25 April 1882, Table Bay Harbour was lit by sixteen 2000 candlepower arc lamps, identical to those being installed in the streets of Kimberley at that time [2].

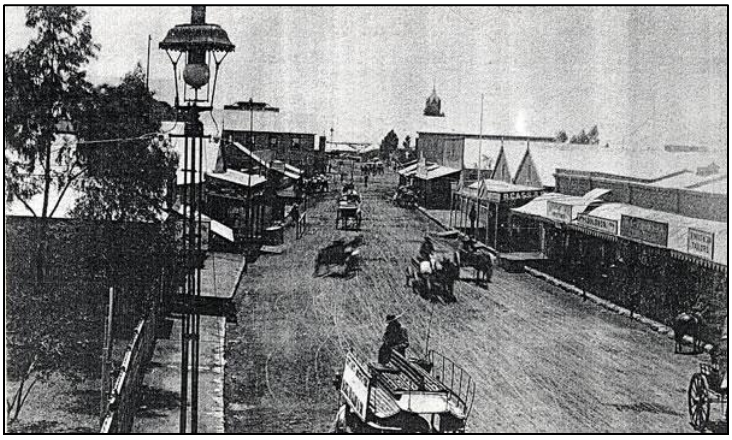


Figure 3: Street lighting in Kimberley [2]

As the mines in Johannesburg became deeper, the need for energy increased for haulage, hoisting and crushing. Electricity, a relatively new technology, was regarded as a costly energy source and met much scepticism. In 1897, the first central power station in the Boer republics came into operation with a 700 kW output capacity – the Brakpan Power Station of Rand Central Electric Works Limited near Johannesburg. Brakpan Power Station used coal as a primary energy source and triple-expansion reciprocating steam engines as the prime movers driving four generators [2].

Figure 4: Brakpan Power Station [3]

The use of electricity rapidly expanded, and in August 1884, a ½ horsepower electric motor was demonstrated at the South African Industrial Exhibition in Cape Town. By 1887, underground electric lighting was successfully tested in Kimberley mines. In 1890, a battery-powered tram service was started in Kimberley, and in 1891, electric motors were used at Kimberley mines for pumping, sawing wood, hoisting and driving ventilation fans underground [2]. By the turn of the century, a Kimberley central power station was planned, and a projected reticulation of 2,5 MW was estimated [2].

Then, by the winter of 1902, 634 electric motors with a total power rating of 12 MW were installed in the Johannesburg gold mines [2].

Hydropower generation was first introduced in 1892 at Pilgrim's Rest gold mine, with two 6kW generators. In 1894, another 45 kW generator was installed. In 1895, on the Molteno Reservoir in Cape Town, two 150 kW generators were commissioned that could be powered with water or steam – the "Graaff" Electric Lighting Works. The first three-phase alternators installed in South Africa were 160 kW Siemens machines that were operational by 1896 at the Pilgrim's Rest gold mine [2].

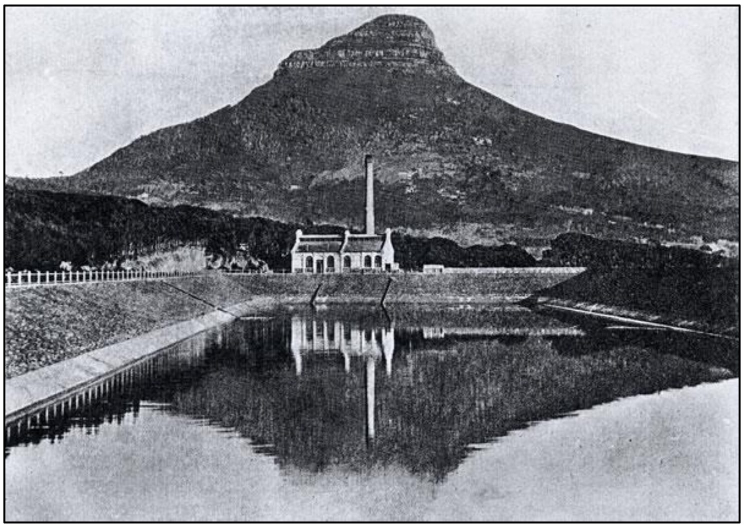


Figure 5: "Graaff" Electric Lighting Works [2]

In 1903, the first steam turbine, a 1 MW machine for De Beers Consolidated Mines in Kimberley [2], was installed for power generation to replace the reciprocating steam engines that were used before.

Since the establishment of electricity as a national energy resource, the demand for the product has increased consistently. The following graph illustrates how electricity sales continued to increase. [2]

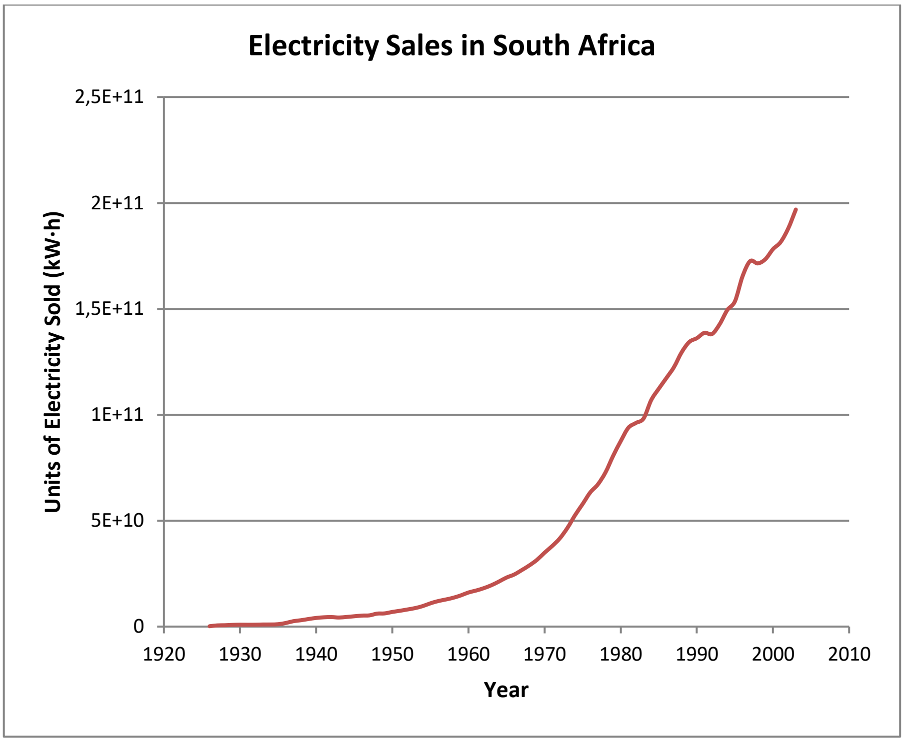


Figure 6: Growth in South African electricity sales

Although Eskom was established in 1923, much of the generating capacity remained in the hands of other parties, and the majority of those parties were not municipal. The following graph shows the quantities of electrical energy produced in South Africa over a 3-decade period. Municipal electricity production remained at approximately 10% of the national production, while the Eskom fraction increased from about 30% to about 40% over the same period [11], [21], [31].

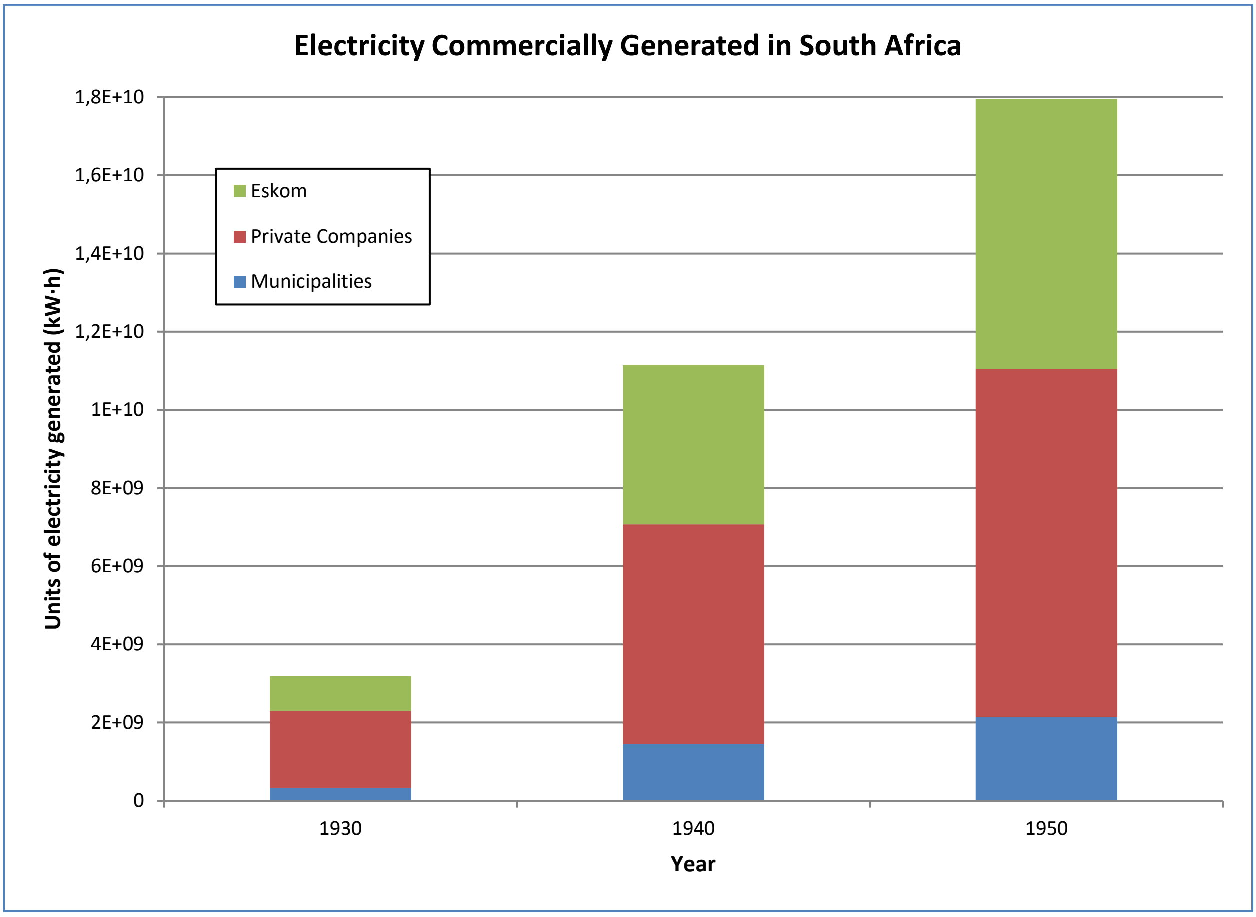


Figure 7: Generation of electrical energy in South Africa [11],[21],[31]

As electricity needs grew throughout South Africa, more municipalities started investing in electrical infrastructure within their towns and cities. The following graph shows the growth in commissioned electrical systems reported by municipalities – containing internal reticulation networks and embedded power generation installations.

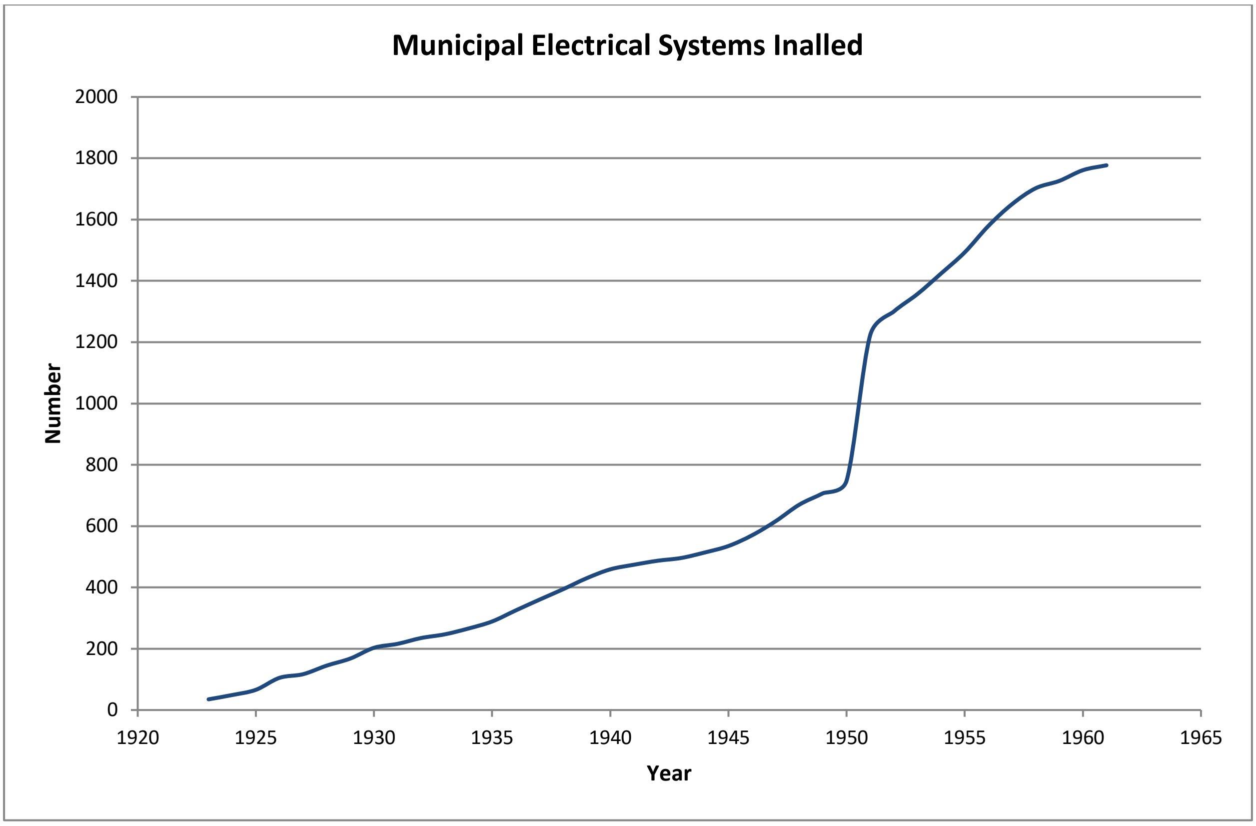


Figure 8: Reported electrical systems existing within municipalities of South Africa

The following section will cover the further development of the power system, with an additional focus on the developmental evolution of power stations.

2.1.2 South African Power Station Evolution

As electricity demand continued to rise, a slow evolution occurred both in terms of power transmission and distribution networks and in terms of the internal structure of power stations themselves. In this section, the evolution of power stations will be explored to better understand disruption events within power stations that will follow in subsequent sections.

In the early days of electricity in South Africa, the *first-generation* of power stations lacked strategic intent and were erected wherever a need existed. These power stations were mainly owned and operated by municipalities or private companies (e.g., mines) for their purposes. They supplied mainly industrial energy in the form of electricity or as compressed air using piping reticulation networks. In isolated cases, private individuals owned generating facilities for their exclusive use. The first-generation power stations were, without exception, operated in the absence of interconnected power systems. Power stations were operated in isolation from one another, and therefore, the reliability of supply was inherently poor. Typically, first-generation power stations utilised primary energy sources other than coal since they were mainly installed remotely from coal fields. Their capacities were small, and their configuration lacked any strategic characteristics.

Figure 9 shows the first-generation power stations that came under utility control, indicating their tenure as utility assets and their respective installed capacities (see [4] to [52]).

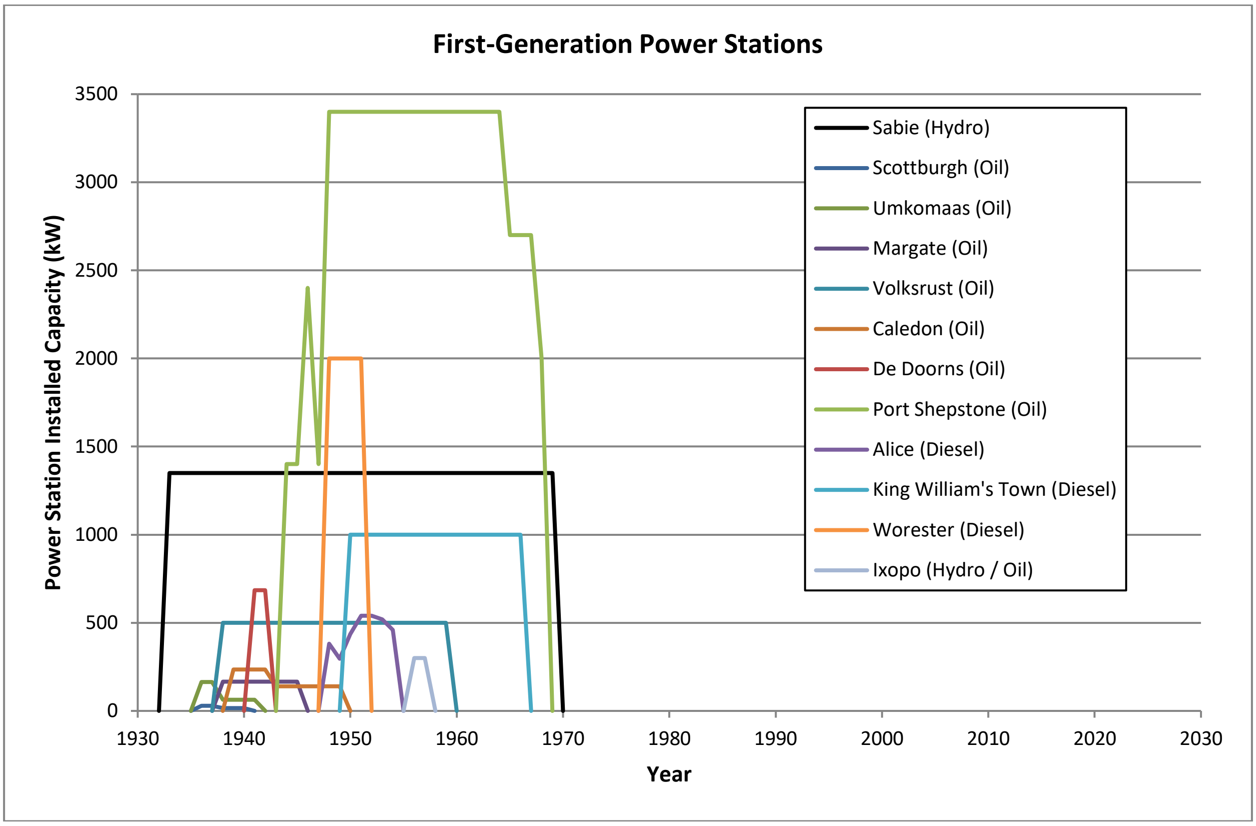


Figure 9: First-generation power stations under utility control

The *second-generation* of power stations in South Africa was known as a *central power station*. These power stations produced electricity shared among various users within direct proximity to one another and to the power station. There was still an absence of interconnection between power stations. Therefore, these power stations were reliant upon themselves for generating and supplying power with so-called "*house sets*" for their own use to supply their own auxiliaries. Therefore, these power stations were generally capable of starting up without any external power supply, because external sources mostly did not exist.

The following graph shows the second-generation power stations that came under utility control and were, without exception, coal-fired plants. Although Eskom never endeavoured into the actual development of this generation of power stations, it did assimilate several such plants over time by absorbing the assets from other entities through amalgamation or agreement – references [25] through [72].

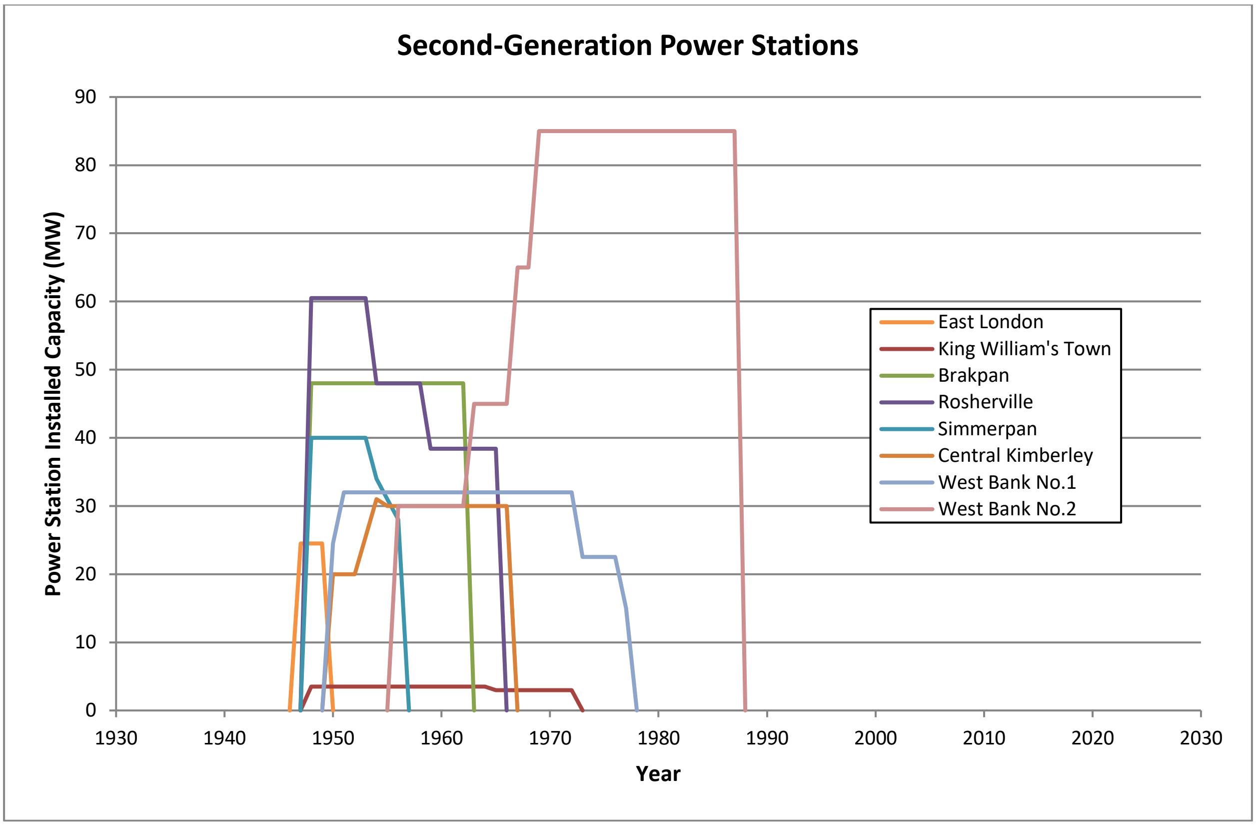


Figure 10: Second-generation power stations under utility control

As can be seen from the graph, these power stations had relatively small capacities and were equipped with generators of not more than 30 MW each. Although the remainder of this section will deal exclusively with electrical power stations, it is worth noting that during the early years of industrialisation, various central "power stations" existed that produced compressed air rather than electricity [2]. Eskom never developed air power stations but obtained several through agreements from other power producers that merged with Eskom. In 1948, Eskom owned and operated six compressed air power stations in mining areas that produced and sold compressed air to mining operations. In the early 1960s, Eskom abandoned air power stations, and mines had to resort to producing compressed air for their own purposes from electricity or combustion engines. At the peak of this period of "generating" compressed air by a utility and selling it to customers as a product separate from electricity, Eskom had an installed capacity of 117,6 MW of compressed air production plant installed in six power stations.

The concept of "*large central power stations*" was introduced in 1905 when Robert Hammond presented a convincing argument in a paper submitted to the Institute of Electrical Engineers entitled Electrical Power Distribution on the Rand. Therein, he showed that large central power stations would produce more economical and reliable electricity than a larger number of smaller plants [2].

Based on the merits of his argument and the realisation that the demand kept increasing, the *third-generation* of power stations emerged. These were large compared to any power stations preceding this period and provided the possibility of increasing the power station's capacity over time by adding more generating sets or increasing the size of existing sets. Power stations of the third-generation became interconnected to one another, starting from about 1912, into small regional networks. This period also saw the establishment of the first control centre at Simmerpan, where one of these power stations was built.

Figure 11: First central control office at Simmerpan (VFP), an early incarnation of the National Control Centre (Eskom) to later also be established at Simmerpan [3]

During the design of *third-generation* power stations, the existence of house sets became superfluous due to the availability of power from the local network. Therefore, these power stations became equipped with auxiliary transformers (later, in subsequent generations, known as unit transformers) to supply power to their auxiliaries, with Vierfontein Power Station being the first. Third-generation power stations widely employed the concept of having several generating sets, each consisting of a turbine and a generator. The boilers were greater in number than the generating sets and a common steam range existed as a large manifold into which all the boilers that were in service delivered their steam, and all the generating sets being used drew their steam from.

This mismatch between the number of generating sets and the number of boilers had the benefit that any of the boilers could be taken out of service for repairs without affecting the power produced by the power station. At face value, it may seem nonsensical in that the same benefit cannot be achieved in reverse, i.e., that any generating set cannot be taken out of service without impacting the total capacity of the power station. Still, it needs to be seen in the light that the unavailability of power stations is dominated by boiler failures and downtime, significantly more so than all other plants and systems combined.

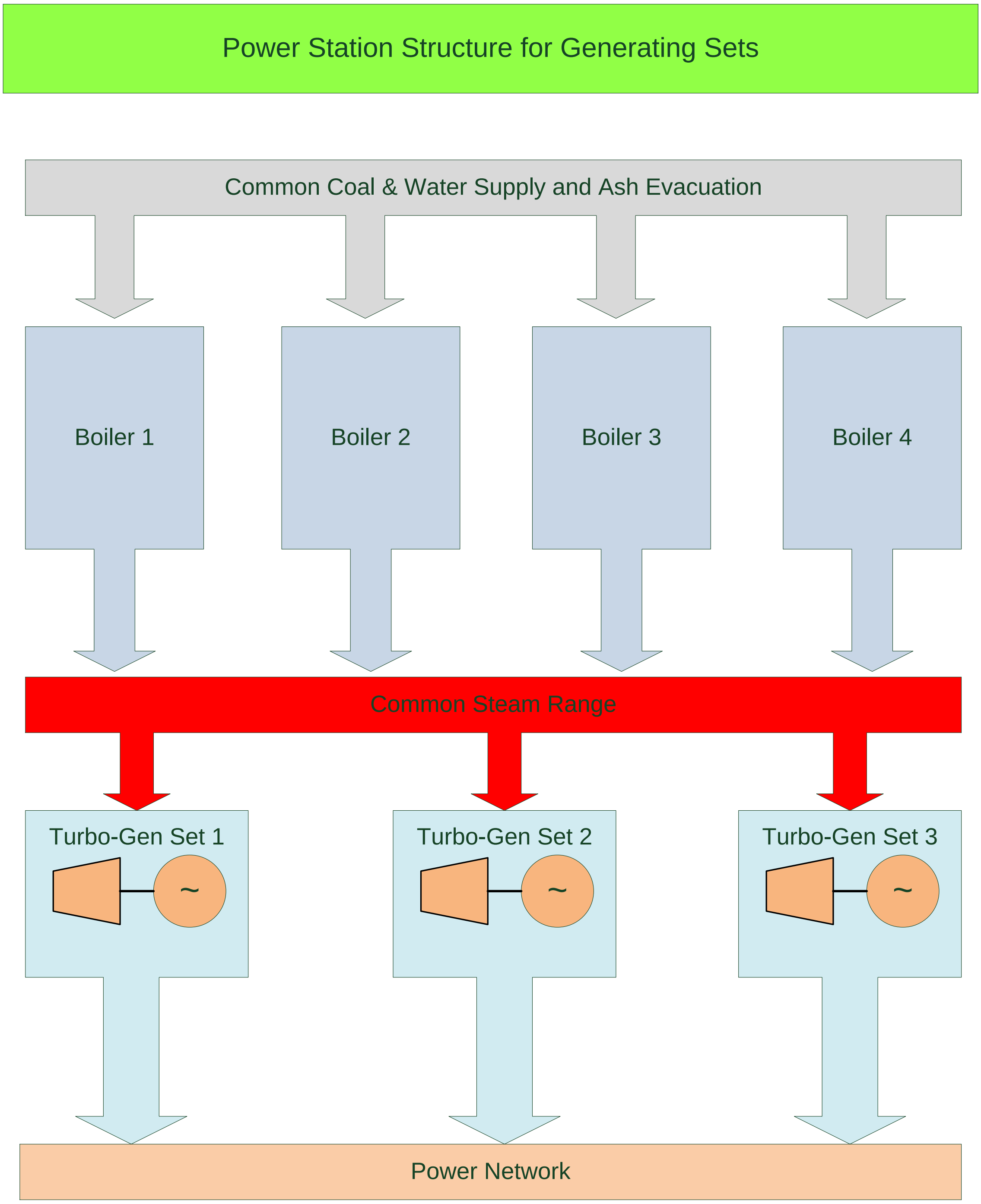


Figure 12: Third-generation power station structure using generating sets

They were being equipped with more boilers than generating sets, which provided great flexibility in terms of reliability of electricity since boiler maintenance could be conducted without affecting the availability of the generating sets. Also, a disruption causing one of the boilers to cease production did not necessitate the disconnection of any generating sets. In the following graph, the third-generation power stations that were under utility control are shown in terms of their installed capacity.

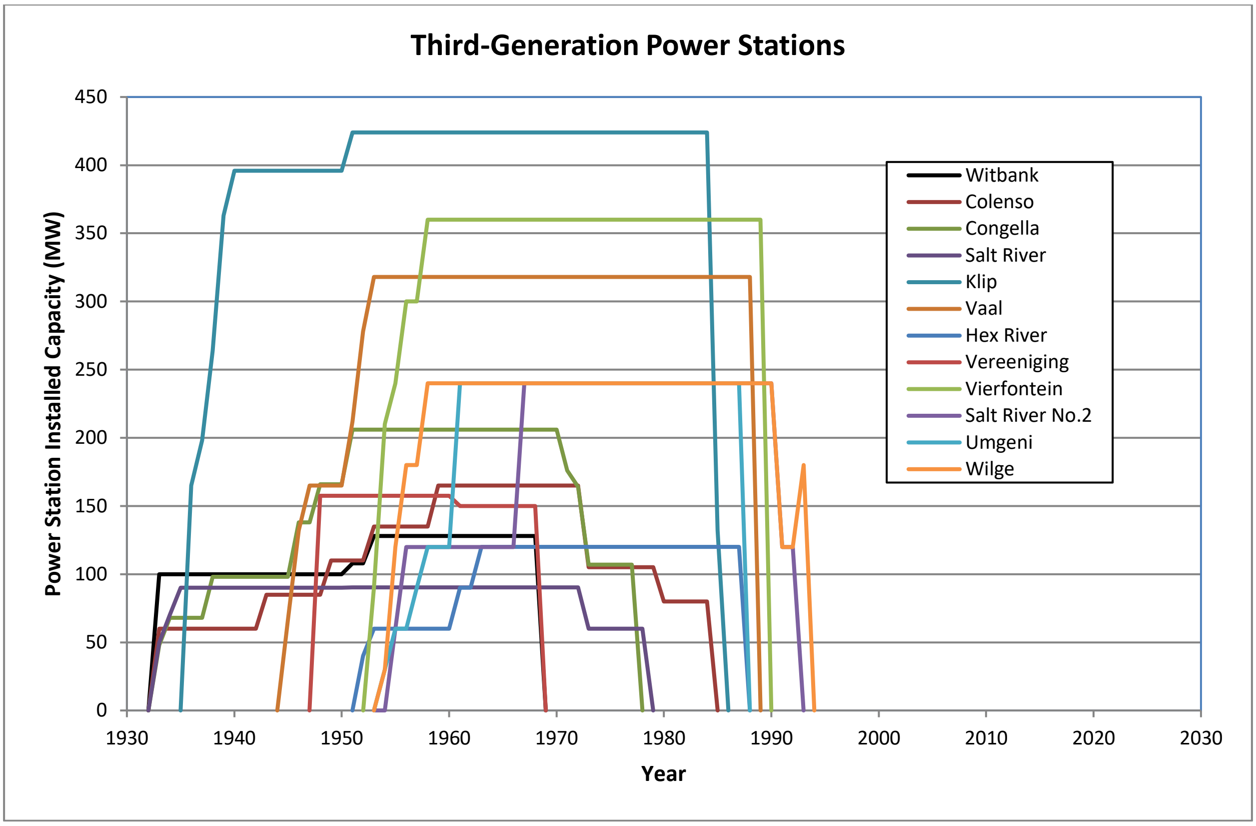


Figure 13: Third-generation power stations under utility control

In 1954, Taaibos Power Station in the Vaal Triangle ushered in the era of the *fourth-generation* of power stations in South Africa. A fourth-generation power station abandoned the concept of having redundancy in terms of the number of boilers to the number of generating sets. Instead, a new concept was introduced, namely that of a *unit*, consisting of a boiler, turbine and generator with all the associated auxiliaries and electrical infrastructure that are needed to generate electricity. This unit approach is shown schematically in the following graphic representation.

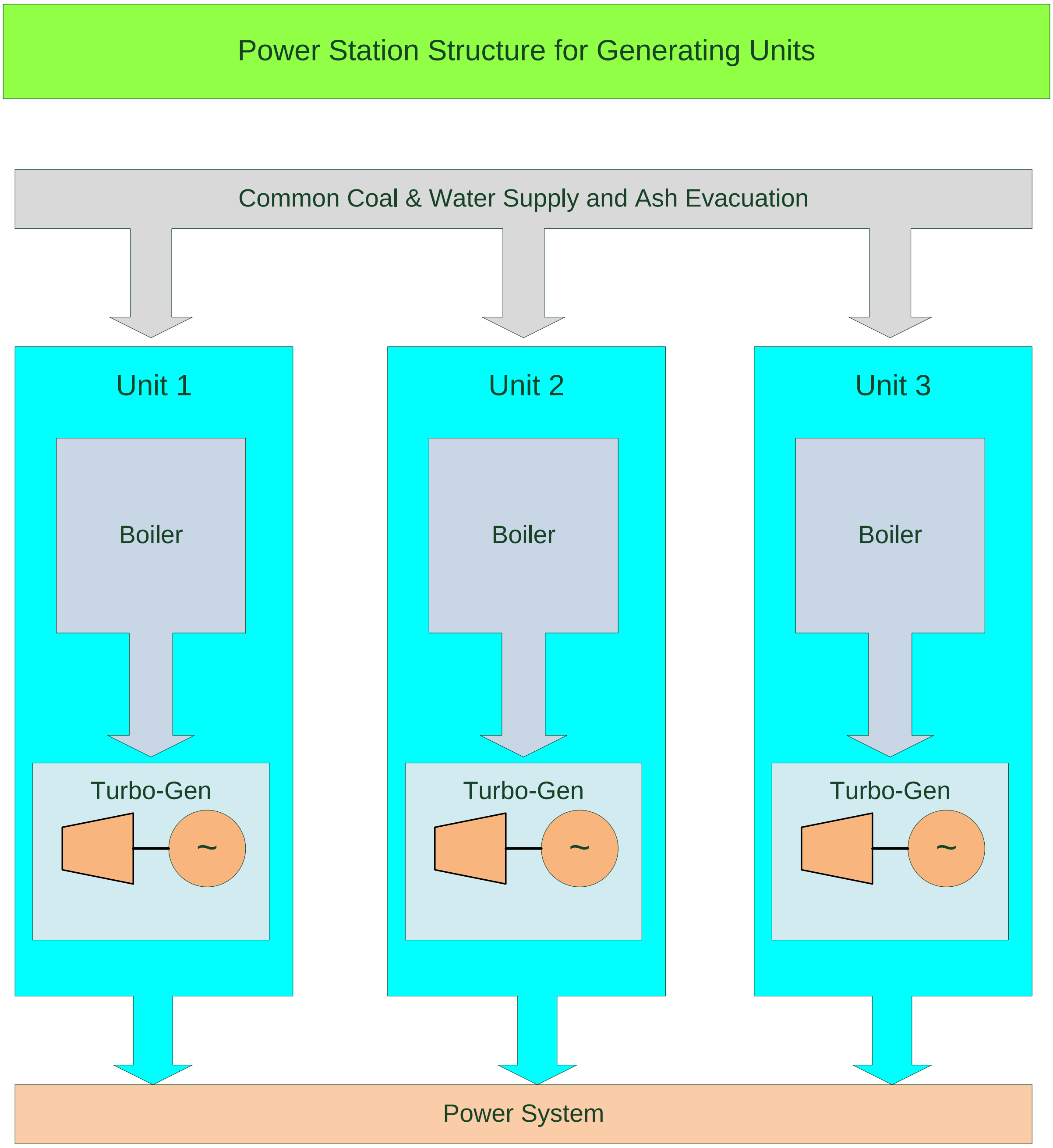


Figure 14: Fourth-generation power station structure using generating units

The unit approach was soon extended to also apply to hydro, nuclear and gas (or liquid fuel) power stations – abandoning the earlier concept of generating sets. In terms of the unit concept, a new term was adopted, namely the adjective "*unitised*", which referred to the systems and plant that existed for the exclusive use or benefit of a specific unit. The South African power stations of the fourth-generation are shown in the following graph in terms of their installed capacities over time. The date range has been extended to illustrate the power stations that are currently under construction or still in operation – references [34] through [114].

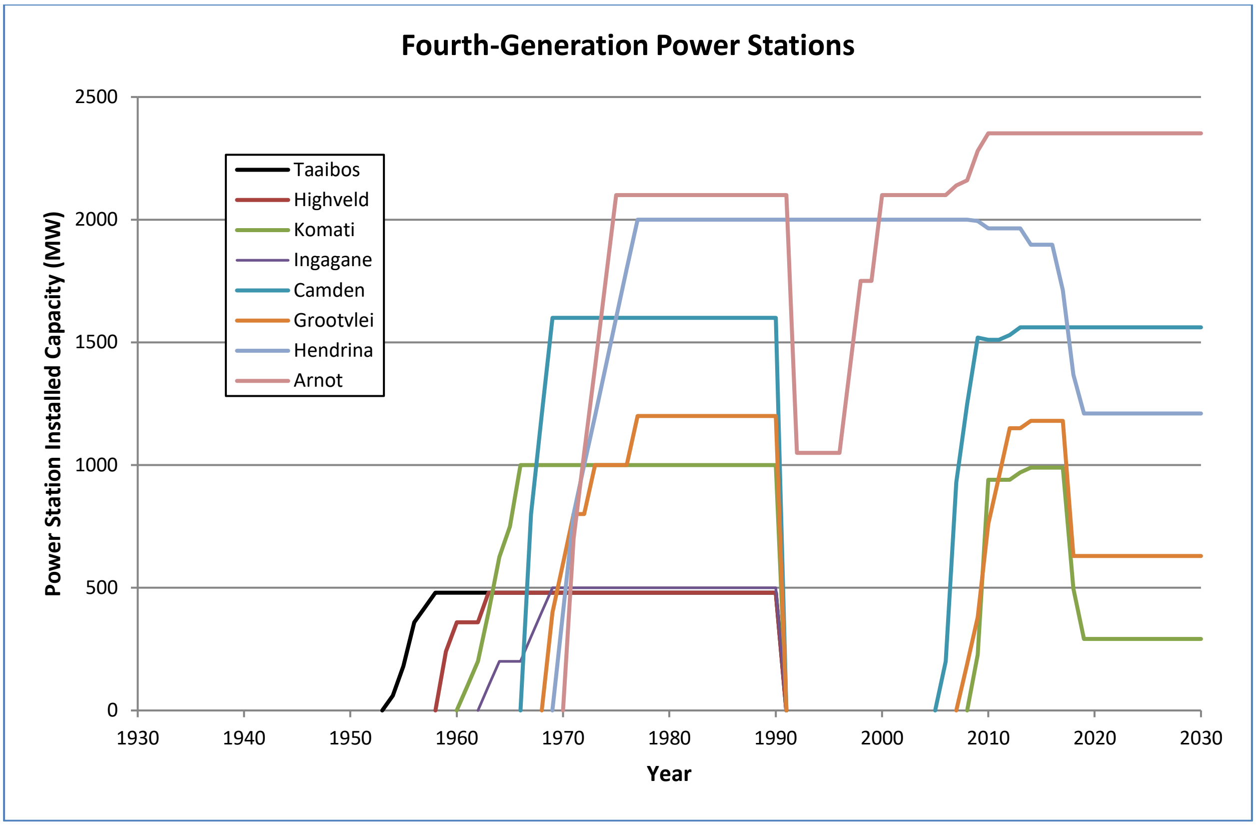


Figure 15: Fourth-generation power stations under utility control

The fourth-generation approach of unitised design brought many advantages, but ultimately, these units still did not reap the full benefit in terms of resilience. Further refinement would be required to make a step change on the front of resilience.

With the ever-increasing size of the generating units as the power stations evolved from the first to the fourth-generation, the design of the auxiliary systems grew proportionally. In the unitised approach, every unit was equipped with its own set of unitised auxiliaries supporting the processes involved in converting a primary energy source into electricity. However, failures within the auxiliary systems of units often result in the tripping of the unit itself.

To reduce the exposure of units to failures within the auxiliary systems, the *fifth-generation* power stations were developed around the concept of dividing each auxiliary system into two 50% auxiliary systems. Such an approach held the promise that failures within the auxiliary systems of a unit would merely result in a loss of output of the unit of about 50% rather than the tripping of the unit with the consequential 100% loss of production. Figure 16 illustrates the difference in the design of the auxiliary systems between a fourth- and fifth-generation unit, respectively.

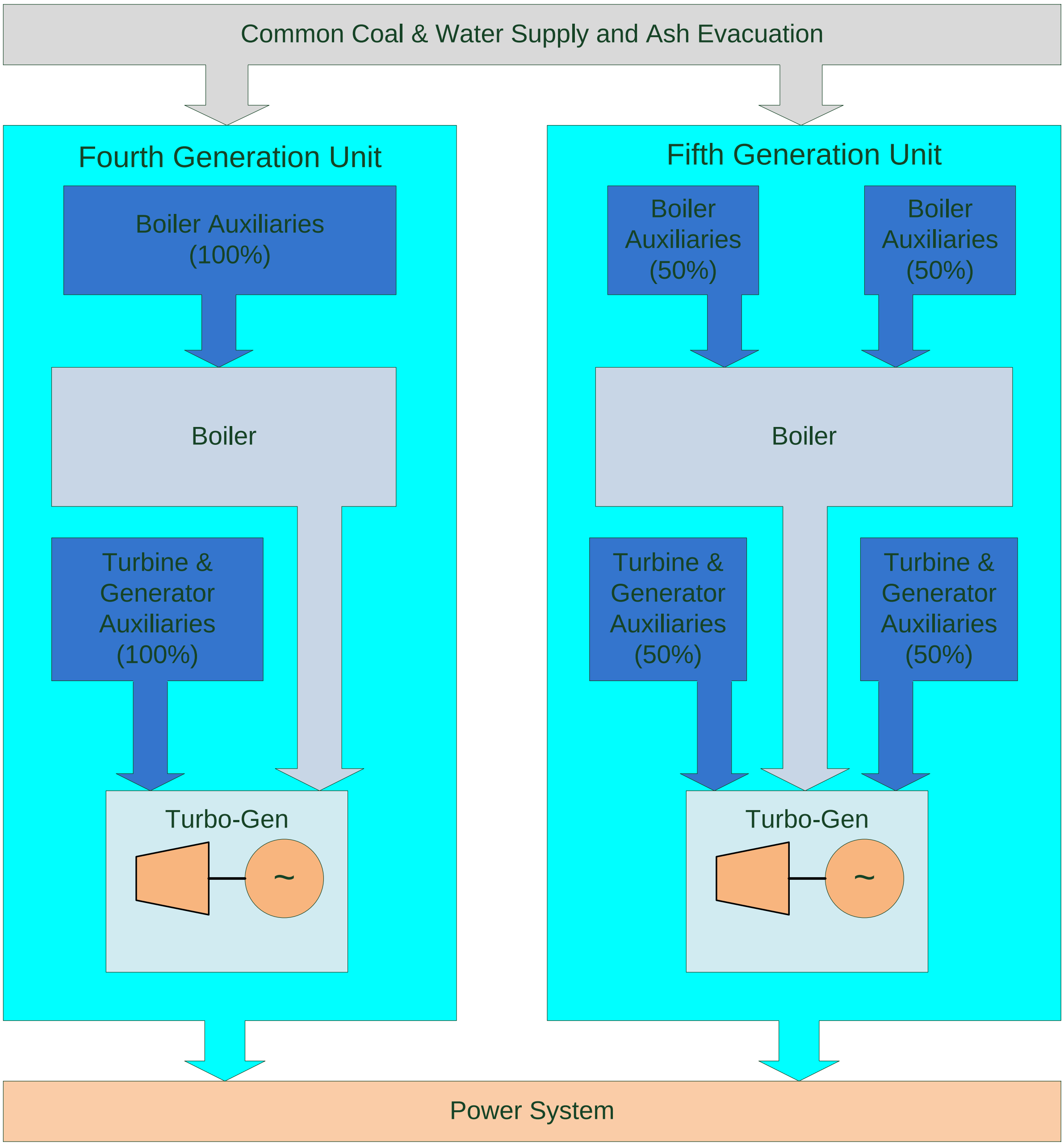


Figure 16: Comparison between a fourth- and fifth-generation unit

Although the concept of a 50% division across all auxiliary systems seems straightforward, it has huge implications in terms of the design, operation and maintenance of the unit. The fifth-generation units have largely been made possible through advances in control system technology and require a very high level of automation of all systems. But besides the investment in automation, the auxiliary systems had to be designed and implemented with the two 50% auxiliary systems being independent of one another. And this requirement for independence had to run through every single aspect of the design. It means that the mechanical systems may not share any interdependencies between the two, but also that they had to be entirely self-sufficient in terms of their power supply, control system, etc.

The various generations of power stations differed significantly from one another, and one specific distinction is the total power station capacity. First-generation power stations did not exceed 10 MW, the second-generation stations had a ceiling of about 100 MW and the third-generation 500 MW. The fourth-generation power stations increased in size to a maximum of about 2 GW, and ultimately, the fifth-generation saturates at about the 5 GW level. A comparison of the total installed capacity of the five generations is presented in the following graph, expressed on a logarithmic scale.

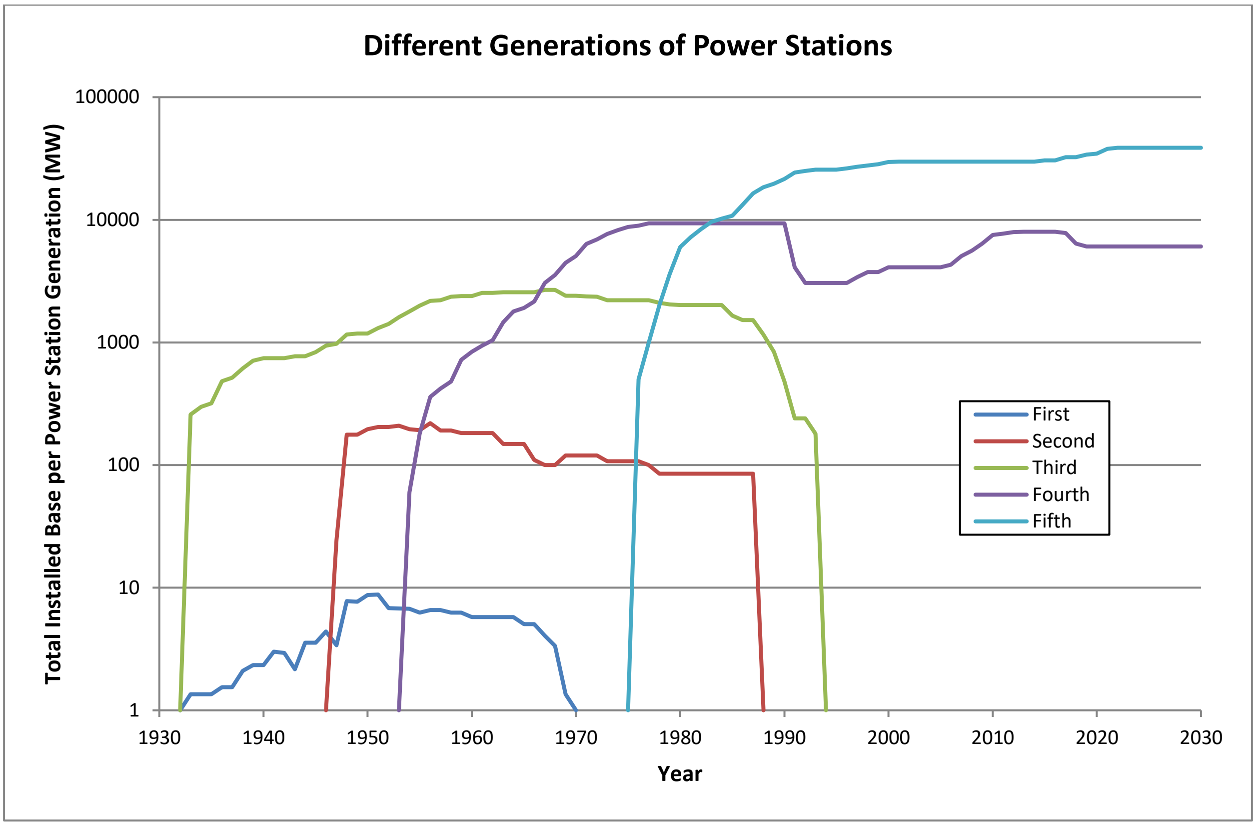


Figure 17: Total installed capacity of the five generations of power stations under utility control

Starting in the late 1960s, lines were being built to form a *national grid* – connecting regional networks. The reason for this initiative was the significant cost differential between bulk coal-based generation in Transvaal versus coastal alternatives. To illustrate the economic argument, at this time, the cost of coal delivered at the coast was 350% more than the cost of coal at the power stations in Transvaal. Although electricity transmission also has associated losses, the cost thereof was significantly less than the costs associated with coal transport.

The last section was completed in 1973, and South Africa had a single power system supplying electricity [53]. With this completed, various power stations in coastal regions could be decommissioned, where the cost of production significantly exceeded the costs of inland coal stations. Also, it became possible for several old coal power stations to be closed down, some with more than 60 years of service, e.g., Brakpan Power Station [2].

With the national grid as a new central resource, the size of generators and power stations increased due to the economies of scale. The following graph shows the size (capacity) of the largest generator of each technology type that formed part of the installed base in South Africa over time – references [4] through [114].

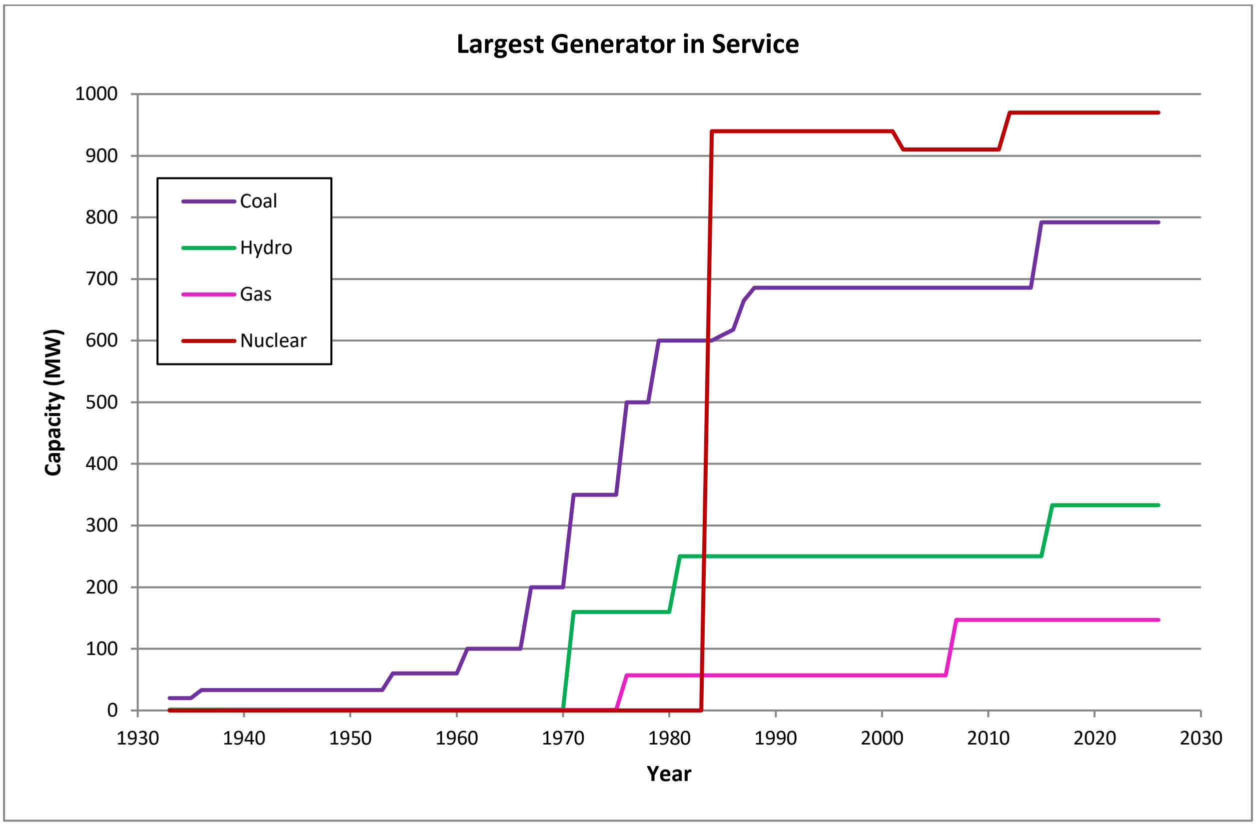


Figure 18: Largest capacity generator (per technology type) in the South African utility fleet over time

The increase in generator capacity over time also increased the capacity of power stations. In the following graph, the largest power station within the South African utility fleet that was in commercial operation at any given time is shown over the same time window as the previous graph (see [4] through [114]).

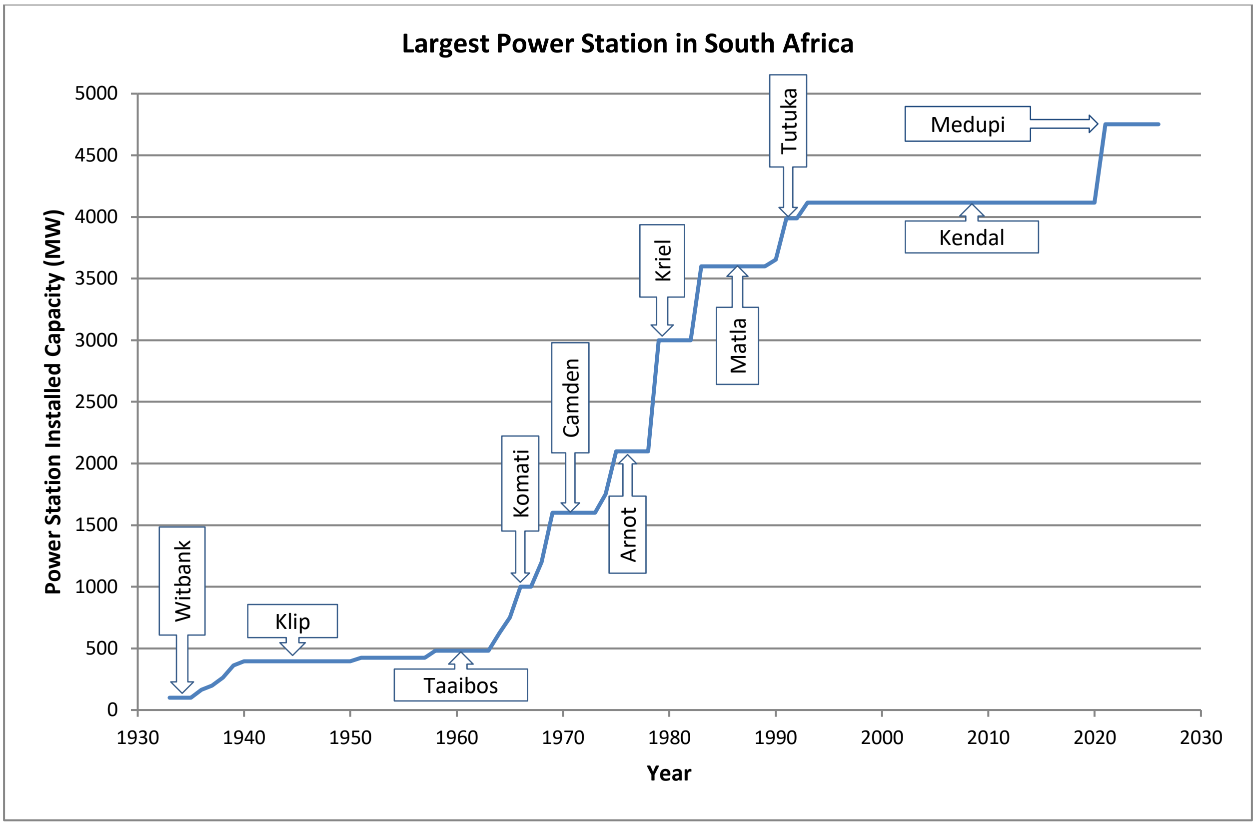


Figure 19: Largest power stations in South Africa based on installed capacity

With the capacity of both power stations and individual generating units having increased significantly over time, the need for reliability also increased. Indeed, if a large power station or generating unit becomes compromised, the risk to the power system increases as the capacities of power stations and units increase.

2.1.3 Remarks

The power system has evolved dramatically since its initial formation, from small and scattered single-generator-single-load applications to an integrated system that interconnects the entire Southern African region, which contains many load centres and power stations.

Power stations have also evolved from a total lack of strategic design intent to vast multi-unit installations that incorporate many levels of redundancy and backup to enhance reliability.

With an understanding of the fundamentals of both a power system and power stations, the next section will deal specifically with the concept of power system disruptions.

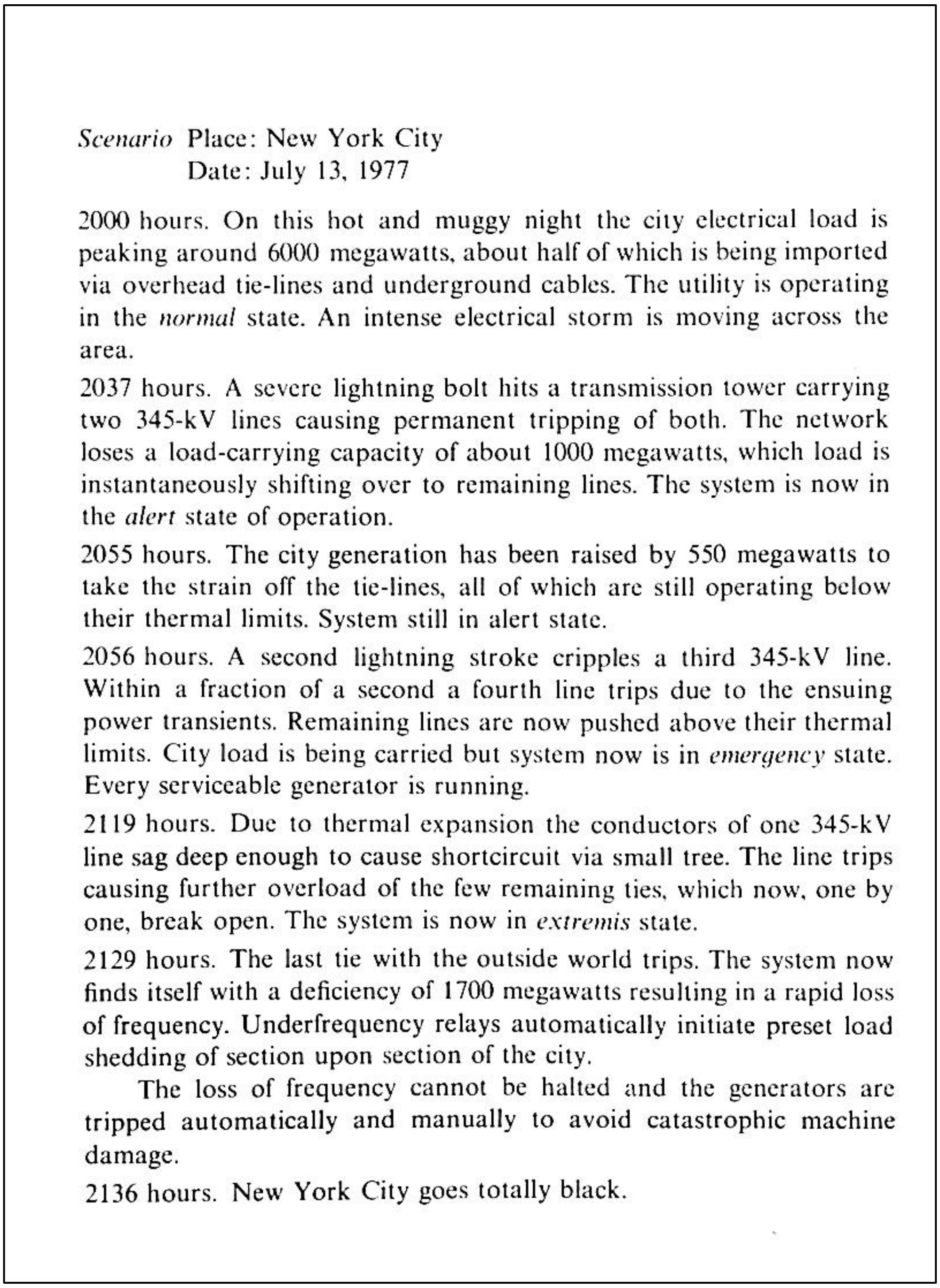
3. Literature Survey

Having established a basic foundation of power systems and power stations as basic building blocks contained within power systems, the focus now turns to the issue of power system disturbances – a risk category that threatens electricity security as a foundational prerequisite for prosperous societies.

3.1 Major System Disturbances

Initially, in the early development of electrification around the globe, generating stations only supplied regional power in relatively small networks since the interconnection between networks to form larger grids was a subsequent development. As electrical energy systems evolved internationally into ever larger networks and grids, the vulnerability of power systems to become disrupted, escalated. The first significant event that attracted international attention occurred in Northern America in 1965 when the loss of 193 generators, totalling 20 GW and affecting 30 million people, engulfed cities like New York, Boston and Toronto – traced back to an incorrect network protection operation during heavily loaded conditions [115].

More than a decade later, on 13 July 1977, New York City was blacked out following a total loss of 6,1 GW affecting 9 million people [115]. The 1977 New York event drew so much public attention due to the vast extent of social unrest and lawless behaviour that ensued that a full-length motion picture entitled *Blackout* was released in 1978. The following excerpt provides a colourful sequence of events that occurred during the event.



Scenario Place: New York City
Date: July 13, 1977

2000 hours. On this hot and muggy night the city electrical load is peaking around 6000 megawatts, about half of which is being imported via overhead tie-lines and underground cables. The utility is operating in the *normal* state. An intense electrical storm is moving across the area.

2037 hours. A severe lightning bolt hits a transmission tower carrying two 345-kV lines causing permanent tripping of both. The network loses a load-carrying capacity of about 1000 megawatts, which load is instantaneously shifting over to remaining lines. The system is now in the *alert* state of operation.

2055 hours. The city generation has been raised by 550 megawatts to take the strain off the tie-lines, all of which are still operating below their thermal limits. System still in alert state.

2056 hours. A second lightning stroke cripples a third 345-kV line. Within a fraction of a second a fourth line trips due to the ensuing power transients. Remaining lines are now pushed above their thermal limits. City load is being carried but system now is in *emergency* state. Every serviceable generator is running.

2119 hours. Due to thermal expansion the conductors of one 345-kV line sag deep enough to cause shortcircuit via small tree. The line trips causing further overload of the few remaining ties, which now, one by one, break open. The system is now in *extremis* state.

2129 hours. The last tie with the outside world trips. The system now finds itself with a deficiency of 1700 megawatts resulting in a rapid loss of frequency. Underfrequency relays automatically initiate preset load shedding of section upon section of the city.

The loss of frequency cannot be halted and the generators are tripped automatically and manually to avoid catastrophic machine damage.

2136 hours. New York City goes totally black.

Figure 20 (excerpt): 1977 North American Blackout [116]

Despite exhaustive investigations into each major blackout event and the making and implementation of many significant recommendations, the number and extent of international blackout events keep growing. Not even the existence and deliberate efforts of international organisations and associations involved in large power systems (such as Cigré) to share learning and avoid or reduce such events seem to stem the incidence rate thereof. The following table details some of the more significant events that occurred internationally over the years.

TABLE I: INTERNATIONAL SIGNIFICANT BLACKOUT EVENTS

Country / Region / City	**Year**	**People Affected**	**Extent** (in GW)
USA	1965	30 million [115]	20
South Africa	1975	[117]	3,6
New York – USA	1977	9 million [115]	6,1
Thailand	1978	40 million [118]	
USA	1982	5 million [115]	12,4
Sweden	1983	[119]	11
Brazil	1984	[120]	15,8
Tokyo – Japan	1987	2,8 million households [121]	8
Canada and USA	1989	90 million [115]	21,4
Israel	1995	3 million [122]	2
USA	1996	2 million [115]	11,9
USA	1996	7,5 million [115]	30
Brazil	1999	75 million [120], [123]	24,7
India	2001	220 million [124]	12
Iran	2003	22 million [125]	22
Denmark & Sweden	2003	4 million [126]	6,5
Italy	2003	60 million [126], [127]	24
USA and Canada	2003	55 million [115]	63
Canada	2003	4,3 million [115]	
Libya	2003	4 million [128]	1,9
Athens – Greece	2004	5 million [129]	4,5
Java	2005	100 million [130]	
Moscow – Russia	2005	10 million [131]	
Pakistan	2006	[132]	11,2
Europe	2006	15 million (10 countries) [133], [134]	14,5
Costa Rika	2007	5 million [115]	
Colombia	2007	38 million [115]	7,1
Brazil and Paraguay	2009	87 million [136]	17
Turkey	2012	20 million [135]	
India	2012	710 million [137]	50

USA	2012	8 million [135]	
Bangladesh	2014	150 million [135]	5
Turkey	2015	70 million [135]	
Pakistan	2015	140 million [135]	
Kenya	2016	10 million [135]	
Venezuela	2019	32 million [135]	
Argentina	2019	48 million [135]	
Indonesia	2019	100 million [135]	
USA	2020	16 million [135]	
Pakistan	2021	210 million [138]	10,3
Bangladesh	2022	140 million [135]	
Pakistan	2023	220 million [135]	

These are merely a sample of the more significant events on record – the vast majority of blackout events that have been recorded do not form part of this list (being less extensive). However, it is clear from the list that the incidence rate and the extent of the blackouts are not subsiding. To represent the information in the list visually, the following graph shows the total population size that suffered each year as a result of blackouts during the given year (only considering the most significant events in each year) (see [115] through [138]).

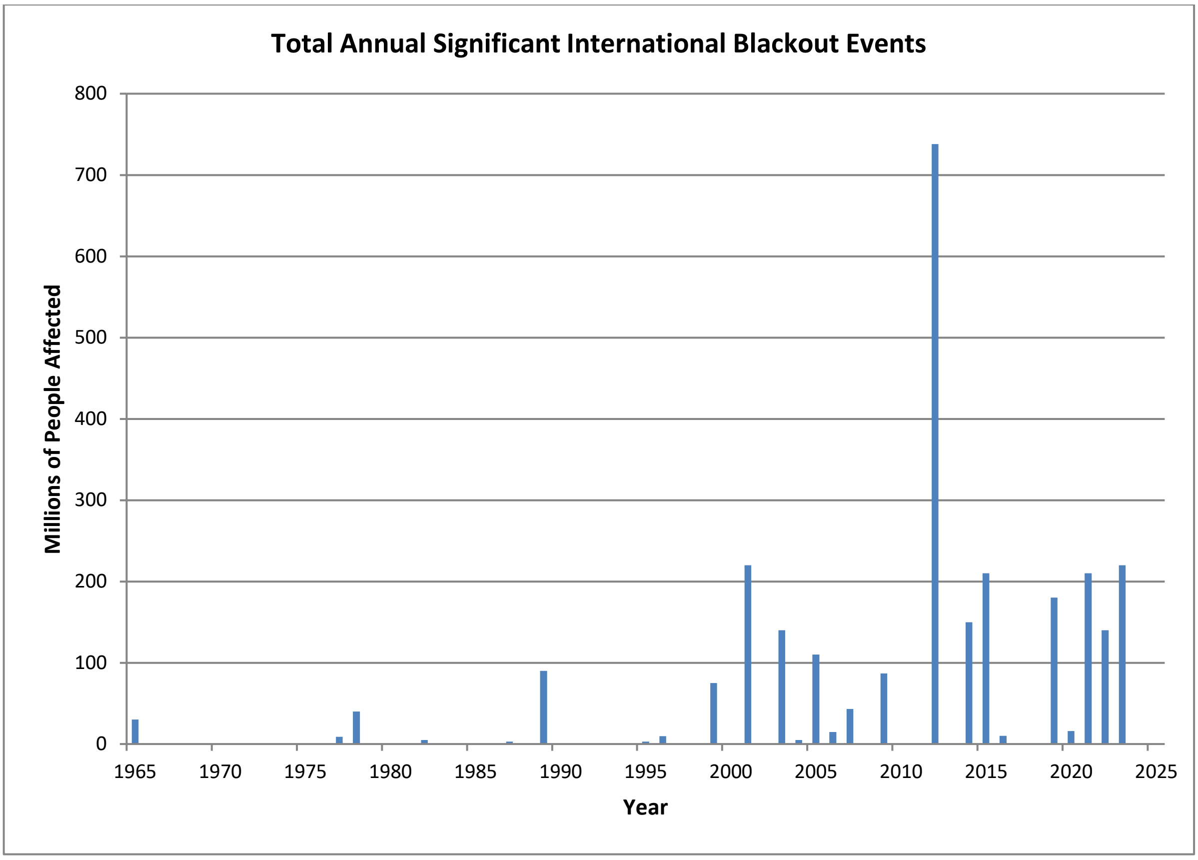


Figure 21: Summary record of global blackout events

As time progresses, the extent of the blackouts as well as the frequency with which they occur are increasing. Although the observed phenomenon might have various explanations, it cannot be denied that the problem of large-scale blackout events is not subsiding. Many governments and regulators are dedicating significant engineering and regulatory resources, to stem the scourge of power system blackouts. International organisations, such as Cigré and EPRI, have established dedicated technical work groups to focus on this problem, but they have yet to succeed.

Various reasons for this increasing characteristic could be put forward, e.g.:

- Increased population densities in electrified areas
- Increased complexity of modern power systems
- Increased liberalisation of electricity sectors

The problem is likely caused by a multitude of factors that collectively result in the increase shown in Figure 21.

The next section will focus on a specific event to emphasise certain relevant aspects to help readers understand the complex nature of a large-scale disruption event.

3.1.1. Case Study – US-Canada Blackout 14 August 2003

Probably one of the most notorious large-scale disruption events that occurred early in the third millennium A.D., was the North American blackout that happened on 14 August 2003. It was initiated by a mundane event of a protection device malfunctioning that caused the loss of a single transmission power line, followed by a next line tripping due to elevated loading that resulted in increased sag on the line that then inadvertently made contact with a tree causing a line fault – and then another. The losses in transmission capability caused a shift in the flow of electric power [115], [116], [139], [140].

Due to various information systems not being available at the time, the developing problem remained largely unnoticed and little action was taken to balance the system. It might not have been obvious to operators since, initially, the generation loss was insignificant, and only a small number of power lines were switched out by protection operation. In Figure 22, the event is visualised on a time basis, showing the numbers of generators and transmission system assets that trip as the event propagates.

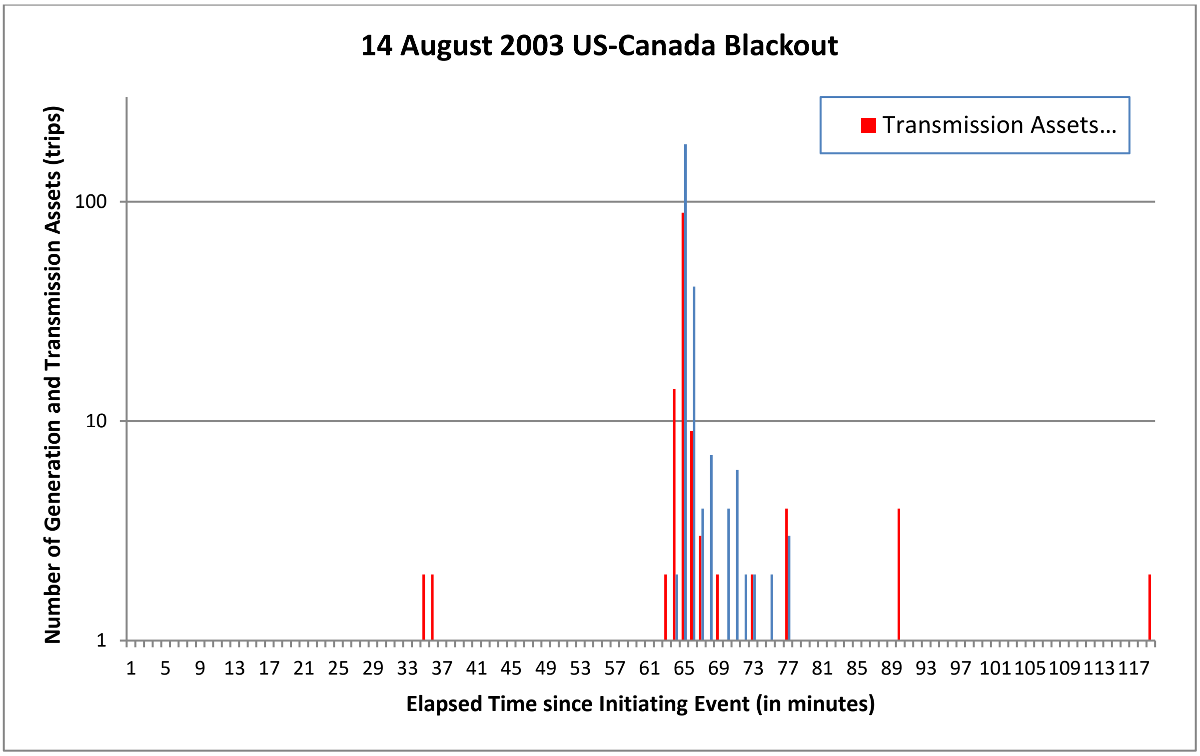


Figure 22: Transmission and generation plant losses

The vertical axis is logarithmic to accommodate the large data variations. It can be seen that for more than an hour, the extent of the disruption remained relatively small, to then suddenly cascade into high losses of generators. Because the bulk of the event occurred between minutes 65 and 67, the resolution of Figure 22 fails to reveal sufficient detail. The relevant two-second view is therefore shown below.

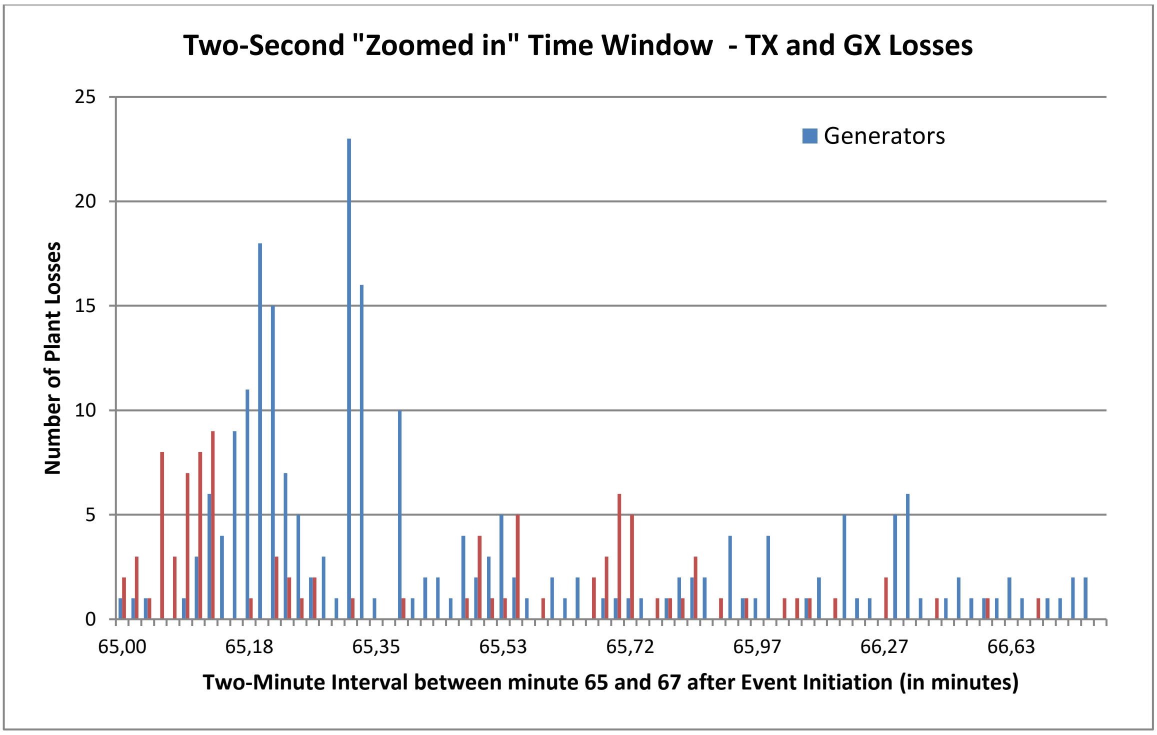


Figure 23: Generation and transmission asset losses (two-second, high resolution)

The generators that tripped included a wide variety of generation technologies, including:

- Nuclear (20 reactor units disconnected) [140]
- Coal
- Liquid fuel
- Wind

The transmission assets include:

- Power lines
- Reactors
- Transformers
- Capacitors

As expected, both manual and automated measures were taken to mitigate (or arrest) the propagation of the event, by shedding (disconnecting) load, by reducing network voltage (through tap changing) and by switching transmission assets into service. The mitigation measures are shown in Figure 24.

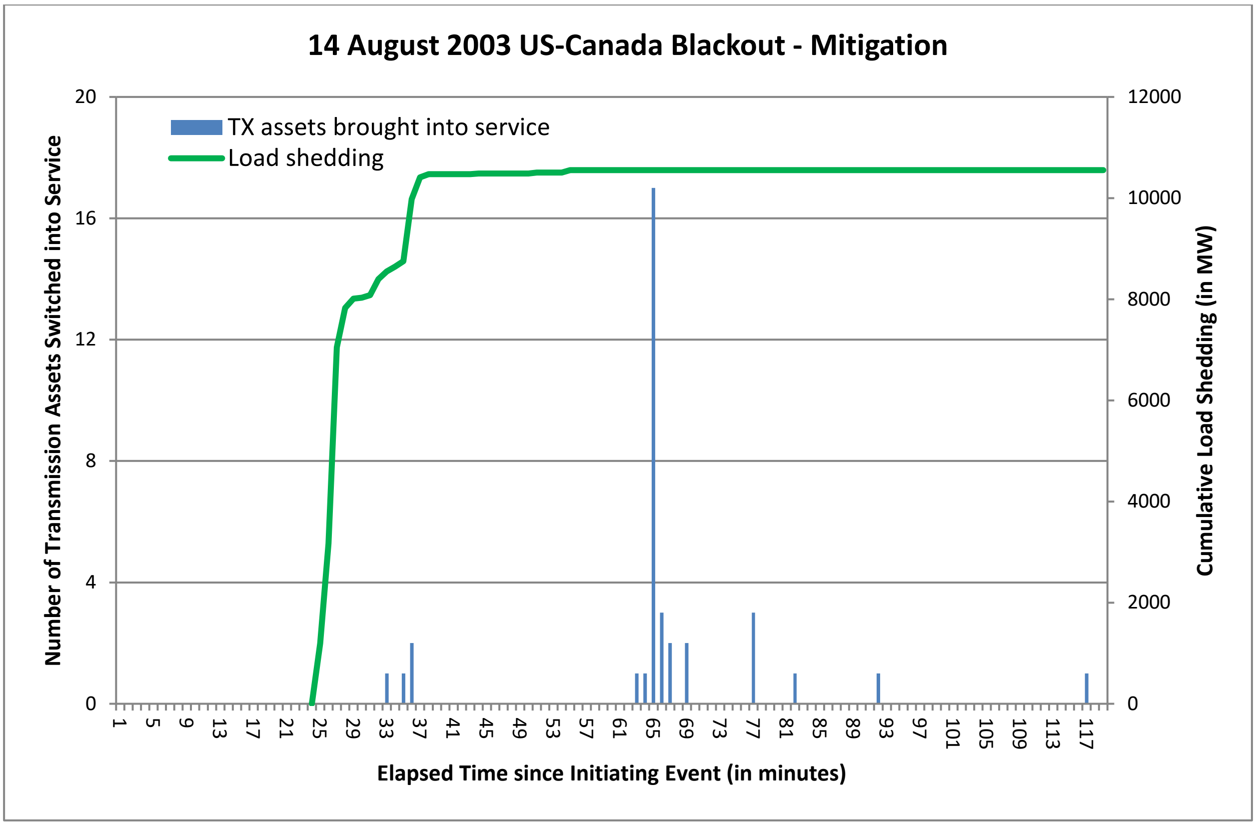


Figure 24: Transmission assets brought into service

However, the collective plant that was returned to service pales compared to the plant losses achieving little to mitigate the escalation of the event. Even the total load shedding of about 10 650 MW was not commensurate with the 63 000 MW that was compromised in total.

Ultimately, the unabated propagation of the event can be attributed to a voltage collapse rather than a disparity between real power being generated and demanded. The frequency extremes recorded during the event were (60-1,54) Hz and (60+3,27) Hz, respectively. The affected region can be seen below [115], [139].

Figure 25: Satellite photo of the region of the USA and Canada that were blacked out [141]

The event affected an estimated 50 million people, and compromised 63 GW of power, with a loss of about 531 generating units at 261 power plants – and the tripping of about 400 transmission lines. It took about a week for the complete restoration following the blackout, after which all effects of the event were normalised operationally. This could have taken even longer, if it was not for four Canadian nuclear units that islanded successfully, allowing for rapid reconnection and loading soon after restoration started [139], [140].

3.1.2. South Africa

Initially, as was the case in the rest of the world, during the early development of electrification in South Africa, generating stations only supplied regional power into relatively small networks since the interconnection between regions, to form a national grid, was a subsequent development that was only completed in 1973 [2]. Although the effects of a cessation of power generation at the earlier stations were inherently limited (due to their supply to only limited supply areas), it still caused much disruption to the industrial, mining and railway sectors, which were the prime customers of many of the earlier networks. The earliest operational failure where multiple generating sets were forced to disconnect from a supply network occurred in December 1925 when the entire Vereeniging Power Station had to be shut down due to catastrophic power station equipment failure causing major pant damage [2].

Before the establishment of Eskom, on 20 January 1901, during the Anglo-Boer War, four generators at the Brakpan Power Station were destroyed on the command of General Louis Botha. The four reciprocating steam engines were destroyed using dynamite and were part of a strategic military decision. This loss in generating capacity caused the local mining activities to cease until September 1901 [2].

The first major blackout resulting primarily from a large-scale loss of generation occurred in 1971 when four power stations were interrupted due to a transmission system fault, resulting in the total blackout of Durban. This occurred due to a fault at the Georgedale substation that caused the tripping of power lines and cascaded into the overloading and subsequent tripping of four power stations, i.e., Umgeni, Congella, Colenso and Ingagane. The loss of all four power stations embedded into the local network, the so-called Natal Undertaking, caused the inevitable interruption of all customers in the entire region [117]. Two years later, in 1973, the interconnection between all regional networks into the South African national grid was completed. This brought to fruition the concept that the vastly more redundant national grid, from a permutational perspective, will essentially always achieve the sourcing of power to wherever it may be needed.

A mere two years following the completion of the national grid, the most significant blackout occurred that, to date, was the most extensive ever encountered in South Africa. On 4 December 1975 at 19:01, a voltage transformer at Vulcan substation failed, causing a double fault. The ensuing transient caused by cascade tripping due to overloading and oscillations in the system frequency caused four power stations to trip all their generating sets – a total of 24 generators and about 45% of the total power being generated in the country at the time. The lowest system frequency that was recorded during the event was 47,5 Hz, but it is believed that the value is based on the lowest instrument scale available at the time and that the actual frequency was even lower. The extent of the blackout was immense and although the power stations that participated in the disconnection from the grid were separated by less than 200 km, the blackout crossed the borders of all four provinces of South Africa at the time [117].

The 1975 blackout brought certain realities into focus that might not have been appreciated before the establishment of the grid, namely that a single interconnected system offers many benefits, especially economically, but also provides the very fabric that is required to cause large-scale disruption and the interruption of customers which the grid was meant to avoid. In essence, the grid itself provided the commonality (the shared infrastructure) that is so pervasive among power generation sources and the users of electricity that adversity during the large-scale disruption thereof has essentially become unavoidable.

Over the years, various multiple contingency events occurred, but only the most severe ones were investigated – and only due to their vast system impact. It was not until the early 1990s that a policy stance was adopted to recognize all events where more than one unit disconnected, as a special class of disturbance event that was referred to as a Multiple Unit Trip (or commonly referred to as an MUT). These events were seen to be significantly more threatening to the integrity of the interconnected power system than unit trip events that occurred daily or unit load loss events that occurred on an hourly basis.

Although South Africa has given formal recognition, in terms of industry regulations, to the threat of multiple generation contingency events, globally, it receives little or no such recognition. This lack of recognition can be attributed to the fundamental differences between South Africa and many other developed countries worldwide. The most significant differences that have bearing on this lack of recognition, are the following.

- South African power generation is dominated by power stations that consist of multiple generating units or generating sets – both by utilities and independent power producers. At most South African power stations, six or more generating units have been installed. In comparison, it is internationally common to find power stations with fewer (and even single) generating units.
- South African power stations are dominated by coal as the primary energy source due to the prevalence of this natural resource. Coal power stations are known for their vast arrays of auxiliary equipment and their high degree of complexity of process interdependencies, dynamics and control requirements. Since systems with higher degrees of complexity exhibit greater vulnerability due their greater proclivity to become compromised, this aspect generally decreases reliability and increases the risk of being compromised during events that create a disturbance or disruption in the energy conversion processes. Internationally, although coal power stations are not uncommon, there normally exists a greater variety of primary energy source power stations – most of which are fewer in number and have a lesser degree of complexity.
- South Africa's role in the Southern African Power Pool (SAPP) is highly dominant. It is indeed likely that a collapse of the South African grid would also result in the cascade collapse of the entire SAPP. Even in the unlikely event that the power pool outside South Africa would remain operational, it does not provide a restart solution to the South African power system due to various technical limitations. Therefore, the South African focus on multiple generation contingency events is justified since it threatens the regional stability of the interconnected power system with limited restart support following a collapse. Most developed countries play a less dominant role in terms of the surrounding countries in such power pools and could often count on strong neighbouring support following a national blackout.

The following section will present an analysis of one of the early multiple-generation contingency events.

3.1.3. Case Study – South Africa 7 October 1975

An important point to emphasize is that all disruption events affecting power stations do not necessarily imply the tripping or disconnection of power generation. Equally disruptive are events where networks fracture into network islands that need to be operated within the capabilities of the remaining generation that inadvertently remained embedded within the island, not specifically matched to the load contained within the island. The event that occurred at 03:16 on the morning of 7 October 1975 illustrates exactly this type of disruption event [117].

During a typical thunderstorm on the Highveld of Transvaal, a lightning strike initiated a flash-over on the 400 kV Atlas-Perseus line – one of only two power lines at the time that connected the Transvaal power generation pool to the southern parts of the country. The total national system load at the time was about 8 000 MW [117].

Due to an inoperable protection panel (owing to human error), network protection performance was substandard and cleared with backup features rather than main protection. The prolonged exposure to the fault caused both of the south-north tie lines to trip, and vast power swings to occur. As a result of this disturbance, the southern grid started to fracture into smaller islands of load blocks with embedded generators contained within [117]. The islands that formed as a result of the disturbance are as follows.

a The Cape Undertaking separated from the IPS while the island frequency continued to decline.

b The Border and Cape Eastern Undertaking separated from the Cape Undertaking with West Bank Power Station remaining connected to East London when the island frequency reached 48,2 Hz with under-frequency islanding protection operating.

c Port Elizabeth also separated at 48,2 Hz with Swartkops Power Station supplying the municipal load, also with under-frequency islanding protection coming into operation.

d The Orange Free State would probably also have remained islanded in the Orange River Undertaking if both feeders from the Hendrik Verwoerd Power Station (later Gariep Power Station) had not tripped, presumably due to power swings. The province was largely left blacked out.

e Eventually, the Cape Western Undertaking separated from the rest of the group due to under-frequency islanding protection, with the load being carried by Hex River and Salt River Power Stations. Acacia Power Station was called up and later synchronised to this island to assist with the load deficit.

f Cape Town separated as a municipal entity from Escom (later Eskom), which became self-supplied with the municipal Athlone Power Station.

g Another island formed in the Vaal Triangle with Taaibos, Highveld and Vaal West Power Stations supplying into it, with the loads connected to the Scafell substation, but the frequency hovered around 46,6 Hz that was only rectified later upon system restoration.

h Another, mainly rural island formed around Vierfontein Power Station on an 88 kV network.

A total loss of 1 000 MW was estimated for the event, and approximately 150 circuit breakers tripped. Despite the vast scale of the disruption, all loads were restored by 06:30 on the same morning. A normal operational event led to the IPS fracturing into eight independent islands, seven of which proved viable at the time, that could readily be assimilated back into a single grid [117].

A very similar event occurred later that same month on 24 October 1975, when again a lightning strike, but this time on the Perseus-Hydra line, caused a loss of about 700 MW on a system load of 8 000 MW – totally recovered within about 1½ hours [117].

Both these events were characterised by high over-voltages due to the long lines and lightly loaded conditions on many corridors. But both these events illustrate a vitally important aspect, which is that if power generation is not lost (i.e. tripped or shut down), recovery can be rapid and merely involves synchronisation and switching. As will be seen later, recovery from events where the generation itself becomes compromised, could be extremely protracted and could have crippling consequences on the economic, political and social spheres of society.

3.2 Regulatory Landscape

Although design standards exist for most equipment used within the electricity industry, industry standards invariably fail to guide on how to design or construct complex amalgamations such as power stations. To enforce principles that are deemed critical, guidance and obligations are outlined in terms of the regulatory frameworks applied in specific regions or nationalities. This section will explore the established regulator industry framework from various perspectives.

3.2.1 International

As discussed earlier, the specific threat posed by the cascading failure of generation is far less pronounced in many countries than in South Africa. Many international power stations have single (or very few) generating units, unlike those in South Africa.

Having made the point that the threat in many countries may vary from the South African risk profile in the sense of multiple generation contingencies, multi-unit power stations do exist elsewhere in the world, many with more units than those found locally. For example, the Three Rivers Gorge Hydropower Station in China has a total of 34 generating units with a total installed capacity of 22 500 MW – the loss of which would inevitably cause a considerable shock to any power system in the world.

Besides the fact that many power stations internationally have multiple units, major power system disruptions and blackouts usually suffer the loss of many generating units from the interconnected power system. As an example, in the blackout event of 10 August 1996 in western North America, 175 generating sets were lost, equating to 25 GW and impacting 7,5 million customers, while 531 generators were lost during the eastern North America blackout of 14 August 2003 with an associated capacity of 63 GW and 50 million people affected [115], [139].

It is especially due to this obvious vulnerability that it is reasonable to suspect that international grid codes would provide a strong regulatory framework to govern the landscape of cascade failure of power-generating facilities within power systems.

A survey was conducted into the grid codes available in Germanic languages, such as English or Dutch, to determine the degree to which grid codes regulate the industry regarding this particular vulnerability.

TABLE II: SURVEY RESULTS OF DUTIES PLACED ON PARTICIPANTS BY INTERNATIONAL GRID CODES

Grid Code Region or Country	**System Operator Requirements**	**Power Producer Requirements**
Western-Australia [142]	No	No
Ireland [143]	No	Yes
United Kingdom [144]	No	No
Germany [145]	No	No
Netherlands [146], [147]	No	No
Italy [148]	No	No
Jordan [149]	No	No
Pakistan [150]	No	No

It is evident from the list above that despite obvious exposure to the risk of multiple-generation contingencies event; most countries have no deliberate measures in terms of regulation to govern participants. The one exception that could be identified, i.e., Ireland has a limited and rather vague duty that it places on power producers, namely:

> "*Each **Generation Unit** shall be designed, where practicable, to mitigate the risk of common mode failure with other **Generation Units**. In particular each **Generation Unit** shall be designed so that it can operate with its essential auxiliaries supplied through a unit transformer which shall be connected between the **Generation Unit** circuit breaker and the **Generator Transformer LV** terminals, or from another secure source as agreed with the **TSO**. Auxiliary supplies may, provided that they are in accordance with **Good Industry Practice**, be taken from an alternative source during commissioning, testing, start-up or emergencies.*
>
> *In the case of a **CCGT Installation** this applies to the **Combustion Turbine Units** only.*" [143]

The only binding implication that stems from the Irish grid code is that each unit needs to supply its auxiliaries from a secure point in the unit. Although it has at least some requirement in terms of multiple generation contingencies, the requirement is in itself almost superfluous since it represents generally accepted power station practice that essentially all modern power stations comply with, regardless of regulations. There is not a single South African power station under the control of Eskom that deviates from this approach, including coal, nuclear, hydro, pump storage and gas power stations. This practice has already become the *de facto* design standard from the third-generation power stations onwards. It is, therefore, doubtful whether the EirGrid grid code adds any material benefit to the management of this specific category of risk to its power system security.

To summarize, despite the obvious reality that essentially all large-scale power system disruptions and blackouts would suffer, in one way or another, from the loss of multiple units and even entire power stations disconnecting from the grid, the regulatory frameworks remain largely lacking.

3.2.2 Africa

Power systems in Africa are generally a more recent development, and installed capacities in many countries are relatively small – a few minor exceptions exist such as in South Africa. Due to growth being foreseen in much of the continent, many countries have developed grid codes for their expansion into the future. It has been found that much of the content of the African grid codes is based on the South African Grid Code, probably the most suitable code to use as a template as compared to codes from first-world countries.

The African continent has various cross-border regions, each containing (or foreseeing) an expanded power system that interconnects various sovereign countries. Each power system is referred to as a power pool. The different power pools are not interconnected and operate entirely independently from one another (refer to Figure 26).

The largest power pool (in terms of geographic reach and installed capacity) is the Southern African Power Pool (SAPP), of which South Africa forms part. It is also the largest contributor in terms of installed capacity, energy production, and collective power line length. The following map shows the present regions wherein power pools within Africa are being divided.

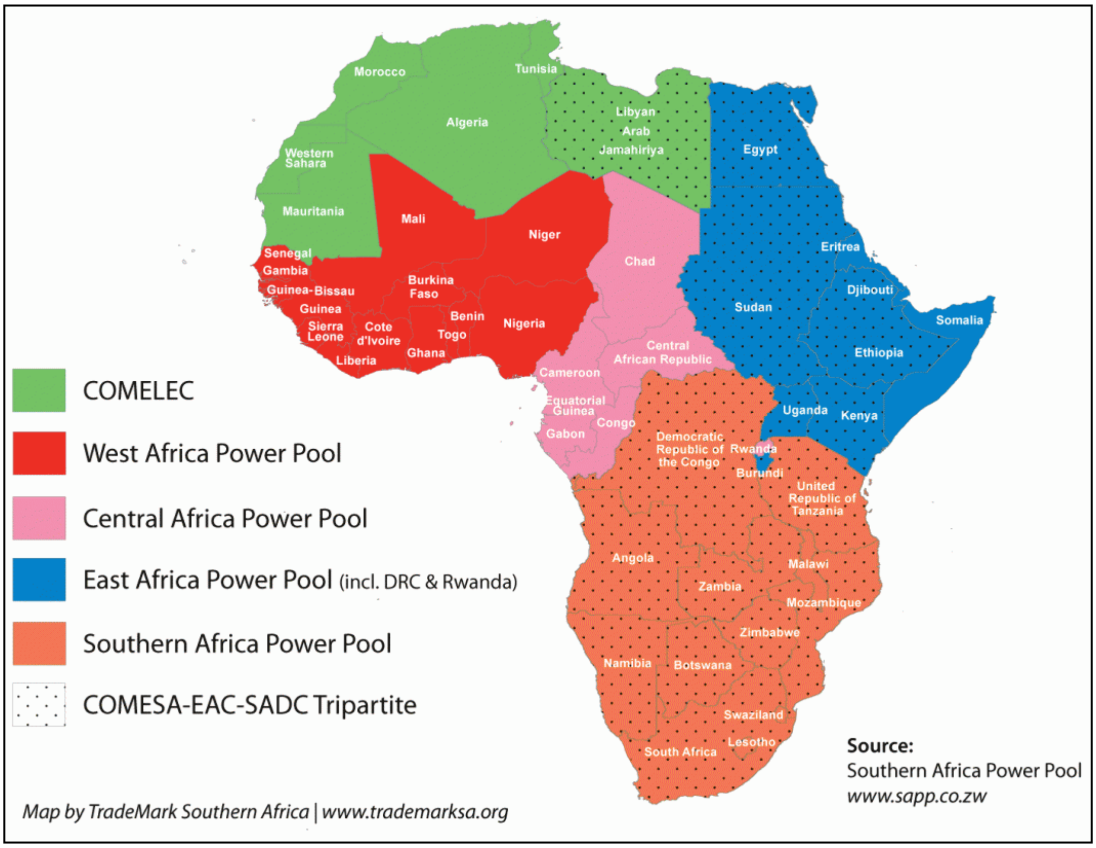


Figure 26: Power Pools of the African continent [151]

The grid codes existing within SAPP (those that exist and could be obtained) have been scrutinized for references to multiple generation contingencies, as was done in the international survey, and the results are presented in the following table.

TABLE III: Survey Results of Duties Placed on Participants by Grid Codes within the SAPP

Country / Region	System Operator Requirements	Power Producer Requirements
South Africa [1], [152]	Yes	Yes
Namibia [153]	No	Yes
Zimbabwe [154]	No	Yes (very little)
Zambia [155]	No	No
SAPP [156]	Yes	No

Similarly, to obtain some degree of insight into the status of countries in northern parts of the continent, a limited number of codes were sampled, which are shared in the table below.

TABLE IV: SURVEY RESULTS OF DUTIES PLACED ON PARTICIPANTS BY GRID CODES NORTH OF SAPP

Country / Region	**System Operator Requirements**	**Power Producer Requirements**
Sudan [157]	Yes	No
Rwanda [158]	Yes	Yes
Uganda [159]	No	No
Kenia [160]	Yes	No
Nigeria [161]	Yes	Yes

Interestingly, in contrast with the results obtained from the survey of the international grid codes, significantly more of the grid codes applicable within Africa (both SAPP and north of SAPP) refer to, and place duties upon participants for the management of multiple generation contingencies. Although the results seem to be irrational, the reason for this anomaly is that most of the member countries within SAPP and Africa, in general, have used the South African grid code as a guide and template in the compilation and development of their grid codes. Therefore, since the South African grid code has referred to these multiple-generation contingencies from the very first revision, the countries that used it as a template also "inherited" these references.

The next section will explore the content and extent of South Africa's regulatory framework in some detail.

3.2.3 South Africa

South Africa, featuring the largest power system on the African continent, also features the most developed framework for the management of multiple generation contingencies. Although the first version of the South African Grid Code (SAGC) was signed by the National Energy Regulator (NER) on 19 June 2003 and came into force on 1 January 2004, Eskom has already taken a policy stance on the management of Multiple Unit Trips (MUT) in the early 1990s. Therefore, when the SAGC was drafted at the start of the new millennium, the Eskom MUT framework was adopted into the grid code. The definition of MUT that is found in the SAGC is the following, visualised in Figure 27.

> ***"Multiple unit trip (MUT)***
> *Two or more units of a power station that trip within one hour due to a common triggering event, and whose total installed MCR capacity exceeds the largest single contingency limit"* [1].

The concept of the largest single contingency limit is further defined as follows.

> ***"Largest single contingency limit***
> *The largest single event of the sudden and unplanned disconnection of the largest unit from the IPS or the largest single credible other contingency constraining the net generating capacity available to the IPS. The largest single contingency limit is 920MW (loss of a Koeberg unit) effective 1 January 2013 and is reviewed periodically by the System Operator"* [162].

And the largest credible multiple contingency limit, as follows.

> ***"Largest credible multiple contingency limit***
> *The largest credible multiple event of the sudden and unplanned disconnection of a more than one unit from the IPS or the largest credible other multiple contingency constraining the net generating capacity available to the IPS. The largest multiple contingency limit is 1800MW (both Koeberg units, 3 coal fired units, or the Cahora Bassa infeed) effective 1 January 2013 and is reviewed periodically by the System Operator"* [162].

The essence of the requirements for managing MUT events has not changed since the inception of the SAGC. The code assigns duties to power producers and the system operator. Duties for power stations are mainly contained within the SAGC's Network Code, which firstly defines the various categories of MUT.

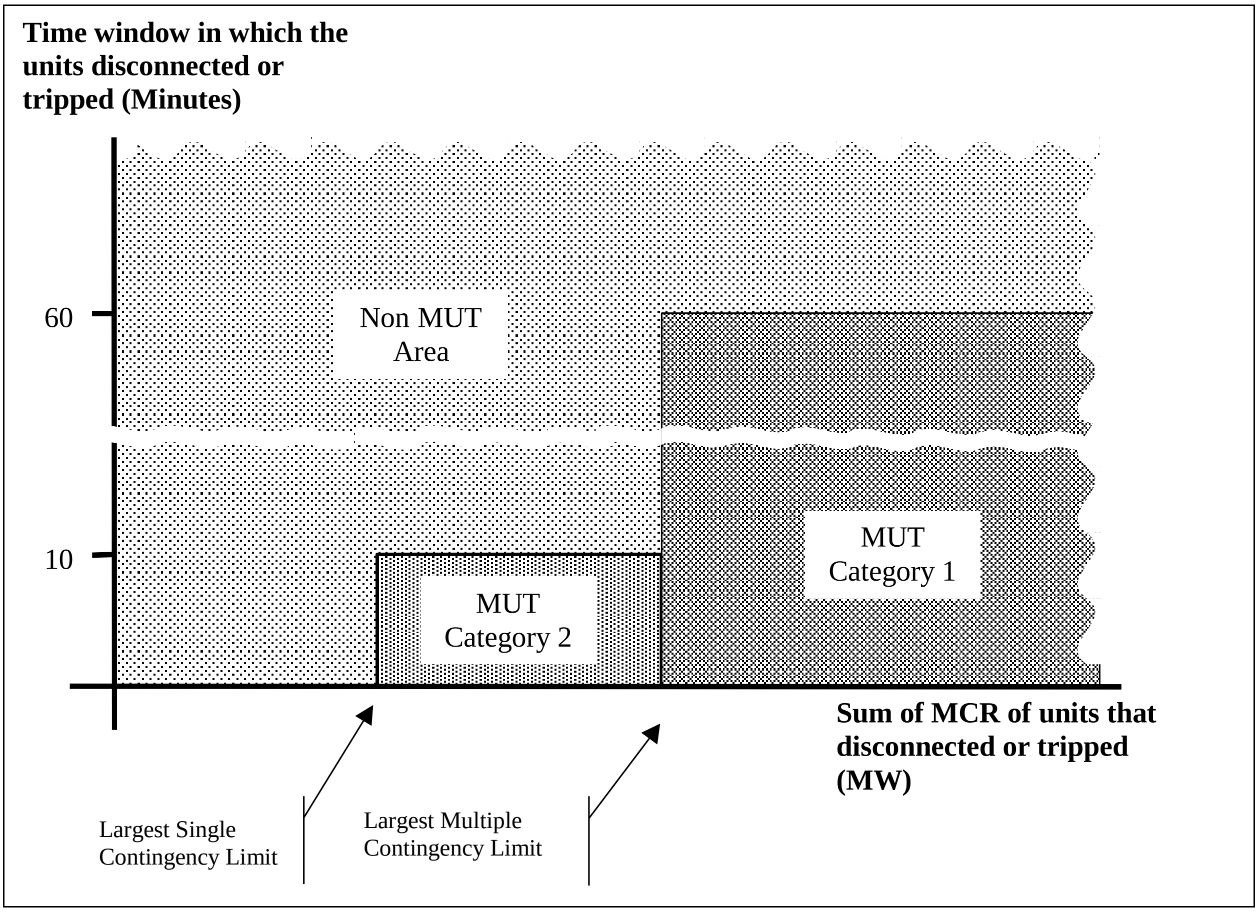


Figure 27: MUT categories used in the SAGC [1]

Power stations are charged with the prime duties of identifying and cataloguing their MUT risks, sharing their risk register with the System Operator, and managing their risks operationally on an ongoing basis. Furthermore, they are required to investigate MUT events suffered by the power station and implement the recommendations [1].

Although the allocation of the MUT identification and management aspect to the power station is appropriate, the investigation duty is less rational. For the duty of investigating the MUT event to be assigned to the power station, it must be assumed that the power station is the likely cause of the event or the party that suffered the greatest from the MUT. This issue will be explored in more detail in Chapter 5.

3.3 Prior Studies and Developments

As stated previously, the typical approach (internationally) to studying major blackout events is to focus on the network triggers and cascades, mostly neglecting the contributions from power generation or treating the generation components with a “black-box” approach.

In one previous study by this author, several useful concepts were developed that are relevant to the continued study of this phenomenon of cascading generation disruption. In the following sections, those concepts will be briefly shown to serve as building blocks for further analysis and development [163].

3.3.1 Magnitude

The concept of the *magnitude* (denoted with G) had been introduced in 2012 as a measure of the extent of an event. It uses real power (P) as the point of departure since the loss of real power is one of the most significant parameters associated with a disruption event. The magnitude is defined as the ratio between the total power that is collectively being supplied into the power system at the time of the event and the power being lost due to the disruption – expressed as a decibel (dB) value, given by the following equation [163],

$$G = 10 \cdot log_{10}\left(\frac{P_{IPS}}{P_{event}}\right) \tag{1}$$

where

G	the magnitude of the disruption event expressed in dB
P_{IPS}	the total power being generated into the IPS just before the event
P_{event}	the total power being lost during the event

The following table gives value ranges of magnitude with power system consequences that have been determined and validated empirically [163].

TABLE V: Values of Event Magnitude (G) in Relation to Power System Consequences [163]

Disruption Magnitude (G) (in dB)	**Effect on the IPS**
G > 18 dB	**Slight** – barely noticeable on the frequency of the IPS.
14 dB < G < 18 dB	**Moderate** – noticeable effect on system frequency, corrected by automatic regulating mechanisms.
10 dB < G < 14 dB	**Significant** – deliberate intervention required.
6 dB < G < 10 dB	**Threatening** – affecting most participants connected to the power system.
0 dB < G < 6 dB	**Overwhelming** – a system blackout is a likely end-state.

3.3.2 Post-Event Recovery

Although the magnitude of a disruption event aids in quantifying the severity of the disturbance on a power system, it fails to provide a means of evaluating the resilience of the power system when the event occurs. To address this shortcoming, a quantitative concept of dynamic restitution (denoted by R) was developed to enable the comparison of power system resilience during different events. The dynamic restitution was defined as the total decline in system frequency compared to the total time taken for the system frequency to recover to the nominal system frequency. Expressed as a formula [163],

$$R = \frac{\Delta f}{\Delta t} \tag{2}$$

where

$$\Delta f = f_N - f_{min}$$

and

$$\Delta t = t|_{f_N} - t_0$$

with

f_N	the nominal network frequency
f_{min}	the minimum network frequency resulting from the event
$t\|_{f_N}$	the time at which the network frequency recovered to f_N
t_0	the time when the event started to manifest in a decline in network frequency.

The dynamic restitution gives an average rate of recovery of the network frequency and is typically expressed in mHz·min^{-1}. Values of less than about 100 mHz·min^{-1} represent a sluggish recovery in system frequency – indicative of poor governing response of generating units or a lack of spinning reserve. Acceptable values were found to be greater than 200 mHz·min^{-1} [163].

3.4 Event Analysis

It was mentioned earlier that, internationally, major disruption events (like blackout events) are seldom investigated from a generation perspective but focus (almost without exception) on network performance and power system operational issues. In isolated cases, a superficial analysis of some of the generation issues has been mentioned, but without any depth in terms of the investigation or the recommendations.

One possible explanation for this phenomenon is that the analysis of generation disruption events is multidisciplinary – necessitating various engineering disciplines and expertise, e.g., electrical, control systems, combustion, materials handling, etc. Unlike network disturbances that are predominantly electrical, generation disruption events require a large resource allocation of skills – preferably independent in the interest of objectivity.

Another obstacle to an in-depth investigation into cascade generation disruption events is that power stations embedded in a power system often have diverse ownership, and information sharing might not be forthcoming due to commercial issues or embarrassment.

Also, a standard approach or methodology has yet to be established due to the limited work undertaken in analysing generation disruption events internationally. Very few metrics exist to quantify, record and compare events. The most universally accepted metric for comparison is the number of people affected by the event. In many of the investigation reports, no reference is even made to the electric power lost during the event or the unserved energy associated with the disruption – values that seem both obvious in their importance and fundamental to the nature of the event.

The necessity of developing tools and methodologies to enable the systematic investigation and recording of multiple-generation disruption events is evident and indeed overdue. In the absence thereof, the incidence rate and the poor level of analysis will continue unabated…

3.5 Summary

The historical record of power systems demonstrates that large-scale power disruption events, culminating in power system blackouts, have occurred since the establishment of power systems globally. However, since the 2000s, the events' incidence rate and extent have significantly increased—clearly growing in prominence as a power system risk factor (see Figure 21).

However, internationally, the regulatory frameworks related to large-scale cascade disruptions of power systems are scant, with the South African Grid Code containing the most comprehensive suite of regulatory provisions found anywhere.

As power systems continue to grow in complexity and size, blackout events can readily be expected to become even more prominent. The following section will be devoted to establishing a contextualised understanding of power stations, their systems, and their role in cascade disruption events.

No evidence could be obtained that suggest any standardised approach exists for the investigation of large scale power system disruption events. In all cases that were considered, power stations were treated using a "black-box" approach during event investigations and analysis. Except for the most rudimentary metrics, event reports were consistently devoid of any attempt to quantify the severity thereof or to compare events to other cases. The hypothesis stated in section 1.3 is therefore supported by the lack of evidence to the contrary, and therefore believed to be valid.

4. Research Necessity: Justification

The context regarding the potential need for developing a methodology and metrics for managing large-scale power system disruption events may not be obvious. This section is intended to provide the specific context to better comprehend the reasons and necessity for this research endeavour.

4.1 Absence of Industry Standard

Electricity supply and distribution are not recent developments, nor are the vast conglomerations of infrastructure that serve this commodity to its users. It would be reasonable to assume that the essential tools for analysing and quantifying disruption phenomena should be well established.

This assumption is, however, invalid. There exists no standard approach to investigating large-scale power system disruptions, no standard for data collection, no standard approach to analysis, and no standard metrics (barring the most basic ones) for evaluating, ranking, comparing, etc., of such events.

The reasons for the lack of a standardised approach to investigating large-scale power system disruption events require specific context, which is summarised below.

a Large-scale power system disruptions only emerged when large power systems were formed in the late 1960s and 1970s. Before this stage of development, electricity was served through smaller power networks that were not interconnected, so large-scale power system disruption was not an issue.

b Initial power systems were rudimentary and robust. As equipment ratings became marginalised and power systems grew in size and complexity, the risk of disruption increased, and more large-scale disruption events occurred.

Following on from points (a) and (b) above, the problem of large-scale power disruption is a relatively recent manifestation and does not date back to the early stages of electricity as a consumer commodity.

c Initial power systems were essentially under the control of single entities (utilities) – facilitating rigorous control and the adherence to standards that inherently mitigated disruption threats. With the relatively recent liberalisation of the electricity industry, the increase in the number of participants in power generation also resulted in a decrease in risk mitigation associated with large-scale power system disruption.

d A relatively small number of (bulk) generation sources, which traditionally warranted extreme engineering effort to focus on risk mitigation. This reality has changed significantly with vast numbers of smaller power injection points in modern power systems. Once again, this is a fairly recent development resulting in an increase in the disruption risk profile for power systems.

Due to the points above (amongst others), large-scale power system disruption events were initially considered to be *ad hoc* occurrences. Since about the year 2000, the incidence rate has increased to a level that is now considered a scourge (see Figure 21). It is, therefore, not surprising that this phenomenon of large-scale power system disruption events is only recently being recognised as a major ailment plaguing modern power systems and the power industry itself.

A further factor to consider is that large-scale disruption events are scattered across many countries globally – all of which have different power system attributes, governance structures, regulatory frameworks and disruption risk profiles. Therefore, investigating such events has mainly remained a local matter, investigated internally by each affected country. Furthermore, since findings are often embarrassing, detailed disclosure of incident investigations is often restricted or barred, and external involvement is generally not encouraged or allowed. Therefore, the investigation of such events has remained largely compartmentalised in regional silos, and sharing of neither (detailed) incident information nor investigation techniques and methodologies has readily occurred over time.

The increase in the global liberalisation of the electricity industry has also resulted in a decline in large monolithic power utility structures that dominated the electricity landscape for most of the twentieth century. Their decline made way for a very large population of independent power producers (IPP) that compete with one another commercially in a market or in a contractual space that was created for that purpose. This development has an unfortunate side effect, namely that details of disruption events often have a bearing on commercial aspects, proprietary plant information or other information that is regarded as intellectual property and is therefore withheld or shrouded in non-disclosure regulatory provisions or agreements.

A further factor in the investigation and the need to understand large-scale power system disruption events is that such events are invariably viewed as a power system issue (from a technical perspective). Therefore, investigations into such disruption events are undertaken by the system operator, co-opting members to assist, as seen fit. Although such an approach is inherently sound, the end result is that such investigation teams are heavily dominated by power system engineers, who possess ample power system knowledge, mainly in the disciplines of transmission and distribution systems and associated technologies. However, it typically lacks expertise from a power generation perspective, and issues relevant to the generation space are often neglected. Power generation issues are, therefore, often treated with a black-box approach while network and power system issues are properly investigated and analysed, representing a biased and one-sided approach. Hence, the few metrics that do exist are mainly focused on the power system and consumers, often disregarding power generation aspects that might be highly significant.

4.2 Eskom

As a utility, Eskom's history dates back to 1924, with well-preserved historical records. Eskom is a utility that features a large interconnected power system since the 1970s, spanning several thousand kilometres and with various AC and an HVDC interconnection to the Southern African Power Pool. It owns and operates coal, hydro, pumped storage, gas, wind and nuclear power stations, including three black-start facilities with a total installed capacity exceeding 40 GW.

Eskom has recognised the unique nature of cascade generation failures since the 1970s and has deliberately embarked on recording and investigating such events since the 1980s.

South Africa has had an official grid code (SAGC) since the early 2000s, issued and controlled by the National Energy Regulator (NERSA). The SAGC has, from its first revision, included regulations regarding multiple unit trip (MUT) events, unlike most international codes (see section 3.2).

As such, South Africa's electricity generation landscape is ideally suited to conducting research into large-scale or cascade disruption events. It exists within a regulatory environment focused on MUT avoidance and has a century-old power utility with a well-preserved historical record.

4.3 Conclusion

Due to the (relatively) recent developments and changes in the electricity supply industry, more investigation methodology and associated metrics are needed. The geopolitical global landscape and sovereign national interests exacerbate this lack of methodology.

Power generation is not seen to be central to power system disruptions, and very limited engineering effort is dedicated to disruption events involving generation cascading events.

Information necessary for addressing generation cascade failure events is hard to obtain due to confidentiality considerations and a lack of recognition and recording of generation cascade failure event data.

It is believed that the author is suitable to undertake the research due to:

a Vocational experience with a specific professional focus and oversight
b Utility historic record access spanning decades of events
c South African location – regulatory recognition of multiple contingency-type events

Therefore, the intended research is justified and needed, and the author is well-placed, specifically within the South African power utility, to undertake it.

5. Power Generation: A Potential IPS Disruptor

Many of the major blackouts that occurred historically have not merely caused an interruption to customers but were often pre-empted by a loss in generating capacity. An example of a loss in generation capacity that ultimately culminated in a blackout is the 2003 North American blackout event when 50 million people were affected, residing in five states of the USA and two provinces of Canada, collectively representing a load interruption of 63 GW. During the event, 531 generators at 261 power stations disconnected from the power system and tripped about 400 power lines [115], [139].

This chapter will be used to place the area of power generation into its requisite context as a means to provide insight into its role during large scale power system disruption events. The chapter will introduce the concept of individual unit tripping, from where the concept of disruption would be expanded into the cascade phenomenon that is based on interdependencies. In turn, the concept interdependency would be elaborated upon to elucidate two classes thereof, namely intra-station and inter-station interdependencies respectively.

5.1 Types of Electricity Generation

To appreciate the role and significance of power generation as a threat element in large power systems, it is necessary to explore the landscape of electricity generation in more detail. To this end, power generation will be unveiled to an extent that would provide a sufficient understanding for the latter part of this publication.

Electricity generation is often undertaken to benefit isolated entities that are not part of a larger or interconnected system. Examples of this type of power generation include the electrification of small isolated communities on islands or ships. Although this type of power generation is not uncommon, it is not explored further since this study focuses on the threat that a large-scale failure in power generation poses to large power systems.

A further form of power generation not explored within the confines of this study is generating equipment owned and installed exclusively to provide a backup source of electricity in events where the main power system fails to deliver electricity to a given consumer. Facilities such as hospitals and emergency shelters are often equipped with such installations, but since they don’t provide electricity to the power system, they are also neglected in this study.

Virtually all forms of power generation that exist to supply electricity to a central power system can be divided into two main categories, namely:

- Power Stations
- Power Parks

Traditionally, most power generation in large power systems occurred at power stations. A ***power station*** typically consists of various sets of relatively large capacity generation equipment that generate electricity and supply it to a power system. The individual sets of generating plants at power stations convert some type of energy into electrical energy and connect individually to the power system in a synchronised fashion. Examples of power stations that are commonly found include:

- Thermal generation
    - Combustion-based generation
        - Fossil fuel
            - Coal or lignite (mined or underground gasification)
            - Natural gas (gas pockets or fracking)
            - Natural liquid fuel
        - Biomass
            - Animal manure
            - Crop waste
            - Lumber and timber (waste or harvested)
            - Pest control and eradication (weeds, vermin, etc.)
            - Biofuel
        - Domestic waste
            - Methane combustion
            - Incineration
        - Industrial process discard
            - Discard gas
        - Non-CO_2 combustion
            - Hydrogen gas (H_2)
            - Ammonia (NH_3)
    - Non-combustion
        - Concentrated solar
            - Tower
            - Trough
        - Atmospheric thermal differential

            - Tall tube-tower
        - Geothermal
            - Natural vents
            - Drilled shafts
        - Oceanic thermal differential
            - Deep ocean fixed or drifting modules
        - Nuclear
- Non-thermal
    - Hydro
        - Dam penstock generation
        - Run-of-river
        - Pumped storage
        - Osmotic

Power parks represent a more recent development in the electricity industry where typically large collections of individually relatively small capacity of power generation equipment are pooled together, and their combined output is injected into the power system. Power parks commonly convert some form of renewable energy into electricity in small generating modules that individually function unsynchronised from one another (or the power system to which it ultimately connects) and, therefore, require an intermediate technology to combine their collective output and inject it into the power system in a synchronised fashion. Examples of power parks include:

- Thermal
    - Solar – Sterling engine modules
- Optic energy
    - Photovoltaic (PV)
- Mass Flow
    - Wind
    - River flow modules
    - Wave
    - Tidal pools
    - Oceanic submarine current

Power parks are often connected to the fringes or remote areas of the power system and, therefore, often inject into distribution networks, while power stations usually inject at the transmission level. Because distribution networks are not under the rigorous control of the System Operator but rather regional control centres, and because distribution networks are more prone to network disturbances than the transmission system, power parks are usually set up to disconnect (and remain disconnected) during severe system disruption events such as regional blackouts. For this (and other technical) reason, power parks play a minor role during system restoration.

Besides *generating* power by converting an energy source into electricity specifically, there is increasing development into various means to store energy temporarily, and extract the energy later and inject electricity into the power system. Various such technologies exist, either as demonstrated systems or commercially available, and include:

- Battery energy storage
- Thermal storage (often used with thermal solar plants)
- Flywheel storage
- Compressed gas (or air) and gas liquefaction and evaporation systems
- Superconductor electromagnetic storage
- Gravity storage (displace mass to higher elevations – not merely water)

These energy storage systems are often used to augment either power stations or power parks. Still, examples do exist where they are used as stand-alone facilities that produce electricity into a power system – either on instruction (signal) or based on predefined criteria.

Two special classes of power stations exist that need to be specifically clarified, which are:

- Embedded generators
- Co-generators

An ***embedded generator*** is a power station that is connected to and operates within an electrical network that the main network service provider does not own. An example is where a power station is embedded within a municipal network owned and operated by a municipal authority but ultimately connects to the main national or regional power system.

A ***co-generator*** is a power station that forms part of a separate industry and utilises by-products or waste to generate electricity. The power station's output is used to offset the electricity consumption of the mother industry, partially or in total. In other words, the main purpose of a co-generator is not to provide electricity to third parties but to produce electricity when conditions are favourable to the industry wherein it is embedded.

Although this study will focus on generating facilities intended to generate and deliver large quantities of electrical power into a power system for commercial purposes, much of its content will apply equally to the other types of power-generating installations highlighted above.

5.2 Tripping: The Incremental Steps of Disruption

Up to this point, a power station and a power generating unit were considered on a mere conceptual level. But, in the practical reality of actual power plants and generation processes, a disruption is always a physical manifestation.

In practice, power stations are designed, constructed, and operated modularly, with a module typically referred to as a generating unit or merely a unit. Each unit, therefore, consists of a collective conglomeration of equipment organized into systems to sustain an energy conversion process that ultimately generates electricity. To add more generating capacity, another *module* needs to be added.

Ideally, each power generation module should be entirely independent from all other modules to eliminate possible common mode failure. However, due to various factors, independencies cannot practically be eliminated in totality – units thus inherit vulnerability to multiple cascade disruptions. In large conventional power generation, due to the risk of common mode failures that stem from interdependencies, an economic optimum is sought between the benefits and risks associated with independence versus interdependency.

In the case of power stations, and specifically units as the basic building block comprising a power station, disruption is typically an incremental phenomenon that erodes the ability to generate electricity – either partly or completely (a quantum of adversity that detracts from the overall intent). The incremental instance that marks the actual manifestation of a disruption is normally referred to as a trip. It invariably involves the automatic disconnection (or isolation) and shutdown of a plant or a part thereof upon receiving an automatically or manually generated instruction (signal).

Conceptually, a trip can be understood as the rapid withdrawal of equipment, plant, system or process from normal operation, resulting in the complete cessation of its function – normally within a very small time interval (often instantaneously for all practical purposes).

In practice, tripping involves various potential steps depending on the equipment, system, plant, process or unit – but the following list includes the most common and typical. Depending on the case, a trip may include some or all of the steps listed below.

- Rapid interruption of energy – often through disconnection and de-energisation.
- Initiation of sequential or group tripping – stopping of other interdependent functions.
- Discharging and dumping of energy or energy-containing fluids.
- Controlled dumping or flaring of hazardous (often intermediate) substances.

- Isolating, cutting off and locking out – avoid introducing new risks.
- Initiation of shutdown and emergency procedures – involuntary damage avoidance.

The simplest example of a trip occurs when a component exceeds its safe operating envelope and is merely switched out of operation by interrupting its electricity supply. In this simple example, nothing else needs to happen, and none of the steps above, except for the first step, is required.

However, in a system comprising various equipment components, the extent of the trip of a single piece of equipment would be very different. The difference between the two examples is that equipment that forms part of a system is not independent. Generally, such components have an interdependent relationship. This implies that the system as a whole cannot continue to function in the absence of one of its constituent parts. Therefore, when a similar piece of equipment (that is now part of a system) exceeds its safe operating envelope, not only is it switched out of operation, but the entire system of which it forms part would also be forced to trip, i.e., shut down (except if the design deliberately allows an alternative means of dealing with the loss of a component). In this case, the first and second points of the above list will be implemented, resulting in the complete loss of a system.

The following sections will explore the concept of a trip in the context of its potential impact on electricity generation. Although a subsequent section will deal with the unitised electrical systems in more detail (section 5.6.10.2), the following section will introduce the general electrical layout of a unit of a fifth-generation power station.

5.2.1 Tripping: A Unit Perspective

Although tripping can be understood or conceptualised at various levels of abstraction, it is commonly interpreted (or meant to be understood) at the level of electrical supply to the equipment, plant, system, or unit. Therefore, in this section, the concept of tripping will be considered specifically regarding a unitised electrical reticulation system of a fifth-generation power station.

Specifically, when electrical switching devices are considered, tripping invariably means opening a switching device, thereby disconnecting a part of a circuit. The opening of the switching device could be initiated manually (by human intervention), by an automatic control system, or automatically by a dedicated protection device.

Figure 28 shows a very high-level schematic layout of a unit's electrical reticulation system. Some predominant components forming part of the system are identified using typical (South

African) terminology. Blue arrows represent the normal flow of electricity when the unit is in operation.

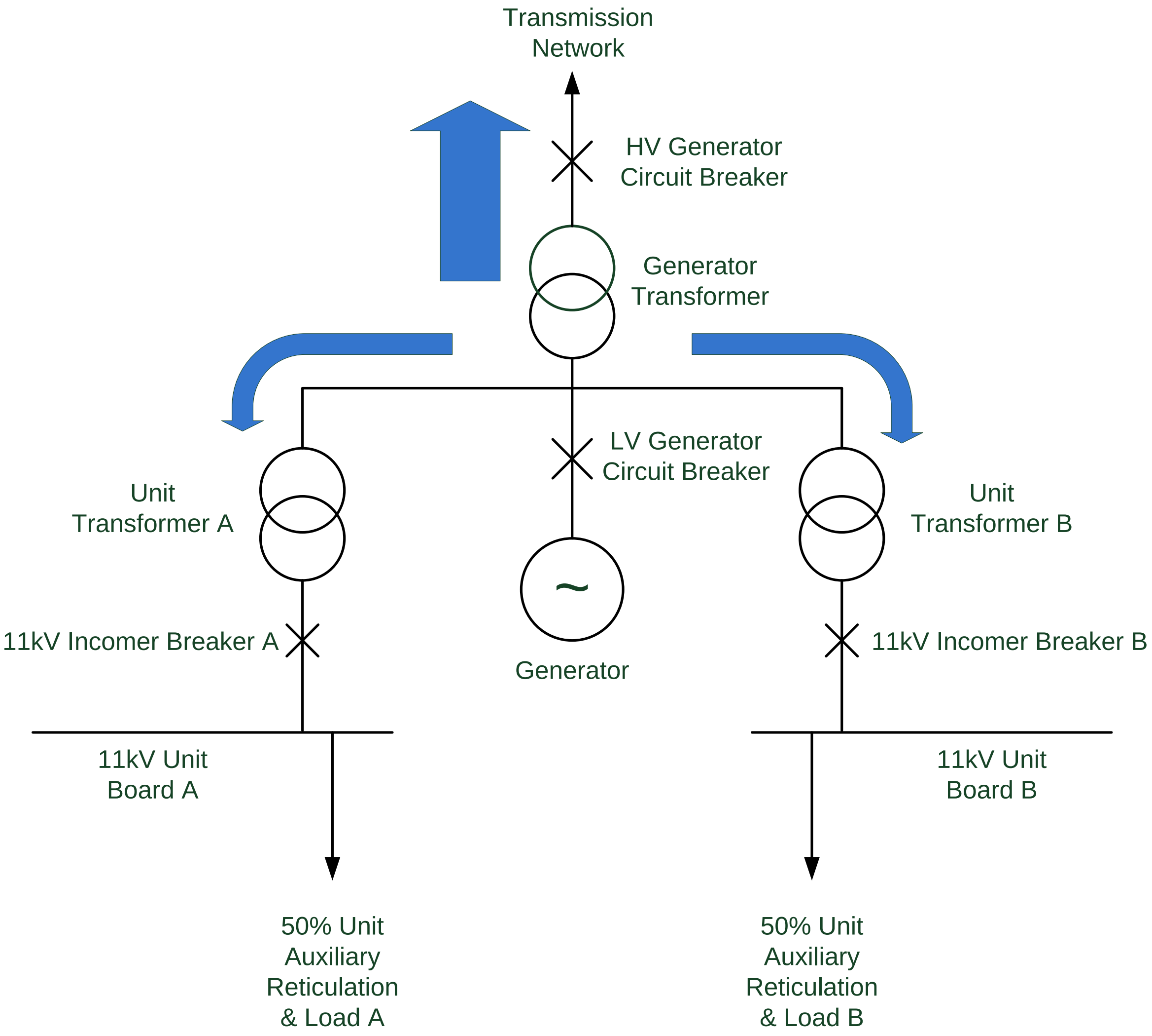


Figure 28: High-level schematic electrical reticulation system of a unit

As can be seen from the illustration above, the unit auxiliaries can be divided into two separate streams or systems (an A and a B stream in this case) – each capable of sustaining about 50% of the unit function. Assuming, as an example, that the supply system to the B-set of unit auxiliaries trips, the remaining auxiliaries will only be capable of supporting 50% of the unit output, and the unit will rapidly transition to the new state of operation, referred to as a half-load operation. Under these circumstances, the schematic will change to the following state (shown below).

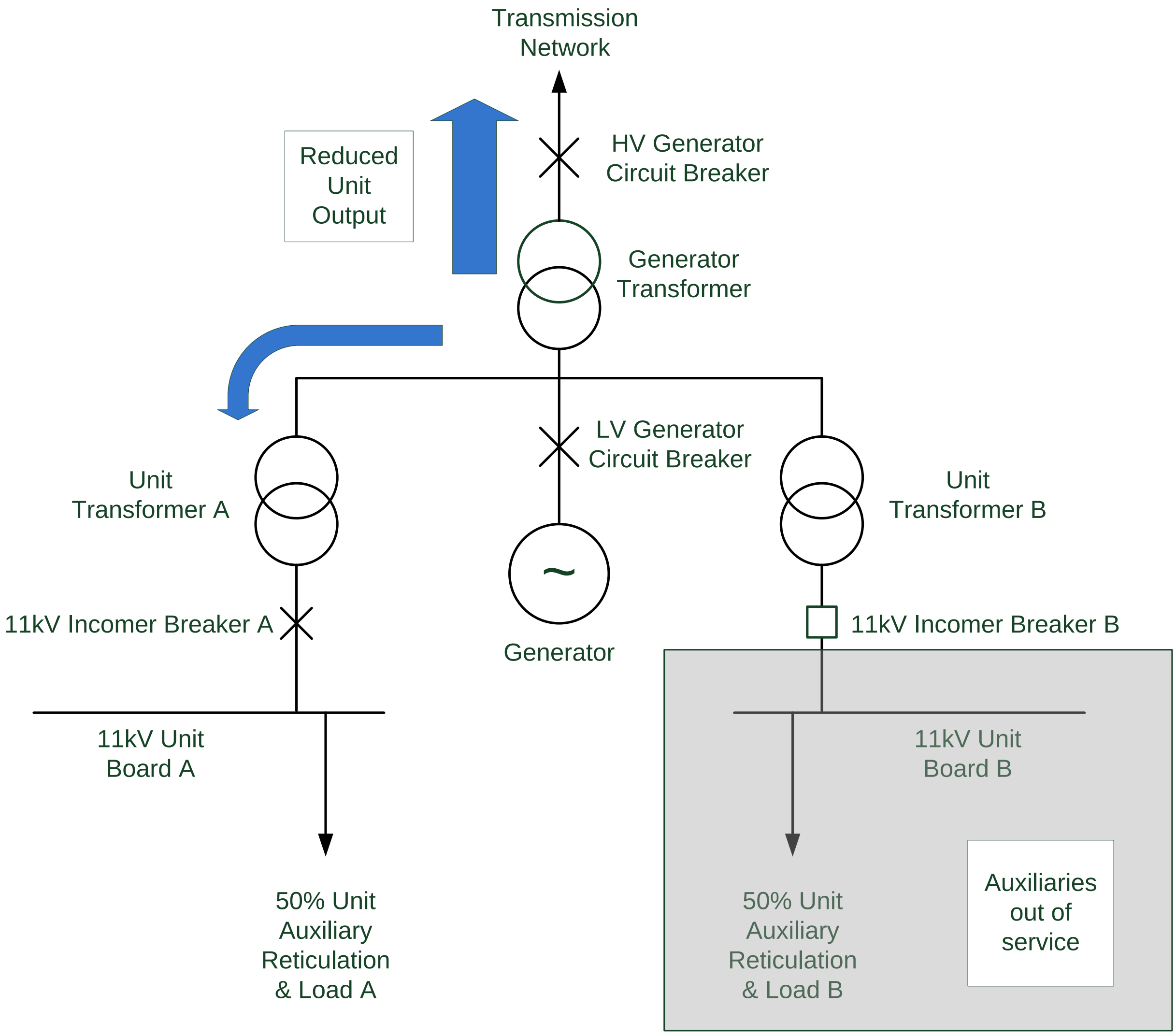


Figure 29: Unit in half-load operation – 50% auxiliaries tripped

In this first example, a trip of 50% of the unit auxiliaries disrupted in unit output matches precisely the loss in auxiliaries – that means that the unit suffered a loss in output that renders the unit capable of only producing half of its capacity.

As another example, assume that the unit protection system comes into operation and causes the LV generator circuit breaker to trip. To illustrate this example, the schematic reticulation diagram has been augmented, as shown below.

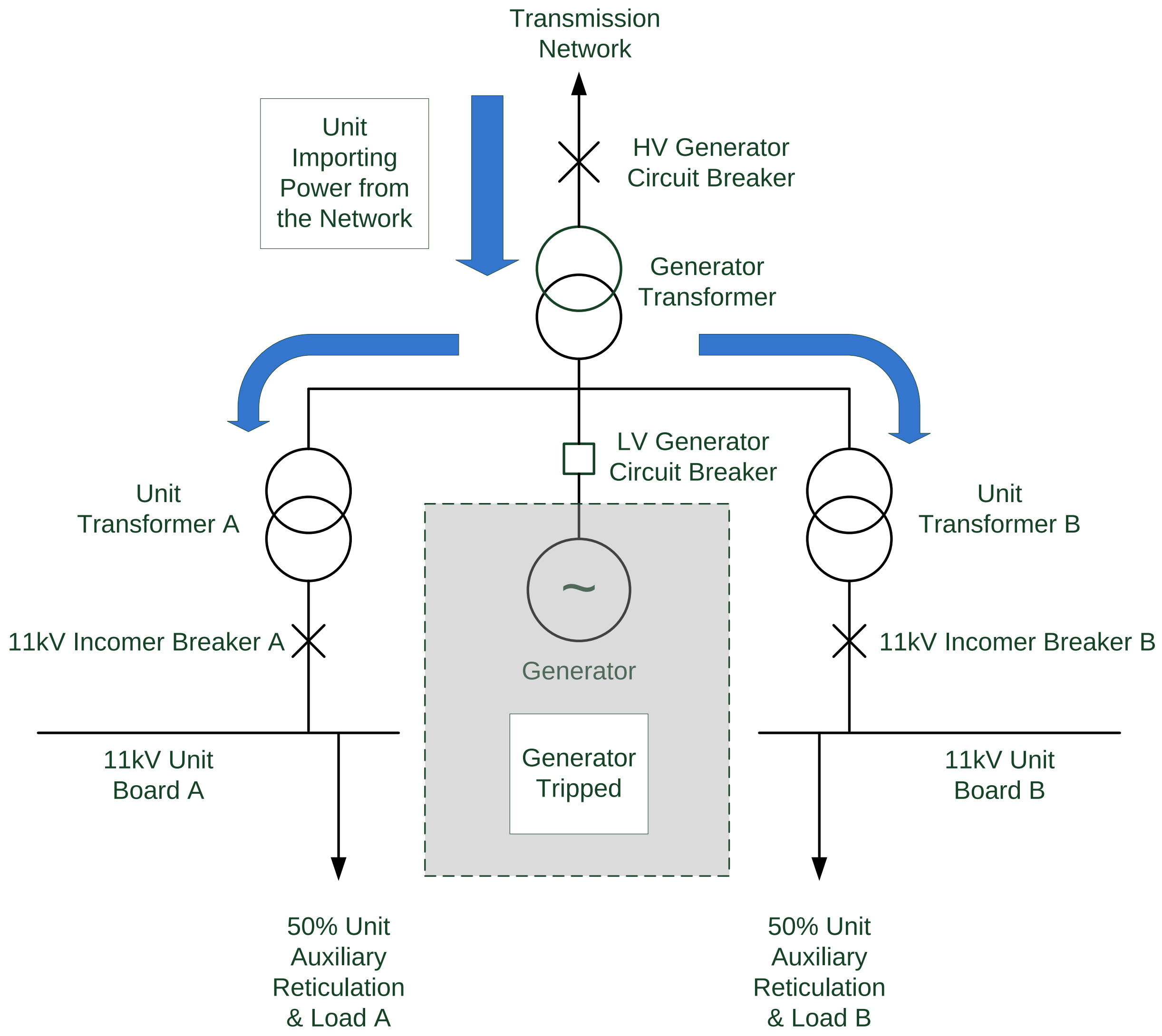


Figure 30: Tripped generator – Unit back-energized (importing power from the network)

This latest example can be regarded as the default method whereby a unit typically trips, representing most unit-tripping events. This default tripping will occur for all fault conditions arising from the turbine, generator, boiler, losses in unit auxiliaries and even manual unit tripping. There are, however, other modes of tripping that will be dealt with in later sections (refer to section 5.4.5).

From the preceding two examples, it is clear that the concept of a trip, although similar in general meaning and understanding, is different in terms of the extent of the disruption. It is, therefore, critical to understand the context of what is being referred to when the term *"trip"* is used.

5.3 The Functional Structure of Power Stations

Power stations, the predominant source of bulk electricity in large power systems, are used to convert some form of energy into electricity. For this purpose, it consumes various resources and commodities and generates various streams of waste, services and materials that have economic value. A visual representation of the input and output streams is shown in the following illustration.

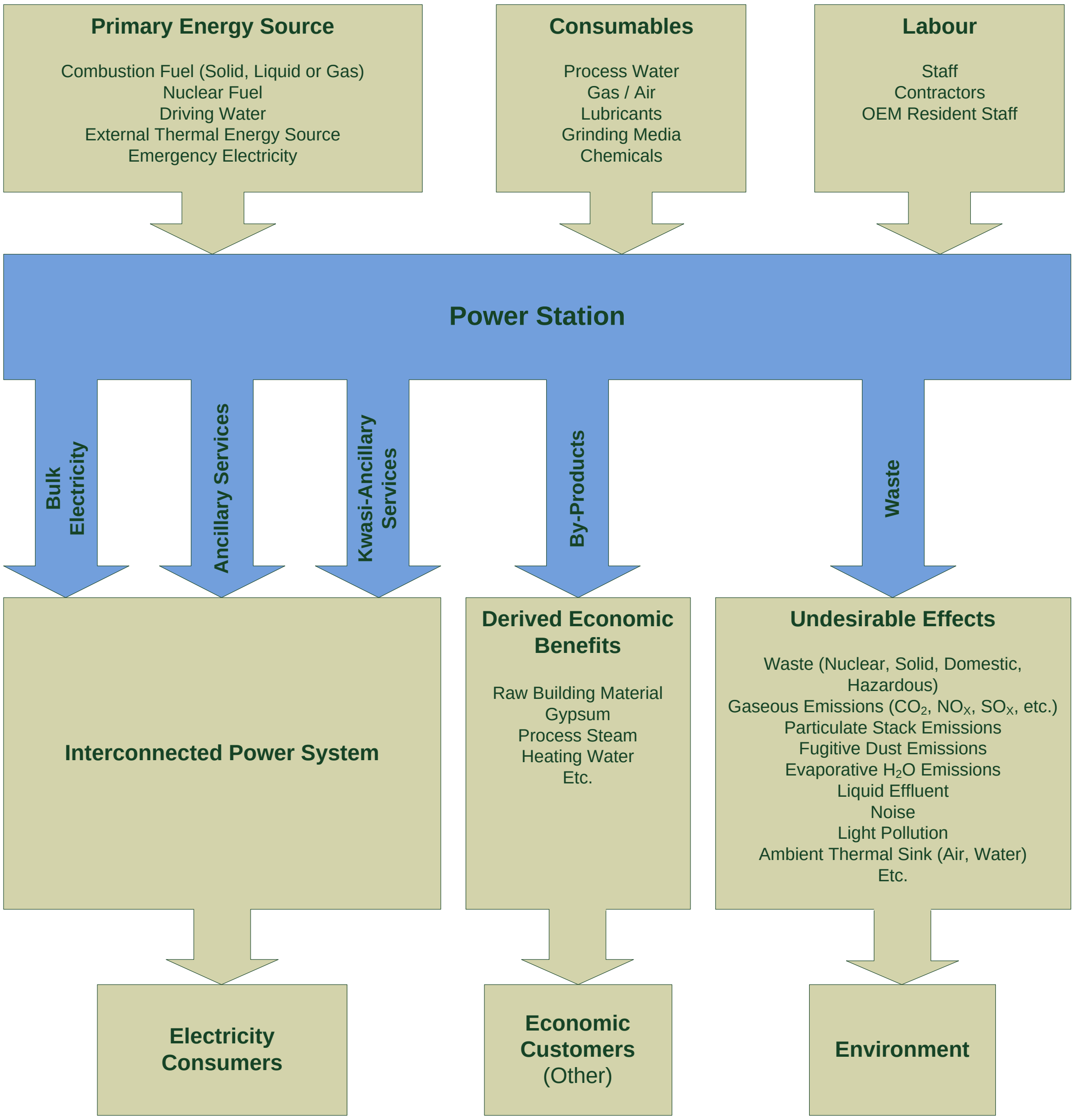


Figure 31: Generic inputs and outputs of a power station

Although earlier generations of power stations had an overwhelming degree of functional overlap between *generating sets*, the fourth-generation power station introduced the concept of *generating units*, boasting a deliberate design effort of avoiding (or at least minimising) interdependence between generating units, as well as the co-dependence of generating units upon shared and common resources and systems. This concerted effort to enhance independence was instituted to reduce the likelihood of adjacent units becoming compromised due to a disruption occurring in one unit. This approach largely limits power station disruptions to unit-sized increments – a loss increment that a power system can readily tolerate without significant upset.

Unitisation cannot be applied to every function and system required at a power station, for example, a coal-fired power station with six units cannot have six mines, each dedicated to a specific unit. Some functions and systems are inherently standard, and although redundancy can be designed into such systems, they cannot be unitised. In other words, it is simply not viable for a one-to-one relationship between the units and those functions and systems that are inherently common. A certain degree of interdependency between units and co-dependency upon common and shared systems is inevitable.

In this respect, the following illustration visually represents a power station, showing the interdependencies and co-dependencies of the generating units and the common plant.

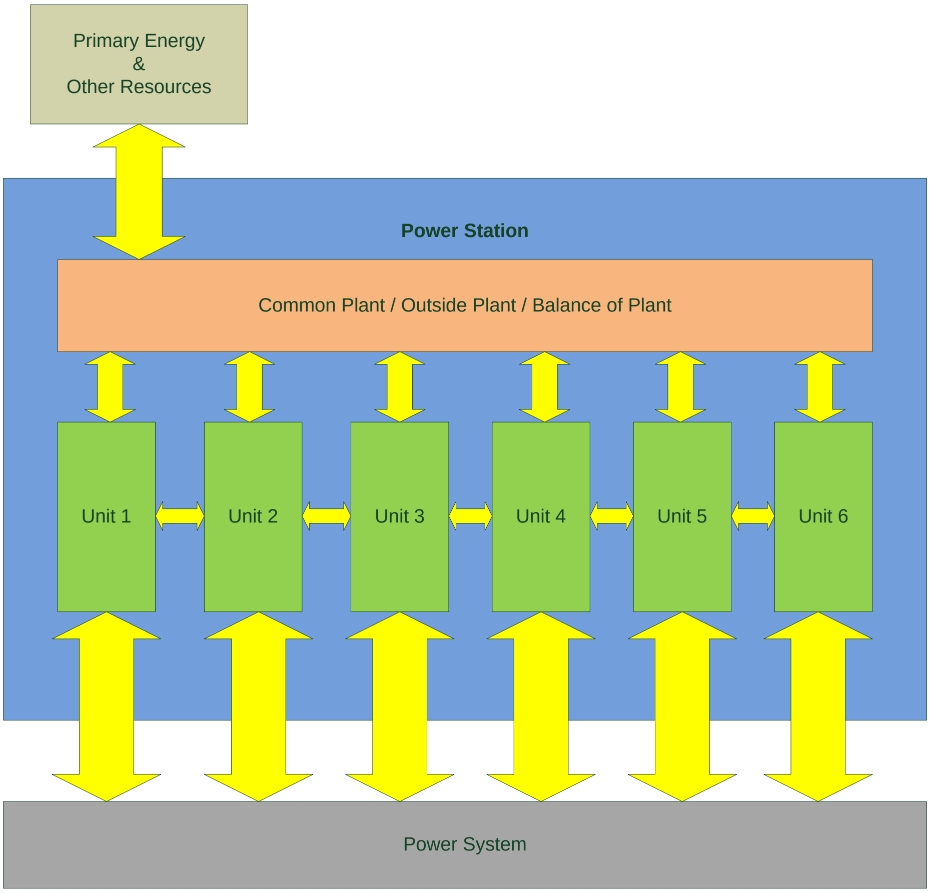


Figure 32: Interdependencies and co-dependencies of a typical multi-unit power station

The yellow arrows in this illustration show dependencies within most power stations. The vertical arrows signify co-dependencies upon non-unitised functions and systems, whereas the horizontal arrows show interdependencies between units. The number of six units in the illustration has no significance and is merely shown since six is the median number of units found in the South African fleet of large power stations.

With the adoption of the unitised concept in the fourth-generation power stations, an increasing degree of emphasis has been placed on a diminishing interdependence between units, conceptually eradicating it. However, this ideal of “zero interdependence” proved more elusive in reality than in theory. The only power station within the Eskom fleet that has largely attained this lofty goal is Koeberg Power Station, where nuclear safety was the driving force for making the requisite "over"-investment to achieve independence between units – and merely because zero interdependence is the international norm for nuclear power stations. The fact that Koeberg Power Station only consists of two units also aided in achieving this ideal.

However, although deliberate design effort reduces the degree of interdependence between units, far less effort goes towards deliberately reducing the co-dependence of units upon shared systems, resources and infrastructure. For example, even Koeberg Power Station has various co-dependencies of the units upon common systems at the power station, e.g., the HV yard, hydrogen generation, the oceanic heat sink, etc.

5.3.1 The Functional Structure of a Generating Unit

The plant, equipment, devices and systems that comprise modern units and power stations can functionally be classified into five groups, namely:

- Primary
- Secondary
- Auxiliary
- Ancillary
- Emergency

Although some equipment could share membership of more than one group, the predominant function of any installation at a unit or power station could be fitted into one of these five groups. The distinction between the five groups is outlined in the following table.

TABLE VI: FUNCTIONAL CLASSIFICATION WITHIN POWER STATIONS

Classification	Description
Primary	Plant, equipment and systems are the main and predominant components in the functional chain of converting energy into electricity.
Secondary	Plant, equipment and systems process electronic signals (binary or analogue) within any part of the operational aspects associated with power stations for control, protection, monitoring, measurement, metering, communication, data recording, indication and alarming.
Auxiliary	Plant, equipment and systems are required to directly support the primary energy conversion installations – unitised and common.
Ancillary	Plant, equipment and systems that are not directly required for the generation of electricity but are indirectly necessary.
Emergency	Plant, equipment and systems that are required to safeguard plant and personnel during abnormal conditions when normal operating envelopes for sustained energy conversion become compromised or when normal operation is not possible.

To demonstrate the use of the above classification, it is applied to a typical coal-fired power station and a unit of a coal-fired power station. The following tables list typical plant, equipment, and systems in the different classifications on both a unitised and power station level.

TABLE VII: PRIMARY PLANT, EQUIPMENT AND SYSTEMS

Unitised	Shared between Units
Boiler	Geographic site location
Turbine	Main civil structure
Generator	Main fuel source supply system
Generator transformer	Main water source supply system
Generator circuit breaker	Main waste sink or containment system

For these primary plant components, the following auxiliaries typically need to exist on a unitised and power station level respectively.

TABLE VIII: AUXILIARY PLANT, EQUIPMENT, INSTALLATIONS AND SYSTEMS

Unitised	Shared between Units
Boiler	**Boiler**
• Mills, classifiers, feeders and burners • Draught groups • Air heaters • Sootblowing system • Water circulation pumps • Electrostatic precipitators and SO_3 • Fabric filter plant • NO_X and SO_X mitigation	• Coal storage and conveyors • Ash conveyors and dumping • Fuel oil storage and pumps • Ignition gas storage • Demineralised water plant • Sulphur handling and storage • Fly ash bunkers and handling • Compressed air • Common steam range • Donkey-boiler steam supply • Smoke stacks
Turbine	**Turbine**
• Feed water pumps • Cooling water pumps • Condensate extraction pumps • Condensate heaters and pumps • Hydraulic oil pumps • Lubrication pumps	• Cooling towers, centre well and ducts • Raw water handling and storage • Chlorine electrolysis • Nitrogen plant
Generator	**Generator**
• Hydrogen cooling system • Seal oil system • Stator coolant system • Excitation system • Generator circuit breaker • Generator transformer and auxiliaries	• Hydrogen electrolysis and storage • Auxiliary cooling water system

Other	**Other**
• Unitised reticulation	• Water and chemistry management • Common reticulation • Earthing system

Secondary systems that are commonly found at power stations include:

TABLE IX: SECONDARY PLANT, EQUIPMENT, INSTALLATIONS AND SYSTEMS

Unitised	**Shared between Units**
• Control systems • Communication interfaces • Field instrumentation • Control rooms and control stations • Automatic voltage controllers • Protection and lock-out • Interlocking • Synchronization • Substation automation • Bright and dark chop-overs • Fault and disturbance recording • Condition monitoring • Variable speed drives (VSD) • Data recording and archiving • Alarming • GPS clocks	• Control systems • Communication interfaces • Field instrumentation • Control rooms and control stations • Protection and lock-out • Interlocking • Substation automation • Bright and dark chop-overs • Condition monitoring • Variable speed drives (VSD) • Data recording and archiving • Alarming, sirens • Environmental monitoring • Building management • Radio and telephone communication • LAN and WAN systems • Interfaces to power system control • GPS clocks

Ancillary systems that are commonly found at power stations include:

TABLE X: ANCILLARY PLANT, EQUIPMENT, INSTALLATIONS AND SYSTEMS

Unitised	**Shared between Units**
• Elevators • Maintenance-power outlets • Unitised lighting • Ventilation and air conditioning	• Elevators • Cranes and hoists • Common area lighting • Security and perimeter fencing • Storm water control and drainage

	• Road and rail access • Stores and spares management • Maintenance workshops • Admin buildings and offices

Emergency systems that are commonly found at power stations include:

TABLE XI: EMERGENCY PLANT, EQUIPMENT, INSTALLATIONS AND SYSTEMS

Unitised	**Shared between Units**
• Smoke extraction systems • Emergency lighting system • Diesel generators and auxiliaries • Unitised DC and UPS supply • Hydrogen emergency venting • CO_2 fire suppression systems	• Fire detection systems • Fire suppression systems • Common diesel-driven equipment (compressors, generators, fire pumps) • Medical and fire station • Helicopter landing site • Aircraft warning lights (smokestacks) • Public address system and sirens • Emergency control centres

Certain plants and components comprising a unit have a complicated relationship between its sub-components and the unit's output. The following diagram represents a typical coal boiler and indicates some of the sub-systems that determine the unit's output.

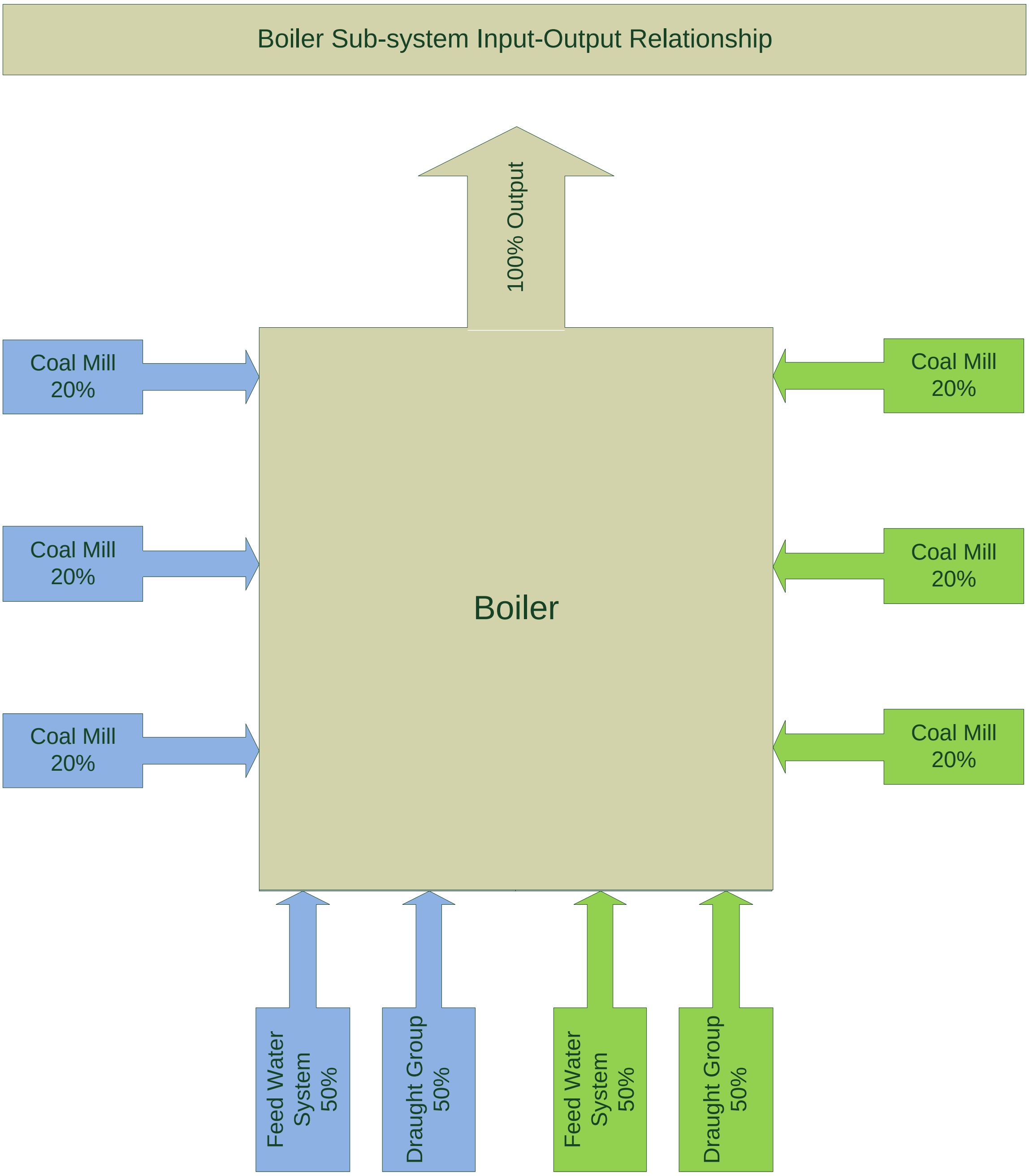


Figure 33: Unit output dependencies for typical boiler sub-systems

The diagram shows three sub-systems of a 600 MW boiler, namely *feed water supply*, *draught plant* and *milling plant* – each of which can be broken down further. In the illustration of a boiler, it can be seen that the loss (or introduction) of a mill of the boiler represents a relatively small output increment, typically between 15% and 25% of the unit's rating. However, the loss (or introduction) of a feed pump or draught group represents a 50% implication on the output of a unit.

This type of design is typical of international boiler design. It shows a deliberate design strategy to achieve, in part, a level of redundancy to enhance the unit's reliability or, more accurately, the output from the unit. It, therefore, follows that the failure of one of the sub-systems of a primary plant would not result in the total loss in output from the generating unit but rather a fraction thereof. This approach would, therefore, mitigate the effect that internal disruptions within a unit would have on the power system to which it is connected.

5.4 Limiting the Consequences of Unit Disruption Events

Generating electricity often involves a large number of interdependent processes. A disruption in one process would, therefore, normally cause an internal cascade of disruptive effects rippling through various systems and processes and threatening the continued operation of the unit itself.

To mitigate the risk of compromising an entire unit due to a disruption of one part of the process, the unit's design has been adapted to provide internal redundancies. Therefore, the generation process has been implemented, not using single systems but redundant systems sharing the total burden demanded by the process. The unit's generation process is collectively achieved by various redundant systems that share the overall burden.

Modern (fifth-generation) unit designs divide the process into two separate systems – each capable of delivering about half the process requirement. Each system can operate independently in isolation from the other, rendering the process capable of 50% output when used without its redundant counterpart. Except for primary plant components, like the boiler, turbine, generator, and generator transformer, the other systems that enable the generating process to function are duplicated, and the processing burden is shared equally between the duplicate systems.

For example, the feedwater system that maintains the water level inside the boiler is divided into two systems, each comprising its pumps, motors, piping, valves, instruments, etc. This is done so that a failure of one of the two systems would merely cause that single system to shut down. In contrast, the other system would remain in operation, thereby enabling the unit to remain in operation, albeit at half the production rate.

The following diagram shows a typical conceptual layout of a coal-fired generating unit, including some of the major duplicated systems.

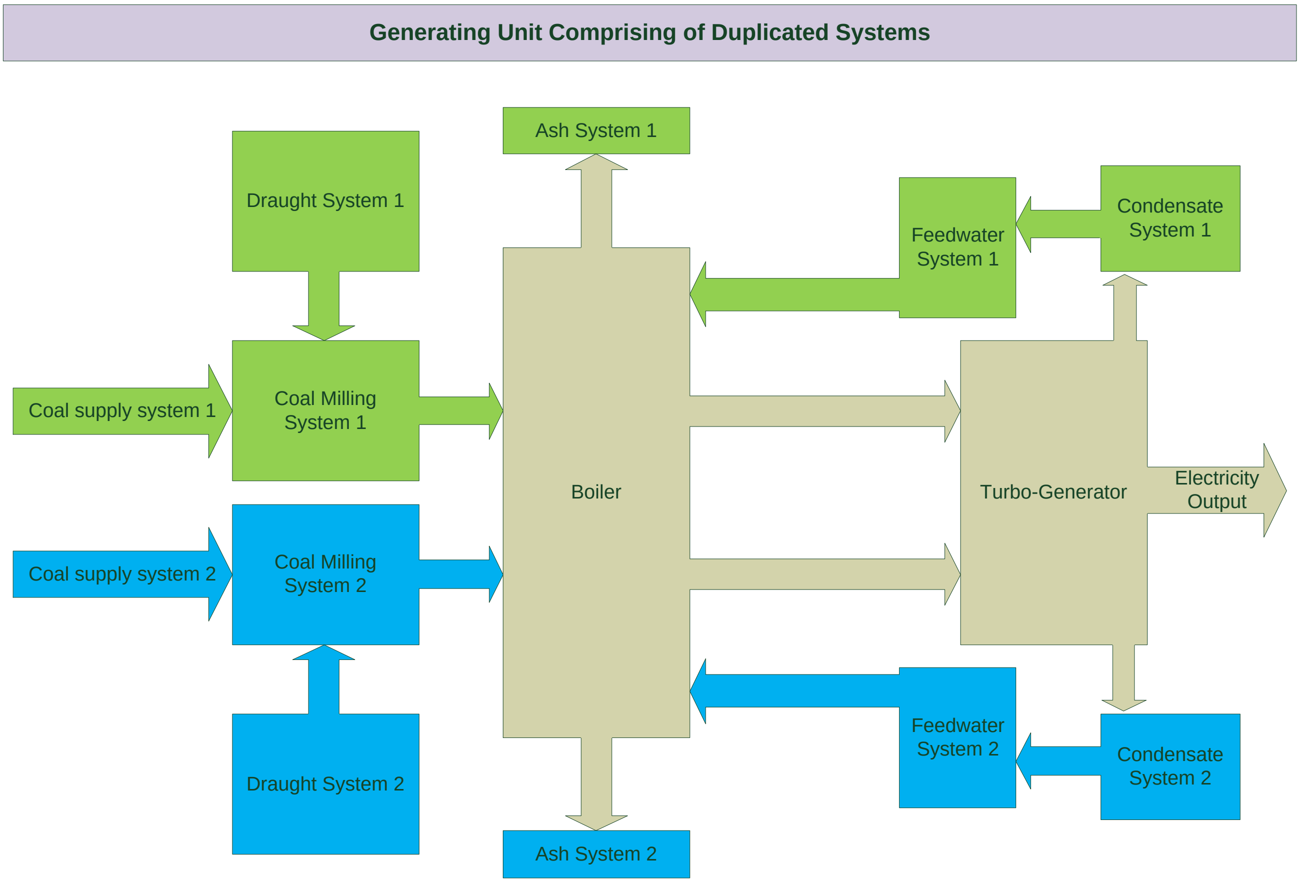


Figure 34: Duplicated systems approach of a coal power station

5.4.1 Intra-Unit Redundancy

Operationally, any disruption event at a power station should be limited to not more than about half of its units [1]. Therefore, large South African power stations are designed to limit disruption events either to single units (in terms of interdependencies between units) or to half of the units at the power station (in terms of the co-dependencies of units upon common systems and resources).

One of the implications of the design objective to limit the participation of units during disruption events is the need to avoid cascading from occurring. Therefore, a generating unit that is required to disconnect from the power system should perform the disconnection without exposing other units to the adverse effects that may have led to this initial unit becoming compromised. Any internal fault condition that necessitated the initial disconnection should, therefore, be arrested promptly – limiting adjacent units from prolonged exposure to the problem and not becoming the trigger for another unit to become disrupted.

As stated earlier, power stations are comprised of many systems that fulfil specific functions – the various systems support generating electricity. Systems, in turn, consist of a conglomeration of equipment and devices that are all connected in one way or another. The failure or malfunction of any of the components of a system may cause the system to fail or shut down. Such a loss of a system is often one of the incremental progression steps in disrupting a generating unit.

A unit should be resilient enough to generally withstand faulted systems and prevent faults from forcing a unit to disconnect from the power system. For this reason, many systems and components have built-in redundancy to enhance the unit's reliability, even when failures occur.

The first level of redundancy is a 100% backup with a full stand-by plant or systems that can be brought into operation by manual or automatic means without impacting the unit's electricity production. A second tier of redundancy designed into new power stations removes faulted plant or systems from operation but with a net effect of reducing (or limiting) the production capability of the unit by a certain percentage.

These redundancies result in units remaining in operation under faulted conditions without disconnection from the power system, alleviating the adverse consequences that internal unit faults may otherwise have on a power system. However, certain components and systems may not allow for the implementation of redundant methodologies, such as primary plant components like the steam turbine or main generator (see section 5.3.1). Faults that occur in such systems will, therefore, always result in an actual disconnection from the power system.

The following table illustrates the typical redundancy level for modern generating units in the 600 MW to 700 MW range.

TABLE XII: TYPICAL REDUNDANCIES WITHIN POWER STATIONS

Plant or System	**Redundancy Profile**
Boiler coal milling system	5 out of 6 mills are required for MCR – a unit can run on a single mill if required – manual starting
Turbine condenser	1 out of 2 can maintain the unit at ½ load
Condensate extraction system	1 out of 2 pumps are needed during operation – automatic starting
Fire-resistant control fluid system	1 out of 2 pumps is needed for unit operation – automatic starting
Boiler draught system	2 sets of 4 components each are both required for MCR – unit can operate at ½-load with 1 set

Boiler feed water system	2 out of 3 pump sets required for MCR – a unit can operate at ½-load with 1 set – automatic starting
HP-heater drainage system	1 out of 2 pumps is required for each of two separate HP heaters to be in service – a unit can operate at ½-load with 1 HP-heater – automatic starting
Auxiliary cooling system	2 out of 3 pumps are needed during operation – automatic starting
Secondary cooling	1 out of 2 pumps are needed during operation – automatic starting
Turbo-generator lubrication oil system	1 out of 2 pumps are needed during operation – automatic starting
Generator H_2 containment system	1 out of 3 (2 AC and 1 DC) pumps are needed during operation – automatic starting
Generator stator cooling system	1 out of 2 pumps are needed during operation – automatic starting
Generator excitation system	1 of 2 channels are required for the unit to remain in operation
Electrical reticulation system	2 sections are both required for MCR – a unit can operate at ½-load with 1 section
Generator protection system	1 out of 2 systems is required to be operable for the unit to remain in operation
Generator circuit breakers	1 out of 2 can effectively disconnect a unit from the power system under fault conditions (one LV and one HV)
Fly-ash electrostatic precipitation system	4 banks are required for MCR to remain within the environmental license – a unit can operate without any if required (violating license requirements)
Boiler water circulation system	2 out of 3 pumps are required to be operable for the unit to remain in operation

Although control systems have also been implemented according to redundancy principles, their profiles are too complex to show in TABLE XII. The only other major unitised system that is not shown above is the main cooling system which has been a significant cause of multiple unit trips in the South African fleet of large power stations spanning decades. It will be dealt with in more detail in section 5.6.7.

5.4.2 Functional Allocation

From the previous section, it is clear that system redundancy can effectively mitigate a unit's disruption caused by equipment failure. A standby or backup plant may often take over the function of failed equipment with minimal disruption.

This approach cannot be applied to every single component comprising a generating unit – redundancy on the primary plant is excluded in terms of unit design (by definition), see section 5.3.1. For example, consider a boiler in a coal-fired unit. It is inconceivable that a unit would be equipped with a separate backup boiler, requiring a complete doubling up of all the boiler auxiliaries. If such an investment would be considered, the additional boiler with its auxiliaries would rather be used for an additional unit that can be operated in conjunction with the other units, maximising the return on that part of the investment.

In a typical large South African power station, the following components are generally not duplicated by some form of stand-by or backup.

- Boiler and internal heater structures (reactor and steam generator for nuclear)
- Main boiler and turbine civil structures (reactor containment structure for nuclear)
- Coarse ash (bottom ash) removal system
- Steam or gas turbine (Francis turbine for hydro)
- Generator
- Isolated busbar system for generators
- Exciter (rotating machine or excitation transformers)
- Generator transformer
- Essential (emergency) AC auxiliary board
- Switchgear rooms
- Equipment room (industrial electronic systems – typically for control and protection gear)
- Unit control room
- Flue gas chimney

This list is reasonably universal for power station units internationally, although exceptions are not uncommon. As an example of deviating from this approach, a generating unit at Chernobyl nuclear power station employs two 500 MW turbo-generators with each unit, which together would generate 1 000 MW from the steam produced by the reactor. The combined electric power would, however, be stepped up to grid voltage by a single generator transformer shared by the two generators.

Also, earlier power stations operated by Eskom (or the VFP) featured more than one chimney per boiler, as opposed to a single flue, which is the current standard. Another example of an approach that changed over time is some of the early fourth-generation power stations (presently still in service), where even the unit transformers are part of the list above.

Even more alien (in modern designs), the third-generation power stations had more boilers than turbo-generators, using the concept of generating sets instead of generating units (see section 2.1.2). These examples merely illustrate that the current reality (regarding power station design) does not remain fixed and could be expected to evolve.

Mostly, though, the other functional systems of a unit (those not listed above) are not primary systems, e.g. auxiliary systems are comprised of sets of cooperative equipment that are collectively capable of achieving 100% of the function while individually only being capable of fulfilling a fraction of the required overall function. Almost all auxiliaries exist as two or more systems, each contributing to its total functional requirement.

The reason for not having single systems but fractionated systems instead is deliberate and done to elevate the overall generating unit's reliability and resilience. Therefore, unit auxiliaries are designed so that a failure of any one of its constituent systems would not cause the unit to be entirely compromised but rather to enter a state of reduced production while remaining in service and connected to the power system. Implementing auxiliary functions through fractionated systems instead of single-entity systems provides the second principle for enhancing unit resilience.

When an auxiliary system component does fail, only the system of which that component forms part will be affected and may become unavailable. The other systems that are cooperatively sharing the burden of the function that they are collectively required to fulfil, will continue to function – thereby still fulfilling the specific function, at least partially. With the unit being designed to assume a reduced state of production and the healthy auxiliary function provided by the remaining systems, the unit does not require shutdown. It could remain in service at a reduced output level. This benefit does not merely enhance the unit's resilience but also reduces wear and fatigue by avoiding high thermal cycling associated with shutdown and restart, saving consumable resources such as fuel oil, demin water, etc.

Although this design feature appears to be simple, it is quite onerous and requires much design effort, upkeep, and ongoing verification to ensure that the requisite investment in resilience is not wasted or eroded over time. To gain insight into the implications of such an approach, consider once more the much reduced and simplified conceptual system duplication diagram for a generating unit presented earlier (Figures 33 and 34).

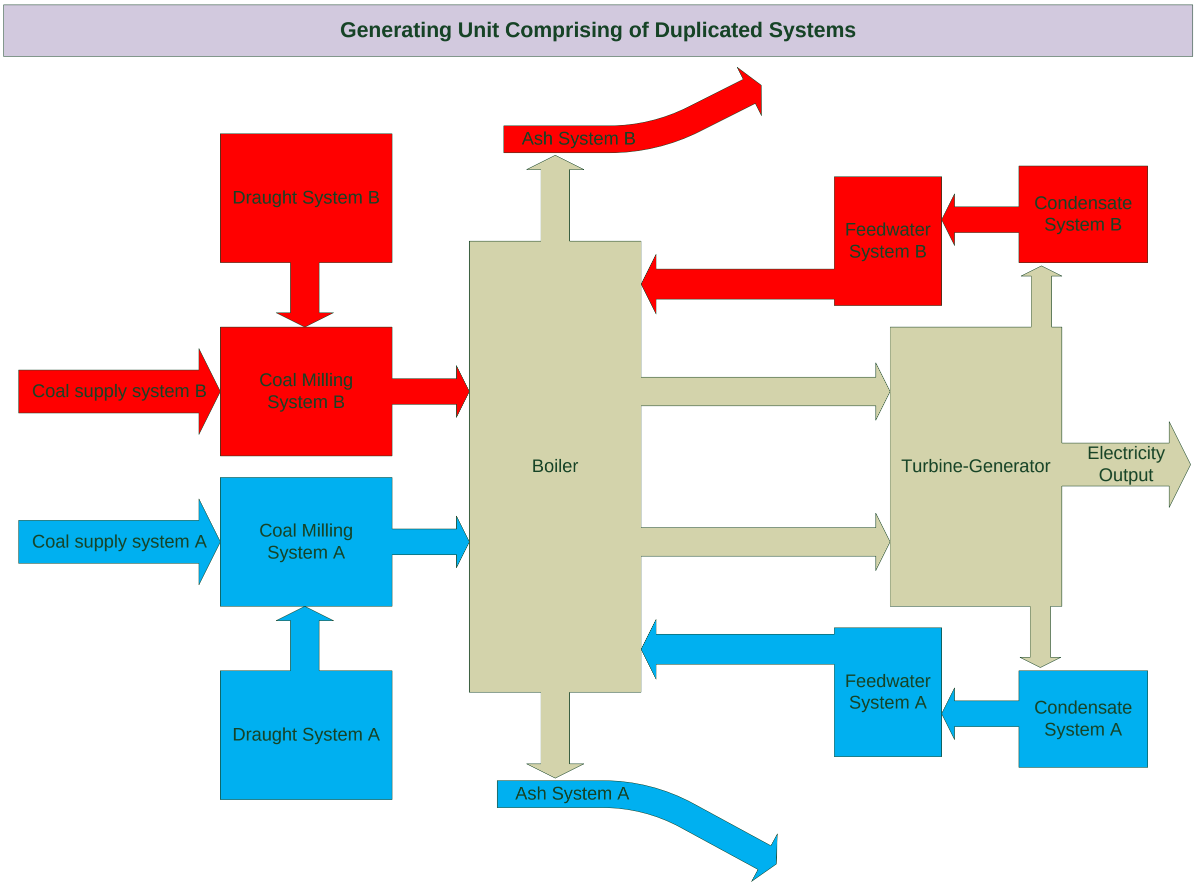


Figure 35: Duplicated systems approach of a coal power station

In this simplified example, the auxiliaries for a unit have merely been divided into two systems per function. As an example, from Figure 35, the coal milling function (as every other auxiliary function shown) has been divided into only two systems – system A (blue) and system B (red). This is deliberately being pointed out since the milling function of a typical large generating unit consists of six rather than two systems, and this simplification is also true for various of the other auxiliaries of a generating unit. However, the two-system simplification will suffice to illustrate this aspect of unit resilience.

Most systems shown can readily be visualised as consisting of many physical components, such as pumps, fans, motors, pressure vessels, conveyors, piping, hydraulics, compressors, servo actuators, valves, pneumatics, etc. What is often not immediately apparent is that all systems also require power (typically from an electrical source) and control and instrumentation (C&I), functions for automation, monitoring and protection. These power supply and C&I interfaces originate from elsewhere in the unit and are merely connected to the system through wiring, fibre optics, radio signals or piping. And because of the central nature of the electrical power reticulation system and the C&I system, it presents yet another inherent vulnerability of causing a failure of both system A and system B simultaneously if either the power or the control aspect of these two systems become compromised centrally.

For the fractionated systems to be truly independent of one another, they also may not be collectively co-dependent on another system that itself may become compromised. This requirement for the fractionated systems to be independent of one another as well as independent of any other systems creates the need to also fractionate the electricity supply system that powers the auxiliary systems of a unit. This is achieved by not only fractionating the auxiliary functions into fractional independent systems (system A and system B) but also fractionating the power reticulation system along similar principles, as illustrated in Figure 36.

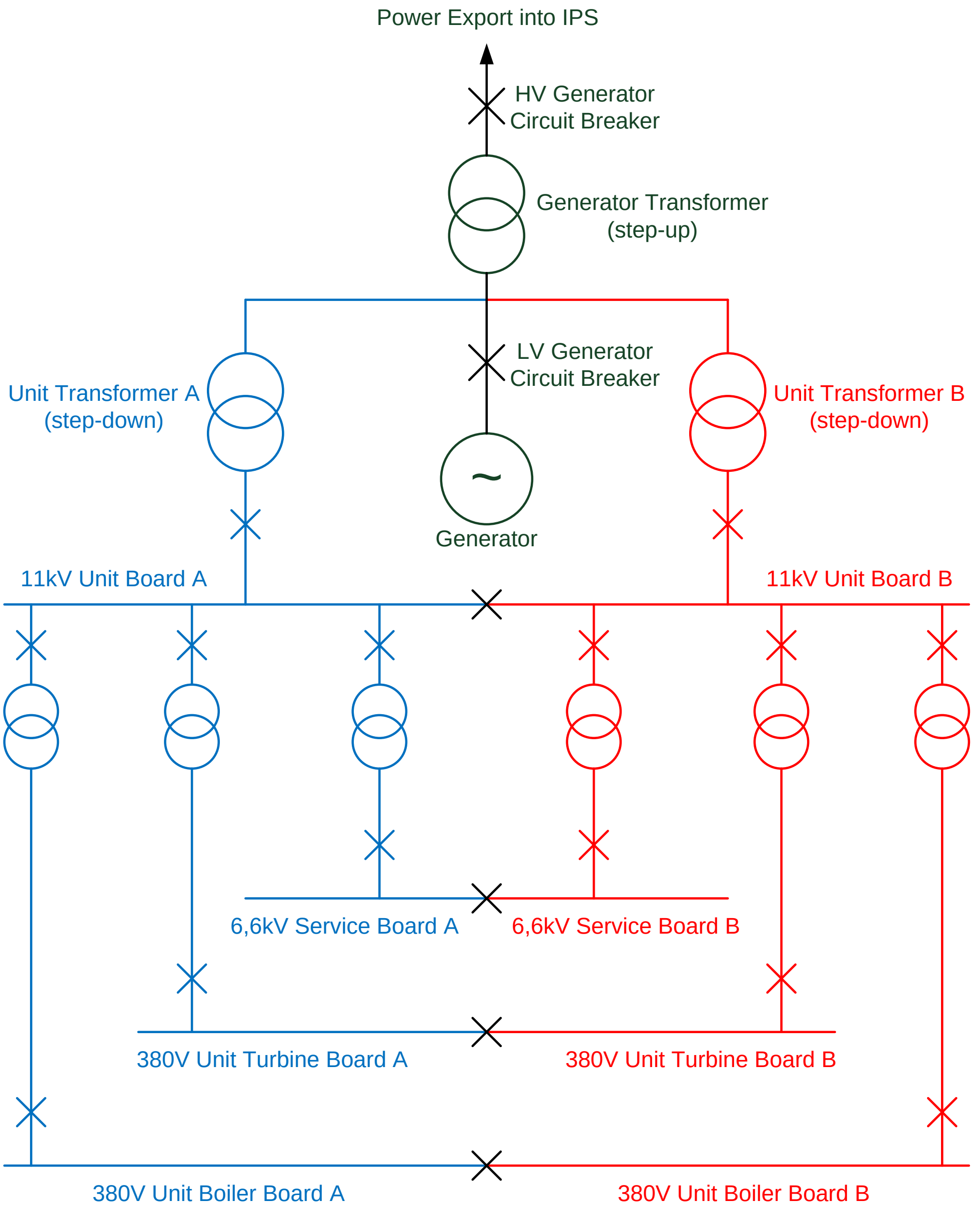


Figure 36: Fractionated unit electrical reticulation system

It can be seen that the power supply to the unit auxiliaries is supplied by two unit transformers, A and B, that are independently powering two sets of reticulation systems, A and B. Therefore, the functional allocation of the unit needs to remain consistent with the principle of dividing the unit into two sides, side A and side B. An A-system, say feed-water system A, therefore, needs to be powered from an A-board in the electrical reticulation system of the unit, and conversely for side B (*mutatis mutandis*).

Furthermore, the black circuit breakers (Figure 36) between the A-boards and the B-boards are referred to as bus-section breakers and provide yet another feature for enhancing resilience. Specifically, it provides a means to supply both the A and B boards from a single source, thereby creating the opportunity to perform maintenance or temporarily tolerate a failure (until the necessary replacement of equipment can be undertaken to return to the default configuration once more).

To achieve similar results of system independence to the control system, a corresponding approach is used to design the control infrastructure. The approach is identical regardless of the specific technology used (hard-wired, PLC, DCS or IED). All aspects of control and instrumentation for an A-system, incoming or outgoing signals, as well as any control algorithms, logics, interlocking, protection, etc., cannot be mixed within hardware devices that also contain similar elements of B-systems, and vice versa. Whether it is communication modules, processors, repeaters, I/O modules, etc., the A-system control must be kept separate from the B-system control at every level, including the power supplies to the control equipment.

The functional allocation is of utmost importance in ensuring that a unit achieves a sufficient level of resilience. Every fractionated system needs to be allocated to a side (A or B) and then kept exclusive to the allocated system in every respect, mechanical, electrical, control, etc. When a unit is returned from maintenance, the independence of the systems is verified by physical demonstration testing, referred to as capability testing. Such testing assures two very specific aspects, i.e.:

a That the functional allocation has been maintained throughout all systems, failure of which will mechanistically lead to an inability to operate the process and subsequent tripping of the unit when disruption sets in.

b That the control systems have been sufficiently optimised so that the unit can survive the transient of operating with two sets of systems (as an example), to instantly being forced to transition to a single system. This is onerous on a unit and will inevitably cause the unit to become unstable and to trip, unless the relevant control loops have been optimised individually and collectively to produce the required result.

Such a demonstration test will typically involve the following. In the case where, say, the draught group capability is to be demonstrated, the unit will be taken to a stable operational condition before one of the fans, for example, the ID fan A, will be tripped manually. The control system needs to recognise the condition then and firstly perform a gang-trip (or group-trip), meaning that it needs to trip all other components that form part of that group – in this case, it will include FD fan A, PA fan A, and all mills (and mill auxiliaries) that are reliant on draught group A. The draught group that has now been taken out of service disrupted the air management within the furnace of the boiler. Since the entire combustion process operates within an envelope of parameters that ensure the correct and safe operation (e.g., the air-fuel ratio), the fuel must be adapted for the new airflow conditions of the remaining draught group. Therefore, secondly, the capability computer needs to match the energy input to the new requirement by removing the correct number of mills by tripping them so that the air-fuel ratio can be restored – mitigating the risk of an explosive mixture being created internally in the furnace. Thirdly, the analogue control loops need to effect a great many changes to various controllers to reduce (or adjust) physical quantities to prevent any process parameter from exceeding any safety limit or plant capability and thereby activating the protection that would cause further tripping – potentially precluding the possibility of saving the unit. In addition, the control system needs to affect all requisite lockouts and correctly bring about the necessary isolations for airflow pathways to ensure safety. The test would be successful if all the automated responses functioned correctly and the unit transitioned to a new and stable load condition that sustains the combustion process within the limitations of the remaining draught group.

It is clear from the preceding example that if the functional allocation had been violated, the unit would not survive the test. Consider, for example, if PA fan B was tripped in the gang trip instead of PA fan A, a second gang trip would then come into operation, causing the tripping of the entire B draught group. With both draught groups being lost, the unit simply cannot remain in operation and would disconnect from the power system.

The above example is merely one of several such capability demonstration tests that are carried out following initial commissioning or major maintenance or project work. Typical tests include:

a	Draught group trip	(40% to 60% capability)
b	Mill trip	(20% to 30% capability)
c	Mill feeder	(12% to 18% capability)
d	Feed-pump trip	(50% to 60% capability)
e	11 kV unit board trip	(40% to 60% capability)

5.4.3 Process Separation

In many cases the tripping of a process or system is unavoidable. If the tripping of a specific process or system renders the unit incapable of further producing electricity, the unit itself is tripped and disconnected from the power system.

One of the advances that has been made possible with the aid of modern control systems is allowing boiler or reactor-associated processes to remain operational while processes or system functions associated with the generator or turbine can be suspended or tripped.

Whenever such a case arises where either the generator or turbine is required to trip while the boiler or reactor remains in service, it is inevitable that the unit as a whole trips by disconnecting it from the power system. If so, it may not be entirely obvious why such a trip of some processes, but not all, would be advantageous or add to unit resilience.

Although resilience itself may not directly benefit from such a state of affairs, the real benefit is derived from the ability of the unit to return to service significantly quicker than otherwise, provided that the cause of the trip can readily be resolved – availability of the unit is thus improved.

The actual difference is drastic and returning from a turbine trip could occur in a mere 10% of the time required for returning from a boiler (or reactor) trip. For this philosophy to be implemented, it is necessary to have an effective and rapid means of diverting the steam from the boiler (or reactor) so that it is not admitted to the turbine. A bypass system is therefore needed that diverts the steam directly into the condenser instead of passing it through the turbine.

Similarly, the processes that form part of the common and shared systems are largely decoupled from those running on the units. This means that trips of common and shared processes generally do not result in a direct automatic trip of a unit. However indirect consequences of disruptions in the common and shared systems could ultimately cause disruptions of the unit processes. These indirect consequences will be the focus of the following sections.

5.4.4 Unit Islanding

One of the novel features incorporated into the fifth-generation power station philosophies is the concept of unit islanding (sometimes called house-loading). The concept of unit islanding is to separate the unit from the power system but not shut down the electricity generation process, thus merely supplying enough power to operate the auxiliary load of the unit itself. Islanding is normally activated when disturbances in the transmission system exceed the operating envelope of the unit equipment or processes.

Islanding, as a function, has many benefits for a generating unit since it avoids tripping and subsequent restarting (which takes a significant amount of time and has a significant implication on cost), allowing for a rapid return to service. It also represents a lesser plant impact than a trip and is thus more beneficial from a long-term plant health perspective.

Unit islanding differs from unit tripping by separating (specifically and deliberately) only by opening the HV generator circuit breaker while leaving the LV generator circuit breaker closed. This allows the unit auxiliaries to remain in operation and the generation process to continue. This electrical configuration for unit islanding is shown conceptually in Figure 37, with the blue arrows showing the flow of electricity.

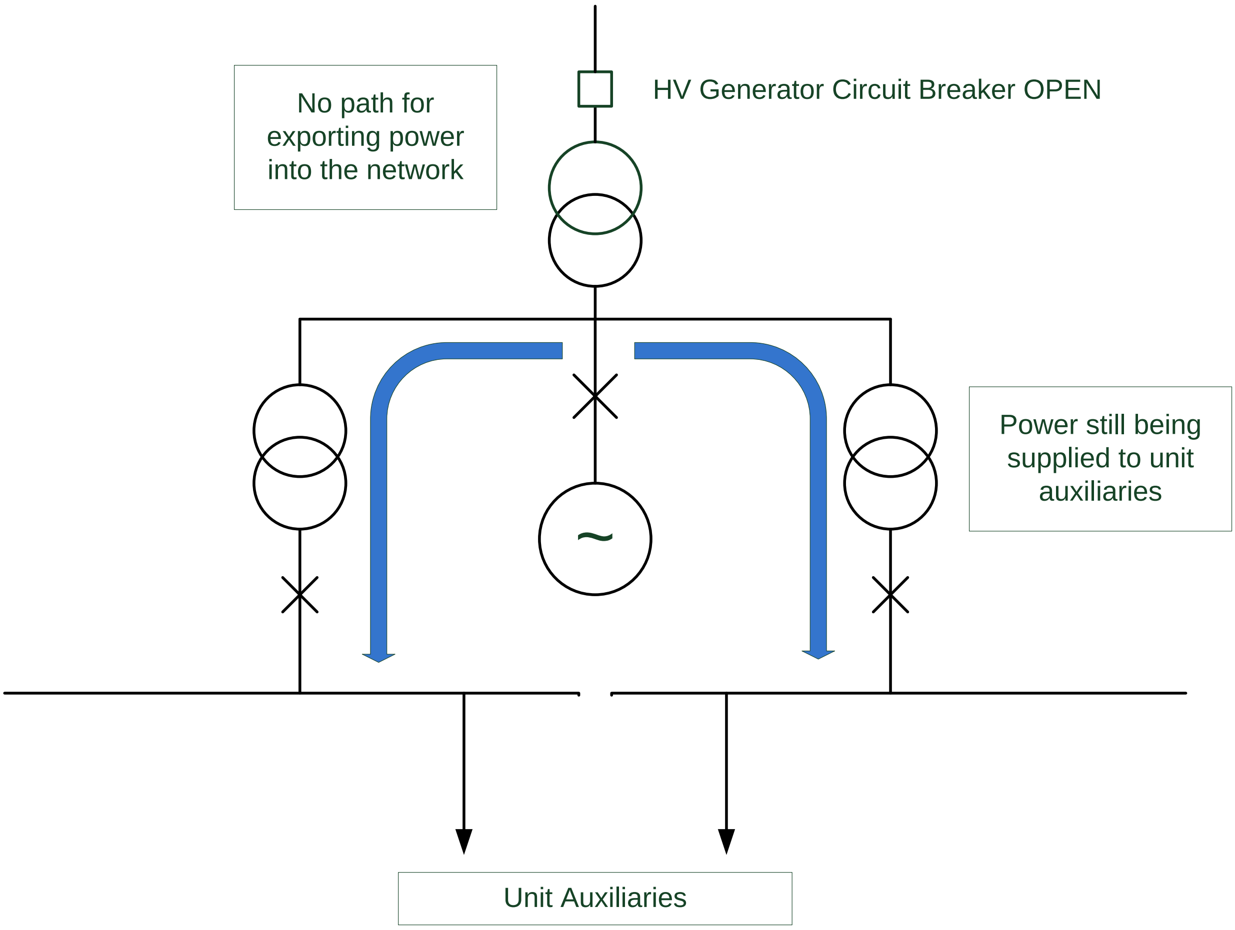


Figure 37: High-level electrical configuration of a unit during an islanding condition

The electrical configuration of the unit is only one part of the islanding function. The transition from a unit in normal operation to a unit in an islanded state is severe, and the unit needs to assume a new condition within a very small space of time. The main difficulty is scaling down the energy conversion process rapidly by cutting back on the combustion process and preventing the steam that has already been generated from being admitted to the turbine. If not implemented swiftly enough, thermal excursions will occur, and the turbine speed will increase beyond its capabilities, causing a total trip and shutdown of the unit, thus entirely defeating the objective of islanding.

To implement islanding, the control system must automatically recognise that the criteria for islanding have been met to initiate the requisite steps needed to implement unit islanding. Islanding is then automatically implemented by taking various simultaneous control actions.

- Combustion is immediately reduced by tripping all mills and mill auxiliaries that exceed the predetermined requisite number, typically two.
- Combustion set-points are changed to establish the new (predetermined) load that is consistent with the unit auxiliary load. The milling and draught plant is thus affected.
- Steam admission to the turbine is immediately diverted by opening the HP turbine, and the IP turbine bypasses to predetermined control settings. Only a small fraction of the steam is permitted to pass through the turbine (just enough to generate the power required to operate the unit's auxiliaries).
- On units with steam-driven boiler feed pumps, the electrical feed pumps are automatically started in anticipation that the steam-driven feed pump could potentially become compromised (due to the process transient), the loss of which would likely result in the unit tripping.
- The control mode of the unit is automatically switched to the turbine speed control mode, typically from a load control mode (or various others) that might have been in operation before islanding.

If successful, the unit will continue generating electricity but merely supply its auxiliaries. A unit may remain in this islanded mode of operation for protracted periods, and various cases have been recorded where units remained islanded for many hours. Depending on the design, the level of optimisation, the standard of maintenance, and the operator's proficiency, the unit may (or may not) consume fuel oil while prevailing in the islanded state.

Unit islanding is technically onerous and is only achieved when units are kept in a well-maintained state, and the control loops and functions have been well-optimised. Long-term statistics gathered over 30 years suggest that units designed and maintained for unit islanding have a 60% success rate, a rate that rapidly erodes to zero when maintenance is neglected.

The South African Grid Code recognises the potential benefit of this functionality and requires it from all future coal and nuclear units, as well as regular testing of existing units with this functionality [1].

5.4.5 Disruption Hierarchy of Individual Units

From the preceding sections, it is clear that every type of disruption experienced by a power-generating facility will not translate into the same final outcome. In this section, we will explore some of the relevant contexts in terms of the different manifestations that disruptions may impose on a unit.

Firstly, it needs to be understood that there is a significant difference between the design approach for power plants and the design approach for factories and manufacturing plants in general. In the majority of cases, the processes that operate within manufacturing plants are intended to ensure a high (or acceptable) quality of manufactured products. This means that the process or system that operates within a factory is often set up to trip when the quality of the product becomes compromised for whatever reason.

A power station, in contrast, is designed to be disruption-tolerant. Tripping of plant is only implemented to avoid damage to plant or harm to people – disregarding (in terms of tripping) the quality of the ultimate product. To embody this concept, most (if not all) grid codes have dedicated entire sections to ensure that units can tolerate abnormal voltage and frequency conditions emanating from the power system.

However, it is not only disturbances that arise from within the external power system that pose a threat to power stations. Most disruptions originate within the power station itself (or are imposed upon a power station from external sources, e.g., adverse weather, social unrest, etc.). To be tolerant of plant or equipment failure, power station designs feature a significant level of redundancy in terms of backup or standby plant, along with automatic control systems to bring the redundant equipment into operation when failures occur – in many cases, without any effect on production.

A philosophy of in-service maintenance is also featured in the redundancy-orientated design of modern power stations and their units. Much of the installed base of equipment can be repaired, replaced or serviced without the need to shut down operations or to cease production. This capability is limited and cannot practically be extended to all plant and systems. However, it nonetheless became a prominent design feature from the third-generation power stations onward and is still featured in current designs. A typical area where this design feature is apparent is the milling plant, where the number of mills is greater than the number required to reach full load. Thereby, mill maintenance can be undertaken without impacting the ability of the unit to produce at full-rated output.

Another example, although not redundancy-oriented, is the ash removal system at the bottom of the boiler where the coarse ash collects. A submerged scraper conveyor system removes ash on an ongoing basis to evacuate the coarse ash. When this system (of which there is only one per unit) fails, the facility has been built into the plant to seal off the boiler and retract the conveyor to a location from where it can readily be accessed and repaired, with the boiler remaining on load. Provided that the repairs can be done rapidly enough, the systems can be returned to service without affecting production or shutting the unit down.

In some cases, the design allows maintenance to be conducted without shutting down the unit but with a reduction in output. An example of such a system is the condenser system for the low-pressure turbines in wet cooling power stations (refer to section 5.6.7.2.1). In this example, a condenser can be removed from service (typically to locate and repair a tube leak) with the unit remaining in service but at half-load.

The requirement for in-service maintenance is even more important for the common systems of the outside plant. Once again, the philosophy of having redundancy as part of common systems and equipment is rife in the design of the outside plant (i.e., the non-unitised plant). For example, very few conveyor belts exist that do not feature 100% redundancy in the form of a backup system. Even cooling towers do not have a one-to-one relationship between the towers and the units. Instead, the cooling towers form part of a ring structure where any single cooling tower can be removed from service without necessitating the shutdown of any unit – providing that the ambient temperatures permit.

Much attention and effort are invested in developing power stations that are resilient to disturbances – both those arising from within the plant, and those emanating externally. The various tiers comprising the plant resilience design framework (for individual units) are not merely a haphazard collection of design principles but rather a hierarchal collective of philosophies underpinning the design and operation of the processes involved in power generation. This hierarchy is conceptualised in Figure 38 below.

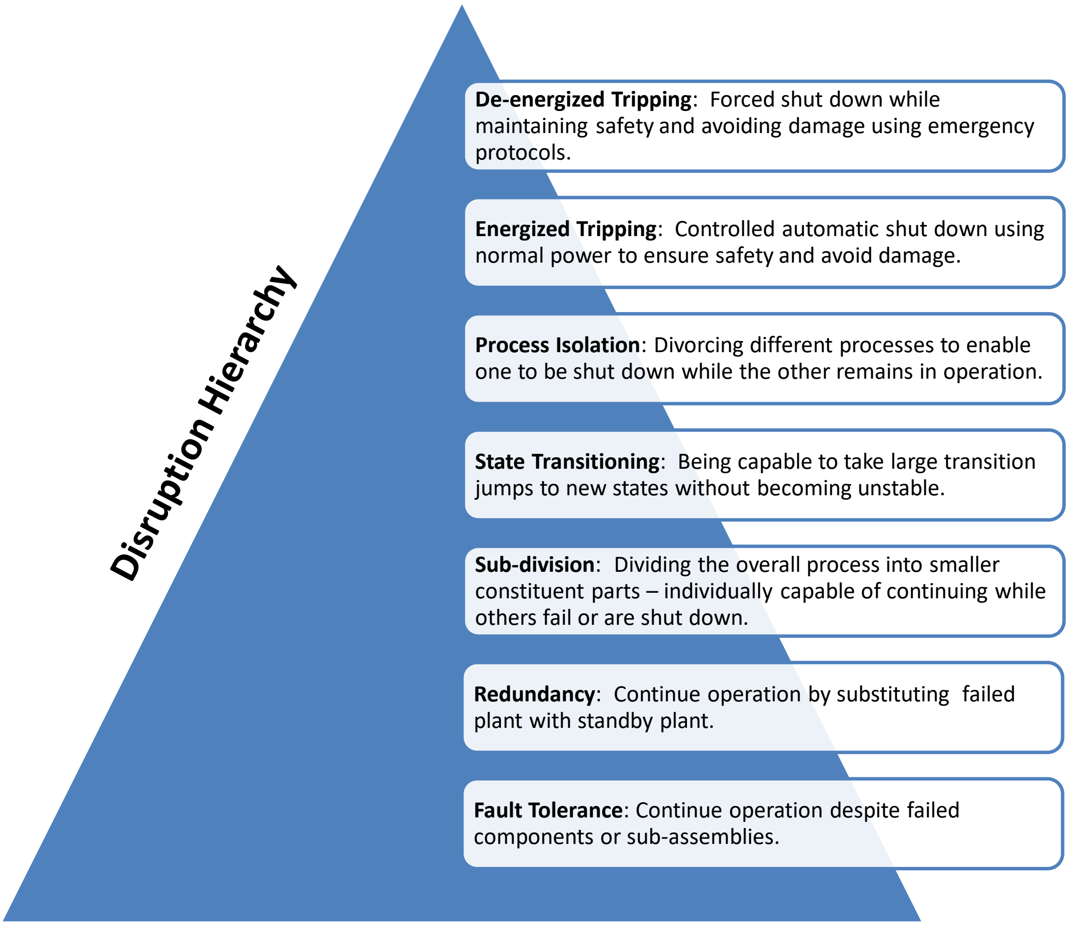


Figure 38: Resilience design tiers of fifth-generation power stations

At the lowest and most fundamental level of unit resilience, as a precondition for the entire disruption hierarchy of a unit, resides a set of specifications that ensures that the unit will be tolerant of electrical voltage and frequency ranges that surpass normal industrial standards. This implies that a unit will generally be able to withstand greater exceedances than other participants who are exposed to the same disturbances to which they are mutually interconnected.

Systems with a significant level of criticality will then be designed to continue operation despite the failure of individual components. This approach is particularly widespread within the control and instrumentation of critical systems. The benefit of such an approach is that systems will continue operating even when a primary instrument fails in service. Another example is the generator protection system, where the protection is implemented through two dual redundant protection schemes that are both permanently operational and in service. Once again, even when one of the protection schemes becomes inoperable, it will not cause the tripping of the generator – since the second scheme is equipped with an equal set of protection functions to the first.

Where systems exist that cannot practically be made to include sufficient additional built-in capacity, a standby plant is typically provided that could be introduced upon the failure (breakdown, tripping, malfunction, maintenance, etc.) of the duty plant. Examples of this are often found in applications where pumping is necessary for process purposes, e.g. the condensate extraction pump. When the duty pump trips, the standby pump starts up automatically, and production is maintained uninterrupted.

The next level in the hierarchy involves plants that are prone to disruption. Milling plants (for crushing coal) would be a typical example. To deal with the propensity of such plants to become disrupted, the overall task of coal milling is subdivided into smaller milling applications, collectively fulfilling the boiler's overall demand. Modern units typically require about five mills for full-load operation and would generally be equipped with six – to allow for maintenance without requiring the unit to be de-rated.

Another instance where the concept of subdivision is popular is where a function is so prominent that its cessation will inevitably lead to the complete compromise of the production of the unit – e.g. draught provision (providing a balance between air input into the furnace and the extraction of gaseous waste products (flue gasses), whilst ensuring the correct air-fuel ratio for safe and efficient combustion). In such all-encompassing cases, the draught function is subdivided into two – a left-hand draught group and a right-hand draught group (refer to section 5.3).

The next tier in the disruption hierarchy is a unit's ability to rapidly transition from one operational state to another whilst not becoming unstable in doing so. The most extreme of such cases occurs when unit islanding occurs, as discussed in section 5.4.4 above. However, there are other cases where similar transitions need to be implemented rapidly – where plants or systems become unavailable, and the remaining systems can only partially support the production of the unit. Modern units are equipped with pre-programmed control systems to recognise such conditions and facilitate the transition to the new state of reduced production.

Process separation (the next tier in the hierarchy) is discussed comprehensively in section 5.4.3. It allows for the turbo-generator to trip while the boiler remains in service – a novel function that allows for the rapid return to service of a unit following a trip.

Energised tripping of the unit (both the boiler and the turbo-generator) involves opening the LV generator circuit breaker while the HV generator circuit breaker remains closed. Electrical power can then be imported from the local network to operate all the systems required for the safe shutdown of the unit. Although the process of generating electricity by the unit is interrupted, electric supply to all the unit loads remains available, and the unit can be returned to service as soon as the problem has been remedied.

The most onerous case, and the last in the hierarchy, is the case where the HV circuit of the unit trips. The HV circuit involves all equipment that is electrically connected to the voltage node that is supplied by the main generator, including the generator, generator transformer, unit transformers, excitation transformers, LV generator circuit breaker, and the interconnecting busbar system. When the HV circuit trips, all the breakers surrounding the transformer island trip to cut off all possible power in-feeds from the generator, the network, or the two 11 kV Unit Boards. With the unit transformers dead, no power is available to operate any normal auxiliary loads. This condition is shown in Figure 39 of the schematic reticulation system of the unit.

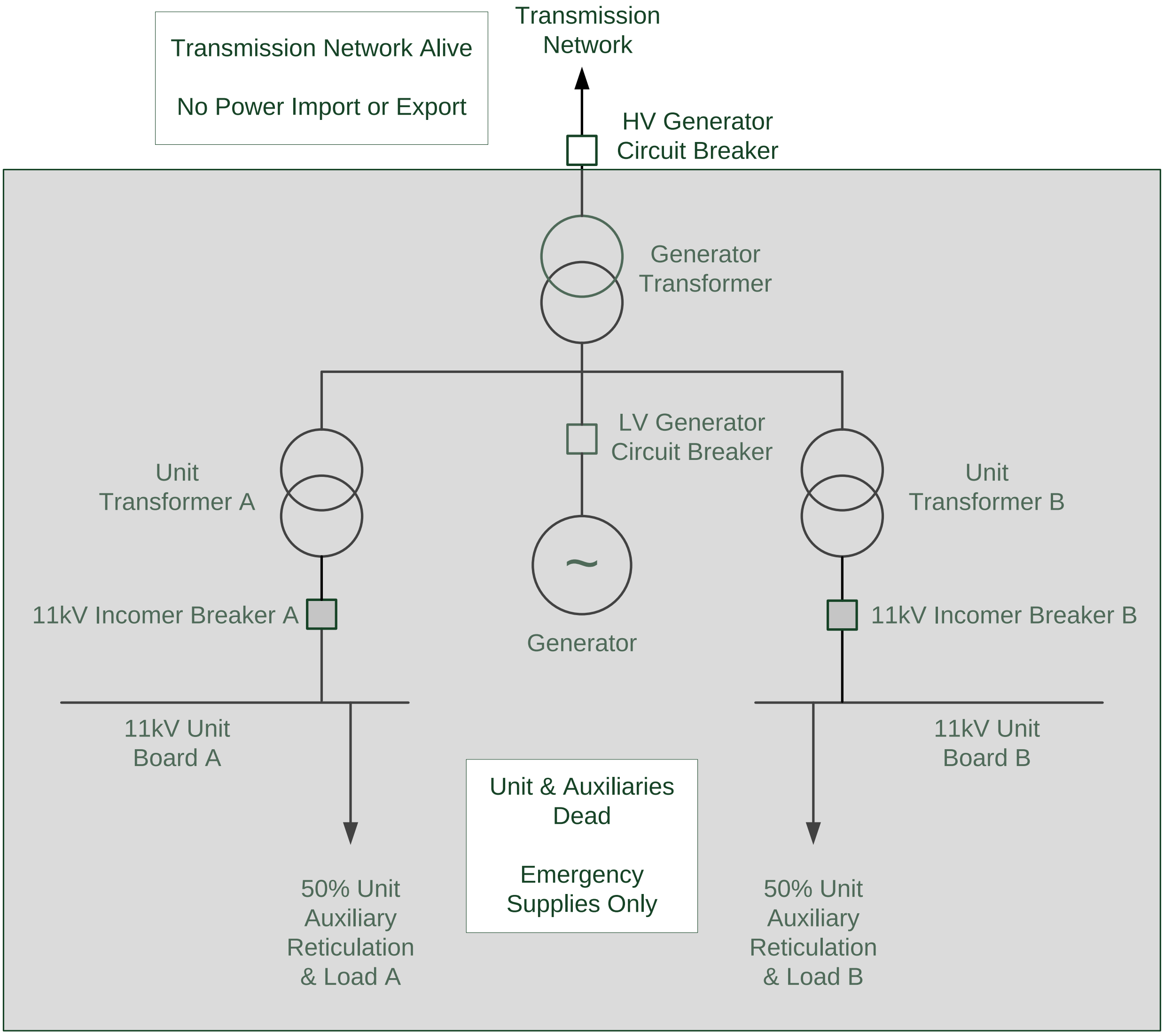


Figure 39: Generating unit with a dead HV circuit

Under these circumstances, all energy requirements are to be met by emergency sources, such as the DC systems and diesel generators, by pneumatic supplies or by pre-stored potential energy devices such as tensioned coil springs or gravity-operated devices.

There are many possible combinations of disruption, not all of which can be explored here. However, the above deals with the main classes in a hierarchal structure supported by deliberate design intent, maintenance and operational practice in modern power stations.

In the following sections, the focus will shift from disruptions of single units to disruptions that propagate and cascade into more than one unit – a higher-risk category of generation disruptions.

5.5 Coincidental Concurrences

At the very core of maintaining the balance between the customer utilising electricity and the generation thereof is the issue of reliability. However, no system, process or device created by man has proven infallible, and therefore, reliability is not absolute – despite design efforts meant to counteract the undesirable effects of failure. Proper design of vast systems, especially those with significant interdependencies, requires deliberate engineering investment to bolster reliability by compensating for those factors that could erode it.

Many factors could adversely affect the reliability of electricity generation in power systems. The electricity supply value chain consists of various functional areas, such as power generation, transmission, distribution, and reticulation. A disruption in any of these functional areas may compromise the continuation of supply to the end user.

Large-scale disruption events such as power system blackouts are incremental. The stepwise increments that facilitate the propagation of a disruption event are tripping. Tripping, in this context, refers to the instantaneous disconnection and isolation of equipment, e.g. power lines, coupling transformers, capacitors, reactors, busbars, units, customer loads, etc.

Because of the focus of this study, those tripping events that affect or are caused by generation facilities are of specific interest. The loss of a single generating unit at a power station does not present a significant risk to the power system as a whole since the spinning reserve is normally shared amongst various units in the overall generation fleet of units – equally so is the collective moment of inertia of the fleet of synchronised turbo-generators (see section 6.2.4.). However, when multiple units are lost within a short space of time, the total reserve in the system may be exhausted, which may, in turn, lead to a rapid loss in system frequency and the consequential compromise of the entire power system. Therefore, the reliability of single generating units is of concern, especially in cases where more than one unit is lost in rapid succession.

5.5.1 The Threat of Single Unit Reliability on the Power System

When the threat of a system blackout is being considered from a power generation perspective, the first question that needs to be considered is the likelihood of two or more generating units arbitrarily disconnecting from the grid at more or less the same time. Traditionally, such an event was believed to be extremely unlikely (although not impossible) and, therefore, never officially recorded. The belief was held that the only instances where more than a single generating unit can trip at approximately the same time would be where a specific commonality would affect multiple units and cause their collective failure or disconnection – a cascade resulting from interdependencies.

Although no deliberate surveillance existed to detect chance coincidences of the disconnection of multiple generating units that are entirely unrelated, the first (known) event of this type was observed on 31 August 2006, when two generating units at two different power stations tripped within seven minutes from one another and caused an under-frequency event. At 05:57, Camden 6 tripped when the system load steadily increased towards the morning peak. At 06:04, Tutuka 4 tripped due to an unrelated issue, causing a frequency decline – only arrested at 49,17 Hz. During this event, although the separation between the two trips provided the system to recover partially from the adverse effects of the first trip, it did highlight the risk that unrelated tripping events of units that coincide in time can have a considerable impact on the state of the system. However, it was deemed a fluke, and although it proved possible, it was probably a very rare event and did not necessitate deliberate management or engineering focus.

On 15 July 2015, an even greater rarity was observed when two entirely unrelated units tripped, coinciding at the very same power station. At 02:10, Arnot 1 tripped from about 220 MW, followed by Arnot 4 at 02:21 from about 210 MW. Since the two events occurred at the same power station, the initial suspicion was that the two events were linked in a way. This turned out to be untrue, and unit 1 was lost due to low boiler drum level protection, and unit 4 was lost due to a temperature envelope violation on the boiler re-heater system. Even an investigation into a more indirect connection came to nought when earthing, EMI, and power supplies were scrutinised. This event reinforced the reality that unrelated events could coincide – even within a single power station. The following graphically shows the system loss of the two units.

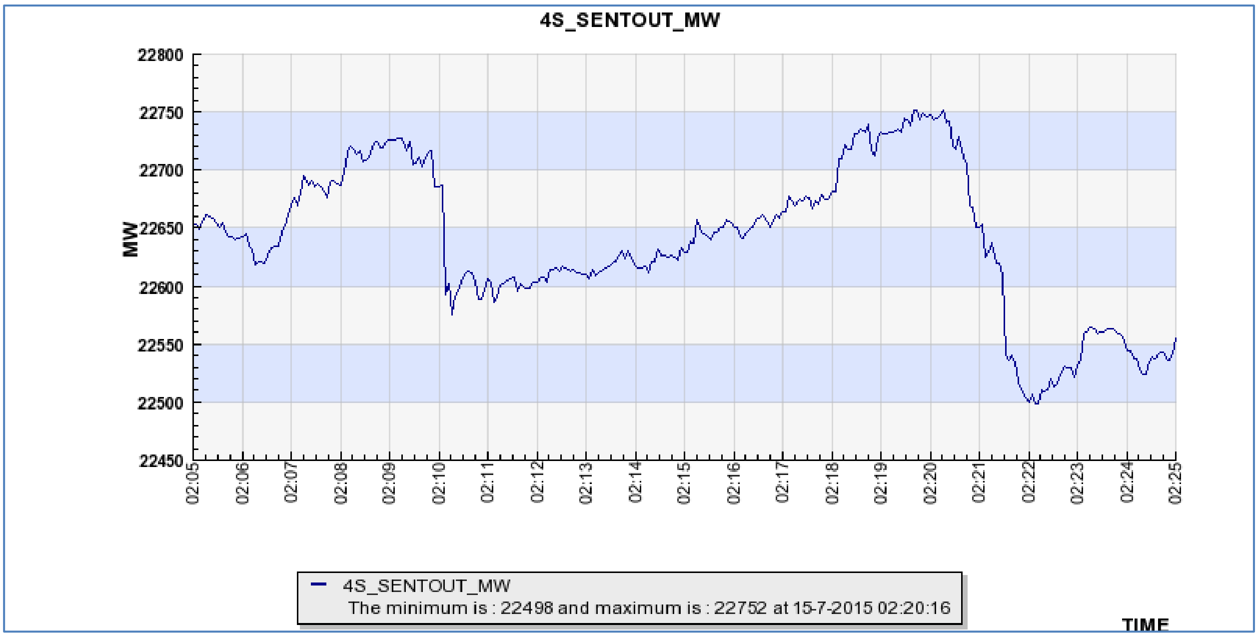


Figure 40: Recording: Unrelated loss of units 1 and 4 at Arnot Power Station

Because of the time of day and the relatively low generation levels of the two Arnot units at the time of the event, the total effect on the system frequency was limited to about 150 mHz. Both the Arnot event and the Camden-Tutuka event demonstrated that multiple events could coincide. Still, the system effect in both cases was minimal due to relatively low power output levels at the time of the events, as well as the individual unit disconnection still being separated by several minutes in each case – and therefore, despite evidence to the contrary, were not regarded as being a material risk to the system.

This notion that unrelated events do not pose a dramatic threat to the system would change on 14 September 2015, when Duvha 4 tripped at 18:40:16, and Medupi 6 tripped at 18:41:08, less than a minute apart, due to entirely unrelated causes. The double loss in rapid succession is shown graphically in the following recording.

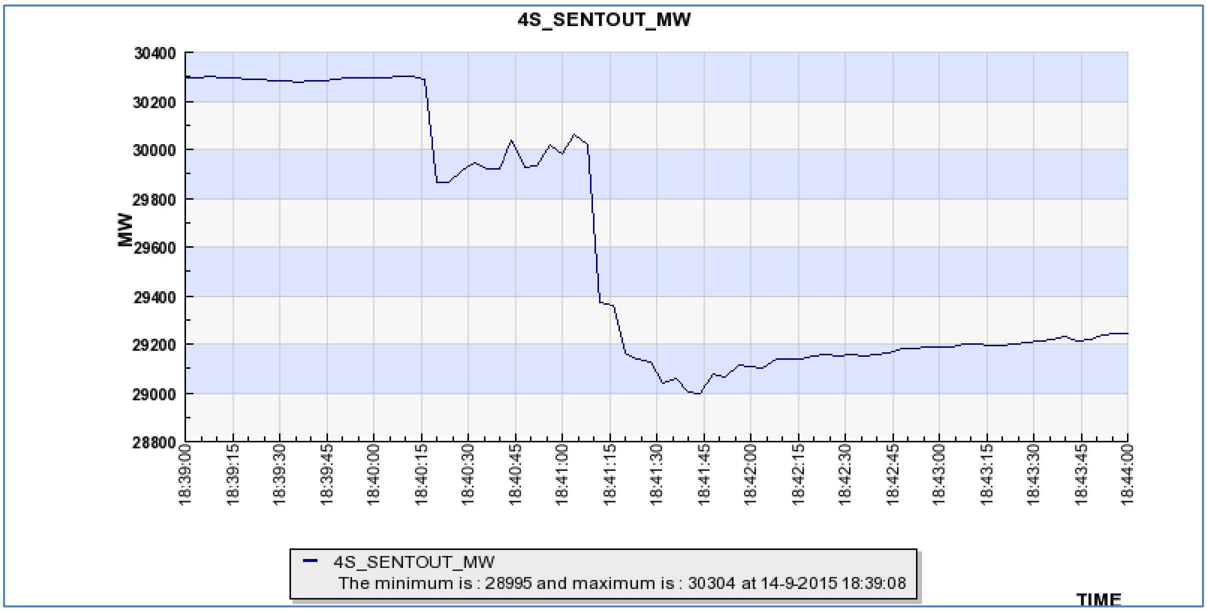


Figure 41: Recording: Unrelated loss of Duvha 4 and Medupi 6

Investigation revealed that the two trips shared no commonality whatsoever. The Duvha unit was tipped manually by an operator following the failure of the hydrogen seal on the main generator, while the Medupi unit tripped due to a low flow condition in the boiler economiser. The effect of this event, which removed 1 298 MW of generation during the evening peak, was that the system frequency decayed to 49,189 Hz – entering the realm of the Under Frequency Load Shedding (UFLS) scheme that produced system relief of 1 058 MW from various regions in South Africa. The effective UFLS response caused the system frequency to recover rapidly following the dual trip, as seen in the following recording.

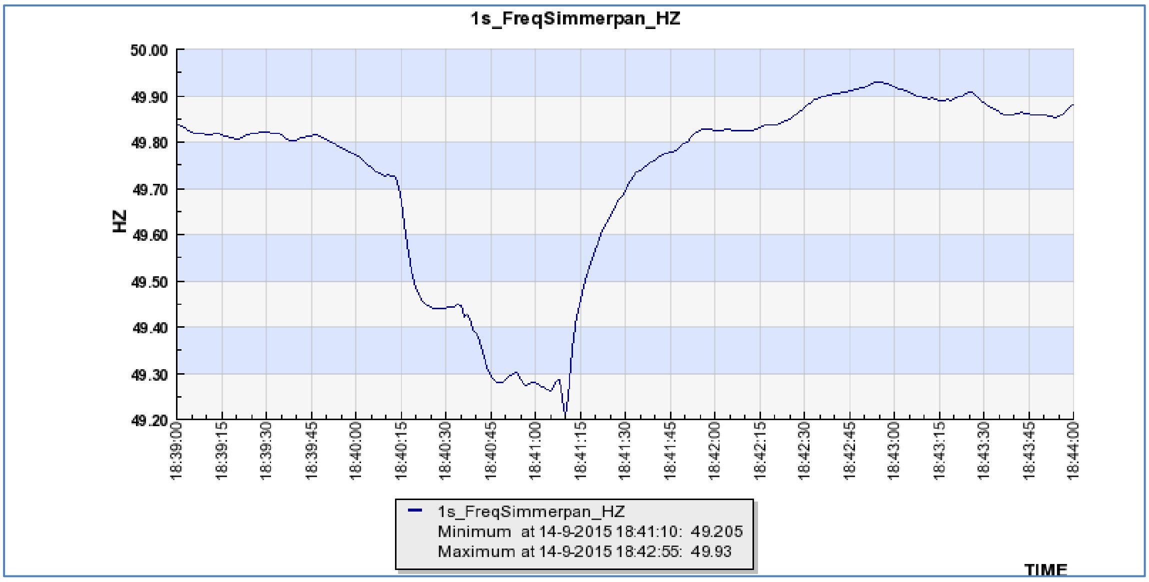


Figure 42: Recording: System frequency response for the Duvha-Medupi event

However, the collision of two major units within a minute of one another forced the realization that multiple unrelated events cannot be ignored. They must be factored into the power system's contingency planning and require further analysis.

The individual trip performance of generating units in the South African fleet was analysed to determine the potential for the loss of more than one unit to coincide. Trip information from 1997 and onwards was used. The time difference between consecutive unit trip times was calculated from 1997 to 2014 to determine the possibility of a two-unit coincidental trip. The time difference, expressed in minutes, was then statistically analysed. The statistical toolbox of Matlab® was used to perform the analysis.

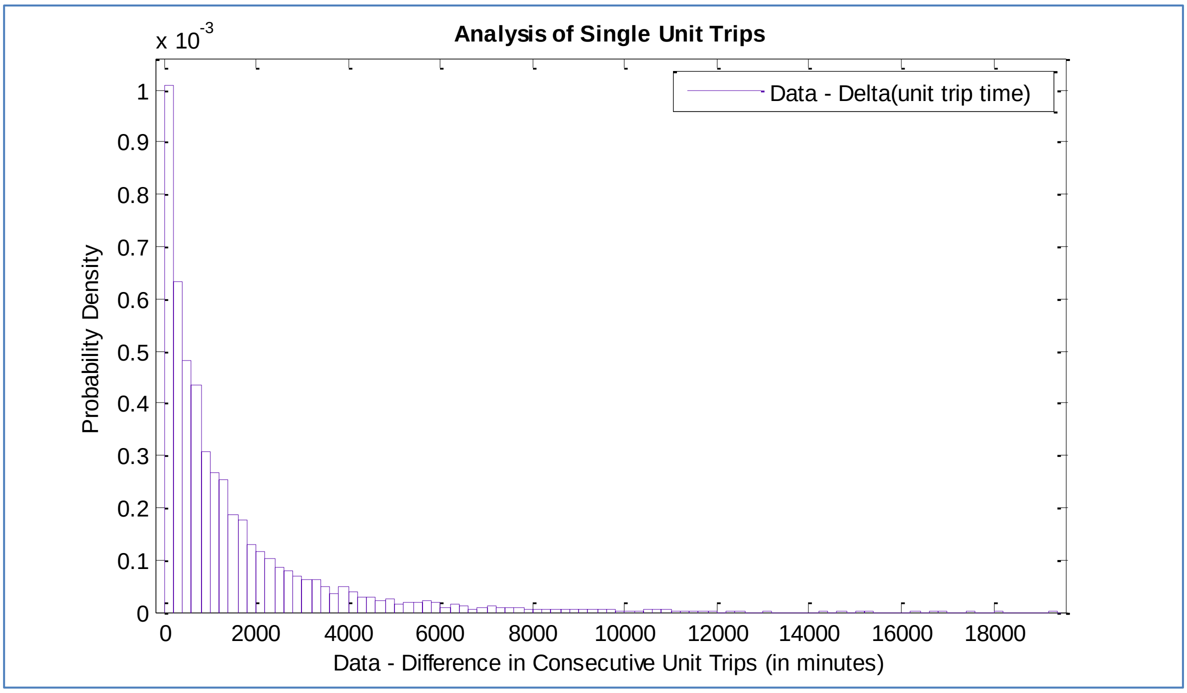


Figure 43: Time intervals between consecutive unit trips

As shown in Figure 44, various probability distribution types were tested against the data in a first attempt to identify possible fit types that deviate from the observed results.

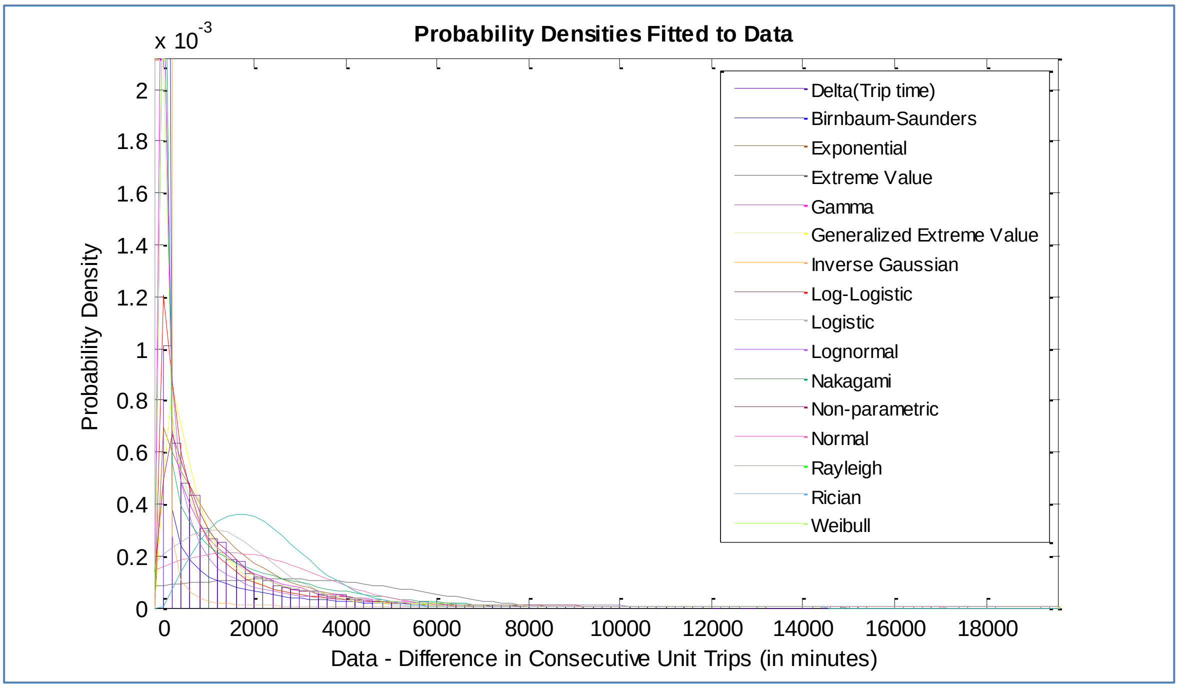


Figure 44: Probability density functions fitted to the data

After eliminating the probability density functions that fail to adequately represent the actual data, a collection of functions with potential merit in providing an acceptable model for the observations is retained. The functions that are left and require further consideration are shown in the subsequent representation.

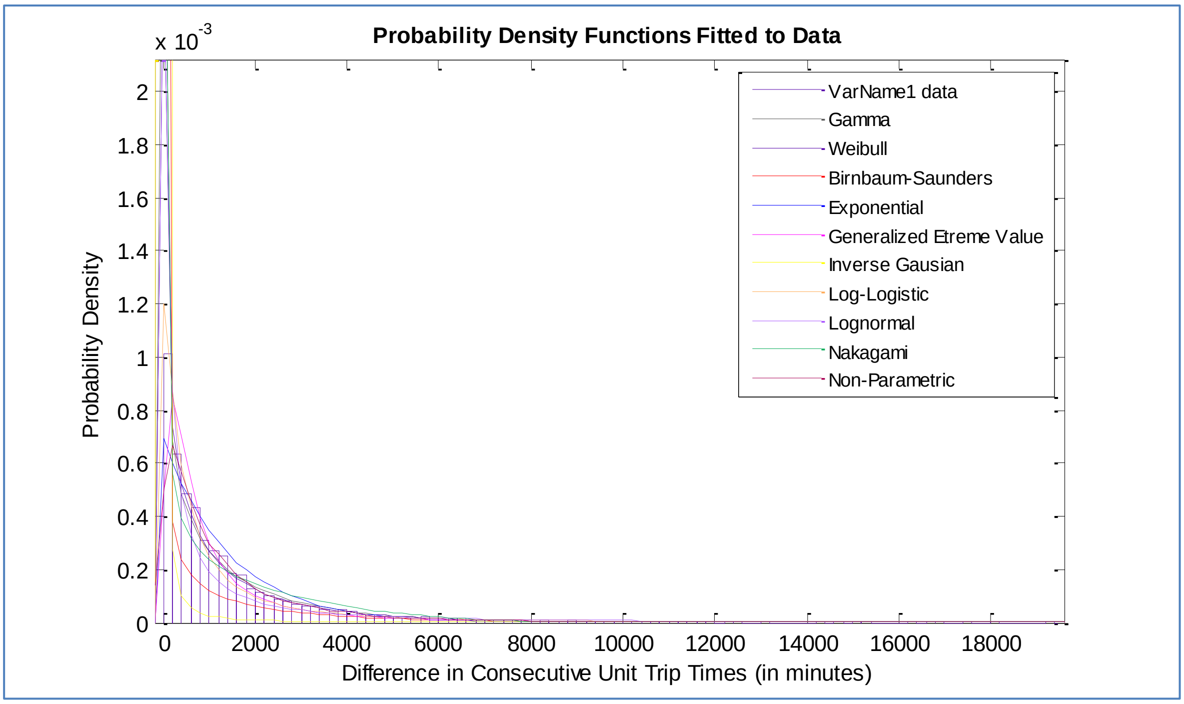


Figure 45: Retained probability density functions

To further evaluate these probability density functions' appropriateness, other statistical perspectives are used to determine the degree to which they represent the data. Firstly, the cumulative probability is represented along with the remaining functions to yield the following figure (Figure 46).

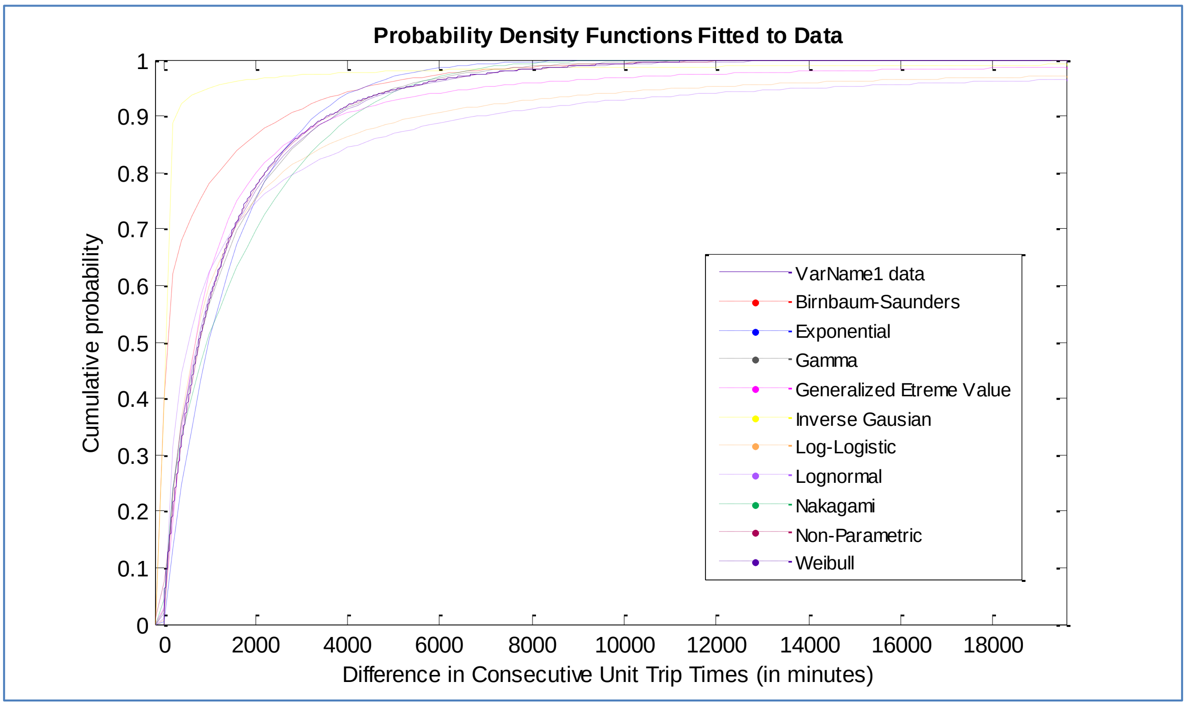


Figure 46: Remaining functions expressed as a cumulative probability – with the observed data

This graph eliminates the Birnbaum-Saunders and the Inverse Gaussian functions due to their degree of deviation from the data. Through successive steps of elimination using the inverse of the cumulative distribution function, the probability plot, the survivor function and the cumulative hazard as different perspectives, all but two functions are eliminated, namely the Gamma and the Weibull functions – both represented on the following graph using cumulative hazard as the chosen perspective against the data.

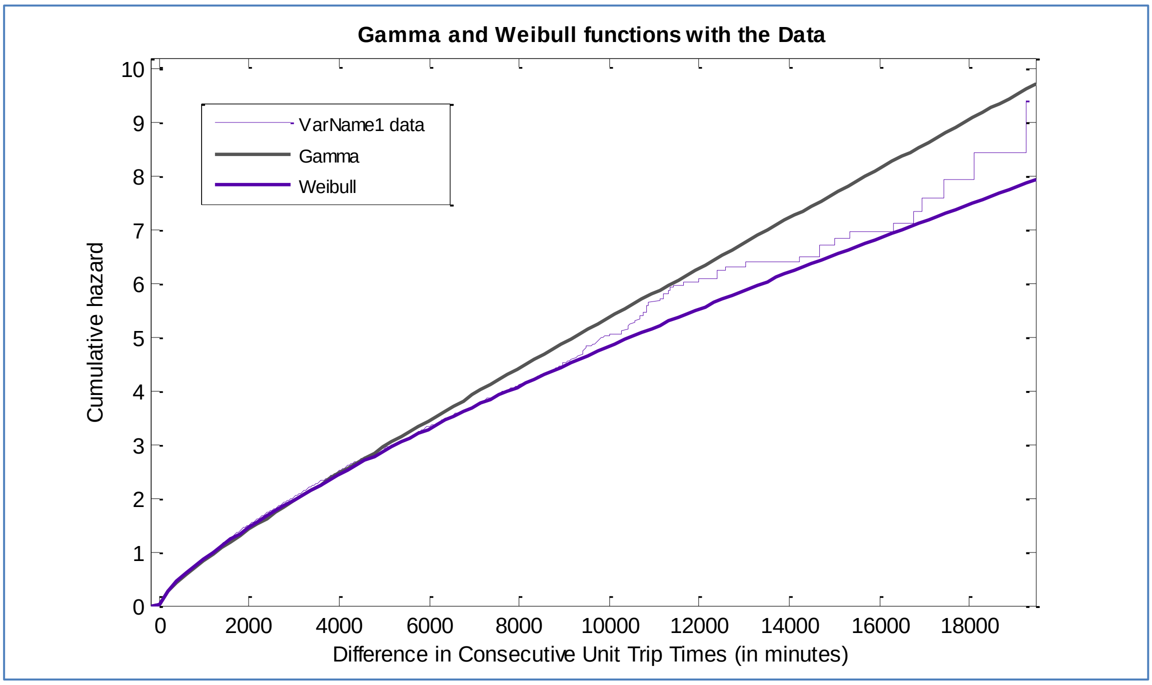


Figure 47: Weibull and Gamma functions expressed as a cumulative probability – with data

Both functions represent the data equally well for minor time differences between trips, and they deviate only for longer time differences. For the key question posed in this section, namely, to determine the likelihood of more than one unit tripping simultaneously, only minor time differences are relevant. Therefore, it is irrelevant which one of these two functions is chosen over the other. Therefore, the gamma function is selected as the probability density function that adequately describes the data. This means that the function is given by [164]:

$$y = f(x|\alpha, \beta) = \frac{1}{\beta^{\alpha}\Gamma(\alpha)} x^{\alpha-1} e^{\frac{-x}{\beta}} \quad \forall x \in [0, \infty) \tag{3}$$

with α and β, within a 99% confidence interval and with a log-likelihood of -56130, estimated at:

	Estimate	Standard Error
$\boldsymbol{\alpha}$	0,627	0,009
$\boldsymbol{\beta}$	2 287,4	47,970

Using the gamma function as the function describing the observed data, the following values were calculated as the population mean for each calendar year from 1997 onwards, given by [164]:

$$\mu = \alpha \cdot \beta \tag{4}$$

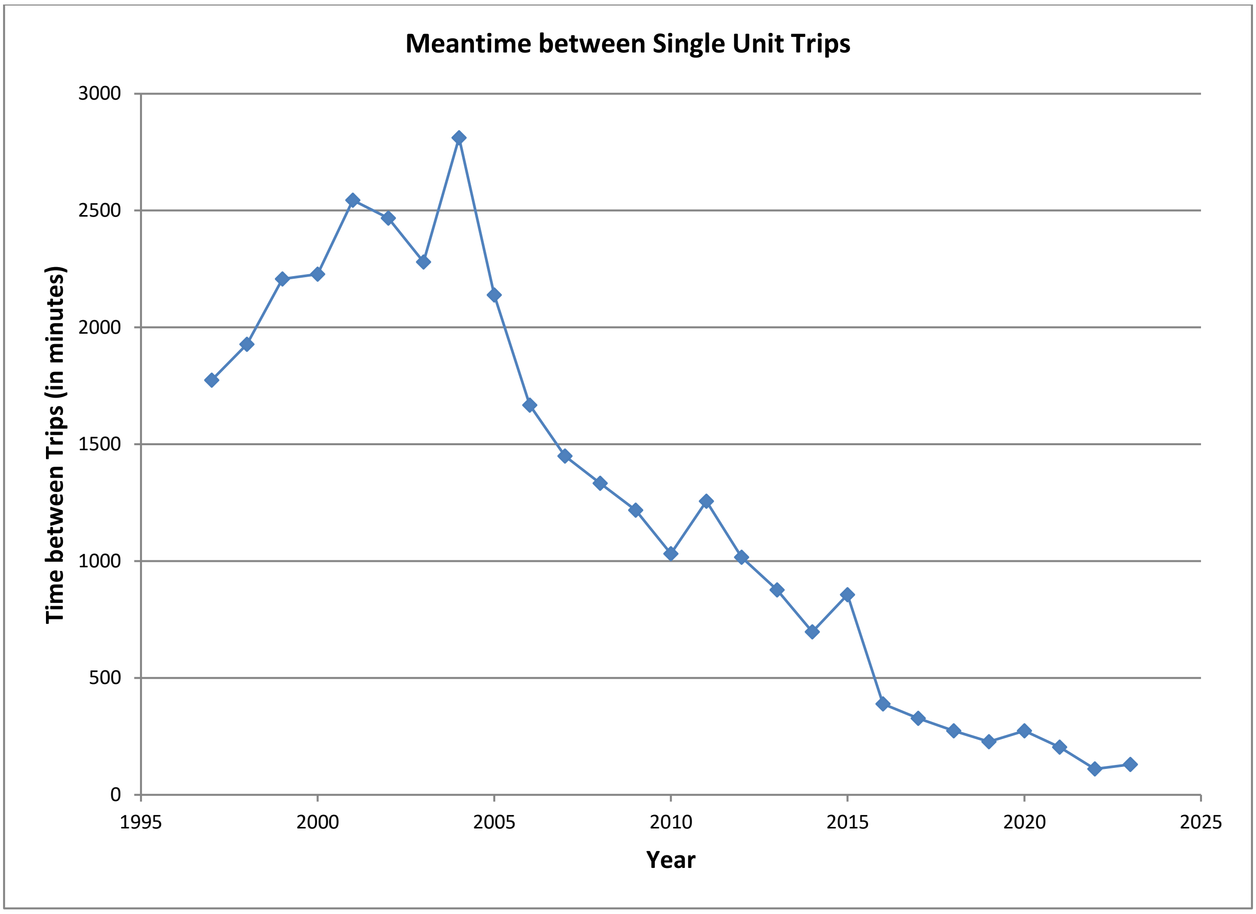


Figure 48: Meantime interval between unit trips of the South African fleet

As can be seen from the graph, the mean time between consecutive unit trips reduced considerably, from a system best (permitted by available data) of 2 812 minutes (46,9 hours) in 2004 to a value of 129,5 minutes (2,2 hours) in 2023 – signifying a 95% deterioration that occurred over about two decades.

This decrease between single unit trips brings about considerably more risk to the power system than previously and should be considered in the management strategy for the power system. For example, in 2004, there were three events recorded where units tripped within less than a minute from one another, while 47 such events were recorded in 2023. It is conceivable that this risk increase could contribute considerably to the risk of a power system blackout. What is of particular concern is that the mitigation of this specific threat cannot be addressed through traditional means because it lacks a common mode interdependency that could be prioritised for management attention to enhance performance. This threat can only be mitigated by enhancing the reliability of the individual units of the power stations. This feat has proved elusive within the context of the South African power system.

5.6 Intra-Station Escalation – Multi-Unit Cascade

It was pointed out earlier that generating units are designed to tolerate internal system failure. Except for a few minor exceptions, most component and system failures merely reduce the unit's output and do not lead to its disconnection. However, various systems are not entirely contained within the functional boundaries of the generating unit and are shared between units. When becoming disrupted, such systems have the potential to impact multiple units.

Figure 52 shows some of the systems that span the units of a power station, potentially affecting multiple units when they suffer disruption.

Figure 52: Power station systems supporting multiple generating units

A disruption of sufficient severity of any of the systems shown above could disrupt multiple, or indeed all, the generating units of the power station. The Eskom event record contains examples of multiple unit disruption events resulting from all systems listed.

Except for the systems shown above, various other (non-technical or non-production) systems also support a power station and, therefore, can affect multiple units. Figure 53 shows several such systems.

Figure 53: Power station non-production systems supporting multiple generating units

Once again, as in the case of the direct production systems, a disruption in any of these systems can also disrupt multiple units, and examples of many such events have also been recorded.

Due to the potential for disrupting multiple units, special precautionary measures must be taken to ensure the risk is sufficiently mitigated. Similarly to the redundancy considerations taken to safeguard individual generating units against disruption stemming from system failure, systems common to multiple units have also been designed with inherent redundancy.

In the following sections, many typical mechanisms and inherent vulnerabilities will be explored that give rise to multiple units participating at a given power station – using specific examples or case studies.

5.6.1 Catastrophic Failure Events

One of the most intuitive types of events that could disrupt multiple generating units is when a catastrophic failure event occurs that is so extensive that it affects adjacent generating units to become functionally compromised. Left to the imagination, various possibilities can be produced where some large-scale failure event could simultaneously disrupt various generating units. Consider, for example, the possibility of a plant fire raging out of control and spreading through the plant, forcing generating units out of operation.

However, despite the many possible scenarios that may lead to such a catastrophic failure event, these events do not occur frequently. One example that illustrates the scale of such events occurred on 17 August 2009 in Russia at the Sayano-Shushenskaya Hydroelectric Power Station when the turbine of unit no. 2 failed mechanically. The failure caused the enclosure of the turbine to become breached, leading to the inevitable flooding of the entire turbine hall, tragically killing 75 people.

Figure 54: Catastrophic flooding failure of Sayano-Shushenskaya Hydroelectric Power Station [165]

The failure was exacerbated by the water, causing all electric power sources to fail due to flooding, thereby avoiding automated protection, mitigation, and isolation functions from coming into operation. From a disruption perspective, the event left all ten generating units of the power station unavailable for operation, some beyond repair. The combined capacity that was lost from the system was 6 400 MW, which resulted in widespread and prolonged power outages. [166]

Another example of a catastrophic failure occurred in South Africa at a third-generation power station in 1925 – the Vereeniging Power Station. During the event, the No. 2 generator suffered a mechanical over-speed event that caused it to fail catastrophically by shearing off its shaft and breaking through the generator casing. With the vibration and the metal fragments flung through the power station, a quarter of the building was destroyed, and all four generating sets installed at the time were rendered unserviceable [1], [167].

Figure 55: Vereeniging Power Station following a catastrophic failure in 1925 [2]

There was no deliberate approach to separate plant functionally in third-generation power stations since operational flexibility was a key objective. This aspect has largely been resolved in the design of the subsequent fourth-generation power stations, where generating units were functionally separate and somewhat isolated, reducing the probability of catastrophic failure events from affecting adjacent units. The benefit of such an approach of separation can be seen in the highly destructive catastrophic failure event that occurred at Lethabo Power Station on 23 November 1989 when the boiler suffered a furnace explosion. Although the boiler was largely destroyed and had to be rebuilt entirely, none of the other units suffered any damage of note and was not affected operationally.

Another event demonstrating the enhanced resilience of fifth-generation power stations during catastrophic failure events occurred at Duvha Power Station in South Africa on

8 January 2003. While the unit was in normal operation, a turbine blade on an LP rotor failed and breached the turbine enclosure at 06:20. The extreme unbalance caused various failures on the turbo-generator, including failure of the hydrogen seal, causing a significant fire and large-scale damage to the centre line.

Figure 56: Duvha Power Station following a catastrophic turbine over-speed failure in 2011 [168]

Even though the entire turbo-generator was essentially destroyed and the fractured pieces were flung great distances, none of the adjacent units tripped or had to be shut down as a direct result of the failure and regular operation continued at the other units.

The most spectacular example on a global scale that illustrates the concept of a catastrophic failure impacting multiple generating units is the failure event of almost legendary status that occurred on 26 April 1986 at the Chernobyl Nuclear Power Station in the USSR (modern-day Ukraine). During the event, the No. 4 reactor suffered a catastrophic failure when a steam explosion ruptured the containment enclosure of the reactor, with a subsequent open core fire ensuing and raging for nine days before being brought under control, with a considerable radioactive release as a consequence.

The event was initiated when a planned safety test went wrong (the emergency reactor cooling system was deliberately disabled as part of the preparations for the test). When operators manually activated a forced emergency reactor shutdown, the shutdown failed due to deficiencies in the design and construction of the reactor and its safety systems. The reactor entered an uncontrolled state instead, wherein the nuclear reaction caused a high level of heat energy to be released. This uncontrolled heat release evaporated the available water into steam, causing an overpressurisation that exceeded the integrity of the containment enclosure and resulted in rupturing. A fire was unavoidable with the core exposed to the atmosphere at extremely high temperatures [169].

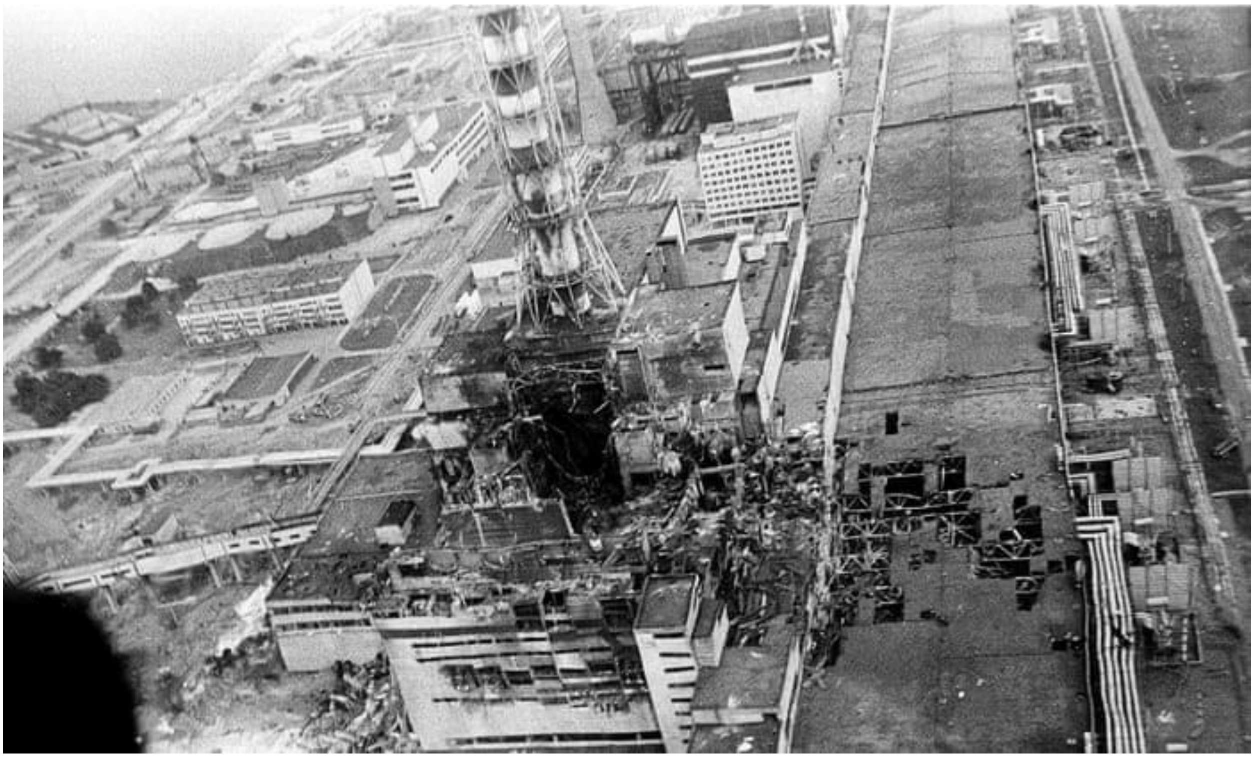


Figure 57: Chernobyl Nuclear Power Station following a catastrophic failure in 1986 [169]

Following the event, all the other three generating units were shut down and remained off for several months before they were allowed to start up again. This event, therefore, resulted in a total capacity of 4000 MW being lost from the system for a protracted period. Also, the additional eight units planned to be added over time to this location, which would have been fully operational by 2010, were all cancelled as a result – the total capacity planned would have totalled 12 000 MW. Instead, unit No. 2 was permanently closed down in 1991, followed by unit No. 1 in 1996 and unit No. 3 in 2000 – all units prematurely.

5.6.2 Single Point of Failure

The inherent vice associated with a design that features a single point of failure has been the feature of many engineering publications, textbooks and articles alike. It is, therefore, hard to believe that such a design flaw could occur in modern power station design. However, although a single point of failure is readily considered based on individual units, single points of failure cases, where multiple units are concerned, are less often less obvious to identify and remedy.

As a case study, consider an event that occurred at Grootvlei Power Station – a fourth-generation power station. Initially, Grootvlei was synchronised to the power system for the first time in 1969 and was finally decommissioned in 1990 when there was a general oversupply of electricity in South Africa and the unit size of the Grootvlei units was small (200 MW) compared to the median size of units in the fifth-generation fleet that was the predominant standard at the time (~650 MW). However, due to the relatively short lifetime of Grootvlei, its units were mothballed, and the entire station was placed in long-term storage until the dawn of the new millennium when South Africa started to face a power shortage again.

It was decided that returning Grootvlei would relieve the constrained power system within a shorter period than building new capacity. A comprehensive refit program was carried out on the Grootvlei units, including renewing its instrumentation infrastructure. Eventually, Grootvlei was returned to service in 2008, when it was envisaged that it would be merely required for about eight years until new capacity could be brought online.

At about 08:45 on the morning of 8 June 2009, two units tripped simultaneously. Upon investigation, it was found that the main CW pumps of both units tripped as a result of a low centre well level (refer to section 5.6.7.2.1) The protection scheme that tripped the main CW pumps used a level detection system that relied on two independent plant instruments to determine the water level in the centre well. A main CW pump would only trip when a concurrence exists between both instruments that a low-level condition occurred (a so-called two-out-of-two philosophy) – the malfunction of any one of the instruments would, therefore, not cause a trip, hence the initial viewpoint that such an installation does not constitute a risk in terms of a single point of failure.

However, when considering the circuit (or scheme) that produces the logic trip state, it remains a single functional block that could suffer failure or malfunction, compromising every main CW pump that takes suction from the centre well. On the day of the trip, the water contained in the CW system was being dosed to eradicate the bacterial problem prevailing at the time. The dosing agent (a biocide) caused excessive foaming of the water that floated on top of the water level of the centre well and eventually enveloped the level instruments, causing the malfunction of both to produce a false low-level signal to the control system. And since both instruments suffered the same fate, the logic condition for a trip was met, and the trip state was set to “true”. Since none of the CW pump protection schemes primarily ascertain the centre well level for themselves but instead rely on a standard two-out-of-two logical function block, all the CW pumps would see the same condition that would cause them to trip – four pumps in this case.

The actual water level in the centre well was not low but within normal tolerances; hence, the CW pumps should have remained in service. It was only realised after the fact that any condition that would violate the integrity of a single protection function (the low-level protection scheme), would compromise all main CW pumps in operation and cause all the units sharing the system to trip. In this case, it was a foaming event, but various other possibilities could readily be envisaged to have a similar result.

The issue, in other words, was not that there may or may not have been a redundant instrumentation philosophy, but rather that multiple units stood to be affected by the failure of a single logical function block – thus, a single point of failure despite redundancy in the primary measurement devices. The design structure for this example is conceptualised in Figure 58.

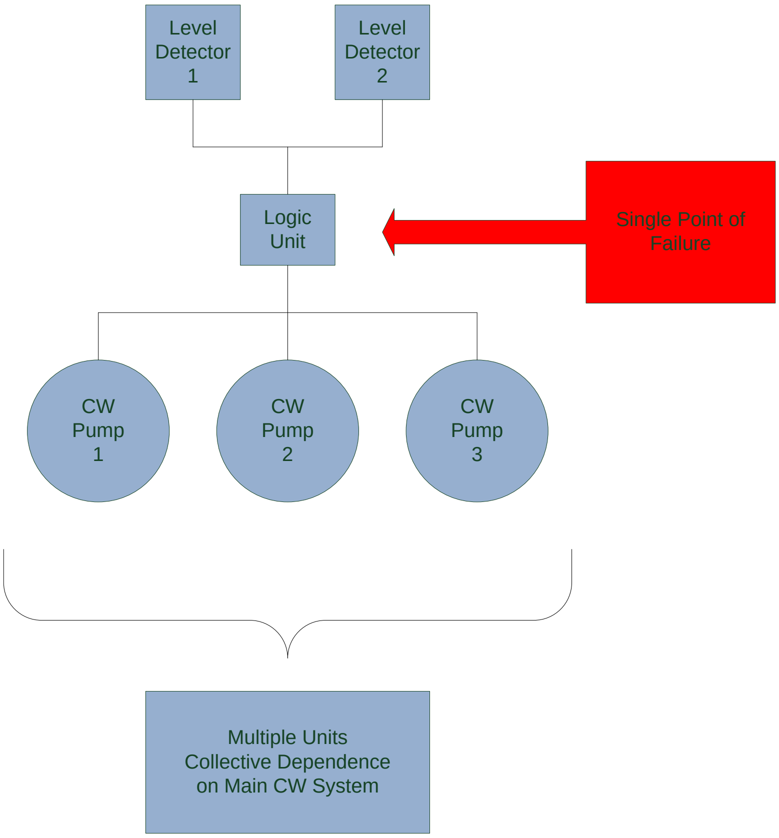


Figure 58: Example of Single Point of Failure for the Grootvlei event of 2009-06-08

A preferred solution to this problem would have been to instrument each unit and each main CW pump with its own unitised protection scheme that would achieve the desired objective – thereby largely divorcing the individual units from each other regarding common disruptors. An even better solution would have been to additionally vary the types of instruments to use dissimilar measurement principles or even to use primary process parameters in conjunction with primary measurement equipment to derive tripping conditions. Thus was the nature of the recommendations following the Grootvlei MUT.

5.6.3 Abnormal Configuration

A point often reiterated in preceding sections is that power station designs are deliberately bolstered with various flexibility attributes, such as redundancy, to make them more resilient. As a result of this design approach, various plant configurations are often possible while in operation.

However, it is often true that one configuration is more advantageous than another, and it is, therefore, operationally desirable to favour the most advantageous configuration over the others if conditions permit. The most advantageous configuration is, therefore, denoted as the default (or normal) configuration. Procedural guidelines direct operations to consistently use default configurations whenever possible.

The general approach is that the plant should remain in its default configuration and only be reconfigured due to a specific circumstance that necessitates it. But as soon as a reconfiguration is no longer necessary, the plant will be restored to its default state (as soon as possible). Abnormal plant states could, in many cases, be required for prolonged periods, depending on the necessity that led to the reconfiguration. And because a reconfigured plant state is not *per se* unacceptable, operators often fail to restore the plant to its default state – nothing automatically flags or alarms the deviation from the default condition.

Managing reconfigured plants and diligently restoring default states require dedicated management, supervision, oversight, operating procedures and systems – it is otherwise readily overlooked.

Although many examples exist where a deviation from a default plant state directly led to a multiple disruption event, it is sufficiently self-evident not to require illustration at the hand of a case study. Suffice it to say that non-default configurations are often identified as the very means through which an event was allowed to develop into a cascade of subsequent disruptions.

Refer to section 5.6.10.2 for a detailed exploration of non-default electrical configurations.

5.6.4 Coal and Ash Conveying Systems

As discussed above, many systems are shared or common between the various generating units at power stations. However, one of the more evident and intuitive systems that would disrupt multiple generating units is a disruption of the common fuel supply to the power station.

Figure 59 shows the typical redundancy levels of a modern fifth-generation, six-pack power station's coal supply and ash removal systems.

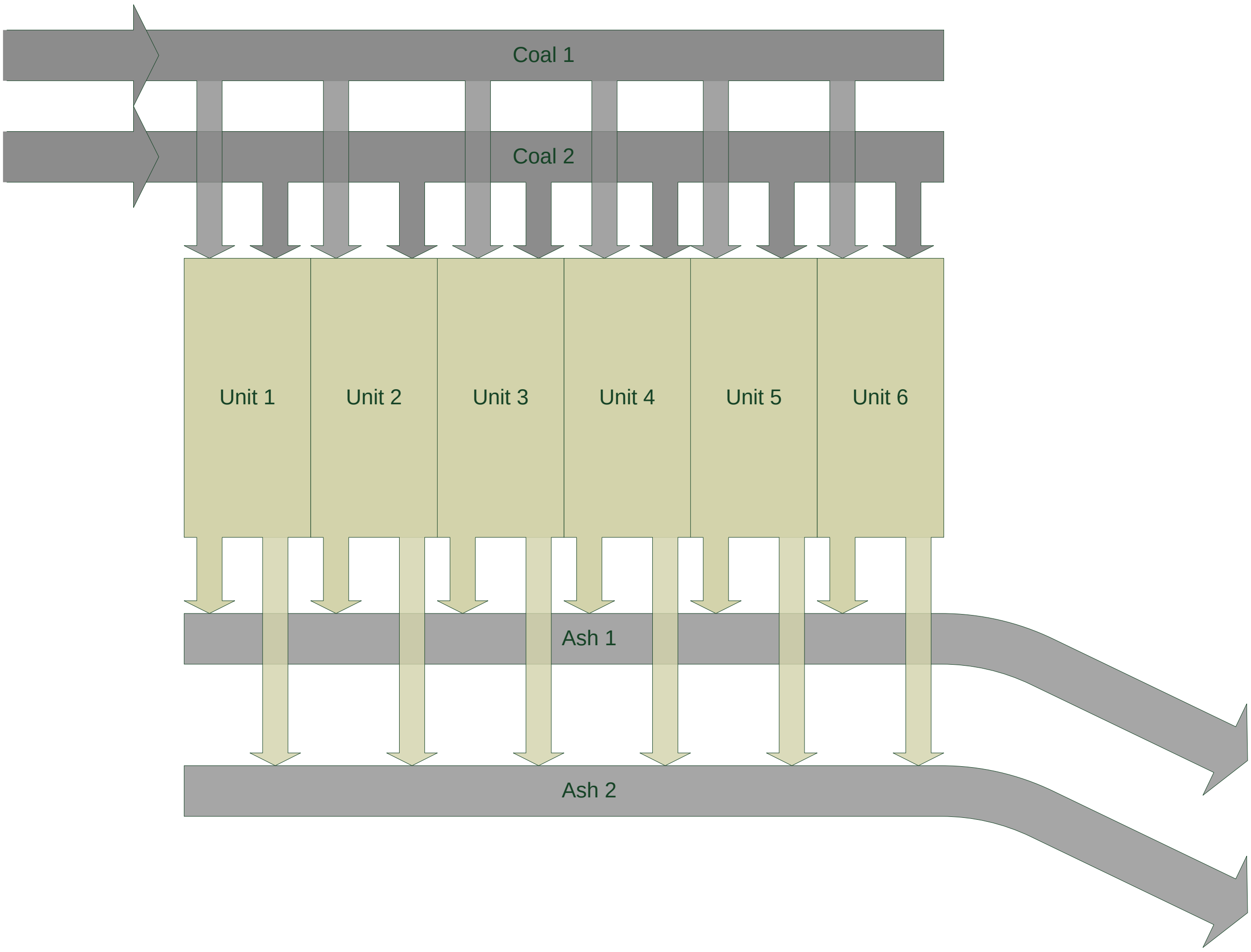


Figure 59: Power station common coal and ash system redundancy

As can be seen, both the coal supply and the ash removal systems are entirely duplicated, and both systems can cope with the total demand of all power station units operating at full load conditions. This implies, that the power station can continue to operate all its units at full production despite an entire coal supply system and an entire ash removal system being unavailable.

Despite the 100% redundancy that has been designed into the coal supply and ash removal systems, these designs still contain vulnerabilities that can lead to an event where both coal or both ash systems fail simultaneously, thereby compromising the continued operation of an entire power station. One such vulnerability is that the two sets of conveyors that comprise the two systems still share a common access corridor. This means that although the two conveyor systems are functionally separated, they are not geographically separated and are vulnerable to an event that threatens the corridor. One example of such a threat is fire. Once a fire starts and forces a conveyor system out of operation, it is almost impossible to prevent a fire from spreading to the second conveyor system that is located adjacent to the first. Such an event often leads to both conveyor systems becoming simultaneously unavailable, leading to the disruption (and possibly the shut-down) of some or all units in service at the power station at the time of the event – depending on the specific case. This type of event is not merely possible but has frequently been recorded.

Precisely such a fire-related event occurred at Lethabo Power Station on 10 October 2007 when a fire started on an incline conveyor transporting coal from a coal silo to a mill bunker of unit No. 1, destroying 250 m of belting and idlers. Due to the proximity of the incline conveyor of unit No. 2 (both sharing the same structure), the fire rapidly spread to the unit No. 2 conveyor, destroying about 150 m. Total conveyor destruction was prevented due to the fire suppression system activating automatically to activate the deluge system in the specific conveyor structure. In a remarkable repair and recovery effort, both units resumed normal service the following day after a 26-hour two-unit disruption event that incurred a ≈30 GW·h energy forfeiture.

A case study of such an event, but on a more dramatic scale, occurred on 1 November 2014, when a coal silo structurally failed and collapsed at Majuba power station. In this instance, although the conveyor system again had a 100% redundancy, both conveyor lines relied on one specific silo as a civil structural support. In this respect, the silo represents a single point of failure within the coal supply scheme of the power station as shown in Figure 60.

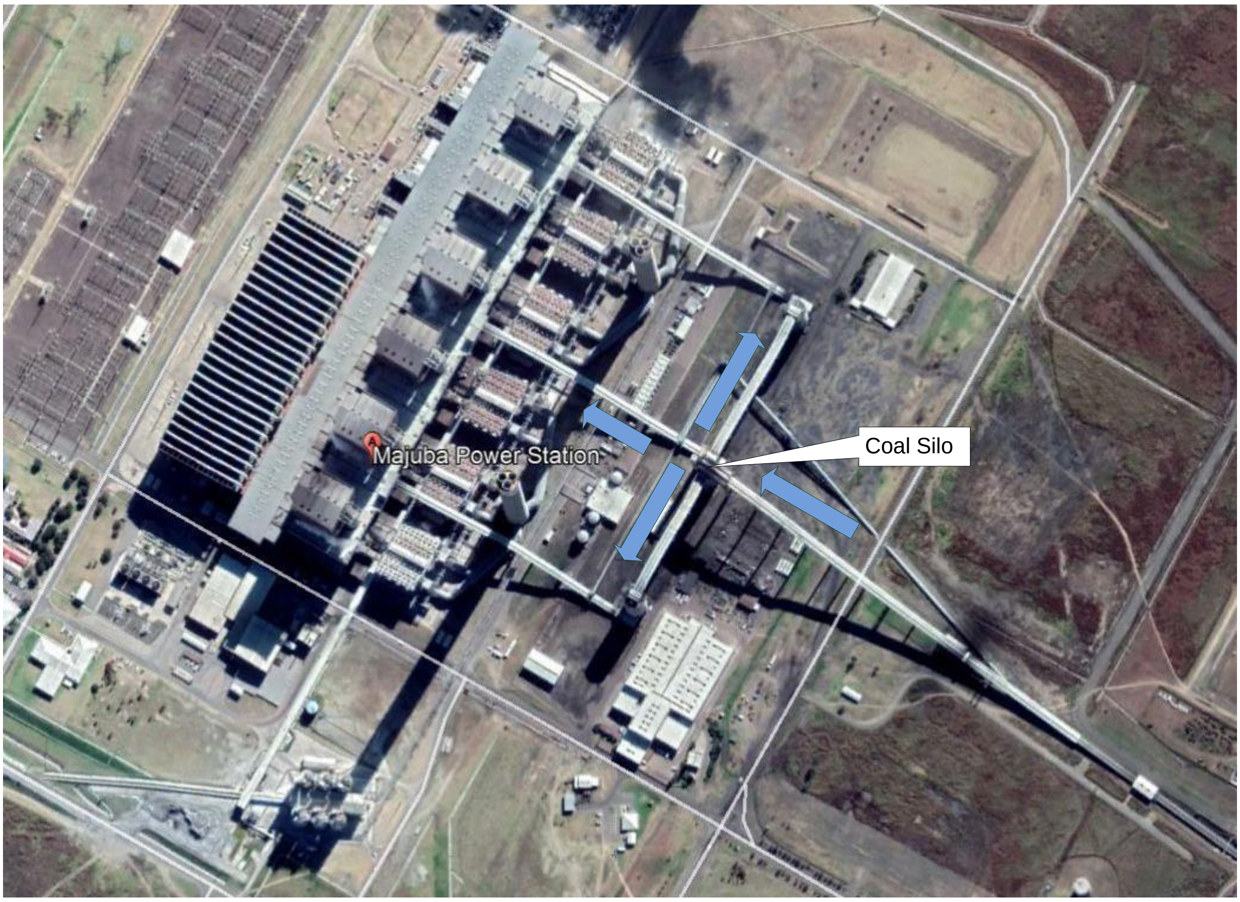


Figure 60: Majuba Power Station coal supply conveyor system [170]

In this aerial view of Majuba Power Station, the blue arrows represent the possible coal flow depending on the plant set-up at the time. When replenishing the coal supply to the power station, coal flows from the coal stockyard up via an incline conveyor, where the coal can either be deposited into the indicated silo or diverted in one of the directions indicated by either of the three arrows leaving the silo. If, however, as in this specific case, the indicated silo itself fails structurally, no further resupply of coal to the power station is possible.

During the failure event, emergency measures had to be taken by erecting temporary makeshift conveyors to enable normal production to resume until the silo could be reconstructed. Only the relatively small quantity of coal left inside the coal bunkers allowed for minor electricity generation volumes. The result of the silo failure event caused all six units of the power station to be adversely affected – all of which had to operate at reduced output levels for about 100 days when the interim system was supplying the power station coal needs once more.

However, during the 100 days, 179,5 unit-days of production loss were suffered at this power station, or a total of 29,9 station-days. This means that during this period if all the energy that the power station could not produce is accumulated, it would amount to the power station being entirely out of service for 29,9 days. Majuba has a rated output of 3,8 GW and was effectively not producing any power for 29,9 days over that period, significantly impacting the power system (1,5 TW·h), about 15% of the power system during that time. This condition was exacerbated because the production impact was unforeseen and therefore unplanned – and far exceeded normal reserves being provided for during contingency planning. The net effect of the Majuba failure was the substitution of electricity by fewer economic sources and load shedding within South Africa, estimated at 500 GW·h during the 100 days.

Another example illustrating such a single point of failure within a coal supply system of a power station occurred in October 2019 at Medupi Power Station. Although most of the coal supply system internal to the power station also features a 100% redundancy level, the main supply system into the power station from the tied mine consists of a single conveyor system. It was believed that the lack of redundancy on the main infeed artery could effectively be offset by a vast silo with a five-day coal reserve that would be maintained by the single infeed conveyor. However, the failure of and damage to the infeed conveyor did result in a significant disruption in production, affecting all six units – proving that the design assumption was inherently invalid. Although the repairs could be carried out on a significantly shorter time scale (only about one month) than the silo failure of Majuba, the production impact was high, with a total of 4,1 station-days being incurred within the month at an energy forfeiture of 419 GW·h – partly because of the larger rated capacity of the generating units of Medupi being 720 MW.

The rate at which energy was forfeited in both the Majuba and Medupi Power Stations amounted to the same volume of 15 GW·h/day, which amounts to 23,4 unit-hours/day in the case of Majuba and 20,9 unit-hours/day for Medupi.

These vulnerabilities of redundant systems exist for every type of common or shared system used at power stations. The greater the degree of redundancy, the lesser the probability becomes for an event to cause all levels of redundancy to fail and ultimately culminate in a multiple-unit disruption event. However, despite the strict redundancy protocols used in the design, operation and maintenance of power station systems, every single common system within the designs of modern power stations in South Africa has suffered total failure and subsequent multiple unit disruption – no exception.

In the preceding two examples, the vulnerability represented by a single point of failure was repeatedly emphasised. However, it is also possible for a fully redundant system to fail. A fully redundant system, i.e., a system comprising of two separate systems that are individually capable of handling the full burden that is required, can also fail in cases where both separate systems become concurrently unavailable – despite this possibility being statistically significantly less probable than for the case where a single system exists in isolation to fulfil the task.

An example of such an event occurred in November 2014 at Lethabo Power Station, attributed to the ash removal system. Like the coal supply to a power station, the ash removal system of Lethabo is also fully redundant, consisting of two separate systems. Each system comprises 18 conveyor belts with a total length of 8 km for each of the two systems. Due to the unusually high ash content of the coal used for electricity generation by Lethabo, ranging between 34% and 42%, and with an exceptionally low calorific value of about 16 $MJ \cdot kg^{-1}$, the power station is producing vast ash volumes to operate at its rated generating value of 618 MW for each generating unit at this six-pack power station. The rate of producing flyash alone amounts to about 135 tonnes per hour within every boiler furnace operating at maximum capacity – the maximum within South Africa and amongst the highest in the world [171].

Due to the dire condition of the Southern African Power Pool at the time, with the Majuba coal silo failure that occurred on 1 November 2014 (as discussed above), conditions necessitated the continued operation of all coal power stations within the Eskom fleet as an overriding priority – unless forced out of service. With the vast ash handling burden of Lethabo, the level of ash plant maintenance is unusually high. But with all six units in service and with system demand requiring high loading at this time (often emergency levels beyond MCR), the ability of the ash plant to cope with the unrelenting production of ash rapidly deteriorated. Ultimately, the combined efforts of the Operating, Maintenance and Engineering functions failed to ensure that ash could continually be evacuated at the requisite rate necessitated by this abnormal loading regime. The long-term effects of inadvertent failures, blockages and stoppages of sub-systems caused all internal interim ash holding facilities that are part of the design of the plant, to become ever more depleted until all holding facilities were filled. Despite load reductions that were implemented to reduce the ash production rates from the boilers, breakdown maintenance could not cope (or catch up) with the ever-increasing backlog of ash requiring evacuation.

In a desperate yet futile attempt to continue operation with the full internal ash holding capacity now being exhausted and with no sufficient means for evacuation, the ash had to be dumped at ground level in various locations within the ash handling terrace of the power station. Since the power station ash handling terrace has not been designed for emergency dumping, it does not feature any ash reclaiming facilities, further worsening the desperate conditions wherein repair work had to be conducted.

This untenable situation resulted in an unavoidable decision to shut down two units, with a third unit that was subsequently forced into shutdown due to consequential damage. At this point, vast external resources had to be mobilised to recover the power station once more to become fully operational. Figure 61 shows the rapid increase in the unavailability of the ash removal systems of Lethabo for the event compared to the preceding months.

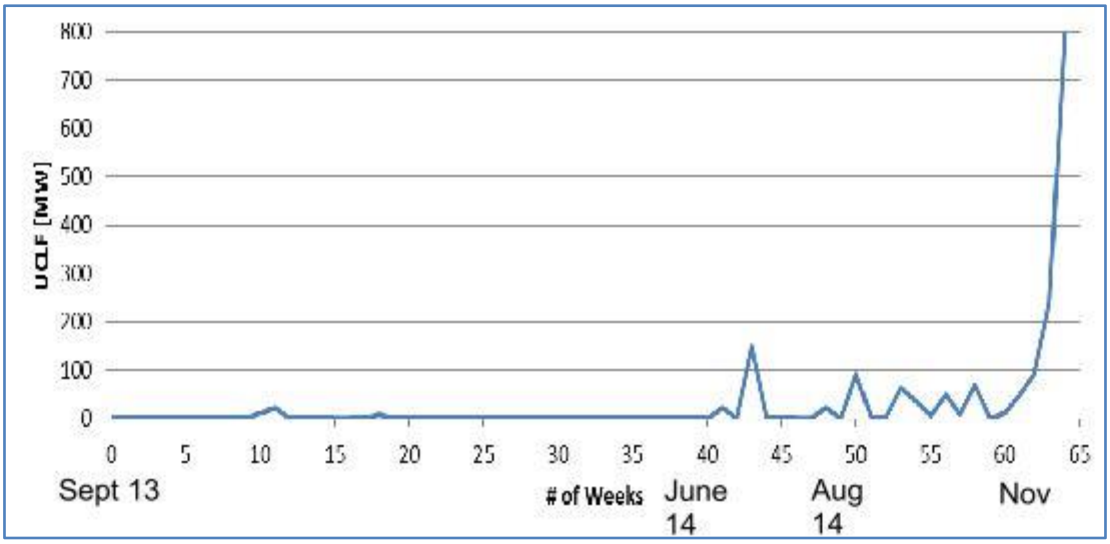


Figure 61: Lethabo ash removal plant unavailability

In this example, both ash removal systems failed due to multiple sub-system failures, causing the partial or total disruption of all six power station units. Lethabo had largely recovered from this event by 14 December 2014 and incurred a total of 5,7 station-days of lost production, amounting to an energy forfeiture of 485 GW·h, an average rate of 11 GW·h/day.

Engineers often maintain the delusion that a single point of failure is effectively mitigated by bolstering the design to incorporate redundancy. Although redundant designs generally perform statistically better than systems without them, the obvious possibility of concurrent failures within a redundant design is often overlooked or disregarded. Power stations are often operated for periods exceeding 50 years, and studies of likelihood over such timeframes reveal that highly unlikely events often materialise. Empirical evidence shows that highly unlikely events occur, often several times over the plant's life.

5.6.5 Fuel Oil and Ignition Gas

Under normal operating conditions, coal power stations derive their energy solely from coal. However, when a coal-generating unit needs to undergo *light up*, a process of starting the unit from a state of being entirely off and dormant to stable electricity generation, other fuel sources are required. This typically involves igniting a jet of flammable gas, usually propane, at each burner entry into the boiler furnace using an electric arc. Once the gas flame is established, a relatively inexpensive liquid fuel is introduced at high pressure (typically ≥4 MPa) through injector nozzles, which are ignited with the gas flame already burning. Once the liquid fuel burns steadily, the gas flow stops, and the flame is sustained only by the liquid fuel. This liquid fuel flame is then used to raise the temperature within the furnace sufficiently to allow fine coal powder within an ample stream of air to be introduced through the burners, which is then ignited with the liquid fuel flame already present.

Once the unit has been loaded sufficiently for coal flame stability to be ensured, the liquid fuel can be cut off, and the unit will operate on pulverised coal powder only. This mode of operation can then be maintained indefinitely until an operating condition forces the unit into a low load condition when liquid fuel needs to be reintroduced once more to stabilise the unit and prevent it from becoming unstable and tripping.

Therefore, it is not apparent that a disruption of the fuel oil or ignition gas systems can cause a severe disruption in generation, seeing that the units are not constantly dependent on these systems. The risk stems from these sub-stable modes of operation, i.e. light-up and low-loading conditions.

Such an example of a disruption event that affected multiple generating units at a power station occurred on the weekend of 15 and 16 May 2004, when Arnot Power Station found itself with insufficient fuel oil stock to return two units that were previously shut down, but which had to be returned to service to meet the Monday morning peak demand on the power system. Although the root cause was traced to a contractor failing to deliver as contracted, the event nonetheless left the power system having to substitute the contracted power from the two Arnot units with more expensive sources, with an energy forfeiture manifesting at Arnot amounting to 10,4 GW·h.

In the case of Arnot, it is clear that the nature of the disruption prevented generating units that were not yet in operation from returning to service but did not interfere with those units that were in operation at the time. However, it is also possible for the fuel oil system to disrupt the operation of units that are generating power. Such an event occurred at Grootvlei Power Station on 11 December 2019. Five of the six power station units were in operation during the event. Due to heavy rain preceding the event, all five units were impacted by operational problems emanating from the coal soaked with rainwater. Specifically, all five units were experiencing combustion stability problems and all units made use of fuel oil to support and stabilise combustion in the boiler furnace.

This is an unusual condition for the fuel oil system of the power station, which normally only requires support for the light-up of a single unit or for supporting one or two units that may experience difficulty with furnace stability. However, with fuel oil support required on all burner rows of all five running units, the fuel oil system was strained and consumed the fuel oil reserves at a high rate. When the fuel oil bulk storage tank reached 31%, one of the six low-pressure (LP) fuel oil pumps tripped incorrectly on a low suction pressure protection function. Despite the remaining five LP pumps remaining in service, the loss of a single LP fuel oil pump (under the conditions of exceptionally high fuel oil delivery flow) caused the LP fuel oil range to experience a low-pressure condition beyond the specification of the high-pressure (HP) fuel oil pumps taking suction from the LP fuel oil range. This low-pressure condition resulted in all HP fuel oil pumps tripping on a low suction pressure protection, starving the HP supply line that supplies the generating units. With the supply line pressure falling, all burners lost fuel oil support, and all five generating units tripped due to furnace instability.

The consequence was that all six units (including the one not yet in service at the time) had to be lit up using fuel oil. Since the level was already depleted, it took a prolonged period before sufficient deliveries were received to allow for the return of all six units. Grootvlei suffered unavailability totalling 7,1 station days with an energy forfeiture of 31,7 GW·h, having to be sourced from elsewhere.

5.6.6 Liquid Fuel – Gas Turbines

The complexity level of power stations using liquid fuel as a primary energy source (gas turbine stations) is far lower than for coal-fired power stations. This attribute is mainly due to the auxiliary footprint of gas-turbine power stations, which is much smaller than that of coal-fired stations.

Due to the absence of abundant natural oil and gas reserves in South Africa, the region did not generate much capacity using this technology. In 1976, two small liquid fuel power stations were added to the South African power system, namely Acacia and Port Rex Power Stations in the south of the country – with three units of 57 MW each. For about 30 years, these two power stations remained the only gas turbine power stations in South Africa. In 2007, two new facilities were commissioned, i.e., Ankerlig and Gourikwa Power Stations, with Dedisa Power Station to be added in 2015 and Avon Power Station in 2016.

The fuel management system is the predominant common auxiliary system shared between gas turbine power station units. It consists of a large bulk storage repository from which a fuel forwarding plant extracts fuel and delivers it at pressure to the units. This fuel forwarding plant, therefore, represents the Achilles heel of gas turbine power stations.

As a case study, consider the event at Ankerlig Power Station of 7 April 2013. A signal from the fuel forwarding plant became compromised, resulting in the tripping of five units in service and being supplied from the fuel forwarding plant at the time. The event caused a total loss in generation of 703 MW, as shown in Figure 62 of the total system load at the time of the event.

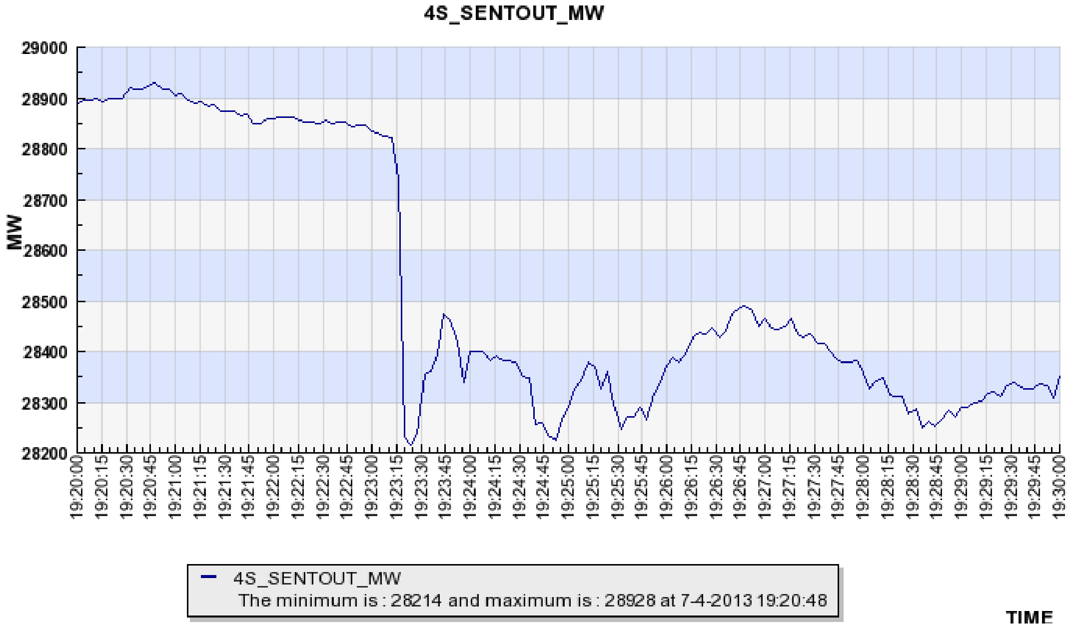


Figure 62: Loss in system power for Ankerlig event of 2013-04-07

A loss of 703 MW may not seem extreme in the context of multiple unit disruption events, but it needs to be viewed correctly. These gas turbine power stations in the South African power system exist purely for peaking duty. This means that when this plant is in service, most of the other spinning reserves have already been depleted, and the peaking plant, Ankerlig, was brought into service to fill the existing gap. Suppose the system is already at a deficit of resources and the peaking plant becomes compromised, it automatically leads to an abnormal, if not emergency, condition in managing a power system.

In this example, the mere loss of 703 MW resulted in a frequency disturbance from 50 Hz down to about 49,297 Hz, which required bringing an additional seven peaking units into service. Two interruptible loads also had to be utilised to recover the frequency.

Although other causes could also disrupt gas turbine power stations, the fuel handling system dominates the disruption profile that compromises multiple units.

5.6.7 Main Cooling Water System

The steam turbine is one of the most fundamental components in various power stations worldwide. It is specifically used in coal, nuclear, geothermal, and concentrated solar power generation. Steam is the fluid that transfers energy from a heat source to a prime mover, which converts heat into mechanical energy required for electricity generation by electromagnetic means.

The steam turbine can extract the heat contained in the steam and convert it into kinetic (rotational) energy. For the steam to flow through the turbine, a pressure differential must exist between the inlet and the outlet. Consider a representation of a steam turbo-generator shaft train that is typical for coal power stations.

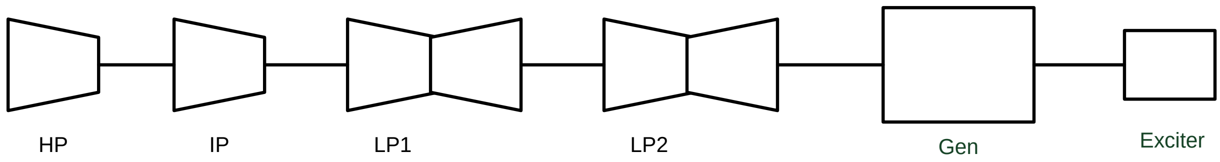


Figure 63: Typical turbo-generator shaft train for a coal power station

The turbine assembly shown features a high-pressure (HP) turbine, an intermediate-pressure (IP) turbine and two low-pressure (LP) turbines, LP1 and LP2. Steam produced by the boiler would be admitted to the HP turbine, then returned to the boiler to add heat to the steam before being admitted to the IP turbine. The steam would then be split into two streams and admitted equally to the two LP turbines. In every one of the turbines (HP, IP and LP), energy will be extracted and converted, and for every one of the turbines, a pressure differential needs to exist between the inlet and outlet of the said turbine to ensure flow. At the point in the process when the LP turbine is reached, there is no adequate pressure differential to achieve the requisite steam flow needed to achieve the desired energy exchange unless the outlet pressure can be lowered to below ambient atmospheric pressure. The reduction in pressure is achieved by condensers at the outlet of the LP turbines which develop the reduction in outlet pressure, called vacuum.

The vacuum established by the turbine condensers is achieved by extracting sufficient heat from the outlet steam so that condensation occurs (through a steam-to-water heat exchange), causing a volumetric reduction and hence a relative vacuum develops. The water introduced into the condensers to absorb the remnant heat for condensation to occur is, in turn, supplied from a cooling system designed to dump the absorbed heat into an appropriate sink.

The amount of waste heat is considerable. If a generous assumption is made that the overall thermal efficiency of a coal unit is 35%, it implies that 65% of the energy released during combustion is not converted into electricity and is, therefore, a loss. The thermal losses typically amount to about 60%, with auxiliary power consumption typically ranging between

5% and 10%, depending on various factors. This means that if a large unit operates at 600 MW, heat needs to be rejected at a rate of 900 MW, which is not converted into electricity and is therefore discarded.

Various methods reject the "non-useful" (waste) heat at power stations. The first general category utilises an external body of water from where water is taken, used for cooling and then returned to where it was taken from. A second general category employs on-site heat dissipation through a waste heat rejection system.

A third category also exists, whereby waste heat is dumped into the water system for an adjacent local community to utilise for residential heating or to prevent water pipe systems from freezing. This third category will not be considered further since it is rare and esoteric.

5.6.7.1 Water Body Extraction and Return

It is evident from the outset that water was an essential ingredient in the process of developing power stations. Therefore, power stations were invariably constructed near a body of water from where water would be extracted to be used in the cycle. However, initially not being a mature technology, waste heat rejection was not regarded as one of the more fundamental problems. Water was circulated through the condensers by taking water from the body and returning it.

5.6.7.1.1 Dams and Ponds

With South Africa being an arid country, obtaining a suitable body of water for a power station is a significant problem. Bodies of water were scarce, and with rivers often not being perennial, water sources often consisted of nothing more than a mere pan with a moderate and finite water volume – dependent on rainfall and sometimes a fountain for replenishing.

Simmerpan power station is a case in point. The power station was built at a pan, serving as both the source of process water and the sink into which waste heat was dumped (see Figure 64).

Figure 64: Simmerpan Power Station (1912) – water return in foreground (40 MW installed) [2]

This cooling method immediately became problematic since the water temperature soon became so high that generating sets could not achieve rated output and had to be operated at reduced production levels. Also, with the elevated water temperatures, evaporative losses from such a pan increased so that the process water (not for cooling) became constrained.

A technological approach to the problem was required. As power stations kept increasing in capacity, later stations started employing spray ponds, where heated water was sprayed into the atmosphere to facilitate increased evaporation and enhance the cooling of the water resource. This significantly improved the water temperature problem, albeit at the cost of higher water losses. Figure 65 shows an aerial view of Witbank Power Station, where such a technology was part of the power station design [2].

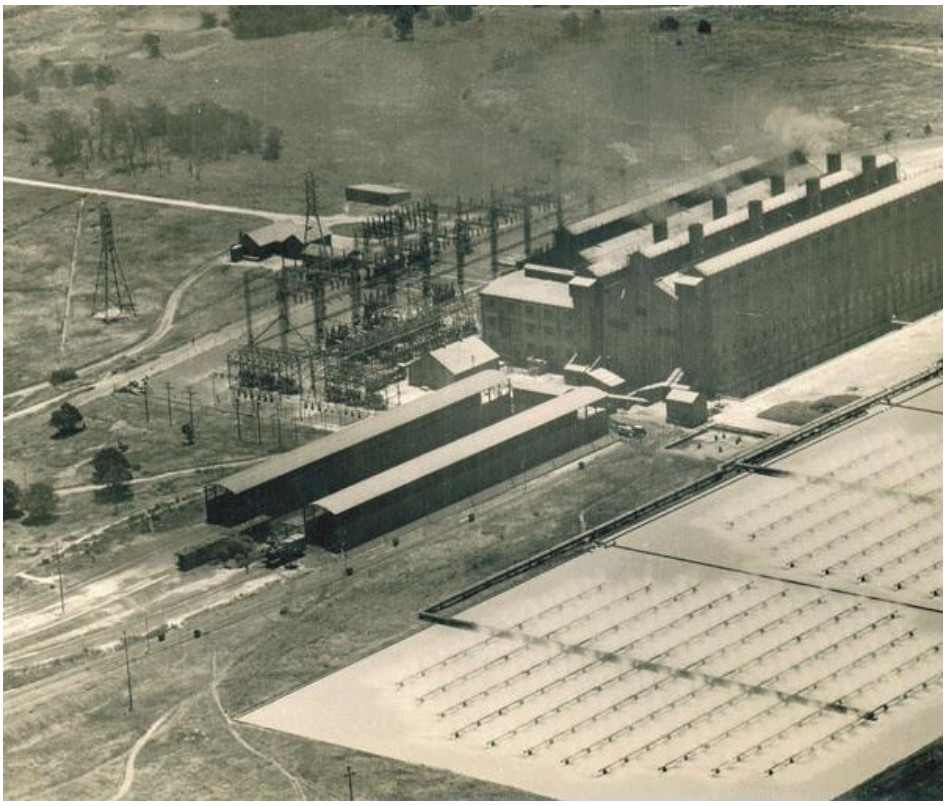


Figure 65: Witbank Power Station (1925) – spray ponds in the foreground (129 MW installed) [3]

Despite early advances in terms of technology, the finite nature of the water resource presented a commonality that readily led to the disruption of multiple generating sets – both from a heat sink and a process water perspective. It also introduced a limit to the overall capacity that a power station can have since the heat-swallowing capacity of a confined body of water will ultimately become too restrictive for the continued generation of electricity at higher power levels.

5.6.7.1.2 Infinite Water Bodies

One obvious solution to the problem discussed in the preceding section is to move from a confined water resource to an essentially unrestricted (virtually infinite) body of water, such as an ocean, perennial river or very large dams or lakes. In such cases, the thermal runaway problem discussed above would essentially be removed, and it would seem logical that the disruption potential for such an approach might be eradicated.

Such an approach to rejecting waste heat was first used in South Africa at Vereeniging Power Station. The power station was built on a coal field and directly adjacent to the Vaal River. Water was pumped directly from the river for condenser cooling and released back into the river. The water return is shown in Figure 66.

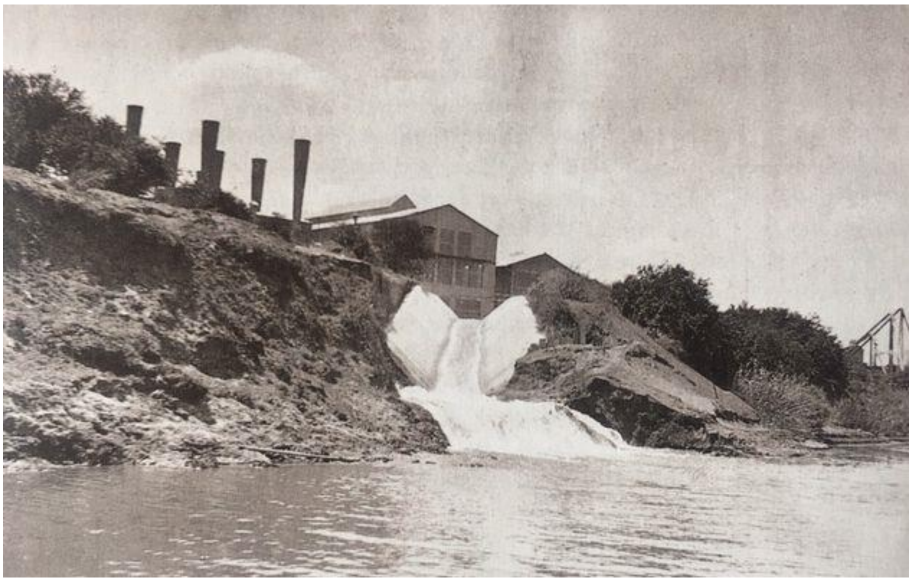


Figure 66: Vereeniging Power Station (1912) – warm water returns into the Vaal River [3]

This approach could have worked well if South Africa was not such an arid country, but due to periodic droughts the (virtually) infinite nature of the river as a heat sink often reverted to the very same constrained commodity with all the problems described above. The following photograph shows Vereeniging Power Station again, but now, during a drought that constrained the river to a limited reservoir above a weir to sustain the facility's operations. Droughts in South Africa are normally associated with high ambient summer temperatures – another undesirable attribute that further worsens the cooling problem for a power station of this era.

Figure 67: Vereeniging Power Station – drought interrupted flow of Vaal River [3]

Although this was not an ideal scenario from a cooling water perspective in the early 20th century in South Africa (before the construction of the Vaal dam that later sustained the river flow), it is nonetheless a method that is used internationally to this day. It is, however, also not a total solution in terms of a source of disruption. With power station capacities that have grown well into the gigawatt range, the amount of waste heat that must be dumped into such a river is vast, ultimately elevating the river's temperature. With an environmentally responsible operating plan, these plants are equipped with river temperature monitoring, necessitating plants to de-load when temperatures rise too much – to limit the impact on fish and other aquatic life. Protection functions that ultimately result in plants tripping from high river water temperature conditions are also common in European countries. Thus, even with abundant sources of cooling water, the threat of disruption persists.

It seems logical, then, that since even perpetually flowing rivers still suffer from temperature-related problems, the vastness of an ocean might provide the ultimate solution. Using seawater as a cooling medium instead of fresh water is common practice, especially in nuclear power stations, since it essentially eradicates the possibility of cooling water unavailability, even despite the most extreme drought conditions.

Koeberg Power Station in Cape Town (South Africa) is located on the coast for that purpose. It has an intake from the cold Atlantic Ocean, where large cooling water pumps take suction at a level lower than sea level to ensure constant water availability. Since seawater has management implications, the choice to use the ocean for cooling purposes does add cost to a facility – not only to the cooling water system but to the entire power station with significantly higher costs on most equipment stemming from a corrosion mitigation perspective.

Since the ocean is essentially an open environment, the cooling water system needs to be screened from debris or objects that may impede the functioning of the condensers. For this purpose, large rotating stainless-steel screens constantly filter out larger particles and objects that could pose a blocking or clogging risk in the condensers. Also, due to the abundance of life in seawater, a chlorine plant needs to exist and be operated (extracting chlorine from seawater through electrolysis) to facilitate the constant dosing of chlorine into the cooling water system to avoid the condensers from becoming a hospitable habitat for molluscs and algae – thereby detrimentally affecting the heat exchange performance of the condensers.

Despite these (and other) design features employed to mitigate against the disruption of the cooling water system, common mode disruption events still occur. One such event occurred on 3 March 1998, when a whale shark entered the sheltered area where the cooling water pumps take suction. To avoid the whale shark from being drawn into the intake itself, both units at Koeberg Power Station had to be taken down in load to 60% of full load each, and cooling water pumps switched off to enable the creature to be removed. Only after that were all cooling water pumps placed back in service, and the unit returned to full load.

Another cooling water event that resulted in a disruption at Koeberg Power Station occurred on 20 June 1999, when an unusually large "school" of jellyfish drifted into the intake basin of the power station. Despite vast efforts by staff, the cooling water screening system was overwhelmed by the immense quantities, and both units had to reduce power to 60% each, where they operated for about eight hours until the situation was under control and normal operation could be resumed.

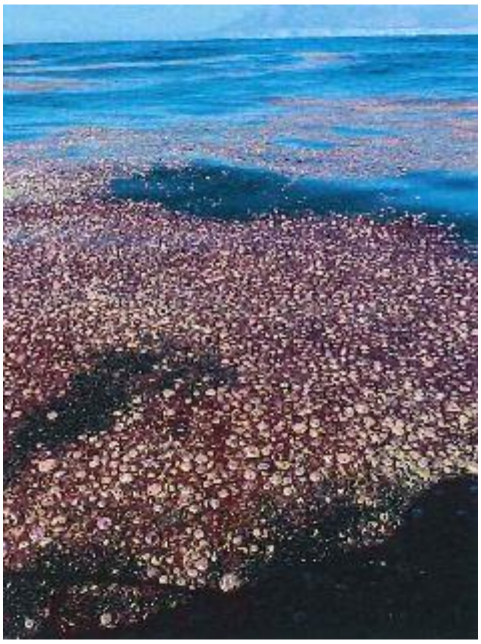


Figure 68: Jellyfish in the intake basin of Koeberg Power Station (1999)

Although an infinite heat sink is desirable, such a choice of technology merely trades one set of disruption threats for another and does not achieve immunity from collective disruption.

5.6.7.2 On-Site Waste Heat Dissipation

On a basic level, there are two ways in which waste heat can be dumped into the atmosphere. A wet cooling system relies on evaporation, and a dry cooling system relies on convection. Both have benefits and disadvantages, and both can disrupt multiple generating units. In the following two subsections, these two basic types will be discussed from the perspective of their individual capacity to cause disruption events affecting multiple units.

5.6.7.2.1 Wet Cooling

Consider the wet cooling system of a typical six-pack coal power station. To handle the vast waste heat burden from a sizeable generating unit, large quantities of raw water must be supplied to a running unit and continuously returned to the cooling towers, a closed-loop cycle. For power stations with multiple units, which is the *de facto* standard in South Africa, it is not practical to supply each unit with its own cooling water system. The bulk of the system is a common infrastructure serving multiple units. Therefore, a sub-surface ducting system is established below the power station units during construction, as shown to the right in the following photograph.

Figure 69: CW ducts being constructed below the turbine hall of a fifth-generation power station

Cooling water (CW) is circulated through the units' condensers and returned as warm water to the cooling towers for evaporative cooling (through which absorbed heat is sunk into the atmosphere), as illustrated diagrammatically below.

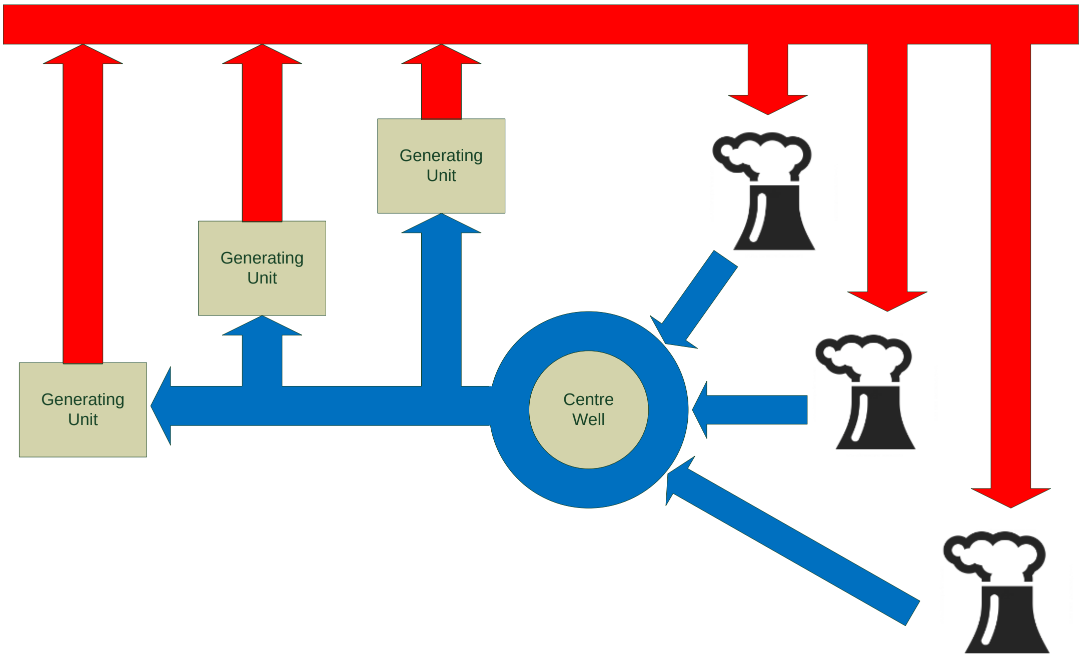


Figure 70: Cooling water cycle – wet CW system

The main CW system is divided into two separate systems, each serving three units (or half the power station units), as illustrated below.

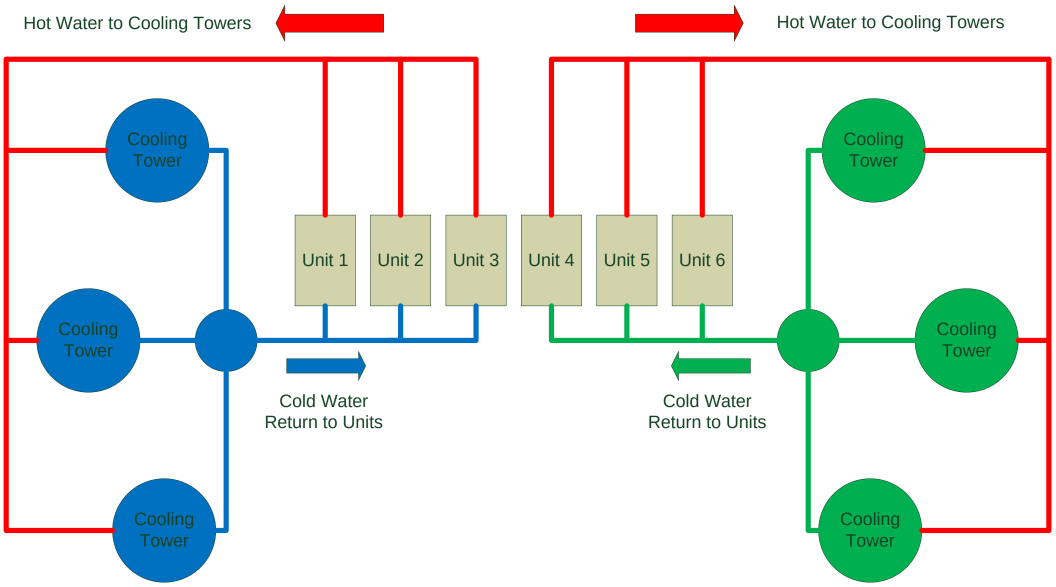


Figure 71: Typical wet CW system

This representation of the main CW system for a six-pack coal power station illustrates how (essentially) two separate CW systems supply water for units 1 to 3 by one system and for units 4 to 6 by the other system. Separating the main CW supply into two separate systems has the obvious benefit that a disruption in one of the CW systems would not disrupt the other CW system – effectively limiting the exposure to a CW system inter-station escalation event to not more than half the power station's units. This philosophy ensures compliance with the SAGC, and the largest three coal units in South Africa automatically set the upper planning limit for reserves, i.e., the *largest credible multiple contingency limit* (referred to section 3.2.3. [1]).

Therefore, the SAGC recognises the main CW system as having the potential to disrupt half of the units of a power station in events where it becomes compromised. A compromise of a main CW system may occur when failures of components of the system result in insufficient CW supply to the condensers of the units. The condenser vacuum will decay under inadequate CW supply conditions to the turbine condensers. A decay in condenser vacuum subsequently erodes turbine efficiency and ultimately results in conditions that are detrimental to the health and integrity of the turbine – conditions against which the turbine is protected by automatic turbine tripping functions.

The diagram above shows that three units (for a six-pack, wet-cooled power station) share a common hydraulic water system for cold and hot water waterways. Considering the details of this system at a lower level reveals a higher degree of complexity and commonality that becomes evident in the following illustration.

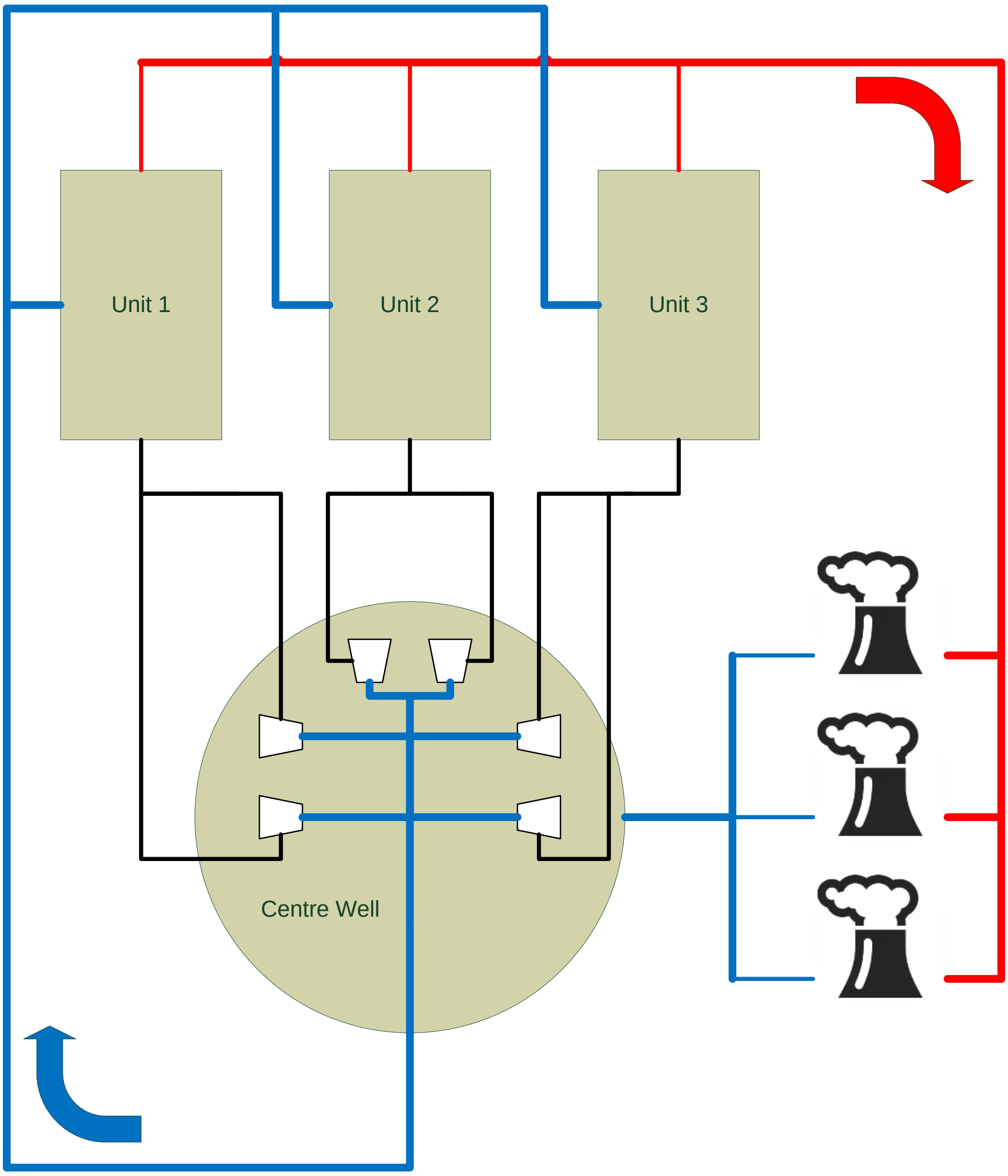


Figure 72: Main CW system – hydraulic and electrical dependencies

Illustrated above is the main CW system that is collectively shared by three units of a six-pack power station. It reveals that every unit has two CW pumps that are electrically powered from the relevant unit (shown by the black lines). All six CW pumps of the three units shown perform the collective pumping required to ensure sufficient CW flow back to the condensers of the units. When a single unit in the group of three becomes compromised to the extent that it no longer powers the two CW pumps allocated to that unit, the CW flow to the units is reduced by one-third of the flow before the event. Therefore, the reduction in CW flow causes a decrease in the condenser vacuum of the other two units in operation and the affected unit before the event. If the vacuum of the remaining two operational units deteriorates sufficiently, they will become compromised by automatically tripping their turbines to avoid turbine damage. Thus, disrupting even a single unit that shares the main CW system could result in an inter-station escalation and ultimately compromise the integrity of half the power station units.

This arrangement implies that not merely a failure in some part of the main CW system, which is truly common and shared by the units, can cause a cascading disruption event upon suffering a failure, but also a failure of one of the units being serviced by the system. This peculiar interdependency is because the main CW system is hydraulically common but electrically unitised.

Finally, even more interdependencies are revealed when considered at a lower level of detail. For example, the pumps are controlled by a common control system that controls all shared equipment installed in a common control room. The control equipment has a redundant set of two independent UPS power supplies. The control system and its power supplies represent another commonality, similar to the main CW system. However, it is not the intention to perform an exhaustive study on all aspects of commonality and interdependence but merely to demonstrate that these systems are inherently complex and that the absolute prevention of common mode failure events is not attainable without considerable skill, experience, funding and an ongoing management focus.

Wet CW systems, therefore, can cause the tripping of multiple units within a relatively short space of time (only separated by a few minutes), causing a repetitive drop in frequency – potentially requiring demand-side resources to avert a collapse in voltage or frequency that may otherwise result in a blackout. Therefore, this system sets explicitly the upper limit for the quantum of reserves to be provided for in the power system by the SO, being the *largest credible multiple contingency limit* as expressed in the SAGC [1].

The repetitive manifestation of system frequency can be seen in Figure 73 – a recording of the system frequency of the South African power system on 30 November 2010, when three units tripped at the Kriel Power Station. The event was initiated by the failure of a current transformer in the HV yard that caused unit 6 to disconnect from the power system. Since the Kriel Power Station is not equipped with unit islanding functionality, the process also tripped, rendering the unit auxiliaries de-energised. At the time of the trip, unit 6 was supplying two CW pumps that ceased to pump when the trip occurred. The common CW system was subsequently left with a deficit of CW flow – having lost 40% of its pumping capacity. This caused a mismatch between the heat being generated and the heat capability that could be rejected. Cooling has reduced by 40% while the rate of heat being generated is reduced by only about 30% – a mismatch of 10% caused a decay in the condenser vacuum of the two remaining units left in service utilising the same CW system. The rapid deterioration in the condenser vacuum subsequently results in the tripping of the remaining units.

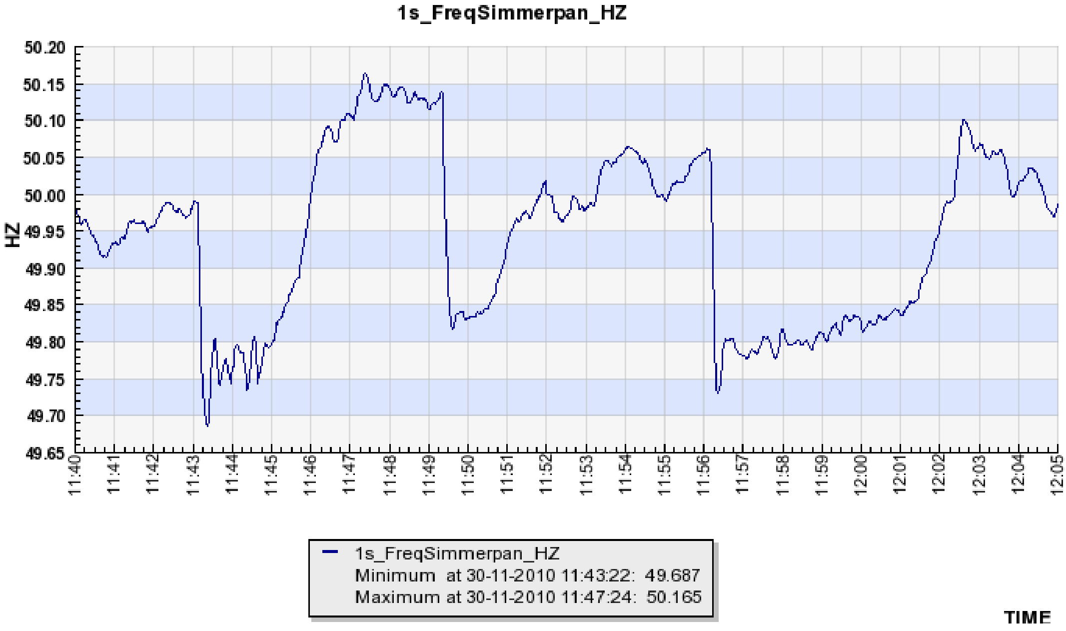


Figure 73: Power system frequency for Kriel MUT of 30 November 2010

For further examples of wet CW system events, refer to section 5.6.10.2 and section 5.6.11 respectively.

A final word on the use of common wet CW systems at power stations about the impact on producing energy to the power system. Wet CW systems that are shared between units periodically require sets of units to be taken out of service to maintain the CW system. This implication significantly impacts outage planning in power systems that may lead to constraints that force an uneconomic dispatch of electricity during such maintenance events. However, wet cooling units have higher thermal efficiencies than similar units with dry cooling systems. Therefore, electricity can generally be produced at a lower cost.

5.6.7.2.2 Dry Cooling

Dry cooling is becoming increasingly viable as a waste rejection technology in countries where water resources are increasingly exploited, and the opportunities to develop more thereof diminish. Especially in arid countries like South Africa, it becomes increasingly less likely that new large power stations would use wet cooling water systems, which for a long time were the *de facto* solution to the problem of rejecting waste heat. The most recent power stations built in South Africa employ dry cooling for the main CW systems.

The main attraction of dry cooling water systems is the reduced demand for water since the evaporative water loss occurring in cooling towers of wet CW systems is eradicated. In addition, significant cost savings can be achieved by not requiring the construction of cooling towers, vast civil structures requiring significant capital, and considerable decommissioning and demolition costs at the end of the power station's life.

However, like most decisions about heat and mass balances, these benefits come as a trade-off between capital and water efficiency on one side of the argument versus the cycle efficiency of the overall power generation process. The dry cooling designs implemented in South Africa were realised with a typical loss of 1,5% in the overall cycle efficiency (confirmed during the monthly thermal efficiency monitoring routines), amounting to a vast quantum of power over the life of a power station that is forfeited.

Essentially, a dry cooling system is similar to a wet cooling system in the sense that both systems use the atmosphere as a sink into which waste heat is dumped. In the case of wet cooling, evaporative cooling is used, while a dry system uses convection.

In most dry cooling applications, convection through airflow is achieved using vast batteries of fan banks driving air through heat exchangers. The auxiliary power required for this function is about 1,5% of the total rating of a generating unit and more than double the auxiliary power requirement of all the other unit auxiliaries combined. In addition, the maintenance associated with the dry cooling air-cooled condensers (and its fan banks) requires considerable and sustained budgetary allocations throughout the power station's life – for routine maintenance (planned and break-down) and life cycle replacements.

Dry cooling CW systems are, however, also exposed to disruption. The exposure that the dry cooling CW systems have stems from the design envelope of atmospheric conditions – which, once outstripped, results in an inevitable erosion of the generating capacity of all the units experiencing the atmospheric thermal exceedance.

Figure 74 shows the relationship of atmospheric temperature to generation capacity for Kendal Power Station.

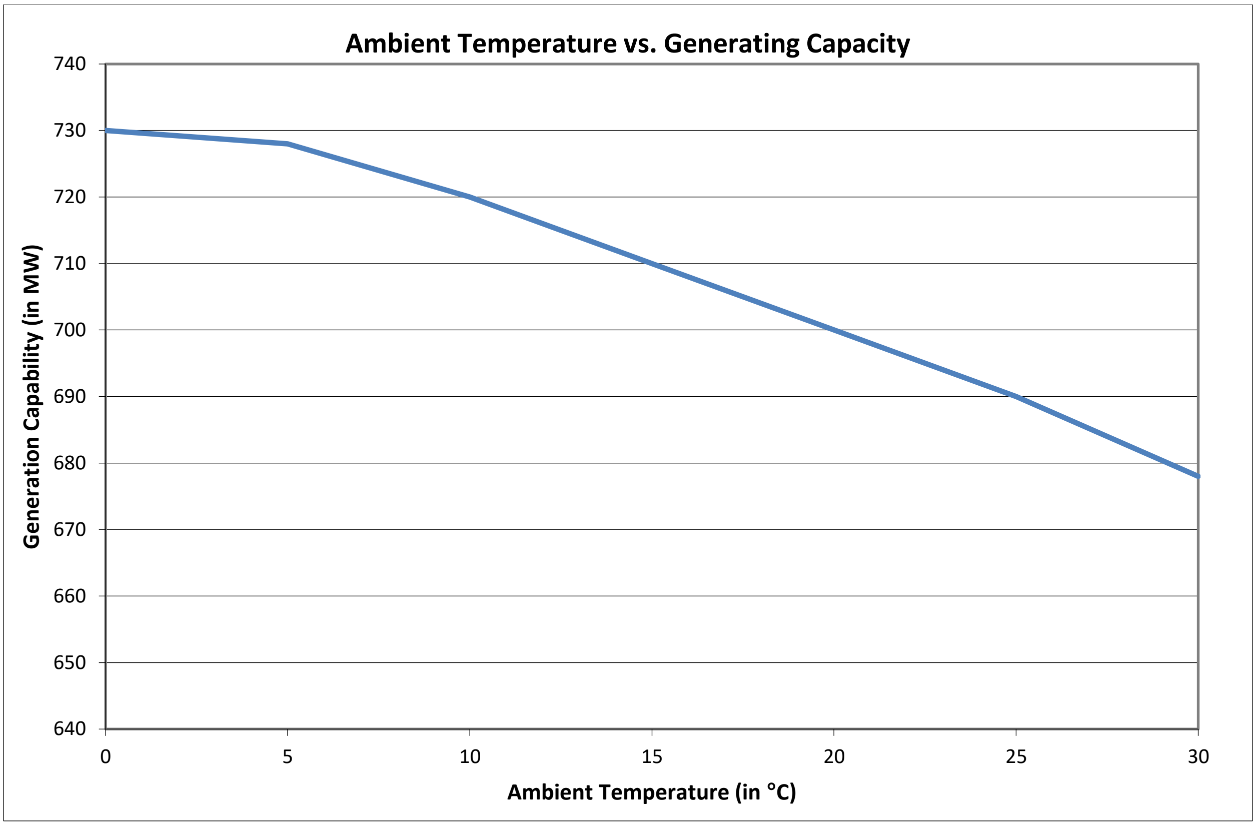


Figure 74: Ambient temperature to power capacity relationship for Kendal Power Station

The characteristic shows that at an ambient temperature of 30°C, each unit is de-rated by about 50 MW, totalling 300 MW for the entire power station.

Traditionally, before about 1990, the overall impact across the entire power system was minimal since the majority of power stations utilised wet cooling CW systems. This issue has been increasingly eroding capacity from the power system since more capacity has been added for dry cooling systems. Figure 75 shows how dry cooling, as heat rejection technology, has increased over time within the South African fleet of large thermal power stations.

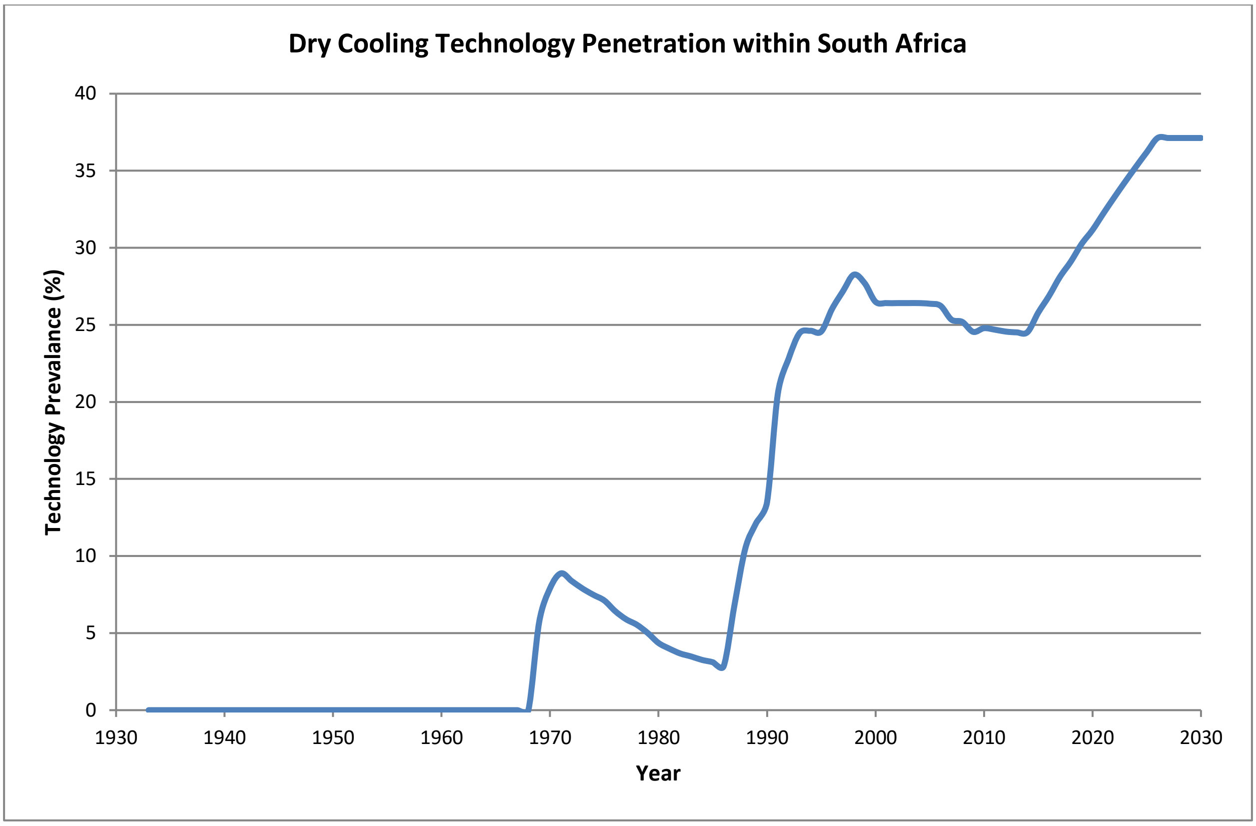


Figure 75: Increased penetration of dry cooling technology into the South African fleet

The first experimental implementation of dry cooling CW systems started in South Africa at Grootvlei Power Station in about 1968. As can be seen, the usage of the technology (as a fraction of the total installed base) declined from 1970 to about 1985. The reason for this decline was that more wet cooling power stations were being built during this period, reducing the relative representation of dry cooling systems.

However, since its inception in 1968, it has increased to over 35% of the installed base. It has become the default technology for the future of coal-fired power generation in South Africa, with a total capacity of 20 341 MW projected by 2030. This introduces a risk of widespread disruption on the overall power system, with a significant portion of the South African installed base likely to be affected during unusually high ambient temperatures, typically during heat wave conditions.

5.6.8 Auxiliary and Secondary Cooling Water Systems

The main CW systems at power stations, dealt with in the preceding sections, reject waste heat from the energy transfer fluid (typically water in either a liquid or gaseous phase) following the extraction of the useful thermodynamic energy by the turbines. However, many auxiliary and secondary systems also generate heat as an undesirable side effect that also needs to be rejected so that those systems will remain within their thermal limits.

Separate CW systems need to exist to provide the requisite cooling for the auxiliary systems of power stations. At most modern wet-cooled power stations, these secondary and auxiliary CW systems are entirely unitised and merely tap into the main CW system for each unit. At such power stations, any disruption to the secondary or auxiliary CW system would only threaten that specific unit – no other unit at the power station would be at risk. Therefore, secondary and auxiliary CW systems pose no threat to multiple units as a collective disruption risk.

On the other hand, dry-cooled power stations cannot use the main CW system since no common waterway exists to reject heat when turbines are not in operation. For that reason, a separate dedicated cooling system exists at dry-cooled power stations that facilitate the rejection of waste heat generated by auxiliary systems (not by the main thermodynamic cycle itself), i.e. heat generated from electrical, mechanical, chemical, etc., sources that typically do not involve combustion processes.

These dedicated cooling systems are wet systems with forced cooling towers serviced with pumps and fans to achieve the requisite heat rejection rate. In South African power stations, these auxiliary CW systems are segregated into two systems each servicing three units, but capable of being linked into a single large system if conditions necessitate. Amongst the dry-cooled power stations in South Africa, Kendal Power Station was the first large application, and its auxiliary CW system was the first to be built. It features four pumps in total for the three units at each side (eight pumps in total for the power station) – an unfortunate mechanical design that does not allow for a unitised functional allocation of the pumps. Due to this peculiar arrangement, the electrical power supply to the pump could not be sourced from any of the units (since the selected units may not be in service) and had to be sourced from common power supplies of the station boards instead, that are theoretically independent of the units and should remain energised regardless of any given unit becoming unavailable.

However, despite the theoretically envisaged independence for the station boards, the practical reality is that one station board is supplied from unit 1 and the other station board from unit 2. This implies that station board 2 will lose power when unit 2 fails and similarly for station board 1 when unit 1 fails. But because of the inherent reliance on the auxiliary CW system, recognition was given to the inevitability that a failure of either station board 1 or 2 would lead to a three-unit MUT. Therefore, it was decided to safeguard the station board supply with a special fast transfer scheme. The fast transfer scheme is an intelligent system that restores the electrical supply from the other station board whenever the supply to one of the station boards fails. It was devised to act with such rapidity and electrical precision that the power restoration would occur without any need for shutting down any of the auxiliary CW system components, and thus, cooling would continue without interruption [172].

However, despite the safeguarding provided by the fast transfer scheme, the system still suffered from two inherent weaknesses.

a If an MUT occurs, causing both units supplying the two station boards to fail, all auxiliary CW pumps will be lost, and all remaining units still in service at Kendal will trip.
b If the fast transfer scheme were called upon to come into operation but failed to function, all units at Kendal would trip.

Although these weaknesses were acknowledged, the likelihood thereof was deemed low enough not to warrant further mitigation.

An unfortunate property of any system that has the potential to compromise an entire power station (as a single point of failure) is that it can never be worked upon for any reason. Therefore, no maintenance of the fast transfer scheme is ever permitted since the very possibility of a single human error causing an entire power station to trip can never be allowed.

Also, although not apparent, no solution exists for replacing such a vital system if it reaches the end of its life before the end of the life of the power station is reached. Because an intelligent system such as the fast transfer scheme is based on digital electronic equipment, the life cycle management requirements are relatively restrictive, with equipment having periodic upgrades and replacement needs normally in the range of less than one decade – often just a few years. It, therefore, is almost unavoidable to become dependent on a single system with the capacity to disrupt various units at a power station and be forced into continued operation long after it becomes obsolete.

The Kendal fast transfer scheme was commissioned in December 1996 and continued uninterrupted service (never switched off) until 6 June 2014, when it malfunctioned when its DC power supply was disrupted. The fast transfer scheme automatically sent signals to trip the incoming circuit breakers to the station boards but did not send signals to close incoming circuit breakers from alternative supplies, as it should have. All four units that were in service at the time tripped, and no doubt exists that the other two units would also have tripped if they were in service at the time – a fortunate circumstance that would have contributed considerably to the impact of the disruption. The four units, supplying 2 514 MW to the power system, tripped within about 30 seconds (from the first to the last unit). Shortly after that, with the frequency severely depressed, the ZESA tie-line also tripped from a power infeed value of

646 MW, bringing the total power loss to 3 160 MW – a loss of 10,3% of the total energy of the power system at the time (30 600 MW), a significant event magnitude of 9,9 dB.

The power loss resulted in a rapid frequency decline that was ultimately arrested at 49,177 Hz, as shown in the following recording.

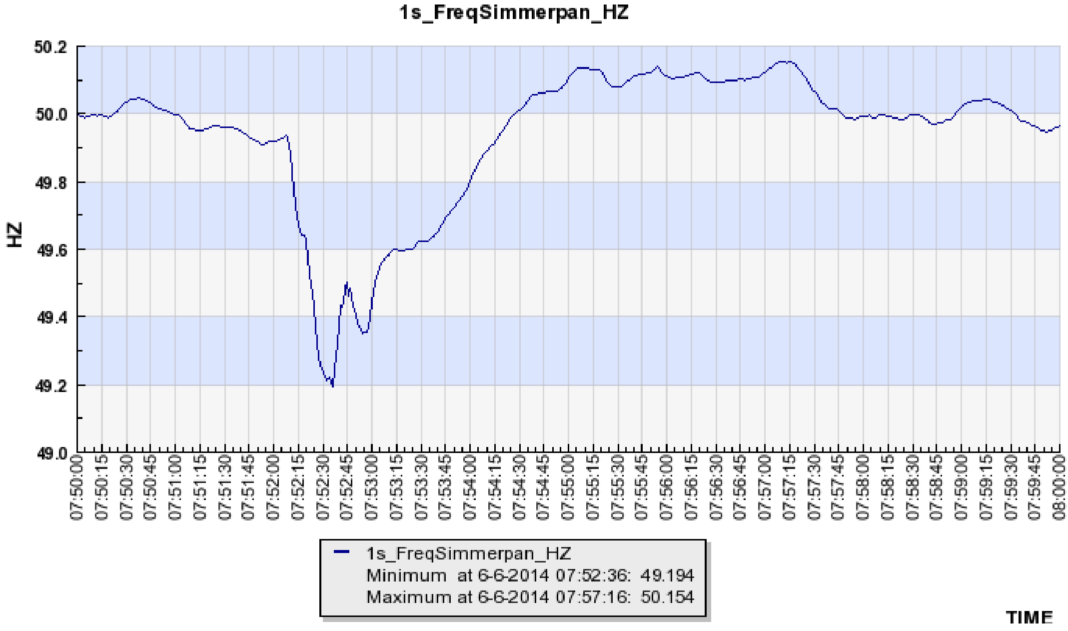


Figure 76: System frequency decay for the Kendal MUT of 2014-06-06

Figure 76 shows the frequency decline for the four Kendal units, after which the frequency starts to recover. Immediately after the initial recovery, the frequency declines again when the ZESA tie-line trips and removes a further 646 MW power infeed into the power system.

The frequency was arrested, and the power system was managed using the following resources.

Mitigation Resource	**Power (in MW)**
Peaking units (12)	1 082
UFLS	1 000
DMP	354
Interruptible load	899
SAPP Support	550
Total	**3 885**

All four Kendal units were returned during the day, incurring an equivalent of 41,9 unit-hours for the entire event.

One significant attribute of the Kendal event of 6 June 2014 is that it occurred at 07:52, while the morning peak had not yet entirely subsided. As a result, when the event occurred, there were already 11 peaking units in service, and peaking reserves were, therefore, already partially consumed.

The subsequent designs were significantly improved since Kendal was the first large South African power station where an auxiliary CW system had to be provided (from a dry cooling perspective). Specifically, the functional allocation was altered so that every unit provided its own take-off and return interface for auxiliary CW, supplying its pumps and electrical supplies for the extraction and return of auxiliary CW.

However, although most of the auxiliary equipment comprising the auxiliary CW system can be unitised, certain of the auxiliary CW system equipment inevitably remain common and cannot be unitised – an inherent vice. Such common infrastructure, once again, represents an inherent weakness that has the potential to become disrupted and possibly impact on multiple units of a power station.

An example of where the common equipment of a later-design auxiliary CW system became disrupted, occurred on 13 December 2019 at Majuba Power Station. The event was initiated when a CPU of the control system failed, causing the system to regulate incorrectly. Eventually, two of the three units on the affected side, sharing the affected portion of the auxiliary CW system, had to be de-loaded to half-load conditions (lightening the burden on the auxiliary CW system) until the control system could be normalised.

Even though the disruption was relatively moderate with an event magnitude of only about 17,0 dB on a power system serving 25 200 MW, the frequency depression was still significant – declining from 50,21 Hz to 49,67 Hz (a decline of 540 mHz) as seen in the following recording.

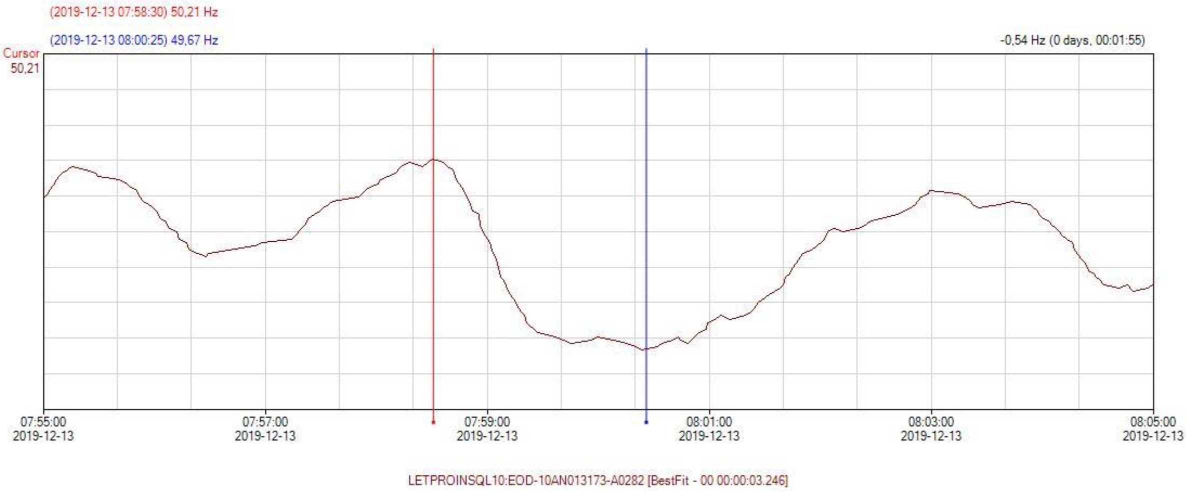


Figure 77: System frequency decay for the Majuba MUD of 2019-12-13

Although the auxiliary CW systems do not represent a major source of multiple unit disruption within the South African fleet of large power stations, the impact could be significant, as illustrated above in the Kendal example. For another example of a multiple-unit disruption involving the auxiliary CW system, refer to section 5.6.10.5.

5.6.9 Fire Protection Systems

Most of the common and shared systems considered in the previous sections that pose the risk of a cascading disruption propagating into other generating units of the power station were themselves production systems. Of course, as shown in section 4.5, various non-production systems are also common or shared amongst the generating units of a power station.

An example of such a non-production system is the fire protection system, which provides pressurised water to the units and common plant areas of a power station for the purpose of suppressing and fighting plant fires wherever they may occur. This system, therefore, consists of a bulk water storage facility, a pump station comprised of multiple electric and engine-driven pumps and a vast piping distribution network covering most of the high-risk and high-value plant of a power station.

A fire protection system presents two threats to the continued and uninterrupted operation of the generating units. Firstly, the fire protection system may disrupt another common system shared among the generating units, thereby indirectly disrupting the production of generating units. Although this possibility seems highly plausible, it rarely occurs, and such an event has never been recorded.

The second possibility is that the fire protection inadvertently activates incorrectly across many generating units, causing various disruption sites where individual unit processes become compromised. Even though this mechanism seems less likely than the first, this second mode of failure has caused various multiple-unit disruption events.

An example of such an event occurred on 21 July 2005, when Matla Power Station experienced a spurious activation of the fire protection system, causing four of the six operational generating units to disconnect from the power system. The event escalated beyond Matla and caused two units at Songo Power Station in Mozambique to also disconnect due to the failure of the control systems of those two units. The total disruption caused a loss of 2 645 MW of generated power, which amounted to 8,2% of the power system load at the time, manifesting as a decline in system frequency from above 50 Hz to 49,92 Hz. The event caused the emergency start-up of 11 peaking units (one failed to start) and a load curtailment of about 700 MW, including mandatory and voluntary participation. At the same time, the coal fleet was placed into emergency generation. Despite these actions, the frequency took over 18 minutes to recover to nominal, as shown in the following recording.

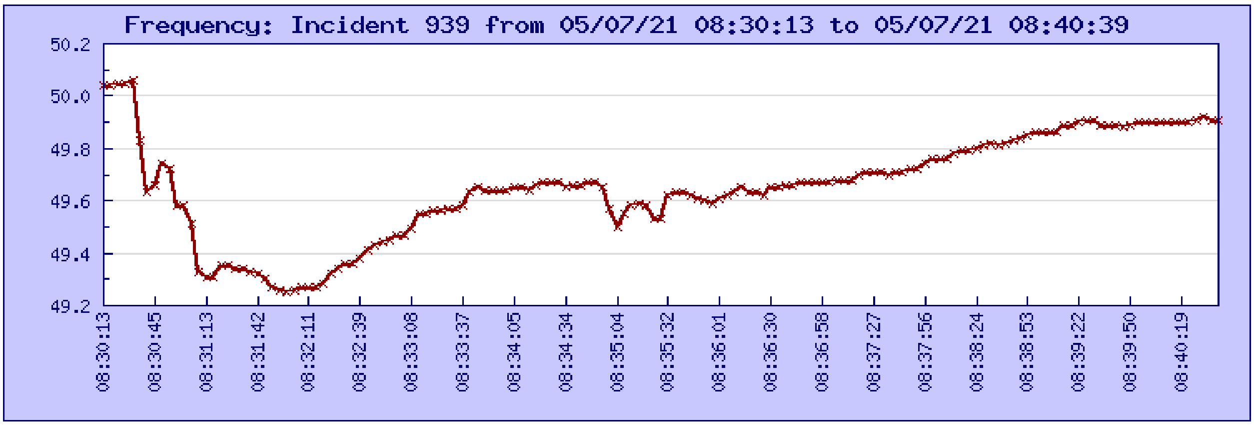


Figure 78: System frequency recording for the Matla-Songo disruption of 21 July 2005

The failure mechanism often centres around insufficient IP ratings of installed equipment within the power station buildings, allowing water ingress during the deluge associated with the activation of an industrial fire suppression system. Equipment used at power stations outside of the protection of buildings is normally specified as IP 65 or IP 66, meaning that such equipment is resistant to directed water jets. Due to cost implications mainly, equipment installed inside buildings at power stations is seldom specified beyond IP 54, meaning that the equipment is merely protected against dust and splashing water but incapable of resisting water jets or immersion into water [173]. Therefore, lacking the resistance level to withstand water jets, an ingress of water into sensitive equipment is likely to occur when the fire protection system activates within buildings where power station equipment is housed, leading to short circuits and, ultimately, equipment malfunction.

5.6.10 Electrical Systems

Fifth-generation power stations are extensive plants that process significant volumes of materials and transform vast quantities of energy. To do so with a small contingent of operating staff, these plants employ a high degree of automation. Furthermore, essentially all auxiliary systems that support the processes of materials handling and energy transformation use electricity as the direct or indirect energy source. To give some perspective of the extent of such an enterprise, the following list contains typical electrical attributes associated with a six-pack power station of the fifth-generation variety comprising 600 MW units – a median within the South African power generation industry.

Electrical motors:	8 000 ± 1 500
Switchgear modules:	12 000 ± 1 000
Reticulation boards:	270 ± 20
Power transformers:	290 ± 15
Power cables:	15 000 ± 1 000

With the vast number of systems supporting the various processes at power stations, along with the vast dimensions of these systems, it is intuitive that extensive electrical reticulation systems need to exist to power these systems. As with other systems, redundancy within the electrical systems is an important design feature to add to resilience and ensure safety during contingencies. A hierarchy of power supplies used within power stations is briefly outlined below.

The most mundane electricity source can be called Normal Auxiliary Power. This is electricity syphoned off from the electricity produced by the power station to power the auxiliaries of the power station, either within the units or in the common plant. In the units, this is mainly for powering auxiliary plant components and systems needed for electricity production.

The next level in the hierarchy is generally referred to as Essential Power. This category of power is required for systems that must remain in service regardless of whether the unit is in normal operation, abnormal operation, or dealing with emergency conditions on a long-term or ongoing basis.

Ultimately, the highest echelon carries the epaulette of Emergency Power. This supply type is invariably backed up with batteries and supplies either DC directly from a battery bank or AC through UPS technology. This Emergency Power is associated with two types of applications. Firstly, those applications that cannot afford to be without power (even for a brief interruption) such as control and instrumentation systems, protection systems, communication and carrier links, etc.

The second type of Emergency Power application is those systems that require electric energy to safeguard plant and personnel directly, even when a unit is completely blacked out, and electricity is neither generated nor imported from the external power system. These applications are often driven with DC motors and sometimes designed to run to destruction.

One such application is the generator seal oil system. Due to molecular hydrogen gas's (H_2) extreme flammability range, its containment within the generator casing is considered an overriding priority. As such, the system features a high level of redundancy. The seal oil system for a typical unit is shown conceptually in the following illustration.

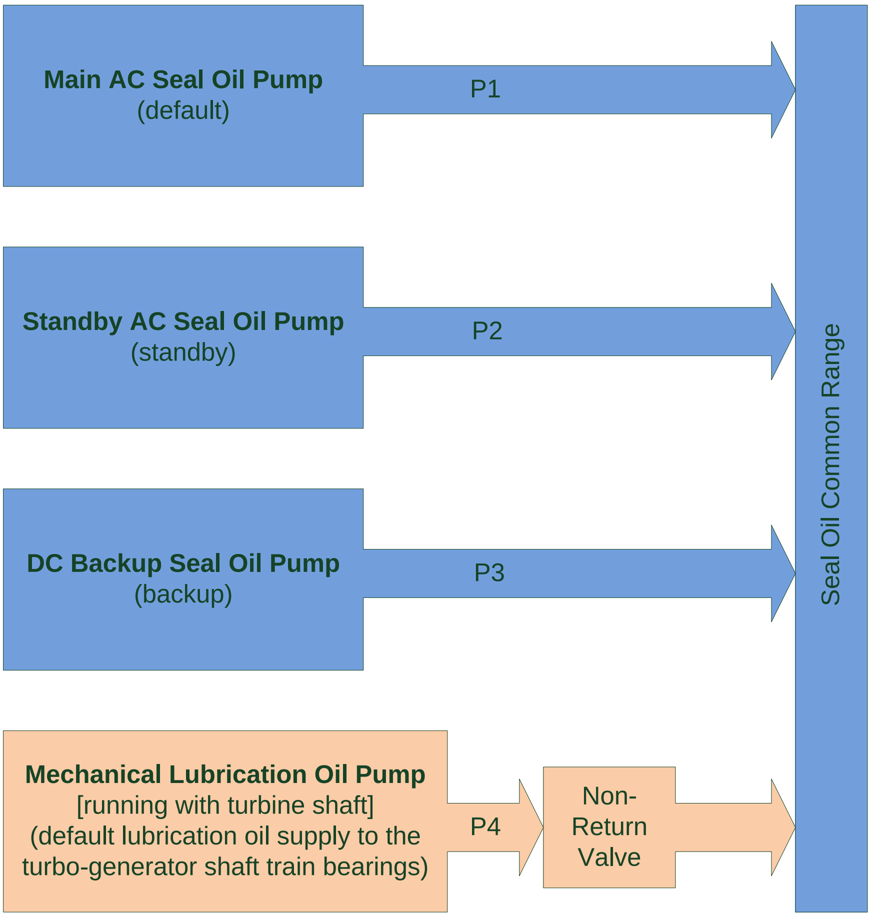


Figure 79: Typical seal oil system for an H_2-cooled generator

In the above example (where P1, P2, P3 and P4 are oil pressure values with P1>P2>P3>P4), the seal oil supply is delivered under normal operating conditions by the Main AC Seal Oil Pump – at a delivery pressure of P1. If the common range pressure decays to below P2, the control system will start the Standby AC Seal Oil Pump, whether the Main AC Seal Oil Pump is still running or not. In a hypothetical event when all AC supplies on the unit fail, the DC supply becomes the only remaining electrical supply still available on the unit, and the control system will start the DC Backup Seal Oil Pump when the common range pressure decays to below P3.

In a worst-case scenario, when all electrical supplies of a unit fail (AC and DC), the common range pressure will decay to below the value of P4, upon which the delivery pressure from the Francis turbine (running mechanically in unison with the main turbine) will mechanically open the non-return valve and flood the common range with lubrication oil in a last stage attempt to maintain sufficient sealing and to avoid an uncontrolled release of hydrogen. This is an undesirable case since the lubrication oil is not maintained at the same stringent purity levels as the seal oil and will contaminate the hydrogen in the generator. It is, therefore, considered to be the last resort. Note also that this final containment action does not rely on control system intervention (being entirely mechanical) and will, therefore, also work in cases where even the emergency supply to the control system has been compromised.

Ultimately (not shown in Figure 79), a dumping valve will open and vent the entire hydrogen volume to the atmosphere based on a further pressure decay (beyond P4) within the common range. Such an H_2 dumping event would typically be associated with an automatic unit trip, and a total H_2 refill of the generator would be required before returning to service.

The following sub-sections will consider, to some greater degree of detail, the electrical systems typically found at power stations.

5.6.10.1 Earthing and Bonding

All industrial plants require a system that provides an equipotential reference at earth (or ground) potential. This requirement ensures the correct operation of electric and electronic systems and personnel safety.

To meet this requirement in the case of power stations, an earth mat (a metal grid) has been embedded at the foundation level of all major structures. Every earth mat of each structure is then connected to the main earth mat below the main power station structure (below the turbine hall and boiler house). Also, the earth mat is interconnected to the earth mat installed below the HV yard and the outgoing power line pylons.

Once all the separate earth mats have been interconnected to form an overall earth mat for the entire power station, all the electrical equipment (including electronic and computer-based equipment) are bonded to the earth mat, allowing for a consistent reference and an adequate sink for electrical energy during fault conditions. If, however, a condition would arise during which the capacity of the earthing system becomes insufficient to cope with the demands placed thereon, incorrect equipment operation or equipment damage could occur, in addition to conditions that threaten human safety.

It may not be entirely obvious why a system designed especially for a given plant may have insufficient capacity when called upon. It's important to note that although plants may eventually evolve to outstrip the design envelope of the original earthing system, it is rare.

The main reason for the earthing system being unable to cope when required to do so, stems from the integrity of the system becoming compromised through neglect (or a lack of discipline), or deliberate acts of conductor theft. Earthing systems are normally constructed from semi-precious metals like copper or aluminium and carry a relatively high scrap metal value. Stealing the conductor of the earth mat embedded into the foundations of structures is not physically possible. However, the conductors used for bonding equipment to the earth points (metal studs protruding from the foundations for equipment earthing) are external and exposed, necessitating the need to be semi-precious to prevent corrosion. Thus, with a valuable material installed to such a vast extent as to cover all plant (too vast to be safeguarded by security initiatives), theft becomes an obvious threat to the integrity of the plant.

Due to the earth mat being common to the entire power station, it poses an inherent threat to the facility as a whole as a means of collectively disrupting multiple units. An example of such a disruption event occurred on 23 October 1996, at 08:02 when lightning struck the no. 2 smokestack at Kendal Power Station. The subsequent investigation revealed that the earth bonding of equipment in the vicinity of smokestack no. 2 was compromised and that the lightning, therefore, caused control equipment and instruments associated with that part of the plant to malfunction, resulting in all three units sharing the smokestack, to trip.

The lightning discharge event comprised five individual strokes occurring within 92 ms, as summarised below. Although the recorded currents were not exceptionally high (possibly due to the height of the smokestack that might have been precipitous in the event), the extent of the overall disruption was considerable.

Time	Lapsed time from start (in ms)	Peak Current (in kA)
08:02:22,895	-	21
08:02:22,926	31	21
08:02:22,941	46	10
08:02:22,966	71	17
08:02:22,987	92	22

The result of the MUT removing 1 749 MW from the South African power system serving 23 850 MW at the time, which caused a frequency depression down to 49,2 Hz is summarised in the following table.

Mitigation Resource	Power Quantity (in MW)
Peaking units (4)	1 000
DMP	174
Interruptible load	400
SAPP Support	400
Total	**1 974**

Lightning can also cause widespread disruption of power systems through other mechanisms than the mechanism discussed above. At power stations, lightning-type disruptions are often associated with insufficient earth bonding and electromagnetic shielding.

One of the areas notorious for causing lightning-related disruption is the ash handling systems that are particularly employed at power stations with dry ash dumps (as opposed to wet ash dams that were the *de facto* standard for many years). Dry ash dumps cover vast areas of terrain over which long ash conveyors must transport the ash, along with ash stackers for discarding the ash into the mine as backfill. And because these conveyors and stackers are constantly moved due to the growing ash dump, these systems often lack proper earthing systems and lightning arrester technologies. The result of this state of affairs is that lightning storms cause widespread damage to the instrumentation and communication equipment used to control and monitor the ashing operation. Once the ashing operation ceases due to lightning damage, ashing reverts to emergency aching, which can be highly disruptive, as explained in section 5.6.4 above.

To mitigate against this risk, signalling in these areas has mostly been converted to fibre optics and radio links, with optocouplers widely employed in instrumentation installations.

5.6.10.2 Unitised Electrical Layouts

The electrical layout of a typical coal-fired unit is considerably more complicated than that of other power generation technologies. To align with the functional layout of the fifth-generation power station philosophies, the unit reticulation system is also divided into two systems – each to provide 50% of the reticulation needs for all auxiliary and ancillary systems. Figure 80 shows a typical fifth-generation unit reticulation system.

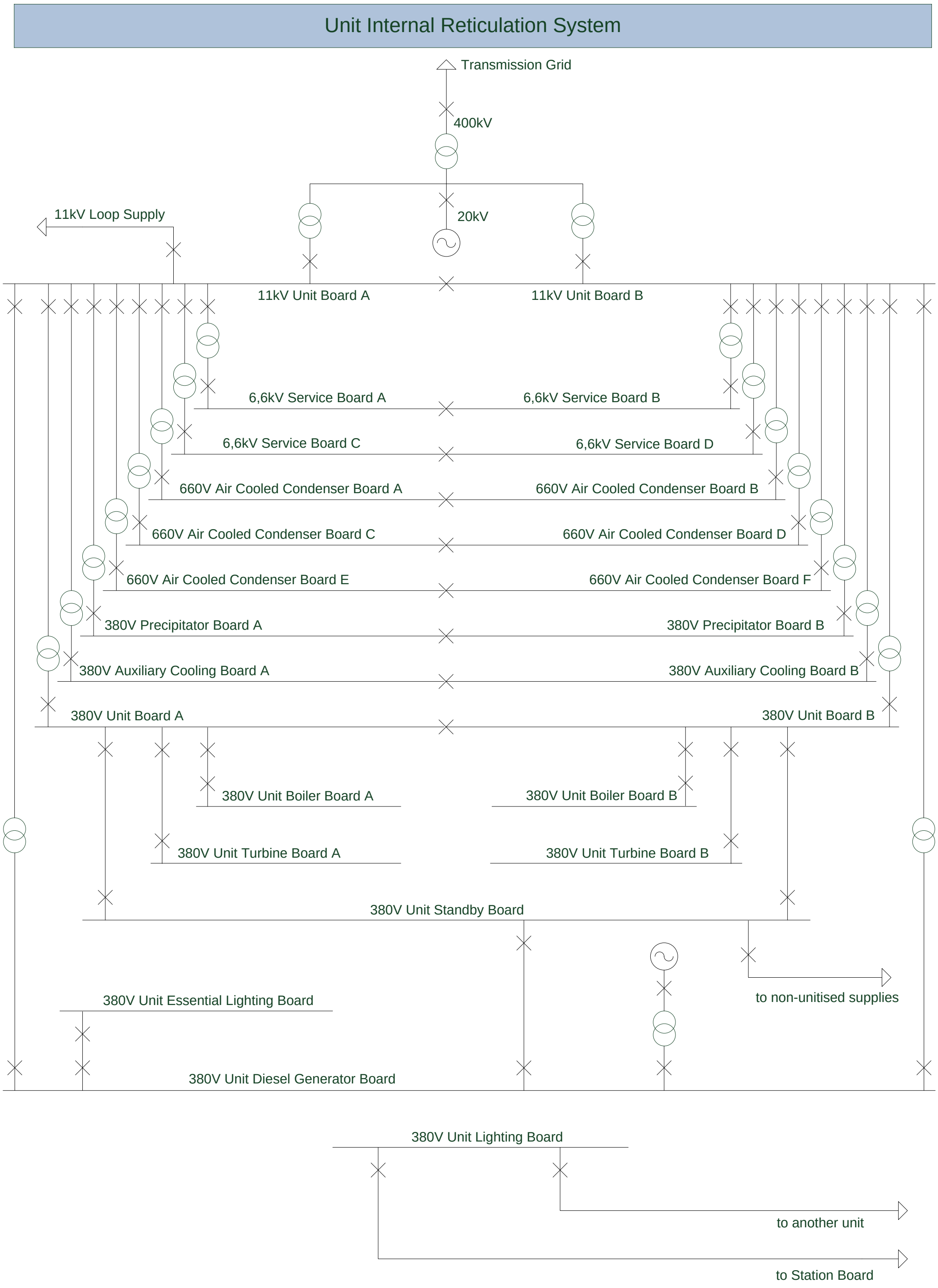


Figure 80: Typical fifth-generation power station unit reticulation system

Most switchgear boards have a default supply from either the 11 kV Unit Board A or B. This means that if one of these 11 kV boards tripped (i.e., the incomer circuit breaker would open), all the boards supplied from that specific 11 kV board would be left without power. All the auxiliaries supplied from these dependent boards will become de-energised and cease operation.

The unit will consequently be forced to transition to a new state of operation of about 50% of the full load condition. However, for that transition to occur effectively, the condition will need to be recognised by the control system and correctly managed to achieve a half-load condition while arresting a further escalation resulting in the total loss of the entire generating unit.

Figure 80 shows that many boards come in pairs (or groups) with a shared purpose, e.g., the 380 V Auxiliary Cooling Board A and B. Also, all A-boards are supplied from the 11 kV Unit Board A and all the B-boards from the 11 kV Unit Board B – either directly or indirectly. However, in many cases, an A-board can be connected to its corresponding B-board by a bus section breaker. This provides a redundancy feature whereby, e.g., the 11 kV Unit Board A can be taken out of service while the unit is on load and at 100% production, while all the electrical supplies (with this feature) can remain in service but energised from the 11 kV Unit Board B. This feature, however, is not an automatically controlled function and needs to be configured for such duty by an operator.

Another observation from Figure 80 is that a unit's electrical system has very few interconnections to other units or common electrical systems. In fact, under normal operating conditions, a unit runs without any electrical link to another system, which does not form part of that specific unit, barring lighting. Being isolated from the unit itself, specifically the lighting board poses no risk to its own unit during disruption events.

Except for the lighting board, only three other connections to other electrical systems are possible: from the 380 V Unit Standby Board, through the 11 kV Loop from an 11 kV Unit Board, and lastly, its connection to the transmission IPS. The interconnections between the unit electrical systems are clarified in the following illustration.

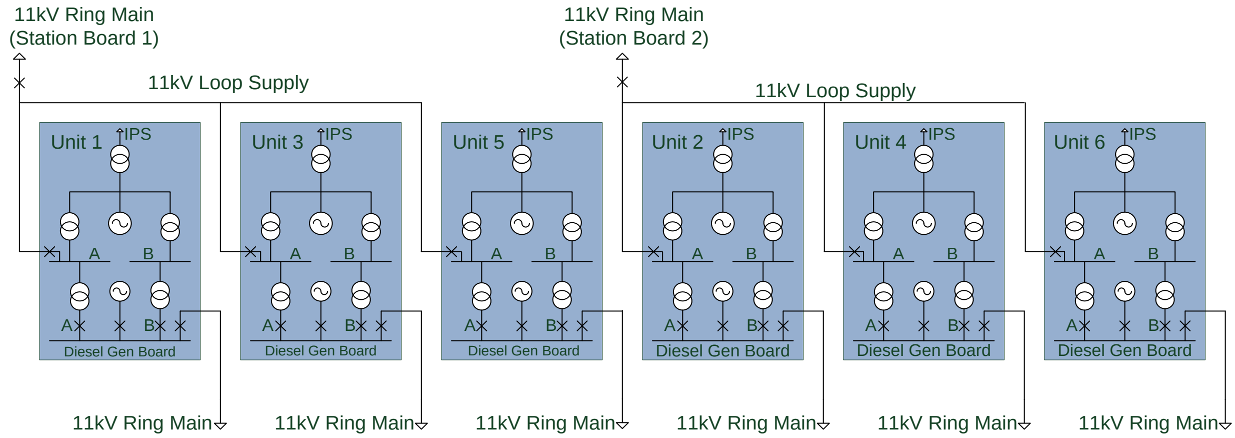


Figure 81: Typical fifth-generation unit electrical interconnections

Each blue block in Figure 81 represents each unit's entire electrical reticulation system, similar to Figure 80, but with a scaled-down level of detail to show only the relevant parts of each system. It can be seen in Figure 81 that each unit can be interconnected to other units in three possible ways.

a. Directly through the 11 kV Loop Supply.
b. Indirectly through the 11 kV Ring Main.
c. Indirectly through the IPS – typically at 400 kV or 275 kV in South Africa.

The normal (default) configuration of units in normal operation, will not have any interconnection through either the 11 kV Loop Supply or the 11 kV Ring Main. Such interconnections are regarded as irregular (non-default) interconnections and are avoided unless anomalous circumstances necessitate it (see section 5.6.3).

However, despite the default configuration of operating units (interconnected to other units only through the IPS), other interconnections (through either the 11 kV Loop Supply or the 11 kV Ring Main) are nonetheless required from time to time to deal with specific circumstances, such as plant failures, urgent work, etc. These exceptional cases (when circumstances necessitate interconnection) expose such units to a vulnerable state wherein an electrical disruption in one unit can directly affect another unit – due entirely to their interconnected state.

As an example of an intra-station escalation event due to a non-default interconnection, consider the event that occurred on 20 October 2006 at Lethabo Power Station. At the time of the event, unit 3 was interconnected to unit 1 through the 11 kV Loop Supply, while unit 3 was disconnected from the power system and was undergoing planned maintenance. The electricity needed for the maintenance was sourced from unit 1, which was generating at full load. While unit 3 was offline and being maintained, its two main CW pumps were in service and were being utilised for the collective cooling needs of units 1 and 2 – both of which were in service at the time. During a switching operation that occurred at 06:47, the restricted earth fault protection of the unit 1 generator transformer malfunctioned and caused unit 1 to trip – shutting down its two main CW pumps that were in service. The unit 1 trip also caused the inadvertent interruption of the supply to unit 3, resulting in the tripping of its two main CW pumps (the only remaining CW pumps that were now in service between units 1 to 3). Unit 2 was now left without main CW flow and tripped about two minutes later due to a loss of condenser vacuum. The following recording shows the impact of this event on the system frequency.

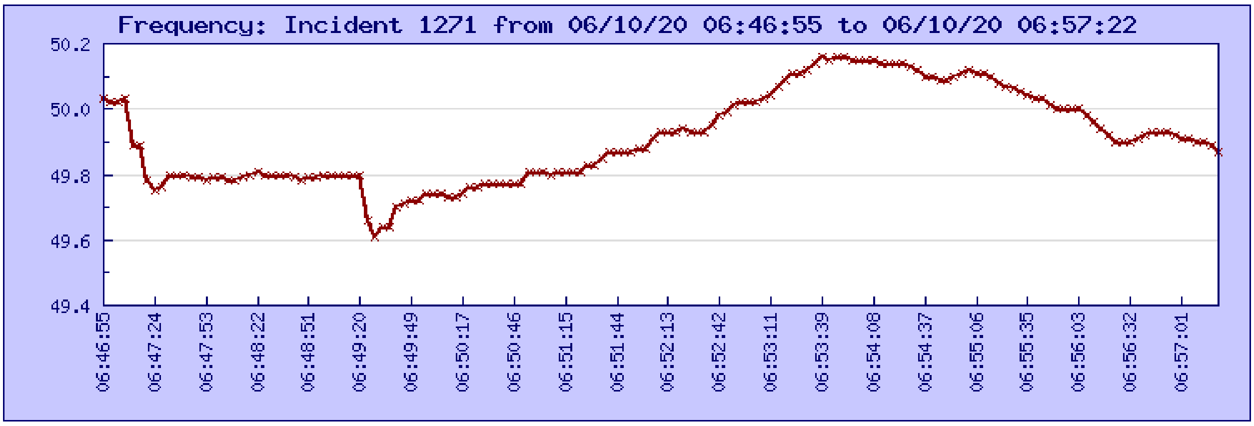


Figure 82: System frequency for Lethabo MUT of 20 October 2006

Even though the event merely signifies a two-unit cascade (totalling a 1 186 MW loss in total) and being separated by a time interval of more than two minutes, the frequency decay was significant with the lowest value of 49,56 Hz being recorded, partly because the event occurred within the morning peak. The event could not be contained within the ambit of generation only and demand-side resources had to be utilised, with about 420 MW being reduced from customer load.

If the two units (units 1 and 3) were not interconnected, unit 1's tripping due to the protection malfunction would not have compromised unit 3, which in turn would not have compromised unit 2.

However, the indirect interconnection of units through the IPS cannot be avoided and signifies an all-too-common channel through which disruption is often proliferated, a disruption mode that will be further explored in sections 5.6.10.4 and 5.7.1.

5.6.10.3 Unit Diesel Generator Board

All the systems at power stations (or even at the unit level) do not have the same degree of redundancy, a point repeatedly made in the preceding sections. Equipment comprising systems that support the power generation processes often features 100% redundancy in the form of backup or standby systems or equipment.

There are cases where no redundancy exists – generally because the specific component does not directly support the electricity generation process. Take, for example, the case of the turbine barring gear. It comprises an installation that would mechanically keep the main turbo-generator shaft train rotating following a unit trip to ensure that the shaft train does not bend or cog while still being hot from the steam flow while it is in operation. Failure to avoid bending or cogging would be detrimental to the shaft train and dramatically prolong the time required to return the unit to service. In other words, although the barring gear does not participate directly in generating electricity, it is vitally important to prevent damage and ensure that the unit can return to service without any undue delay.

Most distribution boards existing within the reticulation system of a unit normally have a default supply and a single redundancy in the form of a bus-section breaker. The said board would normally be supplied directly from one of the 11 kV Unit Boards, but in a case where the default supply would fail, the board can then be energised through the bus-section breaker from its twin board that are supplied in turn from the opposite 11 kV Unit Board.

However, one board within the unit reticulation system deviates from the single redundancy rule and features multiple redundancies, i.e., the Unit Diesel Generator Board. The following diagram shows a typical Unit Diesel Generator Board from a fifth-generation power station design.

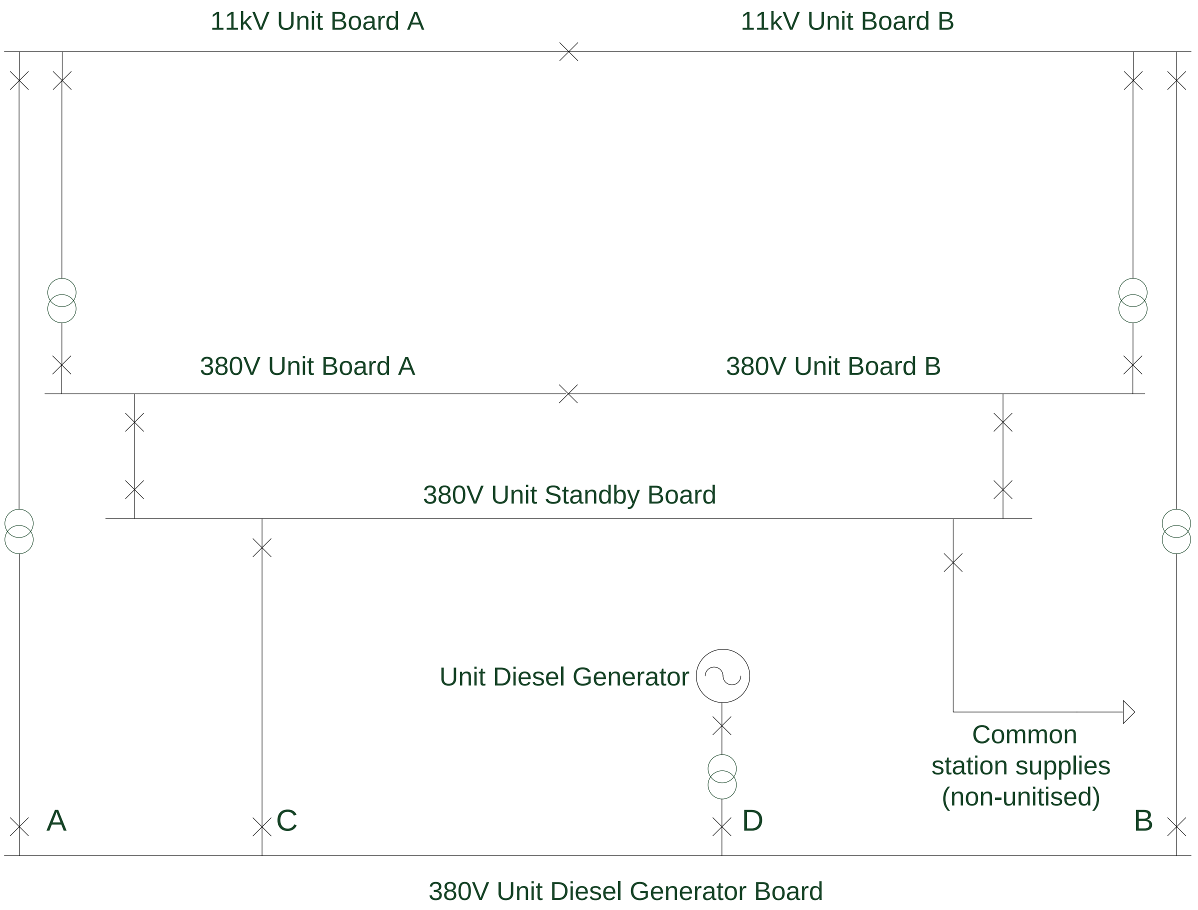


Figure 83: Typical layout for a Unit Diesel Generator Board (fifth-generation)

The Unit Diesel Generator Board, shown above, features four possible options through which it can be supplied – marked A, B, C and D, respectively. Supply A is the default supply and is sourced from the 11 kV Unit Board A of the specific unit. Supply B is sourced from the 11 kV Unit Board B from the same unit and is used in cases where the default supply is not available but the unit reticulation system is otherwise still alive.

The following supply option for the Unit Diesel Generator Board is from the Unit Standby Board – a board that, itself, requires some clarification. The Unit Standby Board is peculiar within the unit reticulation system since it is not supplied directly from one of the 11 kV Unit Boards of the unit. It has, however, interconnection options from both the A and B sides of the unit reticulation system at the LV voltage level. Also, it can be connected to the Unit Diesel Generator Board of the unit. But crucially, in cases where the unit is entirely without power, it can be interconnected with the electrical reticulation systems of the common plant – typically to one of the Station Boards or one of the substations that are part of the 11 kV Ring Main (refer to section 5.6.10.5). The Unit Standby Board is not a distribution board in the true sense of the word. Instead, it is a node used as a connection point for other boards during various types of contingencies (e.g., trips, outages, etc.), and it features no primary loads of its own.

Therefore, the Unit Standby Board is a logical supply option for the Unit Diesel Generator Board to not only be able to provide power from its unit through various means but also from outside the unit in cases where a unit is entirely dead. Ultimately, however, in cases where none of the various possibilities provides a solution, the Unit Diesel Generator Board (as the name eludes) is provided with one (or more) diesel generators that can be brought into service to provide power as a last resort. In addition, the Unit Diesel Generator Boards are the only distribution boards at a power station that feature stand-alone control systems (PLC-based or relay logic hard-wired) that will automatically restore power upon interruption – having access to all four supply options discussed above, including the automatic starting of the diesel generator if needed.

The high degree of redundancy to which the Unit Diesel Generator Board has been designed suggests that its purpose is somehow more exalted than that of the other unit boards. Indeed, the Unit Diesel Generator Board represents a higher purpose than any other boards that comprise the unit reticulation system, as will be elaborated upon.

Firstly, the highest purpose of the Unit Diesel Generator Board is to safeguard the unit against damage following a trip. The default method of tripping a unit is to disconnect it from the power system by opening the LV generator circuit breaker while the HV generator circuit breaker remains closed. This implies that, although the unit is disconnected from the power system, the electrical reticulation system of the unit remains alive. Therefore, its auxiliaries remain energised to enable a safe plant shutdown (see Figure 84).

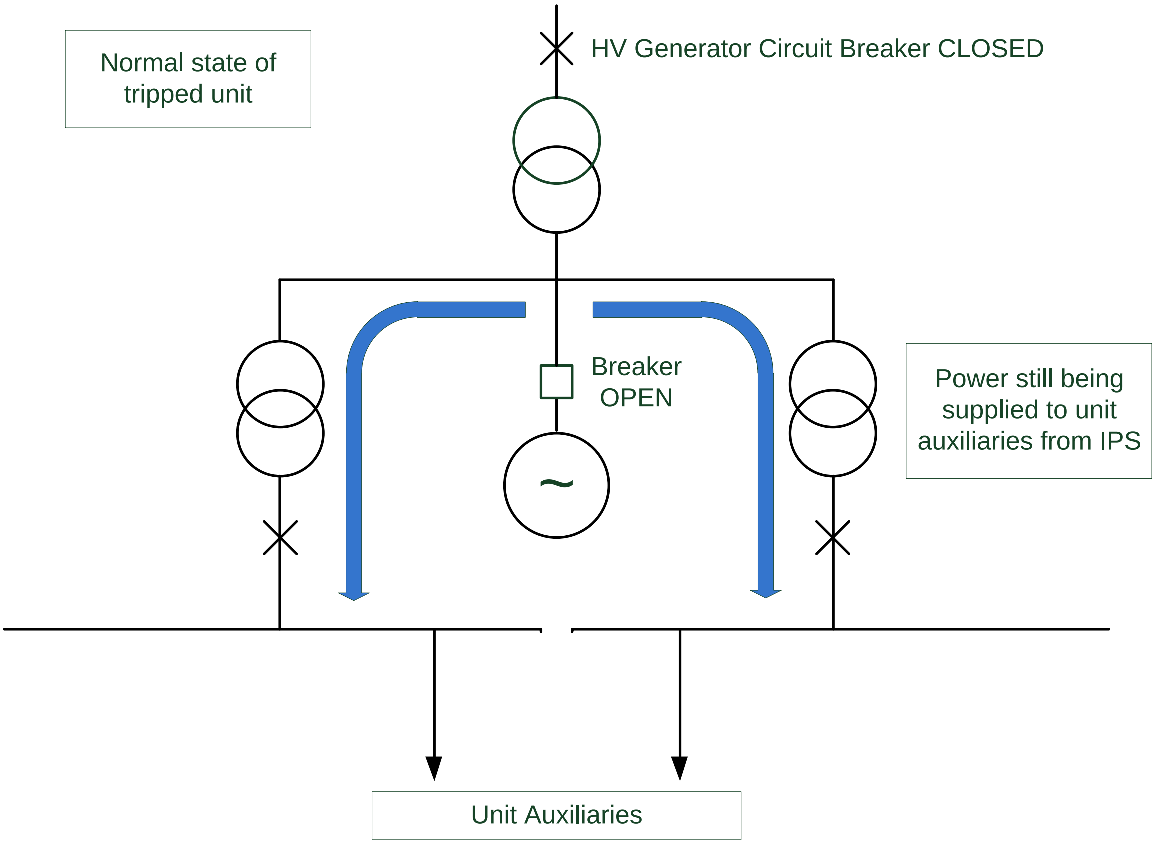


Figure 84: Normal (default) tripped state of a fifth-generation unit – back-energised unit

However, occasionally default tripping is not possible (for sound technical reasons), and an HV circuit trip occurs (refer to Figure 39). Under such circumstances, the Unit Diesel Generator Board becomes the default supply to enable the safe shutdown of the unit.

When an HV circuit trip occurs, the Unit Diesel Generator Board could be supplied from an off-unit source (incomer C Figure 83), or from its diesel generator itself (incomer D) – both of which are independent from the main generator of the unit or the unit's network connection point. Once power to the Unit Diesel Generator Board has been restored, those auxiliaries that are vital for the safe shutdown of the unit can be brought into operation – normally by the automatic control system. Such auxiliaries include lubrication oil pumps, jacking oil pumps and turbine barring gear, amongst others.

The prime duty of the Unit Diesel Generator Board, to act as an emergency supply, is critical to the process of safeguarding the unit following an HV circuit trip. Still, this function of the board normally does not lead to cascading failure events. The significance of this board as a source of cascading disruption events stems from the secondary purpose of the Unit Diesel Generator Board, namely, to power auxiliaries that do not follow the functional allocation principles discussed in section 5.4.2. As discussed earlier (in section 5.4.2 and section 5.6.10.2), the unitised electrical reticulation system comprises two semi-independent sides, normally referred to as the A- and B-side power supplies. One of the benefits of having the two auxiliary supplies is that unit operation remains possible even when one of the sides is removed from service, either through tripping or by manual switch-out (typically for maintenance). Loads so vital that unit operation cannot continue when power to the load is interrupted are then deliberately supplied from the Unit Diesel Generator Board instead of a Unit Board A or B (in case either the A-board or the B-board is switched off). An example of such a load is the generator seal oil differential-pressure regulating valve – since only one such valve exists for each unit. Supplying this valve from either the A- or B-side of the reticulation system would compromise the unit since the unit operation is not permissible when the integrity of its hydrogen seal has been lost. However, with this valve supplied from the Unit Diesel Generator Board, the unit can remain in operation regardless of whether the A-side or B-side boards are taken out of service.

Although the benefit of supplying certain production loads from the Unit Diesel Generator Board is clear, it is also clear that the unit would be unable to tolerate a condition where this board becomes compromised – since there is only one such board. And precisely therein lies its weakness. Although the Unit Diesel Generator Boards is heavily backed up with four potential in-feeds, the chop-over that has to restore power to the board when a supply is lost is not rapid enough to save a running unit from tripping. Instead, the chop-over is effective in restoring power to the board following the tripping of the unit so that the unit can be safeguarded against damage.

Although the Unit Diesel Generator Board is normally not the cause of an event that escalates into a multiple unit disruption event, there are various examples where it plays a contributory role.

5.6.10.4 HV Yard

The HV yard at a power station is merely the closest transmission substation, connecting the power station to the IPS. Consistent with redundancy standards used in power station design, the HV yard also features various redundancy principles. The following diagram shows a typical (high-level) layout of an HV yard of a six-pack, fifth-generation power station.

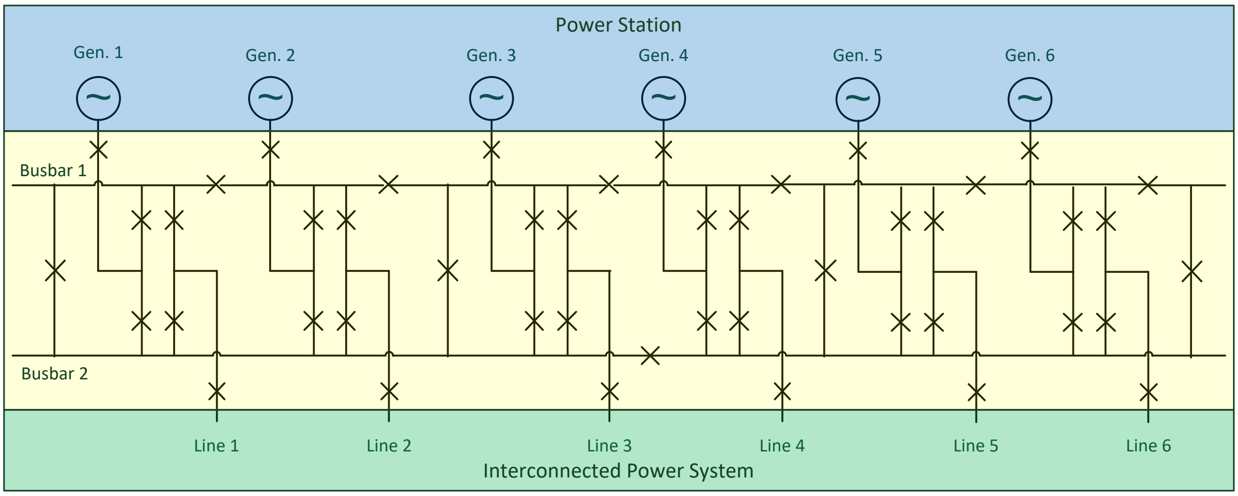


Figure 85: High-level layout of a fifth-generation, six-pack power station HV yard

The yellow-shaded region of the diagram above represents the HV yard, the blue the power station, and the green the external power system. The HV yard is shown at a very high level only, with much of the details and components being omitted to focus merely on a conceptualised level.

In the diagram (Figure 85), each cross (×) represents a circuit breaker that can be closed, opened or tripped automatically and remotely under loaded and faulted conditions. Some of the salient points to observe are the following:

- There are two busbars for redundancy and operational flexibility.
- Both the generators (units) as well as the outgoing feeder lines can be linked to either of the two busbars.
- On busbar 1, each generator can be separated from every other generator.
- Busbars can be subdivided into smaller sections (or zones) by bus zone breakers.
- Bus coupler breakers can connect the busbars.

Since the HV yard represents a single node in the IPS, a disruption in the integrity of the node could compromise multiple or all the units at the power station. The HV yard is, however, not a standalone or independent adjunct of the power system but is strongly interconnected to the rest of the power system via multiple power lines. Therefore, disruptive conditions in the broader power system would also manifest (to some degree) in the HV yard, subjecting all connected units to the disruptive occurrence – potentially triggering a multiple-unit disruption at the power station.

To counteract such a potential multiple-unit disruption stemming from a disruption within the power system, immunity standards are normally stipulated within the relevant grid code applicable to the region where the power station is located – the SAGC in the case of South

Africa. The immunity standards provide a technical management framework to govern the power station and network service provider's requirements and obligations to ensure appropriate behaviour from the relevant stakeholders. Therefore, both parties ensure that adequate equipment specifications are applied and protection functions are set appropriately.

Despite the most comprehensive regulations and utmost rigour and discipline in managing the HV yard, it remains the Achilles heel within a power system that readily triggers or proliferates multiple unit disruption events. One example that illustrates the susceptibility of power stations to suffer multiple unit disruptions due to HV yard events occurred at Kendal Power Station on 23 November 1997 at 12:07 when a pantograph isolator malfunctioned, causing another isolator to open under load conditions. Due to arching, electrical faults were detected by the protection systems in two zones of the HV yard – clearing both zones and disconnecting two units that were encapsulated within the affected zones. The effect of the two-unit MUT was relatively minor (780 MW) due to the event's time. However, many HV yard-related events have been recorded over time – many having far-reaching consequences causing cascading disruption events.

5.6.10.5 Station Electrical Layout

As seen in section 5.6.10.2, the electrical layout of a unit is an extensive reticulation system – a system replicated for each power station unit. Although the combined electrical infrastructure of the six units represents a vast electrical network, an additional electrical reticulation system exists at each power station for powering the common auxiliary systems shared amongst the units. The following illustration shows a high-level layout of a typical power station electrical reticulation system.

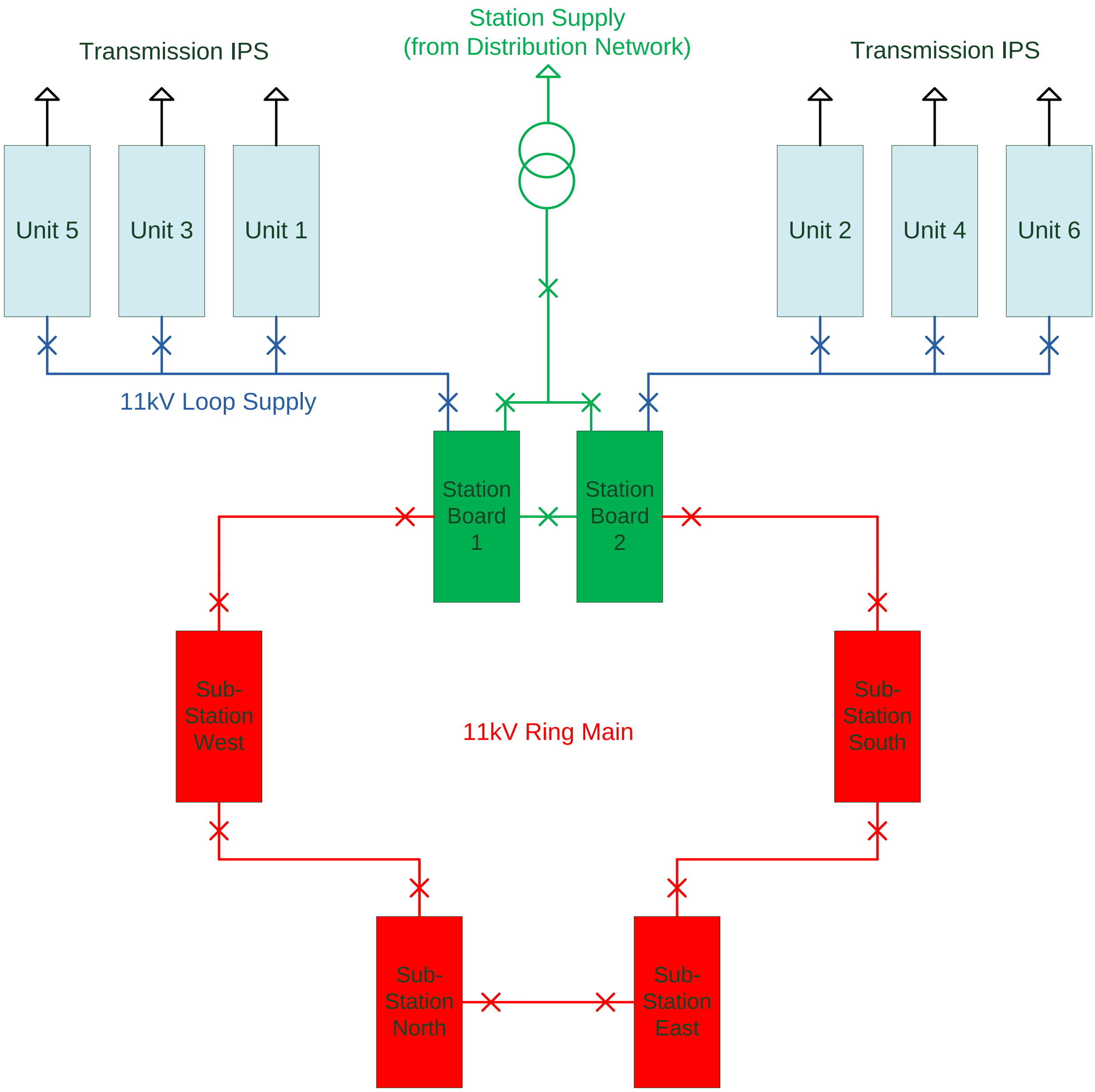


Figure 89: A typical electrical reticulation system of a fifth-generation, six-pack power station

In the diagram above, each blue block represents the entire electrical reticulation system of a single unit similar to that shown in Figure 80. Equally, each red block represents an electrical reticulation system that exists in the common plant of a power station – a system with roughly the same level of complexity as that of a unit, consisting of multiple distribution boards at various voltage levels, metal-enclosed switchgear, transformers, power cabling, etc. Those reticulation systems physically constructed outside the main power station civil structure are referred to as substations. Two common reticulation systems are inside the main civil structure and are referred to as the Station Boards, although they are entire reticulation systems in their own right. These station boards are where the units' electrical systems are interconnected to the common plant electrical systems, as shown above (Figure 89).

Notice the two 11 kV structures shown in Figure 89. The blue blocks are interconnected through blue lines, a structure known as the 11 kV Loop Supply. This structure is provided mainly for maintenance and is sometimes utilised during unit light-up activities. It is not used as part of the default configuration of the power station under normal operating conditions with all units in service.

The second 11 kV structure is the red blocks interconnected with the red lines in Figure 89. This structure is known as the 11 kV Ring Main and is permanently in service to provide power to the common auxiliaries. To avoid circulating currents, the 11 kV Ring Main is always configured to be open at a single location that changes from time to time due to various considerations.

One further feature of the electrical reticulation system of a power station that needs to be highlighted is the so-called Station Supply, indicated in green in Figure 89. The Station Supply is generally not in service but provides an independent supply to the power station that can be utilised for either the units (through the 11 kV Loop Supply), or for the common plant (through the 11 kV Ring Main) – in both cases via the Station Boards. A general rule of thumb is that the Station Supply is supplied from a different network than the one into which the power station delivers its generated electricity – preferably from a distribution network at a different voltage level. Although this normal rule represents the ideal and desired state, various exceptions exist due to the availability and proximity of such suitable other networks. The concept of a Station Supply is to obtain an off-site supply that has the potential (at least) to be still alive, although the local HV yard (as a network node) has been lost (i.e., dead). This serves as an emergency power source to run emergency and essential loads – reducing the demand on the diesel stock held at the power station for emergency purposes.

The vast extent of the power station's overall electrical reticulation system provides ample exposure to disruption events, allowing propagation into multiple units. This exposure of the units to cascade disruption becomes more pronounced when the configuration deviates from the normal (default) state to accommodate special circumstances. When operated in the normal state, the interconnection between units is minimised, and the units are less exposed to common mode disruption events (see section 5.6.3).

To illustrate how the electrical system of the power station could compromise multiple units, consider the event that occurred at Matimba Power Station on 24 October 2012. At the time of the event, four Matimba units were in service; one was on outage, and another was being returned to service with the light-up in progress. Because of the maintenance work being conducted and the unavailability of two units, the electrical configuration was changed to accommodate the requirements at the time. Specifically, the 11 kV Loop Supply was being utilised for power delivery, and the Station Supply was being used to provide power to both Station Board 1 and Station Board 2.

At 02:16, while experiencing a particularly intense thunderstorm involving a heavy downpour, an ingress of water occurred into the marshalling enclosure of the pressure relief device of the station transformer (the transformer that forms part of the Station Supply – green in Figure 89). The water caused a short circuit and resulted in the subsequent tripping of the station transformer. With the station transformer switched out due to the incorrect protection operation (emanating from the short circuit of the pressure relief device), both Station Boards 1 and 2 were left without power and unable to supply the reticulation systems that form part of their respective layouts. Amongst the loads being supplied from the two Station Boards are the auxiliary CW systems of the power station, one board servicing three units and the other board servicing the other three (see section 5.6.8 to clarify the role of the auxiliary CW system).

With the auxiliary CW systems devoid of electrical power to run their auxiliary equipment (e.g., pumps, fans, etc.), the coolant water temperature rapidly increased. Within 8 minutes, all four units that were in operation tripped on temperature-related protections of the draught group and feedwater system components. Figure 90 shows how this four-unit MUT manifested on the system frequency.

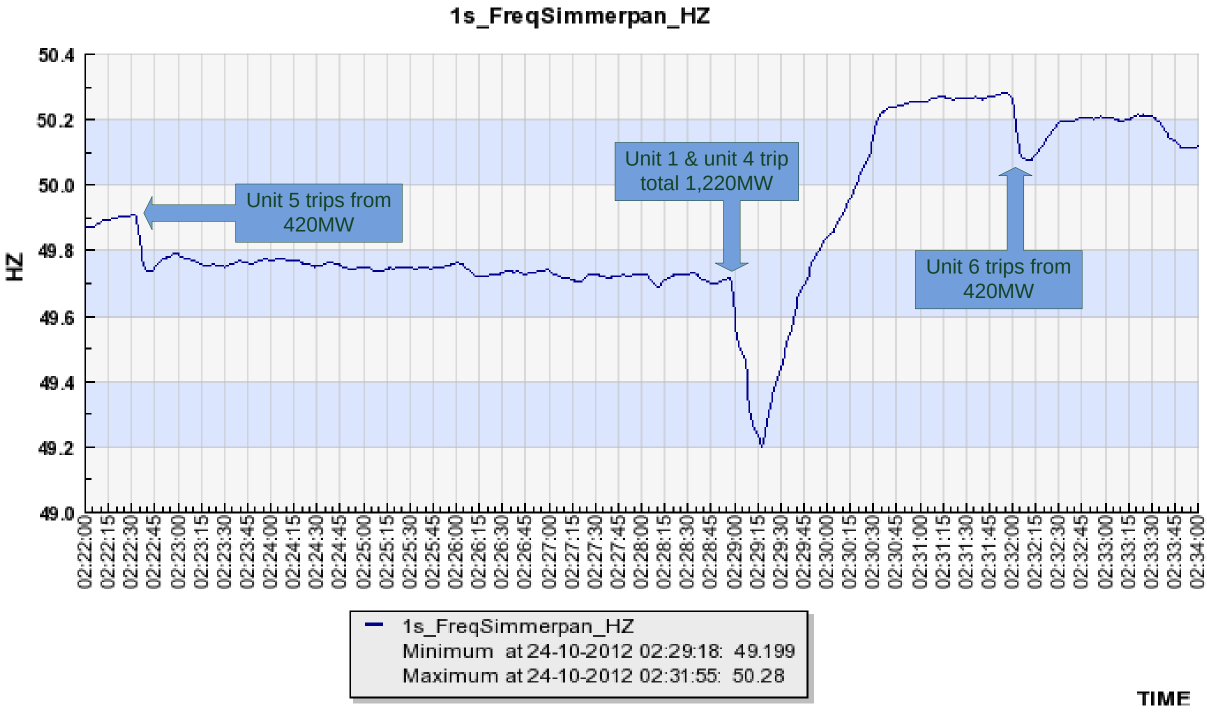


Figure 90: Effect of the four-unit MUT of Matimba on 2012-10-24 upon the system frequency

Due to the nature of cooling system failures, the trips of the individual units often do not coincide and depend on various factors. However, despite the 8-minute period over which the disruption was spread out, units 1 and 4 tripped at about the same instant (only 8 seconds apart) and caused a particularly deep depression in the system frequency, with a minimum value of 49,197 Hz being recorded.

Despite the deep frequency depression, the recovery in system frequency occurred rapidly. This was due to the tripping of six pump storage units that were in pumping mode at the time (typical for the time of the event) to yield 1 334 MW, the under-frequency load shedding scheme that provided 568 MW from across the system and 189 MW from contracted demand resources providing instantaneous reserve. The overall recovery from the event also involved the automatic starting of two units at Port Rex Power Station that contributed 108 MW. The shortfall was made up by units at other power stations that automatically responded using governing and by the interconnection tie-lines that increased electricity imports in response to the under-frequency condition.

Many examples exist of disturbances emanating from disruptions in the power station electrical reticulation system, but the majority stem from not adhering to the default configuration principles (often for legitimate reasons) prevailing before, thus increasing the units' susceptibility to electrical system disturbances.

5.6.10.6 Station Supply

As was mentioned in the previous section, most electrical systems of modern power stations feature a so-called Station Supply. The Station Supply provides an off-site source of power that is distinct from the normal grid connection of the power station (the HV yard) and is, therefore, normally (if possible) not sourced from the HV yard of the power station. Instead, it is normally sourced from the distribution system through a dedicated overhead line.

The Station Supply is conceptually shown in Figure 91.

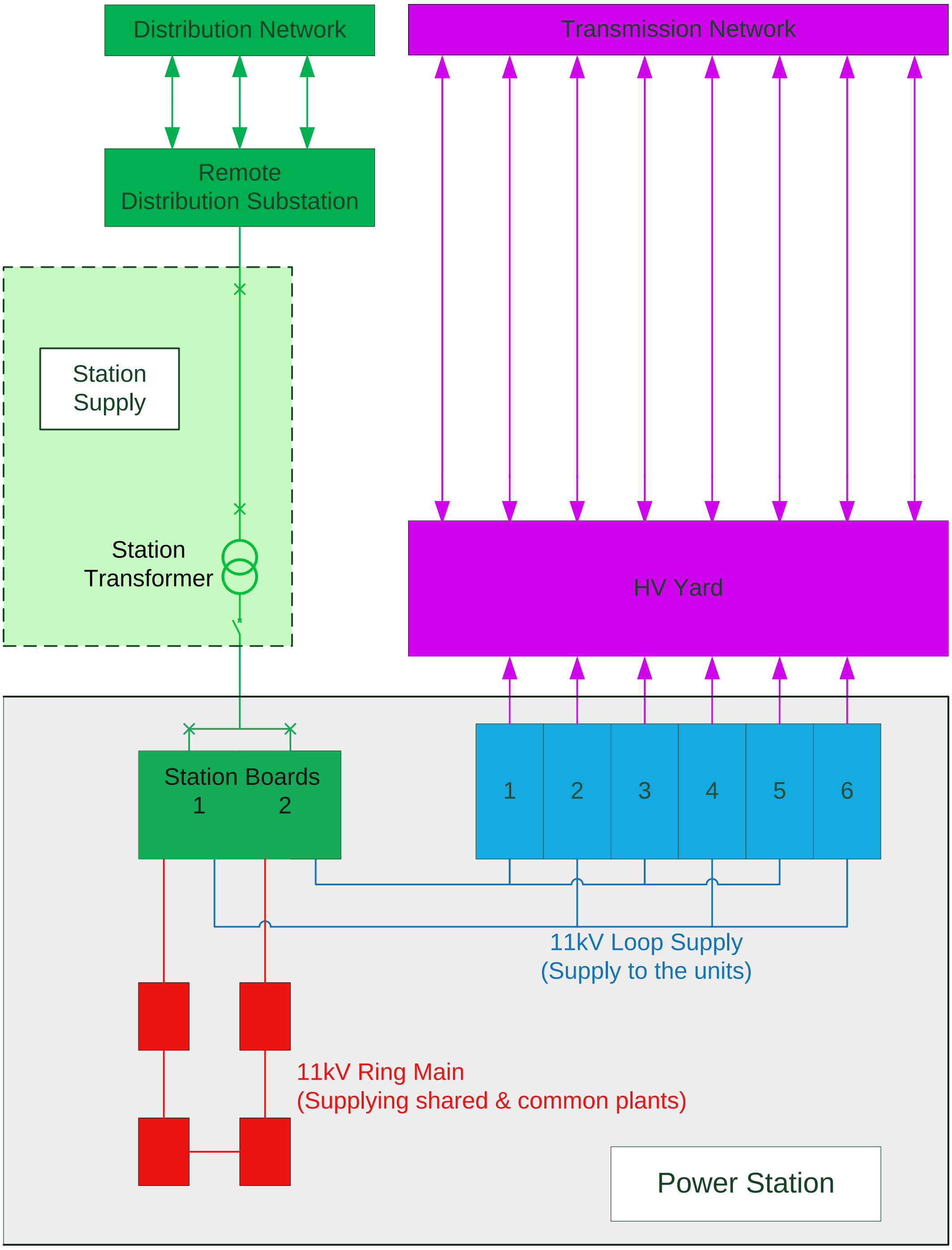


Figure 91: Typical layout of power station with its network interconnections

The purpose of the Station Supply can be summarised in terms of the following functions.

- Providing power during construction and decommissioning of the power station in the absence of any units generating or connected to the transmission system.
- Providing power to the common plant when units cannot supply the 11 kV Ring Main through the Station Boards.
- Providing power to specific units through the 11 kV Loop Supply while it is undergoing maintenance.

- Providing power to specific units through the 11 kV Loop Supply while it is being brought into operation after it has been off.

The Station Supply is normally a dedicated feeder from a distribution substation that is not shared with other participants. As illustrated in Figure 91, the Station Supply is permanently kept alive with the Station Transformer being energised (with only the LV breaker open), so that the supply can be brought into service rapidly and whenever necessary by closing a single breaker. However, the default configuration of the Station Supply is to be switched out and the power station is entirely being supplied by its units, either through generating units or by being back-energised from the HV yard.

If the Station Supply becomes compromised while being utilised by the power station, it normally causes widespread disruption. The reason for this rather high likelihood is an inherent vice associated with this supply since it is central to both the common plant supply and possibly some of the units. Also, if this supply is in service, it automatically implies that an abnormal condition pre-exists that deviates from the default arrangement, a condition that predispositions power stations to disruption events.

To illustrate this point, let us consider the following case study. On 27 January 2001, Lethabo Power Station had an unusual set of circumstances. Not only were both Lethabo unit 1 and 2 simultaneously on outage (a notoriously vulnerable condition since these two units are the default supply to the two Station Boards), but both units had their respective HV circuits out of service for maintenance. Therefore, with no viable other supply option available, the Station Supply was used to supply both Station Board 1 and Station Board 2, through which the 11 kV Ring Main was energised.

Due to a failure of the forced cooling system of the Station Transformer, the transformer tripped causing both Station Boards to be lost and rendering the common auxiliaries to be compromised. Among the common auxiliaries were the station compressed air compressors that could no longer remain in service, necessitating the two diesel-driven compressors to start. However, the diesel-driven compressors could not cope with the total load on the pneumatic system, and eventually, two units tripped due to the failure of pneumatic actuators. The remaining units were saved from tripping through the isolation of the tripped units from the pneumatic system (reducing the pneumatic load), and by operating personnel reverting to manual operating procedures in the absence of certain pneumatic components.

The Station Supply was never intended as a normal supply option. Therefore, it is only used when conditions do not permit other options. However, the number of cascade disruption events that are attributed to this system is significant and continues to rise over time.

5.6.10.7 DC Systems

Power stations have a vast footprint of auxiliary loads that are constantly in service while the power station is in operation. The majority of the loads are AC and, in most cases, require three-phase supplies. However, DC supplies are also required on occasion for one of the following reasons.

- To supply electronic systems that require DC for power supply purposes.
- To power coil-type electromagnetic actuators e.g., valves and contactors.
- To power DC motors under emergency or abnormal conditions.
- To provide essential and emergency lighting.
- For excitation flashing during start-up.

For normal purposes, two DC supply systems exist, a common system and a unitised system. The unitised system is shown in Figure 92 (for a single unit) [174].

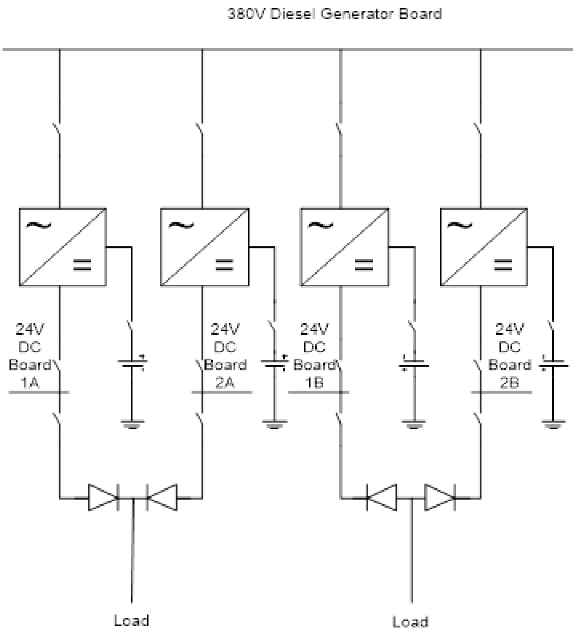


Figure 92: Typical layout of the unitised DC system of a single power station unit

Again, similar to much of the design of the systems at power stations, the DC systems also feature significant redundancies. It has two 24 V systems, a negative and a positive that can also be used to supply 48 V when needed. Each 24 V system is 100% redundant in terms of the battery, charger, etc., to allow for maintenance.

To allow for mechanical applications, DC motors and coil-type actuators are required. The voltage level for such applications cannot readily be satisfied with 24 V or 48 V. For this purpose, a 220 V DC system is supplied in terms of the standard DC design of a power station. The 220 V DC system is provided as a central, common system shown in Figure 93 [174].

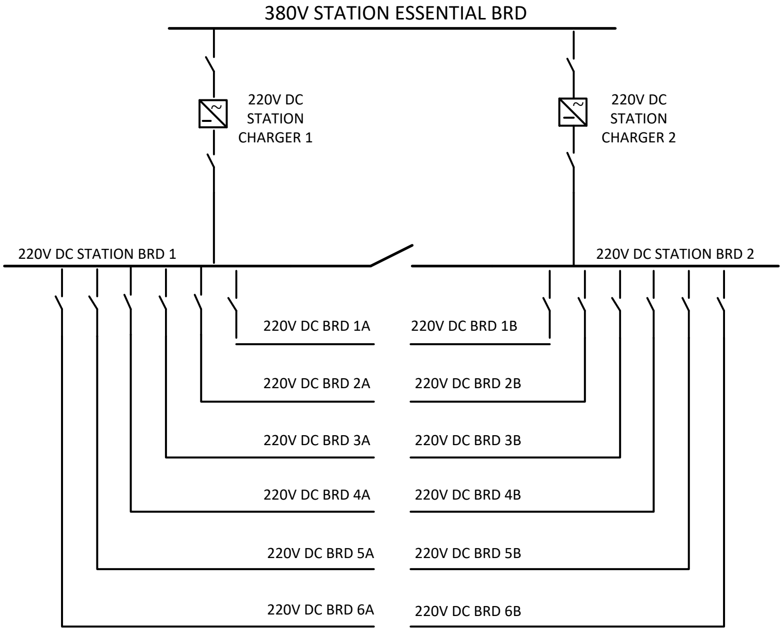


Figure 93: Typical layout of the common 220 V DC system of a power station

This design, just like the unitised design, features 100% redundancy with two independent chargers and batteries (not shown) to supply all six units. It is evident from Figure 93 that, despite the redundancies, the design is indeed vulnerable in the sense that a fault at one unit would affect all other units since they all share the same DC voltage node of the DC board.

A notorious example that demonstrates the vulnerability that this DC design poses to a power system, contemplates the multiple disruption event of 24 November 1992, when a human error occurred at Duvha Power Station. At 14:27, a technician performed standard fault-finding work on the main CW system at the centre well when AC, rather than DC, was connected to the terminals of the DC relay. The AC, through the 220 V station DC system, were superimposed on the DC node (220 V Station DC Board), thereby subjecting all 220 V DC circuits to the quasi-AC supply with a 50 Hz component. Relays across the power station malfunctioned and caused all five units that were in service at the time, to trip. The system frequency decayed rapidly, and two Kendal units tripped due to incorrect protection settings within their islanding schemes. The result of the event was a loss of 3 755 MW and a total frequency depression to 48,45 Hz.

This event caused major changes within the design and specification spheres of power stations. Equipment standards were changed so that future equipment would be less susceptible to accidental AC exposure. Islanding schemes had undergone review across all power stations, and the common 220 V DC design was changed. In a total redesign of the 220 V DC system, the 220 V DC were relocated to the units so that each unit would have its own 220 V battery and charger as shown in Figure 94.

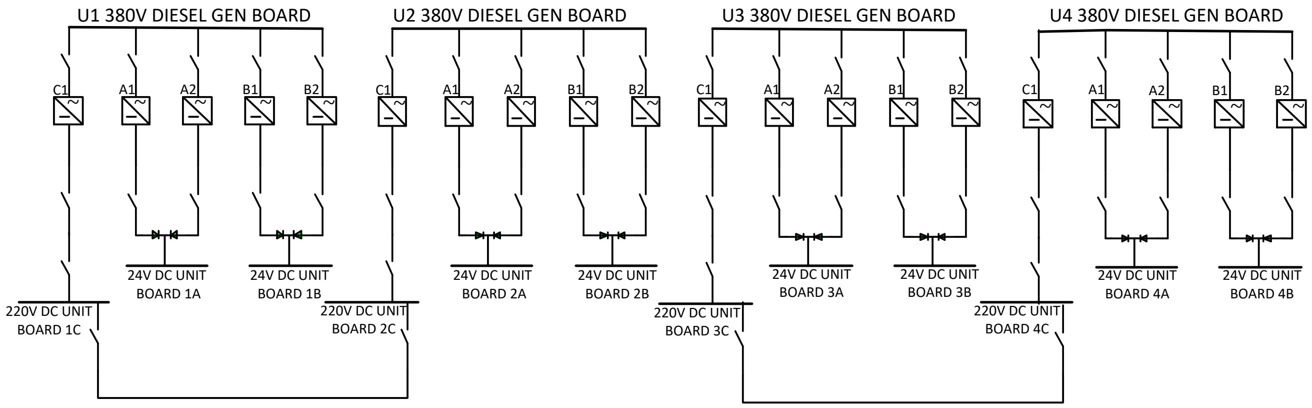


Figure 94: Redesigned unitised DC layout for fifth-generation power stations

Figure 94 shows the layout for four units only, as an example. Each unit is now equipped with a positive and a negative 24 V DC system (100% redundant) and a 220 V DC system, backed up with a DC loop to an adjacent unit.

5.6.10.8 Centralised Electrical Control

Modern power stations typically feature an electrical control room from where the power station's electrical reticulation system is managed, as well as the interface of the power station to the local transmission and distribution networks. The control room is normally equipped with an extensive control system that provides remote control functions over the supply circuit breakers forming part of the reticulation system. The control system also provides alarm functions and visualisation of field information, enabling an operator to make decisions and perform remote switching. Recent developments in substation automation also feature control functionality deployed both within and between substations, based upon digital control bus technology.

Since there exists only one electrical control room, it presents a fairly unique problem when it becomes obsolete. The problem is obvious: How can a system that is common and essential to all units and systems at a power station be taken out of service and replaced without having to shut down the entire power station?

Although a complete shutdown of an entire power station would be the only way to perform a risk-free upgrade of the control system of the electrical control room, it can never be achieved due to the vast quantity of energy and power that will have to be forfeited. Therefore, the practice invariably involves high-risk activities that need to be well planned and executed to perform the upgrade work while the power station remains in service. However, despite mitigation and contingency plans, high-risk activities remain exactly that, high-risk. This means the probability for such activities to go wrong, is higher than for other types of activities.

One such example occurred at Matimba Power Station on the afternoon of 25 June 2003 at 16:23. During an upgrade of the control system of the electrical control room, deliberate contingency plans were devised and executed. However, due to a human error made by a technician involved in executing the risk mitigation plan, a cascade event was put into motion that tripped three of the five units in service at the time and caused the remaining two units to transition to half-load conditions. In addition, and as a direct consequence of the event, one of the Tutuka units also tripped due to its inability to respond correctly to the frequency disturbance caused by the Matimba event.

The total loss suffered by the power system was 2 854 MW, which resulted in a minimum system frequency of 49,09 Hz being recorded. The event activated various stages of the under-frequency load shedding, which had a total yield of 939 MW. Also, the automatic starting triggers were activated at Drakensberg Power Station, where three units responded and at Palmiet Power Station, where both units started up automatically. Furthermore, two hydro units at Vanderkloof Power Station and three units at Gariep Power Station were called up into service – a total of 10 hydro units assisting, and an emergency generation condition was declared to support the power system to manage the system frequency and to handle the evening peak that was due to start. However, as the evening peak mounted, the slight margin of spinning reserves was rapidly depleted, and further interruptible loads had to be utilised to arrest frequency decay – totalling 1 892 MW.

Despite the significant scale of the disruption and its inopportune timing, all the units were returned to service by 23:30, within the applicable grid code requirements.

5.6.10.9 Cabling Systems

Modern power stations, with their high levels of automation, have vast amounts of power and instrumentation cabling. The cabling requires dedicated structures for handling and routing the cables.

In the outside plant, it is not uncommon for cables to be buried in trenches specifically created for this purpose or even for overhead power lines to connect to remote substations. However, handling the vast cabling requirements within the main structure housing the units is problematic.

The reticulation boards of each unit are housed within the confines of that unit, and the cabling connecting to the switchgear typically enters and exits the switchgear room through cable-spreading basements. The bulkiest of these cabling applications are those with the highest power levels, which are invariably the MV rooms (substations containing switchgear of 1 kV and above) of each unit. These MV rooms are physically situated at zero-meter level, allowing the cable entries from sub-zero levels (below ground level). To allow for cable routing, a tunnel structure exists below the power station main structure, running from end-to-end of the main power station structure – allowing for cable routing to connect unitised loads to switchgear that are physically remote from one another.

The cable tunnels typically consist of four parallel tunnels, all running from end-to-end, and various perpendicular tunnels intersecting across the four tunnel ways. All tunnels are stacked on both sides with successive sets of cable racks (or trays) from the floor to the roof of the tunnel, in which the cables are routed. For immunity and other practical reasons, signal and power cables are not routed on the same cable racks.

Although the cable tunnel infrastructure provides a neat and convenient solution to the cabling problem, it presents one major risk: a cable tunnel fire. If a cable tunnel fire occurs, the tunnels provide a fuel-rich corridor for fire to spread throughout all the units. It could destroy the entire reticulation system and all control and instrumentation in a single event. Such a risk is regarded as one of the greatest threats existing at a power station and, therefore, requires a deliberate planning framework to mitigate sufficiently against such a destruction event. The salient points of the mitigation framework are tabulated below.

- Correct sizing of cables for applications to avoid inadvertent overload during normal operation.
- Correct and efficient electrical protection application to ensure rapid fault clearance – including backup protection principles.
- Effective earthing of cable racking to facilitate correct protection operation.
- Diligent sealing of all cable entries where cables terminate.
- Specifying fire retardant and halogen-free cables.
- Extensive fire detection throughout the cable tunnel infrastructure.
- Automated fire suppression installed throughout the cable tunnels, with effective drainage interconnections.
- Automated smoke extraction systems to allow firefighting teams to operate inside the tunnels.
- Dedicated radio repeaters to allow radio communication within the heavily shielded cable tunnel system.
- Public address system extended into the cable tunnels.
- All human entry points to the cable tunnels are to be closed by rated fire doors.
- Sectionalisation of cable tunnels with rated fire doors.

- Physical inspections of cable tunnels to identify and resolve problems.

Although no significant cable tunnel fire has been recorded within a South African power station, it remains one of the paramount risks receiving constant focus. If such an event occurred and spread throughout the tunnels, it would remove the entire power station from service for a very long period, with permanent decommissioning as a distinct possibility.

5.6.11 Control Systems and Instrumentation

Generating electricity is complex and requires continuously operating control systems and the automation of equipment distributed throughout the plant – spanning significant distances. This control equipment (sometimes referred to as secondary plant equipment) is used to implement various functions, including:

- Continuous and binary control
- Sequential control (sometimes referred to as step-and-criteria control)
- Limiters avoiding process parameter exceedances
- Interlocking and lock-out systems
- Start-up and shutdown procedures
- Chop-over routines
- Process protection
- Capability computers – automated plant state transitioning
- Signal transmission and remote communication
- Alarming and indication
- Interfacing with operating panels, mimic panels and SCADA systems (HMI)
- Data collection, recording and archiving
- Condition monitoring

Modern power stations feature a high degree of automation to ensure safe and efficient operation of the plant and processes and to limit the staff contingent required to operate it. Fifth-generation units typically feature the following in terms of control and automation.

Control elements (valves, switchgear, actuators, etc.):	972 ± 50
Input signals (field devices and monitoring):	8 500 ± 250
Binary input signal state changes (per second):	1 200 ± 300

A compromise in the automation structures of a unit could readily disrupt the unit itself, possibly resulting in its shutdown. Such an event is usually limited to a single unit, since the control systems are essentially completely unitised.

However, except for the units of a power station, all the common and shared systems of a power station are also highly automated. Suffering a disruption within the control and automation infrastructure of a common system has a high propensity to compromise such a common system that may, in turn, lead to a compromise of several operating units that were using the disrupted system. Due to the inherent susceptibility of units to disruptions of common systems, the designs of common systems generally feature high redundancy levels.

Notwithstanding redundancy features, failures do still occur. Consider the event that occurred at Palmiet Power Station on 6 April 2007. Palmiet is a two-unit pump storage power station situated in the Western Cape of South Africa and part of the peaking reserves used within SAPP.

The headrace supplying water from the top reservoir is remotely located from the power station cavity itself. It uses a 100% redundant communication link between the control and monitoring equipment of the headrace and the power station units. At 02:10, one of the two redundant communication links failed – an event that was immediately actioned due to the importance of ensuring communication to protect the facility adequately. After fault finding throughout the day, the evening peak was approaching, and at 18:21, Palmiet 1 was called into service, followed by Palmiet 2 at 18:25 – both rapidly ramping up the 200 MW each (rated capacity). At 19:58, the second communication link failed, causing both units to trip as part of their protection logic. The power system operated at 27,2 GW at the time, and the system frequency declined from 50,03 Hz to 49,69 Hz, constituting a magnitude of merely 18,3 dB.

A rather more significant event occurred on Tuesday, 24 June 2008, at Lethabo Power Station. This fifth-generation power station, consisting of six 600 MW units and using a wet CW system, was first commissioned in 1985. The control and automation of the main CW system are coordinated from the Outside Plant Control Room (OPCR), where a dual redundant DCS serves as the control system. The two control systems are individually supplied from two entirely independent UPS supplies.

On the day of the event, while five units were in service, one UPS was taken out of service to perform battery discharge testing on its battery. For the duration of the test, the second UPS had to supply the full power requirement of the control system equipment in the OPCR. It was not realised at the time that the power supply to the second UPS (which now became the sole duty UPS) had also inadvertently been switched out (in error) due to the unrelated failure of the specific alarm. This unfortunate (and undetected) error had two undesirable consequences, namely:

- It allowed the battery of the second UPS to be drained without being recharged, and
- It rendered the static bypass of the UPS unavailable.

While the planned discharge testing of the battery of the first UPS was being carried out, the battery of the second UPS was also being drained – carrying the total load of the OPCR and all its control equipment. Ultimately, when the second UPS finally shut down at its designed threshold level, the entire control system lost its power and all control system states became static (frozen). Realising that the UPS supply was unavailable, prompt operator action was taken, and the power supply to the second UPS was switched back into service, precipitating a full system reset. The reset caused all auto-closing valves of the main CW system to close. At 15:58, all five units in service at the time tripped due to the ensuing CW starvation that caused a decay in the condenser vacuum to the point where the turbine protection systems tripped the units.

Fortunately, the units were not heavily loaded at the time, and the combined loss in power was 1 900 MW – removing 6,2% of the power being delivered into the power system operating at 30,6 GW, resulting in a frequency decay to 49,3 Hz. Various load-shedding schemes operated that collectively removed 535 MW from the system. At the same time, 12 peaking units were called into service to assist with the evening peak that was just about to start.

While the impact on system frequency was significant in itself, the loss of every unit at Lethabo compromised the support of the voltage node. The collective reactive power exported by the five units was 516 Mvar, causing significant voltage excursions at voltage nodes in relative proximity to Lethabo. Figure 95 shows a recording of the 275 kV busbar voltage at Glockner substation, where various 275 kV to 400 kV coupling transformers are installed, about 17 km from Lethabo.

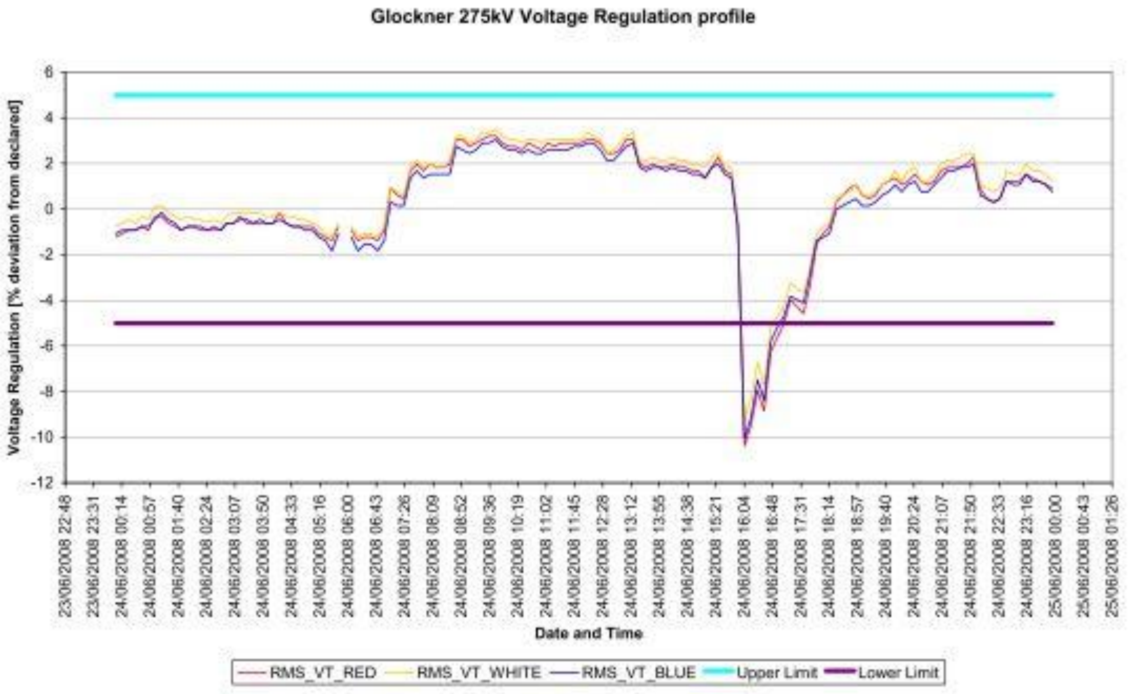


Figure 95: Recorded voltage deviation at Glockner during the Lethabo MUT of 2008-06-24

Although various MUT events were recorded at Lethabo, voltage depressions were never significant whenever a single unit remained in operation. This event illustrates the vulnerability of a grid node when all usual reactive power in-feeds are compromised, a risk that in itself could become a precursor to cascade failure and a subsequent system collapse.

5.6.12 Data Networks

An emerging threat that has been seen to cause multiple generation disruption events is the emergence and adoption of data networks in control system applications. Being a relatively new application in power station practice, time will be required for the technology to sufficiently mature to the point of it being tolerant of failure and the proactive detection of developing issues that may ultimately impact the reliability of the systems it serves.

Although a number of multiple contingency events were recorded that were attributed to data networks, it is ascribed to the lack of maturity level of the technology. It is envisaged that the technology would evolve to gain the requisite resilience level needed within power station environments.

5.6.13 Compressed Air Systems

Similar to the electrical reticulation system inside power stations, a pneumatic reticulation system also exists inside power stations, possessing considerable complexity. This pneumatic system, commonly referred to as the compressed air system, is essentially comprised of two main sub-systems, one being the service air system and the other being the control air system.

These two sub-systems are differentiated at the individual purpose level of each. The control air system provides high-quality compressed air to plants and systems that require it to fulfil a specific function. This function is often required for actuation or sustaining components or assemblies in a specific state (removing the air pressure will cause the state to change). Therefore, the control air system is integral in maintaining the plant in a safe state, supporting continued operation and allowing for the safe shutdown (even when electrical energy sources have failed).

On the other hand, service air can be used for maintenance purposes or to provide power to systems that are not essential for the safety or continued operation of the units. A major use of service air is to provide dust suppression in coal and ash handling plants, which assists in atomising water as part of a spraying system.

This description clearly shows that control air has a higher priority than service air. The high-level compressed air system of a typical fifth-generation power station is shown in Figure 96 (many variations exist, though). The two sub-systems are shown in green (service air) and blue (control air). The two sub-systems differ, not only in terms of their overall purpose but also in terms of the air quality, with control air being maintained to higher standards of dryness than service air.

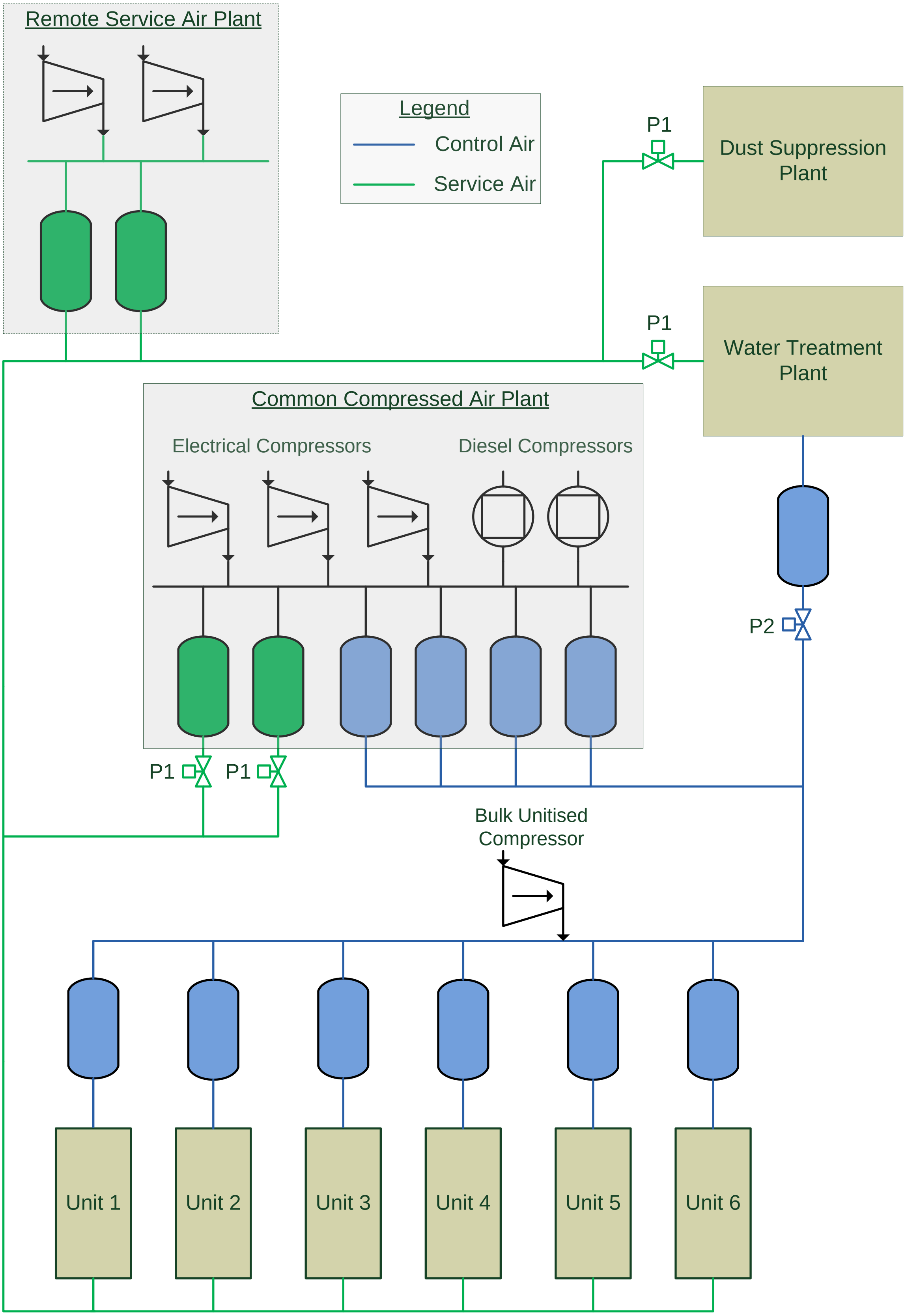


Figure 96: Typical high-level compressed air system of a fifth-generation power station

The common compressed air plant is at the heart of the compressed air system. This plant houses three large turbo compressors that are driven by MV motors and two reciprocating compressors driven by diesel engines (as a backup). It also houses a large set of pressure vessels as receivers to provide storage and buffer capacity to the system. The distinction between the control air and service air becomes evident in the design of this common compressed air plant – a mere two receivers are connected to the service air system. However, it is also clear that the two sub-systems (i.e., service air and control air) are not entirely independent from one another but are joined together inside the common compressed air plant. It can also be seen that the control air sub-system is equipped with more than double the number of receivers, to bolster control air reserves far more than for the service air.

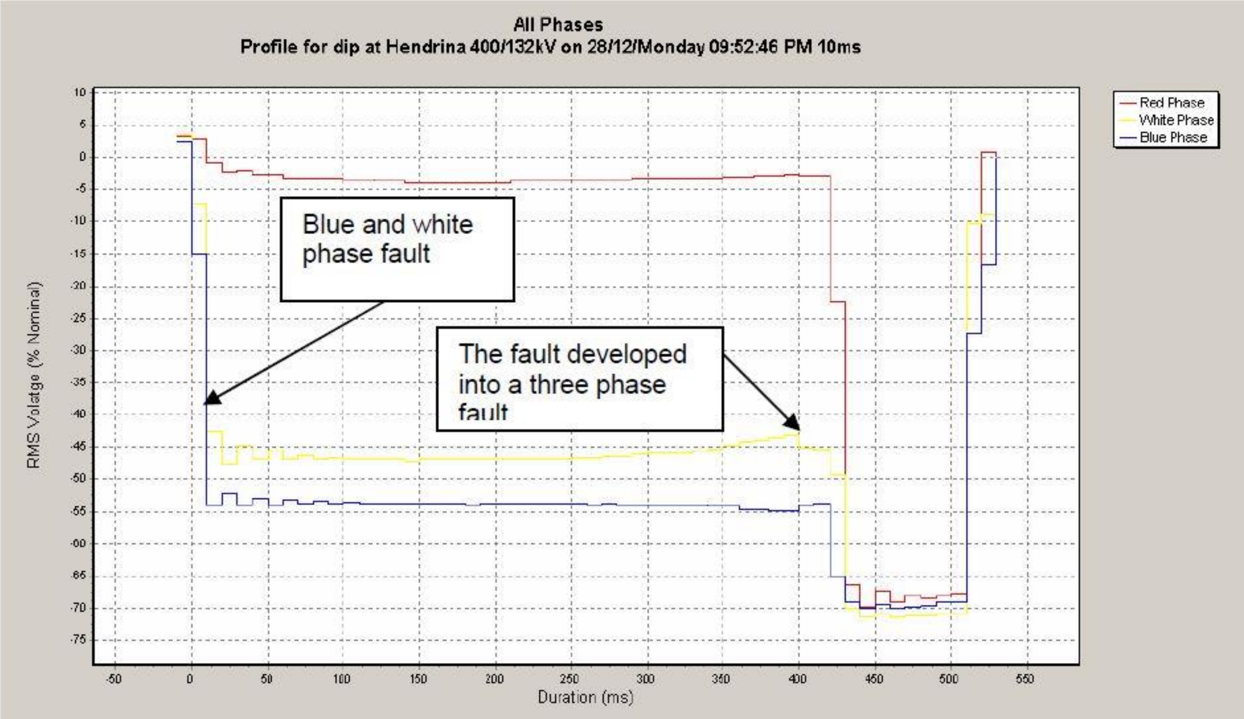
Because of the vast distances over which service air needs to be provided, a set of secluded compressors are used to supplement the service air in the remote areas where the over-land conveyor systems operate.

Compressed air is provided to all the units and some common plant areas, specifically the water treatment plant and the conveyor belt systems for dust suppression. Important to notice, though, is that all the service airlines are equipped with automatic cut-off valves that are pre-set to a pressure P1, which is about 25% below the system's normal operating pressure.

At pressure P1, the supply to the service air loads will be cut off to reduce any possible drain on the remaining compressed air reserves and dedicate all remaining compressed air for control air purposes. When the control air pressure further decays (even though the service air has been cut off), the control air supply to the water treatment plant will also be cut off automatically at pressure P2 (with P2<P1) – further prioritising unit operation over common plant services.

Ultimately, if control air pressure continues to decay, the bulk unitised compressor could be activated to support the control air pressure. However, using the unitised bulk compressor will always be a last resort since it is not ideally integrated with dry air quality as a prime objective. One of the key benefits of the bulk unitised compressor is that it can be utilised even when the electrical supply to the common plant areas is compromised since it is electrically supplied from one of the units.

With the critical role that compressed air has in power station operations, the dire effect that a disruption of this system could have needs to be understood. In one example, Hendrina Power Station lost five of the seven units that were in operation on 28 December 2009 when an external line fault occurred at about 21:52. The phase-to-phase fault rapidly developed into a three-phase fault causing an overall voltage depression of about 70% in the HV yard, as can be seen in Figure 97.



Blue and white phase fault

The fault developed into a three phase fault

Figure 97: Recorded depression in voltages for Hendrina network fault of 2009-12-28

The ensuing voltage depression interrupted several auxiliaries. Although automatic restart functions are designed into the control system for vital auxiliaries, the PLC controlling the compressor plant failed to restart the cooling water systems for the compressors (due to a design oversight), inevitably leading to overheating and tripping of the compressors by their protection schemes.

With compressors shutting down, the backup diesel compressor (only one exists at Hendrina – a fourth-generation power station) also did not start up due to a known defect that was, as yet, unresolved. The pressure in the compressed air system plummeted, and soon the threshold levels were reached – activation of the rapid closing isolation dampers of the boiler was triggered (in line with boiler operation safety principles). This boiler starvation condition led to boiler protection systems issuing total boiler (and unit) trips of five units, fortunately, staggered over 40 minutes with minimal impact to the power system.

5.6.14 Distributed Intelligence

In most intra-station escalation modes of disruption, single systems, plant equipment components or processes are responsible for the weakness resulting in multiple unit disruption events – outlined in the sections above. However, there is a less specific potential weakness that could be equally subversive and potentially highly pervasive, depending on a power station's design and technology profile – the threat of distributed intelligence.

From the fourth-generation and especially the fifth-generation power stations, there was a rapid increase in intelligence that was not centralised in concentrated nodes like central computerised systems. It became increasingly common for local controllers to become embedded within systems – often rendering plant control distributed instead of centralised. It may seem unimportant whether or not the control is centralised or not, in terms of the effectiveness of controlling the plant. However, distributed control does introduce further elements of risk that are not inherent to centralised control, of which the more prominent risks are listed below.

- When control parameters need to be set up in various devices across the plant, it becomes increasingly more likely that a person applying the configuration settings may erroneously load an incorrect setting or omit to set up some of the device functions.
- Controllers with sensitivity to external parameters may be deployed over a wide area and throughout various (and otherwise independent) systems and may individually contribute to collectively cause widespread disruption.
- The ambient and power supply conditions of central installations can be controlled with more rigour and effectiveness than for a distributed intelligence footprint, increasing the likelihood of disruption.

For example, consider a unit with many electric motors in operation to power its various auxiliary systems. Traditionally, such a population of electric motors would have been direct-on-line started and would not in itself be used to control any of the process parameters. The actual control would have been achieved through the use of other control elements, such as valves, actuators, dampers, vanes, etc., that would act to vary the degree of throttling to achieve the desired process parameters such as flow, pressure, temperature, etc. Then consider a case where these motors are not used in direct-on-line starting applications but rather being driven through variable speed drives (VSD) so that the control is not achieved through throttling but rather through varying the speed of the motors that drive primary plant elements such as fans, pumps, mills, conveyor belts, etc.

In the example above, consider a condition where the electrical supply to the VSD loads is disrupted, e.g., by a short circuit within the local reticulation system. Being complex electrical devices, each VSD would have some degree of sensitivity towards the health of the electrical supply to which it is connected. To avoid damage to the VSD, it would typically employ certain protection functions to protect the device from inadvertently being damaged when an unhealthy supply condition occurs. Such self-protection functions can be implemented in various ways but could cause the VSD to interrupt the power flow to the motor for as long as the supply disruption lasts. With the motor loads not receiving power, all primary plant components slow down, causing the process parameters to suffer. Such a state of affairs could readily develop into a compromise condition whereby an entire unit needs to trip. If, the disruption in the electrical supply does not emanate from within the unit but rather from the HV yard, every VSD across all the units may be affected, potentially causing an MUT.

In the early designs of fifth-generation power stations, VSD applications were uncommon and only used in exceptional cases. In the late 1980s, three South African power stations, Kendal, Matimba, and Majuba, experimentally featured large VSD applications, specifically on their boiler feed pump applications.

At 17:07 on the afternoon of 27 December 2009, the South African power system was experiencing a rather low evening peak. It was operating at 23,8 GW (it being the Sunday after Christmas) when the corona ring of one of the surge arresters installed at Majuba 1 broke off and caused a short circuit on the HV side of the generator transformer. The generator transformer's restricted earth fault and differential protection functions operated and tripped Majuba 1. However, due to the sensitivity of the VSD-driven boiler feed pumps on the other Majuba units (four units were in operation) all operational units suffered losses, while Majuba 3 and Majuba 6 tripped due to the process being compromised with insufficient feed-water flow. Majuba 2 managed to survive the disruption due to a standby boiler feed pump starting up after the disruption in the electrical supply had been normalised. Although not specifically investigated, three units at Hwange Power Station in Zimbabwe also tripped in response to the Majuba trip – presumably related to the ensuing frequency decay.

The frequency recovered from a turning point of about 49,085 Hz, arresting and recovering the frequency decay through six hydro peaking units, six aero-derivative gas turbine units, and using two stages of the under-frequency load shedding scheme. A total loss of 2 550 MW was suffered, but due to the state of the reserves and the many supply side and demand side resources utilised, the frequency was restored to 50 Hz within about 3 minutes after the event occurred. The load curve for the power system during this event is shown in Figure 98.

Figure 98: Power system load graph for the Majuba MUT of 2009-12-27

As can be seen, the load reduced from about 23 800 MW before the incident to about 21 800 MW at the lowest point, signifying a loss of about 2 000 MW overall (the black line). The difference from the stated 2 550 MW was due to the governing correction that occurred during the event's propagation and power transfers from international SAPP tie-lines. The purple-coloured line shows the system without the effect of the interconnecting tie-lines to neighbouring countries.

It may be argued that the loss of the three units might have occurred regardless of the distributed intelligence contained in the VSD equipment. However, no other motor loads tripped throughout the power station due to the disturbance to the electrical supply (LV or MV) – a deliberate focus area of the investigation that followed. The vulnerability in the Majuba design was a direct result of the application of the VSD technology.

The example above differs from previous examples in preceding sections in the sense that the consequence of the event resulted from an unintentional outcome brought about by the introduction of distributed intelligence – causing aberrant event branching. An event that occurs (within a larger disruption event) where generation capacity becomes compromised due to undesirable operation (or “inoperation”) of intelligent devices or systems is referred to as an apparition – the trigger for the apparition is known as the invocation. Such events are not a consequence of the electrical (or mechanical) dynamics, transients or component properties of the power system or power station. It is an unforeseen and undesirable outcome caused by an intelligent device that malfunctioned, entered an unconfigured state, was configured incorrectly or deviated from the product specification or technical documentation.

The vulnerability of distributed intelligence is not limited to coal-fired generation only. The MUT suffered by Matla Power Station on 21 July 2005 (refer to section 5.6.8) caused a severe frequency depression to 49,23 Hz. Songo Hydropower Station in Mozambique was in operation and connected through AC and DC connections within the SAPP. Songo 1 and 2 tripped in response to the Matla MUT when four Matla units were lost. The control systems of the Songo units had been replaced not long before the event and were not yet optimised and configured with sub-optimal settings. The rapid frequency reduction caused both units 1 and 2 at Songo Power Station to overload and subsequently trip, aggravating the overall severity of the disruption within the greater power system.

On a smaller scale but equally relevant is an event that occurred at Sere wind energy facility on 11 April 2018. At 17:45, an operating error at Helios substation, where a 132 kV breaker was inadvertently closed onto a solid earth, caused a significant voltage depression sensed by all 46 wind energy turbines installed at Sere. Based on requirements contained in the renewable sections of the grid code, settings were applied to the controller of each machine to comply with specific *fault-ride-through* requirements. However, the applied settings failed to consider the entire disturbance envelope and were thus insufficient for the Helios-event. Following the fault clearance, a significant three-phase voltage oscillation ensued, with voltage peaks exceeding the safety envelope of the individual converter equipment situated at every machine – causing the tripping of all 46 wind turbines. Although this event was insignificant within the broader context of the overall power system, it does illustrate how a single parameter could affect various independent components that could potentially present a collective threat to the power system.

A truly spectacular example that illustrates the vast distance over which a disruption could affect remote intelligent devices occurred on 18 February 2006, when a unit trip at Kendal Power Station in Mpumalanga caused a subsequent unit trip of a unit at Koeberg Power Station in Cape Town – with a separation of about 1 500 km between the two sites. Kendal lost a single unit while carrying out a pre-planned test on the unit's automatic voltage regulator. The Koeberg unit was lost due to an inappropriate protection setting applied to its loss-of-field protection function. The remote intelligence situated at Koeberg created the predisposition of Koeberg to become susceptible to remote disruptors that may cause a disturbance in the local grid parameters where Koeberg is located. The Kendal-Koeberg event was calculated as having a magnitude of 12,9 dB in the power system, and the system frequency decayed to 49,19 Hz.

In each of the cases above, the initial disturbance occurred relatively distant from where the subsequent disruption manifested – a remote location where a distributed intelligent function, with a predisposition susceptibility to parameter disruption, was excited at a trigger location and sensed at a manifestation location and responded to it. This highlights an inherent flaw in the popular notion that plants can be isolated, insulated or unitised to create immunity to external disruptors – even disruptors emanating from other plants that do not share any plant, equipment or process amongst them.

And herein lies much danger for large-scale disruption of power systems. As power systems and generating units develop to incorporate ever greater quantities of intelligent systems, fully understanding the functioning of the devices and systems under all possible conditions becomes vital. This, however, is not a trivial expectation. Consider the following realities:

- Modern power systems and units are highly complex, and the ability to model all possible (or even just the most likely) states and conditions is virtually impossible.
- Although intelligent functions must be properly set up to deal with the various possible conditions, much of the risk profile involves those states, conditions and coincidences that have not previously been recognised or anticipated. Failure to configure two remote intelligent devices for a specific condition would almost certainly result in dissimilar responses, especially if the two devices had different suppliers, leading to unpredictable and uncoordinated outcomes, a perilous threat.
- Traditional devices were well understood and had long product lives. Modern devices are developed on relatively short timescales and have an equally short product life before becoming obsolete. Many of the products' inherent vices have not yet been identified by the time they are due for replacement.
- Due to the relative ease of effecting firmware changes, many products have several firmware versions, and it requires a concerted effort to ensure that all revisions are maintained at the latest revision, especially on a plant that is in service and requires planned outages to receive the upgrades. Also, the upgrade may require full recommissioning of the plant after the fact, which may not be possible to accommodate within the allotted time of the planned outage.
- Dwindling expertise internationally, at the utility, OEM, and consultancies levels raises the risk level for proper modelling, setting calculation, and configuration management. Due to shortening product life timescales, even the OEM often cannot maintain adequate expertise to support product ranges that are no longer current but still in widespread use in many applications globally.
- Intelligent devices tend to increase in complexity and the levels of expertise required to effectively configure every aspect of the device in catering for every aspect of its operation and every aspect of possible fault conditions it may be subjected to.

Specific technologies have emerged to be of particular concern, such as:

a Variable speed drive (VSD) applications – due to the vast potential spread throughout power stations, each having invocation potential with the possibility of further cascading.

b Substation automation applications with a large and distributed footprint of intelligent electronic devices (IED) throughout internal reticulation networks – complicating configuration management, firmware upgrades, etc.

c Distributed control applications with significant distance separation, e.g. wind farms.

Therefore, the likelihood of ever-mounting large-scale disruption events either attributed to or aggravated by distributed intelligence is predicted to increase unabated.

5.6.15 Demin Water

In section 4.5.5, the threat of fuel oil has been explored in some detail. Demineralised (demin) water is another threat with similar attributes from a risk perspective.

Demin water is an ultra-pure form of water produced at many power stations and normally used to generate electricity. Removing impurities from the water renders the fluid less chemically reactive and even yields a cooling medium with near zero electrical conductivity, which is needed for cooling large generators.

The multiple disruption risk posed by demin water is twofold. Firstly, an event that would compromise the purity of the demin water supplied to the various units could compromise the cycle chemistry of multiple units – having significant long-term plant health implications that may necessitate the shutdown of more than one unit.

Secondly, if insufficient demin water is available, it may significantly delay the return-to-service if multiple units need to be started concurrently or consecutively.

Both of these risks have manifested within the South African power station fleet. One example occurred on 28 September 2022 at Camden Power Station when caustic injection into an anion vessel occurred while one of the demin trains was regenerated. This event necessitated the shutdown of seven of the eight units in service at Camden – removing 1 356 MW from the system for the duration of the decontamination process that was needed afterwards.

Refer to section 5.6.20 for another example of a demin plant disruption event.

5.6.16 Operational Envelopes

Any process is bounded by limitations that cannot be transgressed – physical, legal, licenced, etc. These boundaries, if suitably designed, need not encroach upon the normal operation of a power station. However, it occurs occasionally that design assumptions underestimate actual conditions or that legislation and licenses are retroactively applied to limit or discourage certain behaviours, impacts or technologies. When boundaries restrict normal operations, deliberate actions are taken to limit output and remain within the normal and acceptable envelope for plant operations.

A prominent example of a physical limitation is at Matimba Power Station. As an experimental design, Matimba was the first Eskom power station that featured a direct-condensing dry-cooling system. However, it is situated in a particularly warm part of the country with a prevalence of unfavourable wind patterns for much of the year. The combination of the design of the plant and the environmental conditions resulted in high load losses across all units during warm summer days, from first commissioning to present-day operation.

Another example is the legislative restrictions that present-day air-quality statutes and regulations impose upon much of the coal-fired fleet of power stations (see section 5.6.22). Once again, the collective load losses that such legislative revisions have brought about are considerable and often contributed significantly to the need for load-shedding during 2022 and 2023 in South Africa, which was already facing a general deficit of power-generating capacity across the power system.

This highlights the need to verify design assumptions and observe international trends in legislative changes since retrofitting countermeasures is often prohibitively expensive.

5.6.17 Lesser Interdependencies

Although the sections above deal with the more significant risks of multiple disruption events, several other threats can potentially also disrupt more than one unit. Most of these have already caused or threatened to cause disruption but are less common than those dealt with in the preceding sections. Some of the more prominent ones are listed below.

a Raw water supply infrastructure and storage
b Molecular hydrogen gas (H_2) for generator cooling that is produced and stored on-site
c Chemical availability for managing chemistry functions at the power station
d The auxiliary steam range interconnecting various units through steam piping
e On-site availability of process gas (N_2, SF_6, CO_2, Ar, He, etc.)

f Consumable stocks, e.g. lubricants, grinding media, diesel and petrol fuel
g Spares holding and repair capabilities
h Air quality control and mitigation systems
i Heating, ventilation and air-conditioning systems
j Elevators and cranage

Each item listed above could be expanded to a separate section. Still, the statistical propensity to cause multiple unit disruption events has proven to be less pronounced, so it is, therefore, merely listed.

5.6.18 Maintenance Restrictions

One of the salient features of modern power stations, specifically from a maintenance perspective, is that much design effort goes into allowing maintenance whilst causing as little overall disruption as possible. This feature applies both to unitised and common systems.

Common systems are mostly designed using one of two standard approaches.

- The entire system is 100% redundant, e.g., coal or ash conveyor streams.
- The system consists of several constituent components, of which fewer than the total number of components are required to achieve the system's objective, e.g., the compressed air system where more compressors are installed than are necessary to supply the full pneumatic load of the power station.

Conversely, on the unit level, most of the auxiliary systems can be taken out of service for repairs while the unit itself remains in service, an inherent feature of modern (fifth-generation) power station units as elucidated in sections 5.4.1, 5.4.2 and 5.4.3. Unlike the auxiliary systems, the primary unitised systems mostly require that a unit be shut down entirely, with limited in-service maintenance opportunities.

Modern units normally (on average) are taken out of service for planned outage execution about every 18 months, with every alternate outage being longer to execute a more encompassing work scope. There would always be units on outage in a large fleet of power stations. However, the peak winter (or peak summer) months are more or less devoid of planned outages to maximise capacity when ambient conditions dictate the domestic load profile. In South Africa, winter has a higher peak, but it is not uncommon for a summer peak to be dominant in countries with very warm climates.

Despite the segregated design of both unitised and common plant systems to minimise the overall impact of maintenance on a power station's production, practical or technological considerations sometimes force a condition where multiple units are at risk of disruption or are to be removed from service to allow for maintenance. One such example is the main CW system of wet-cooled power stations (refer to section 5.6.7.2.1).

Channelling hot cooling water from the units to the cooling towers and cold cooling water back from the cooling towers to the units on power stations with four units or more, typically requires two extensive subterranean ducting systems, each of which services half the units at the power station (see Figure 69). This type of design necessitates that, from time to time all the units sharing a main CW system need to go concurrently on outage to allow for the draining and isolation of the system, allowing access to inspect and maintain the system. In the median South African wet-cooled power station, every group of three units needs to be shut down concurrently for about one month once every decade to facilitate the execution of the requisite maintenance of the main CW systems. This could significantly impact a power system, both from a total power availability and stability of the power node view that the specific power station represents in the overall system.

It is not only primary plant and systems that present the potential for disruption of power systems. Control and instrumentation (C&I) systems employed on units normally do not present a significant risk to adjacent units. However, all the common and shared systems also use C&I systems that are independent of those used for the units. There are essentially two main C&I applications at fifth-generation power stations that render a power station vulnerable to disruption, i.e.:

- The C&I system for the common and shared systems – all of which are contained within a single system that is normally interfaced with a single control room (OPCR) with dedicated operating staff (refer to section 5.6.10.8).
- The C&I system for the electrical reticulation systems and interfaces to the local power network that is contained within a single system that is normally interfaced with a single control room (EOD) with dedicated operating staff (refer to section 5.6.10.8).

These systems are normally designed to be highly redundant with standby processors and very secure power supplies, with much design attention given to functional allocation and the separation between control and protection. However, despite the use and adherence to strict design principles and the application of world best practices, one crucial weakness is inherent to the nature of the technology – the limited life of product ranges with the implied need for repetitive and periodic replacement.

The need to upgrade or replace C&I systems exists equally with the units, but any unit can readily be taken out of service for the duration of the replacement, often requiring 120 days.

The problem, however, is that the common systems serve all the units, and it is not practically possible to shut down all the units at a power station for a full-out replacement of an entire common plant C&I system. The impact on the power system would be entirely unacceptable. Therefore, these C&I systems are invariably replaced while units remain in service. Although many precautions and contingency plans form part of the replacement process, many systems are required to operate with non-standard configurations and limitations in functionality while the upgrade is being carried out. Such deviations from default operating practices are often a precursor to widespread disruption, a phenomenon that has often been observed, refer to sections 5.6.10.8 and 5.6.8 for typical examples.

5.6.19 Wear and Ageing

Coal-fired power stations are constantly subjected to various wear phenomena, particularly coal and ash-related erosion of the boilers and boiler auxiliaries. Although this phenomenon is inherent to the design of coal-fired power stations, it is not constant.

Generally, the largest contribution to the unavailability of a coal-fired unit emanates from boiler tube leaks, mostly wear-related thinning of the high-pressure metal tubes existing inside and exposed to the boiler's furnace and associated gas flow paths. The perpetual combustion process required inside the boiler furnace demands a continuous gas flow that transports fine coal powder into the furnace and removes the remnant combustion waste particles as fly ash. In cases where the generation fleet is dominated by coal-fired power stations (such as in the South African case), the unavailability of the entire fleet is also dominated by boiler tube leaks, in other words, by a wear-related phenomenon.

Therefore, if this wear phenomenon increases, it would have a direct and adverse effect on the availability of units that could compromise the greater power system. The following power law expresses the wear associated with particles within a gas flow path [175].

$$\varepsilon = a \cdot V^{\alpha} \tag{5}$$

with ε being the erosion rate, V being the velocity and a and α are material constants that characterise respectively the relative erosivity and the velocity exponent. The values of a and α are normally determined empirically for a given case. The values for a and α have been quantified for three of the large South African power stations, i.e., Matimba, Lethabo and Matla Power Stations, and the values are as follows [176]:

Matimba $\varepsilon = 0{,}0004 \cdot V^{3{,}09}$

Lethabo $\varepsilon = 0{,}002 \cdot V^{2{,}42}$

Matla $\varepsilon = 0{,}00002 \cdot V^{3{,}64}$

To illustrate the effect of boiler erosion, consider the case of Lethabo. Babcock, the OEM for the Lethabo boilers, provided the following airflow information.

TABLE XIII: BOILER AIR FLOWS FOR LETHABO POWER STATIONS

Gas flow velocities in a Lethabo boiler (m·s^{-1})			
Region of Boiler	Average Flow Velocities		Comment
	MCR 618 MW	**EL1** 635 MW	
Screen tubes	11,5	11,9	
Superheater 1 stage 1	9,1	9,4	
Superheater 1 stage 2	9,7	10,1	
Superheater 1 stage 3	11,3	11,7	
Superheater 2 stage 1	9	9,3	
Superheater 3	8,2	8,5	(Final Superheater)
Reheater 1 stage 1	10,8	11,1	
Reheater 1 stage 2	11,2	11,6	
Reheater 1 stage 3	12	12,5	
Reheater 2	12,1	12,6	(Secondary Reheater)

This OEM data was used to calculate the relative increase in boiler tube erosion rates between MCR operation and EL1 operation, using the Lethabo-specific relationship, $\varepsilon = 0{,}002 \cdot V^{2{,}42}$, to provide the following results.

TABLE XIV: INCREASED EROSION RATE BETWEEN MCR AND EL1 FOR LETHABO POWER STATIONS

Gas flow velocities in a Lethabo boiler (m·s^{-1})			
Region of Boiler	Average Flow Velocities		% Increase in Erosion (from MCR to EL1)
	MCR 618 MW	**EL1 635 MW**	
Screen tubes	11,5	11,9	8,63%
Superheater 1 stage 1	9,1	9,4	8,17%
Superheater 1 stage 2	9,7	10,1	10,27%
Superheater 1 stage 3	11,3	11,7	8,78%
Superheater 2 stage 1	9	9,3	8,26%
Superheater 3	8,2	8,5	9,08%
Reheater 1 stage 1	10,8	11,1	6,86%
Reheater 1 stage 2	11,2	11,6	8,86%
Reheater 1 stage 3	12	12,5	10,38%
Reheater 1	12,1	12,6	10,30%
		Average	**8,96%**

For context, MCR is the maximum continuous rating of a unit. EL1 (emergency level 1) is a level of power output from a unit that exceeds MCR, and that is demanded by the system operator in cases where the power system is under duress.

In the case of Lethabo, operating a unit in EL1 generates an additional 2,75% of power (17 MW), while the boiler erosion increases by 8,96% on average.

Normally, EL1 is only used for short durations, but prolonged exposure to a predominantly coal-fired fleet of power stations has a highly deleterious effect on the units, manifesting in reduced average unit availability and leading to an overall power shortfall. Ironically enough, such a shortfall normally necessitates a greater dependence on EL1 operation, a cycle that becomes increasingly difficult to break once entered.

However, it is not merely wear-related conditions that manifest in an adverse production effect of a plant that fails to continuously perform at original levels of production but various other age-related factors that impact power plants over time. Ageing is indeed a daunting topic and has many facets, with some of the more obvious ones listed below.

- Wear
- Fatigue
- Corrosion
- Obsolescence
- Lack of OEM support

- Changes in underlying technologies
- Changes in legislation or the regulatory environment
- Depletion of local resources
- Depletion of available sink for waste (ash typically used as a wastewater sink)

Many of the ageing factors above would translate into a reduced capacity of individual units, with a net reduction of the overall capacity of the power station. Also, as the power station nears the end of its life, much of its capital value has already depreciated to zero. This depreciation implies that significant plant failures often spell total decommissioning of the affected unit since major repairs would necessitate either a loss of revenue or a recapitalisation, both options having adverse implications for an old power station. Therefore, when a unit suffers a major failure, it normally is taken out of service permanently, and the capacity of the power station is adjusted down to reflect it as such; the unit then merely serves as a source of spares to be cannibalised by the units that remain in operation.

To illustrate the effect described above, consider the case of Hendrina Power Station in 2019. The first unit at Hendrina went into service in 1969, and the power station was in full operation in 1977, featuring ten 200 MW units. This overall capacity remained at that level until 2008 through consistent maintenance programs. In the years thereafter, the funding requirements to further maintain all units at their designed values would have required considerable investment, funding that could be applied more prudently at other facilities with remaining life expectancies far greater than Hendrina's. Therefore, the total capacity at Hendrina was allowed to reduce, as seen in Figure 99.

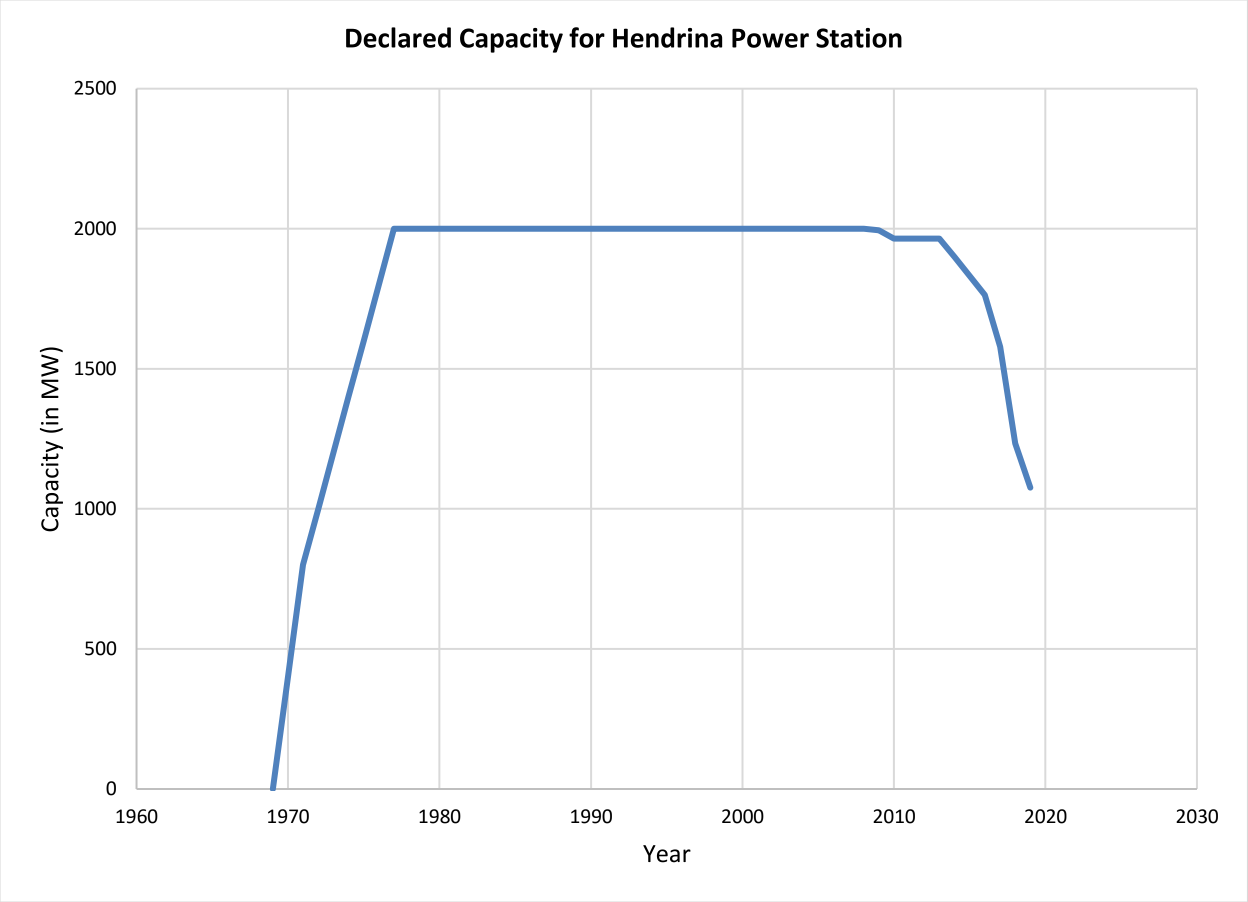


Figure 99: Installed capacity at Hendrina Power Station over a 50-year window

As can be seen above, Hendrina's capacity has nearly halved over the last decade, starting in 2009. This phenomenon is not atypical for power stations and needs to be taken into account when studies of capacity sufficiency and reserve margin are conducted.

5.6.20 Life Cycle Management

Life cycle management is strongly associated with the preceding topic of wear and ageing. As vast conglomerations of technological equipment and systems, power stations are highly dependent on the diligent execution of life cycle management plans and principles applicable to each technology as an overarching asset management approach.

This implies that the equipment and systems should periodically undergo major refurbishment, upgrade and even replacement over the life of the power station to ensure that its functionalities and capabilities do not erode over time. Since many technologies have a very limited product life expectation, the plant requires regular updating to ensure it remains fully functional, reliable and fit for service. Digital equipment features are amongst the most susceptible to obsolescence and typically require upgrade and replacement at intervals between 8 to 10 years.

Due to funding constraints manifesting in the South African electricity utility (which occurred for various reasons), life cycle replacements and upgrades started lagging. In the early 2020s, it was not uncommon for upgrade and replacement projects to be delayed by more than a decade (in a few cases, by more than two decades).

When life cycle management is not executed according to industry standards, various undesirable consequences start manifesting – the more pertinent ones are listed below.

a Increased unreliability
b Increased failure rate
c Decline in OEM support
d Lack of spares (and exorbitant prices for spares)
e Decline in expert support from the service sector
f Increased risk to plant, personnel and the environment
g Decline in efficiency

The risk imposed by a lack of adherence to life cycle management plans was highlighted at Kendal Power Station on 22 February 2024, when all running units were compromised and subsequently tripped, removing a generating capacity of 2 560 MW from the power system within a time window of 8 minutes.

The replacement and upgrade of the control system of the demin plant (refer to section 4.5.15) at Kendal was repeatedly postponed. Consequently, the existing control system became increasingly obsolete and unreliable and various functional capabilities compromised. Eventually, the burden of operating the plant shifted largely from the control and automation system to human operators, with the associated elevation in the risk of human error. In addition to a reduction in automation, various alarm and protection functions implemented by the control system became compromised.

Inevitably, when a significant error occurred, all running units' chemistry was affected, and the units were lost. Fortuitously, two units were not operating, curbing the disruption event's extent. Nonetheless, the event resulted in a 268 GW·h loss of production and an associated increase in the level of load-shedding at the time, from stage 2 to stage 4.

5.6.21 Adverse Weather

Weather is a potential common disruptor in most spheres of human endeavour, from air travel to normal day-to-day life and at power stations. Every power station has an envelope of maximum and minimum limits for every ambient and environmental condition within which operation can continue unhindered. Still, operations become impacted when the bounded envelope becomes compromised.

Weather-related parameters that are known to disrupt power stations include the following:

- Temperature (both high and low)
    - Atmospheric
    - Water bodies
- Wind (both very high levels and very low levels)
- Rainfall
- Drought
- Snow
- Cloud cover (especially for solar generation)
- Storms
    - Thunderstorms (typical to South Africa)
    - Gales
    - Blizzards
    - Cyclone storms
- Solar radiation (at ground level)
- Lightning (refer to section 5.6.10.1)

There are numerous examples of multiple unit disruption events affecting power systems due to weather-related reasons. One example is an event that occurred on 20 October 2020 when a severe windstorm occurred in South Africa near Grootvlei Power Station. Only two of the six units were in operation at the time of the storm. During the storm, the wind reached such severity that the metal roof of a minor structure was blown off and into the HV yard, causing an electrical fault across multiple zones and tripping both running units.

Weather conditions remain a major contributor, globally affecting power systems. It will receive further focus in sections 5.7.4, 5.7.7 and 5.8.1.

5.6.22 Legislative and Regulatory Framework

Power stations invariably form part of power systems within the borders of specific countries and, therefore, need to conform to the legislative and regulatory frameworks of the applicable region. When statutes and mandatory requirements change, power stations are often affected.

Legislation can affect power stations in one of three ways.

- It can set future strategies that will affect the design and operation of future power stations as it may affect its cost of generation and render certain projects unfeasible and, therefore, abandoned.
- It may change the existing power station requirements and compromise its economic model, forcing it to cease operation and rendering a stranded asset.
- It may change the existing requirements for power stations, which may necessitate additional investment and encroach on their ability to generate electricity and participate in the market.

The most prominent examples pertain to the management of air quality. In South Africa, electricity generation is being kerbed due to increasingly restrictive air pollution standards that are retroactively applied to power stations. In 2023, it is typical in South Africa that, during any given day, between 10 and 20 units are operating with restrictions in terms of electricity output, affecting the running fleet of large coal-fired power stations, despite a semi-permanent state of load shedding implemented across the country. These restrictions are only rescinded when emergencies are declared by the system operator.

Legislative changes also affect other aspects of electricity generation and affect issues such as:

- Primary fuel types
- Water usage allocations
- Equity in terms of procurement
- Etc.

Although many legislative requirements are not technical in nature, they very often have operational consequences in terms of the generation of electricity that affect multiple power stations and, therefore, remain relevant within the context of this study.

As stated earlier in section 3.2.3., the South African Grid Code (SAGC) does impose certain regulatory requirements on power stations pertaining to MUT events. Among those requirements is each power station's duty to compile and regularly update a register of plants and systems that may result in an MUT. The power station is further obliged to share the register with the system operator.

Although the risk registers are compiled and shared diligently, the code fails to enforce any similar requirement on power stations regarding MUD risks. Nor is any effort made to systematically track and analyse the collective impact of MUD events – an endeavour that could have a pragmatic influence on future legislation along the lines of mandated impact studies before promulgation.

5.7 Inter-Station Escalation – Multi-Station Cascade

It is apparent from the preceding section that many interdependencies exist between generating units due to systems that have certain commonalities among them. However, it is not merely the individual units that share commonalities between them, even on a more macro level, there exist commonalities between different power stations within a power system. These commonalities also result in interdependencies between the different power stations on the one hand and between individual power stations and common resources (or commodities) on the other.

The interdependencies between power stations occupying the same power system have the characteristic that a disruption at one power station may inadvertently disrupt another. The foremost commonality in this realm is the interconnected power system (IPS) that links power stations together and upon which they are collectively dependent for stable operation. Since a disruption at one power station typically affects various electrical parameters, a second power station embedded within the same IPS could become exposed to those affected parameters. Suppose the exposure level to the affected parameters at the second power station significantly breaches the envelope of normality. In that case, the second power station may not be capable of continued operation and suffer disruption due to the original disruption at the first power station.

The various commodities, resources or systems that could expose multiple power stations within a power system to a common mode disruption include:

a The networks or grids connecting power stations (IPS)
b Fuel supply value chain making primary (and secondary) energy available to the power stations
c Water sources on which power stations depend
d Social environment within which power stations need to function, including political and economic influences
e Legislative and regulatory frameworks
f Markets for access to consumables, spares, replacement installations, labour, repairs, funding, etc.
g Geographical features common to multiple power stations
h Climatic occurrences affecting multiple power stations
i Extra-planetary events exposing multiple power stations

These dimensions will be explored in some detail in the following sections.

5.7.1 The Interconnected Power System

Modern regional power systems typically interconnect many power stations and renewable energy facilities to form a power pool, often spanning different countries. Although such an IPS has much economic benefit by pooling generation resources, it also inadvertently forms a significant commonality between power stations, one that is particularly susceptible to disruption.

A set of rules, standards and norms govern the participation of power producers within such an IPS and provide the technical margins within which participants need to operate and for which power stations require the capability to tolerate. However, two main categories of disruption could violate the allowed margins governing the power system and may lead to cascading events that could compromise stability. These two disruptor-classes are:

a Disruption at one power station resulting in the exceedance of technical margins that, in turn, disrupt another power station.
b A disruption within the power system that results in the exceedance of technical margins, which, in turn, disrupts more than one power station.

Disruptions at one power station that cascade into disruptions at other power stations are not uncommon, and one such event has been recorded on average every two years within the Southern African Power Pool (SAPP). For example, on 6 September 2012, an event occurred where 125 MW was lost from the SAPP IPS at Kariba Power Station due to a disturbance caused by a trip of a Kendal unit that removed 640 MW from the IPS just prior. The effect on the frequency of the IPS can be seen in the following recording captured at the time of the event.

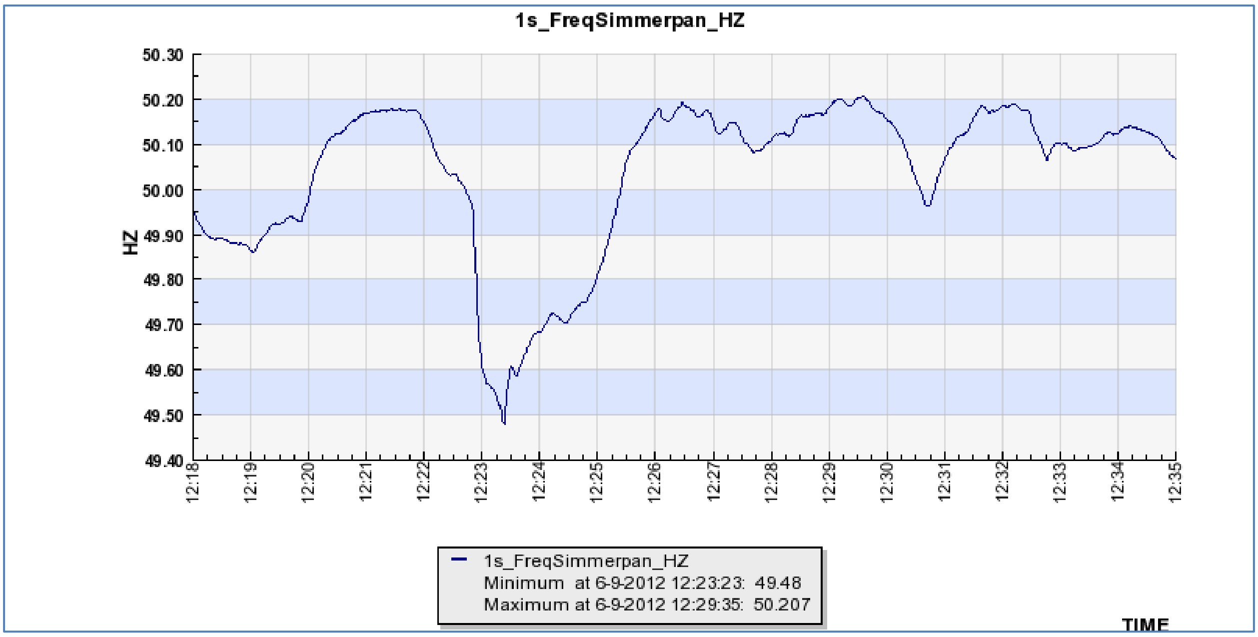


Figure 100: System frequency during the Kendal-Kariba trip of 2012-09-06

Although the sympathetic trip of the Kariba unit, as a consequence of the trip at Kendal, can be traced back to a malfunction in equipment installed at Kariba, this is invariably the *de facto* state of affairs during such events (refer to section 5.6.14).

In the other class of event, where a disturbance within the power system itself, and not at another power station, triggers an event where more than one power station suffers disruption, various examples exist that were recorded within the SAPP. An example of this class of event occurred on 10 January 2011, when a fault in a transmission substation caused two units at Majuba Power Station to disconnect from the IPS and another two units at Drakensberg Power Station shortly thereafter. Once again, the system frequency suffered a severe decline, which is evident from the following recording.

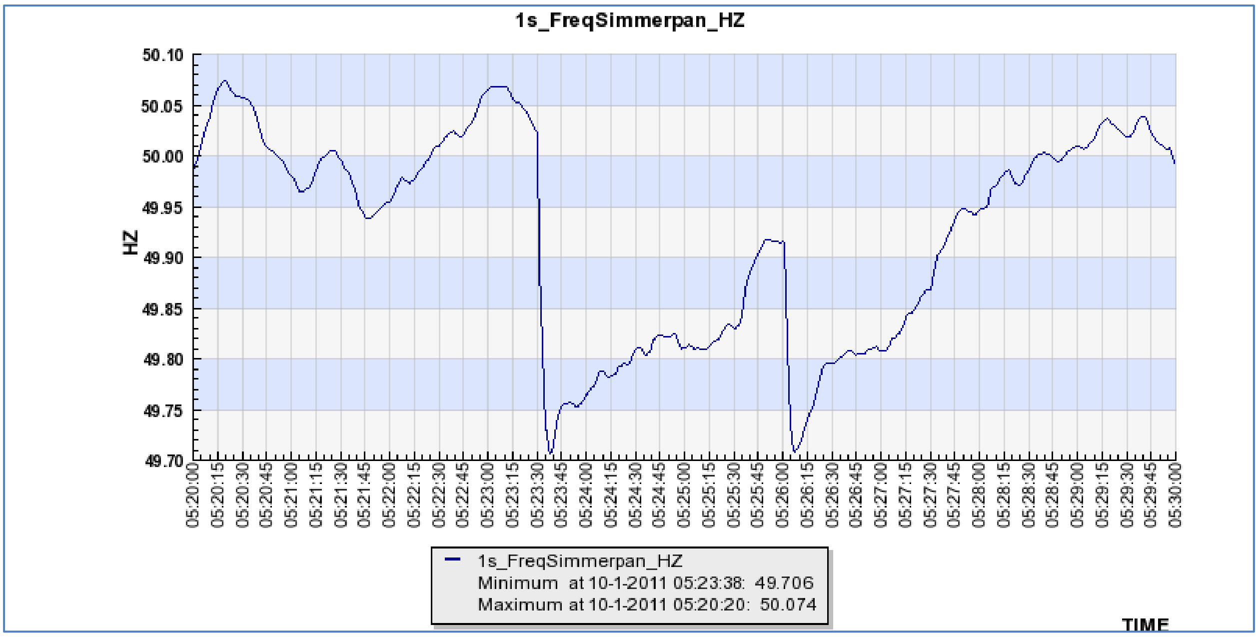


Figure 101: System frequency during the four-unit Majuba-Drakensberg trip of 2011-01-10

During this event, no malfunction occurred at either of the two power stations involved, but the event within the IPS itself caused the disconnection at Majuba, followed by the exceedance of certain parameters at Drakensberg that tripped to protect the generating units.

In these examples above, the IPS transmits the disruption between power stations, a mechanism that merits further analysis but is beyond the scope of this study.

5.7.2 IPS Power Deficit

The preceding section discussed the reality of disruptions being transmitted across an interconnected power system. However, the examples show that disturbances are transmitted electrically, usually by a specific electrical property (or parameter), such as voltage, frequency, etc.

However, an interconnected power system is ultimately used as a medium over which electric energy is made available from producers to consumers. In this role of a power system, a central coordinating function in the form of a System Operator performs the task of balancing the supply and demand within the power system. When a shortfall in the electrical commodity occurs, the System Operator dispatches additional supply to correct for the deficit.

But in cases where a total system deficit exists while all available production resources have been consumed, no other option exists but to interrupt or reduce consumption to restore the balance between an overall deficient supply and a subset of the total demand, to the extent that the supply can balance the demand.

However, during events where the total of all available sources is insufficient to satisfy the demand, other factors come into play that are beyond the normal intent of the power system as a national or regional resource. Such factors include political, socio-political, and strategic.

To illustrate this phenomenon, refer again to cases presented in section 5.6.4. The event that occurred on 1 November 2014 where Majuba Power Station suffered a total station disruption due to a single point of failure event when a central coal silo collapsed, thus interrupting the coal supply to all six units at Majuba.

This Majuba event caused a general electricity shortfall following the failure while measures were implemented to resume normal operation. During this time, electricity production at the remainder of the coal power stations within the South African fleet was being prioritised to minimise the adverse effect of the Majuba failure and the resulting unplanned multiple contingencies that disrupted all six of its generating units.

With the elevated strain from this approach to operate the rest of the coal fleet beyond its normal loading envelope, other power stations began to experience the adverse effects stemming from overutilisation. During this time, Lethabo was operating all six of its units and was subsequently required to operate at higher levels of power production – much of the time at emergency generating levels (exceeding the maximum continuous rating of the units). This continuous operation at very high output levels exposed a functional plant area at Lethabo that is marginal in design (even though it is fully redundant), namely the ash removal system. The overutilisation of the ash removal system gradually eroded all internal buffers for backlogging ash pending evacuation. Eventually, with no more ash-holding capability and insufficient means of evacuation, the system could no longer fulfil its function, which caused a subsequent six-unit disruption, directly resulting from the Majuba failure that forced the need for overuse in the first place.

Therefore, the disruption event needs to be considered in the wider context of an inter-station escalation event. Considered in the context of an inter-station escalation event, the combined event caused a total energy forfeiture of 2,1 TW·h, with an average daily impact of 21 GW·h/day until both stations could resume normal operation.

In this specific example, the Majuba central coal silo represented a single point of failure that, upon its collapse, disrupted 12 large generating units (all with capacities exceeding 600 MW) within the SAPP. Furthermore, the means through which the disruption was transmitted from Majuba to Lethabo was through the consequential energy deficit created within the IPS when the primary energy input to Majuba was compromised.

This call of inter-station escalation is distinctly different from the previous category discussed in section 5.7.1. since the two power stations in this example would hardly be considered to share an electrical interdependence, seeing that the two power stations feed electric power into the IPS in two different networks. Majuba supplies power at 400 kV while Lethabo forms part of the older 275 kV network, and the effects of electrical faults experienced in one of these voltage networks normally have a minimal effect on the other. The commonality here is the total power demand on the IPS.

5.7.3 Fuel Supply to Power Stations

Fuel remains a predominant source of primary energy converted in power stations through combustion processes and dominates the South African power generation scene. In addition to fuel used for combustion, “nuclear fuel”, albeit not used in a combustion process, is nonetheless seen in the same light as bio-fuels (fossil or cultivated) or waste dependant fuels, in the sense that the availability thereof is vital to the process of generating electricity.

A disruption in fuel availability will ultimately impact the continued generation of electricity, but what is less obvious are the factors concerning commonality. Although the sources that fuel power stations are normally different, they do often share certain commonalities. For example, several different mines in a given region operated by different companies may still draw on a workforce that shares a common affiliation and may, in solidarity, embark on collective industrial action. This phenomenon has occurred several times in South Africa, the latest being in 2015 and again in 2018. Such collective strike action from mine workers places the long-term continuation of power generation at risk.

Another commonality is that of regional weather events. In South Africa, many coal mines exist in the Mpumalanga province, most of them open-cast operations. When widespread and persistent rain occurs, the moisture in the coal at the power stations exceeds standards, causing handling and combustion problems. These problems lead to concurrent load losses on various units in the fleet, some of which are forced to disconnect entirely. Once again, the cumulative losses may exceed the reserves on the power system, resulting in customer interruptions.

In Eastern Europe, Russia (the Russian Federation) stopped providing liquid and gas fuel to certain countries in the winter of 2014, resulting in power stations being unable to meet the electricity demand. In this case, international politics was the reason for the disruption due to fuel. Although some interconnections to other countries did exist, many people were still left without power (and fuel). Similarly, in 2023, Russia interrupted liquid fuel supplies to Europe due to the anti-Russian diplomatic actions taken by NATO and European countries, with electricity prices becoming elevated due to supply shortages and rises in demand during the winter. This resulted in previously mothballed coal-fired power stations being returned to service, causing increased coal imports into Europe from countries such as South Africa [177].

5.7.4 Water Availability

In hydroelectric power stations, water is used as the energy source instead of fuel. These facilities are normally constructed within major waterways that provide assurance regarding the continued supply of electricity. However, despite this planning safeguard, droughts that exceed hydrographic data records pose a risk of disruption to a power system, especially when the power supply is not diversified and depends largely on hydroelectric power within an entire region.

During a severe drought in 2015, Brazil was forced to institute power rationing when water reservoirs could no longer sustain power generation. São Paulo and Rio de Janeiro, both of which rank among the largest cities on the planet, were affected. The electricity demand was also unusually high due to air conditioning during exceptionally high summer temperatures. An estimated 3,9 million people were affected during this event [178].

Similarly, Malawi was forced to limit power generation in 2017 due to a severe drought in the region, where hydroelectric power generation constituted 98% of the country's power generation capacity [179].

In 2019, Zimbabwe implemented reduced power generation when water availability dwindled. The water constraint resulted from the lowest rainfall in 40 years [180].

In all three of the above-mentioned examples, hydroelectric power generation was the predominant source of electricity and all three regions had a very limited degree of diversified electrical energy sources.

However, water is also significant in power generation based on combustion processes, predominantly for cooling and as the fluid employed to transfer the energy from the combustion process to the turbines, where steam turbines are used. Although the quantities of water required are orders of magnitude smaller than in the case of hydroelectric power generation, the quantities are still significant and widespread droughts could adversely affect the sustainability of power generation.

Similarly to power generation systems with many interdependencies is the water supply system of a country. In Figure 102, a representation is given of one of the national water supply systems of South Africa as it pertains to power generation that makes use of the specific system.

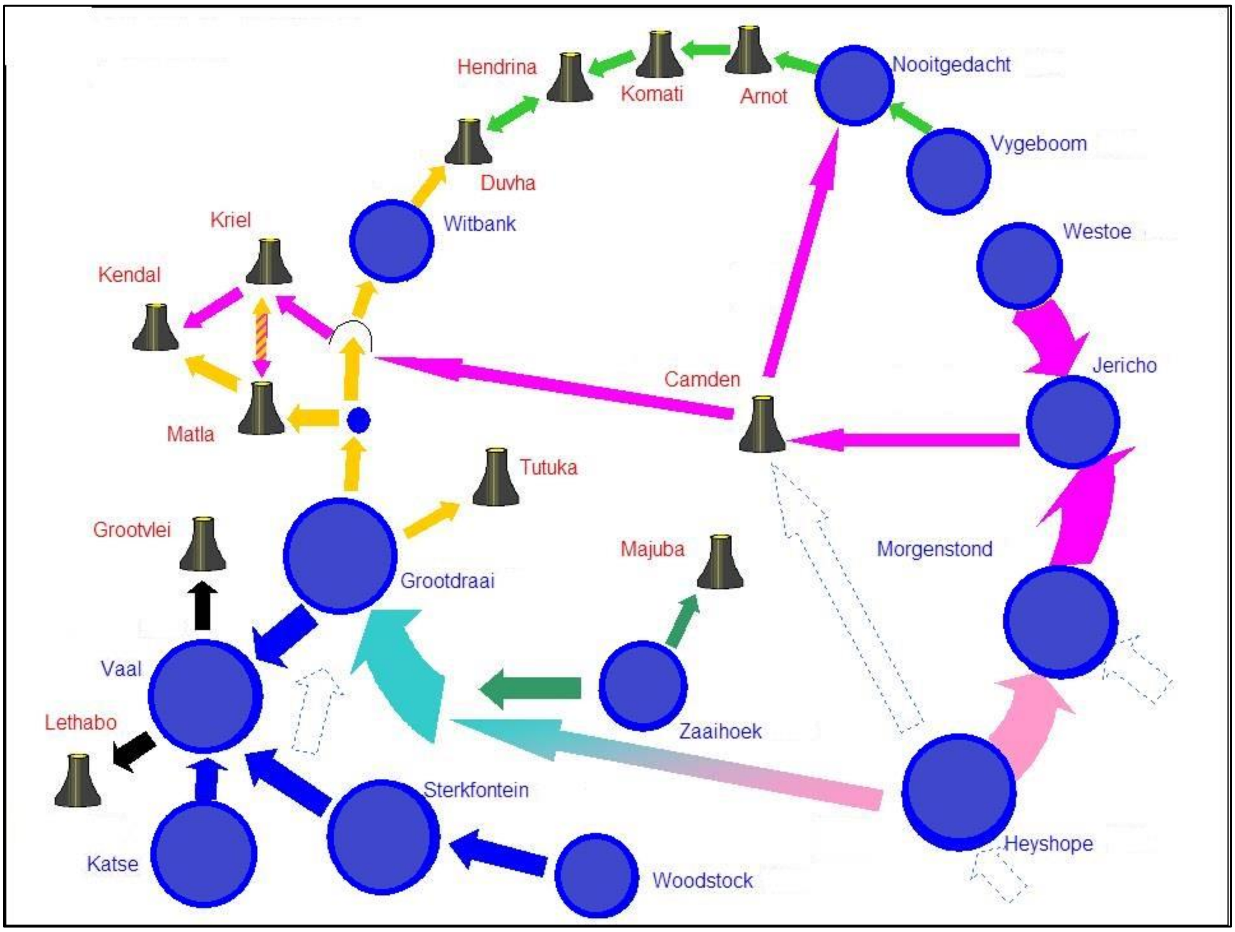


Figure 102: Interdependencies of water resources to power stations in South Africa

In Figure 102, the arrows represent the various possible flow paths that could be used to direct the water supply. The arrows with dashed lines represent planned enhancements to the water supply system to ensure water security into the future.

Although the present system has never yet (in modern times) failed to provide an adequate water supply to the power stations, it is conceivable (even probable) that a widespread and long-lasting regional drought would adversely impact the security of electricity supply in Southern Africa.

To reduce the dependency on water, modern coal-fired power stations use so-called dry-cooling, where the evaporative water loss is significantly reduced through the facility's design. However, such plants remain dependent on relatively large water quantities – albeit far less than wet cooling plants. And whilst such a design feature seems an obvious choice, it comes at a significant long-term cost of elevated, lifelong parasitic power consumption by the facility for own use and a reduced condenser vacuum that has an adverse impact on the overall cycle efficiency of the power generation process. It is by no means a foregone technical conclusion that the benefits of dry cooling outweigh its disadvantages, not even from a perspective of susceptibility to disruptions affecting multiple units (refer to section 5.6.7.2.1 and section 5.6.7.2.2, respectively).

5.7.5 Fleet Operators

Part of the legacy of the utility approach to the supply of electricity is the existence and prevalence of owners and operators of large fleets of power stations. Although such a fleet ownership approach has many benefits, it also presents a host of risks that could threaten the sustainability or reliability of the electricity supply.

As an example, consider the fleet management approach of standardisation, a practice that is invariably followed by fleet operators. Although such an approach yields many benefits from the point of view of the economy of scales, it also introduces certain risks. If, for example, a philosophy contains an inherent yet unintentional and unknown flaw, the flaw would permeate the entire fleet and subvert the fleet as a collective and possibly the power system wherein it operates.

This argument may seem aloof and hypothetical, but there are several cases where this exact mechanism has proven very real, manifesting tangibly in adverse effects where such fleets are operated within power systems.

Consider the following scenario as a case study. It is the early eighties in South Africa, and due to high growth in the electricity sector, the local utility (Eskom) is developing its fifth-generation power station fleet during an accelerated construction program. Within a period of just more than a decade, units from seven of its new fifth-generation power stations go into operation, all with capacities exceeding 600 MW. All the equipment installed under this construction program is approximately the same age.

Specifically, the fleet featured 42 generator transformers installed at the seven power stations, all with the same age profile. The standard practice of the utility at the time was to have a single spare generator transformer at each power station, one spare for every six transformers (on average). Although the utility ran an extensive and sophisticated condition monitoring program, after 20 years of service, the wave of end-of-life failures overwhelmed the utility's ability to curb the tsunami of failures. Units were either forced out of service due to failure or were handicapped, with pre-emptive load losses being imposed to retard the rate of deterioration of the transformers to manage the availability of operable units.

Figure 103 shows the production losses suffered by the utility's fleet, specifically from transformers, from 1996 to 2020.

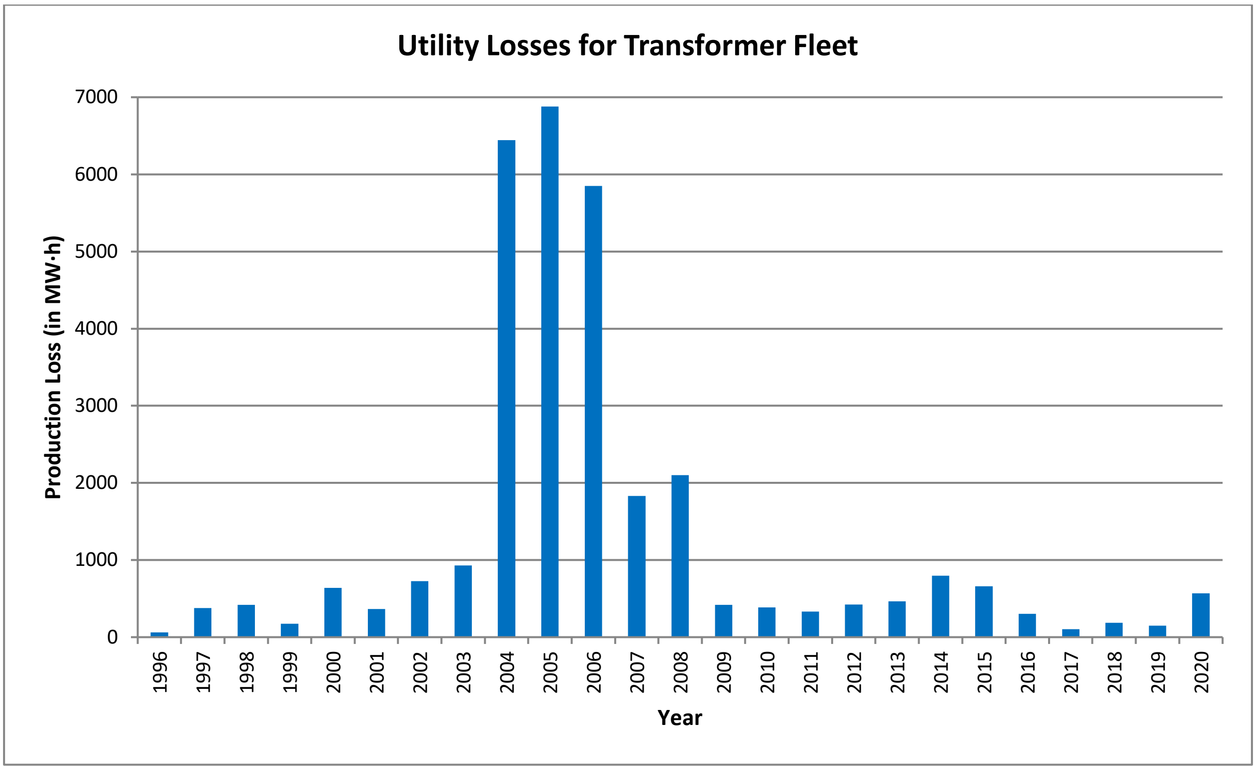


Figure 103: Generator transformer losses in the Eskom generation fleet in a 25-year window

In the above example, it took the utility five years to recover from the oversight, an extensive period to suffer the ill effects of any disruption. The problem was exacerbated by the fact that such large transformers have long procurement lead times, and due to the inability to manufacture transformers of the required size within South Africa, all transformers purchased had to be imported and slowly hauled over vast distances by road trains.

Although the example above provides a graphic representation of fleet ownership risk, various other examples exist. Consider, for example, the potential threats implied within the following:

- Protection or dynamic control system settings dispersed throughout an entire fleet of facilities (refer to section 5.6.14).
- A fleet owner facing financial constraints necessitating a restriction in fleet wide maintenance or resourcing.
- State ownership or control over fleet operators (typically former utilities) mandating practices that undermine sound and effective industry or business principles. This risk becomes ever more threatening when the possibility of state capture is considered.
- A fleet owner limits the number (or diversity) of manufacturers providing production equipment or the number of contractors providing goods or services.

The above list is certainly not comprehensive but illustrates some of the various ways in which fleet ownership can compromise power system operations.

One other point to consider becomes particularly relevant in the context of section 5.6.19, regarding the effects of ageing and eventual derating of a power station. As demonstrated in section 5.6.19 for a typical power station example, a station can undergo a dramatic derating in capacity within a relatively short period of time (ten years in the example provided). If such a phenomenon of derating becomes applicable to a fleet owner who operates a large number of power stations of similar age, such a derating could pose a very real threat to a power system as a whole. This situation currently (2024) prevails within Southern Africa and could have dramatic consequences in terms of the security of supply in years to come. And, of course, the problem should not merely be considered in terms of derating but extrapolated to the point of decommissioning an entire fleet of power stations.

5.7.6 Geographic Commonalities

Power stations that are close to one another could readily be affected by events occurring at or near their location. It could be as simple as local unrest preventing workers of the power generation facilities from reporting for work.

But, although power stations could be located remotely from one another, they could still share a common geographic feature that could threaten them collectively despite their significant geographic separation. An example of such a common feature is that of a shared coastline.

On 11 March 2011, the Tōhoku earthquake off the coast of Japan caused a tsunami to impact the coastline at a height of 10 meters when it reached landfall. The event disrupted operations at the following power stations, all located on Japan's eastern coastline [181].

- Fukushima Daiichi Nuclear Power Station – 3 units (the other 3 were being refuelled)
- Fukushima Daini Nuclear Power Station – 4 units (entire installed base)
- Onagawa Nuclear Power Station – 3 units (entire installed base)
- Tōkai Nuclear Power Station – 1 unit (the other unit was not in service)

Figure 104: Map of Japanese nuclear power stations and the Tōhoku earthquake [181]

None of the nuclear units in the vicinity of the event that were in service at the time survived – all were automatically shut down. This loss of generated power and the associated destruction of network infrastructure resulted in the unavailability of electricity to customers for several days.

This example demonstrates a problem inherent to nuclear power stations, namely that due to the emphasis placed on its cooling, the vast majority of nuclear facilities internationally are located on the coast. Although it addresses the problem of cooling water availability, it presents the risk of being overwhelmed by a combined onslaught of earthquake and tsunami events.

However, geographic commonalities are not unique to coastal effects illustrated in the example above. Consider Figure 105, which shows a map of South Africa with the bulk electricity power stations indicated thereon.

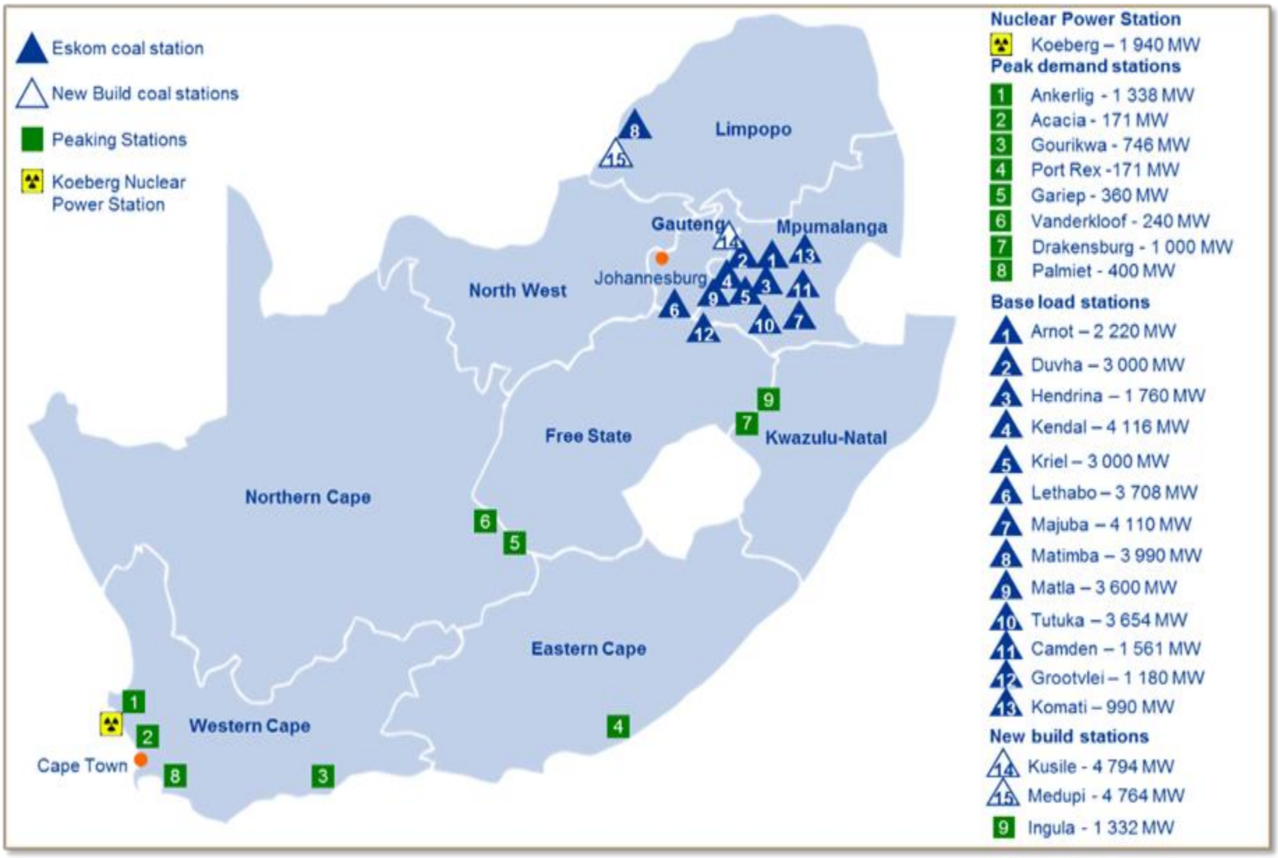


Figure 105: Map of locations of South African power stations [3]

The high degree of clustering of coal-fired power stations in South Africa is obvious and stems directly from the availability of coal itself. However, since similar technologies often suffer from similar weaknesses, clustering the bulk of these into the same geographical region would introduce certain risks. The next section will examine one such risk in more detail.

5.7.7 Extreme Weather

Adverse weather is a disruption factor that may be limited to single power stations (see section 5.6.20) or it could be so extensive that it could affect vast regions or even multiple independent power systems.

It is rather intuitive to expect that weather can disrupt electricity production. After all, the ambient conditions under which a system should function are a basic assumption that underlies the design of any plant. Therefore, when conditions exceed the design assumptions, failure, malfunction, or a reduction in efficiency could readily be expected, typical triggers for a disruption.

One of the most obvious areas of power generation that would be prone to weather-related disruption is renewable energy facilities. The vast majority of renewable energy sources currently being employed internationally either directly extract energy from weather elements (such as wind) or are entirely dependent on the weather for energy extraction (such as solar).

Take, for example, a condition where a widespread weather pattern occurs over a vast region, e.g., widespread stormy conditions. All solar plants would suffer from a lack of solar energy that fails to penetrate through the cloud cover, and wind turbines would need to shut down under high wind conditions to protect the plant. In such an example, the weather triggered a multiple-generation disruption event and could even be considered a single point of failure…

Renewables are not the only technology with weather-related vulnerabilities. Weather is often a factor in safely operating power systems in general, and many examples exist where extreme weather causes failures or tripping within substations. However, extreme weather affects power stations equally, which could disrupt entire power stations or multiple power stations sharing a geographic region where the weather is being experienced.

In the USA, nuclear power stations often shut down all units during hurricane-class storms. In September 2017, three nuclear power station units were shut down when Hurricane Irma made landfall in Florida, while 12 units were being planned for shutdown in September 2018 on the coast of South and North Carolina in anticipation of Hurricane Florence. These measures are not uncommon for nuclear power stations and are part of the international requirements for the operation of nuclear power stations. The advantage in these cases is the foreseeable nature of the events and the proactive measures that could be taken in anticipation [182].

The risk posed by adverse weather conditions cannot always be handled proactively, as demonstrated in the examples above. Often, circumstances arise that cause a power system to become compromised during a storm or blizzard. An example of such an event occurred in Brazil on 11 November 2009, when a severe lightning storm (through a combination of lightning, heavy rain and gale force winds) compromised three power lines, causing all the units at Itaipu Power Station to trip, 17 GW was removed from the Brazilian power system that left cities like São Paulo and Rio de Janeiro without electricity. 18 of the 26 states were blacked out, and 50 million people were affected by the event [183].

Adverse weather also disrupts power generation in South Africa. Although normal rainfall is regarded as a normal weather phenomenon that should not have significant detrimental effects on power stations, it does pose a disruption risk when the quantum of rain significantly exceeds typical precipitation patterns. During October and November 2019, the north of South Africa was exposed to unusual rain – more than half of the annual average was received within just 10 days. Due to the high degree of clustering of power stations within a relatively small region of the country (see Figure 105), many power stations were exposed to the same rainfall.

During this time, South Africa's generation fleet suffered major disruption, and the collective loss in generation capacity peaked at 5,2 GW (about 30% of the total power served through the power system). Rotational load shedding had to be instituted to manage the power system, resulting in about 400 GW·h of unserved energy [184].

The following graph shows the correlation between the cumulative rainfall and the cumulative loss in generation capacity.

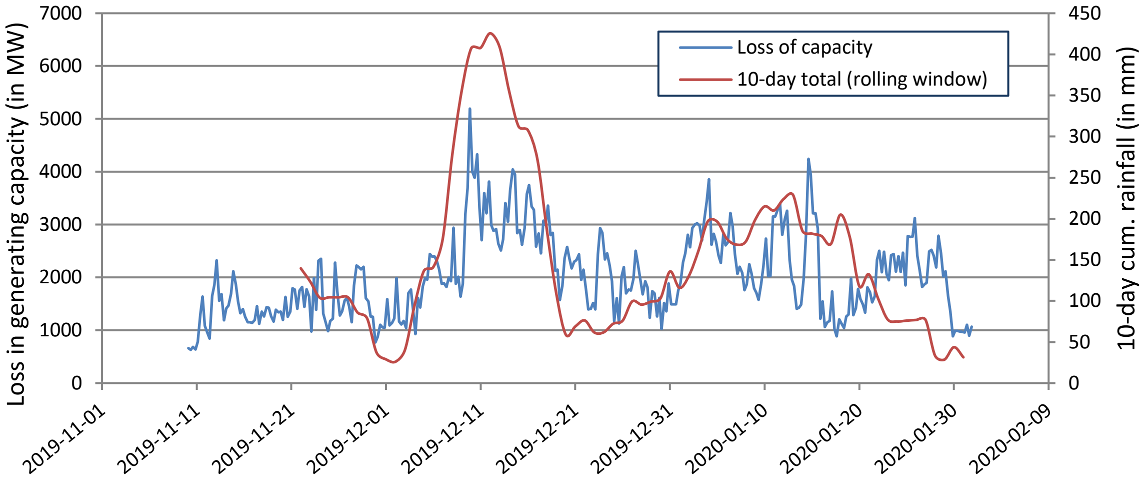


Figure 106: Correlation between the fleet disruption in generation capacity and rainfall [184]

The South African rainfall event of 2019 was not under storm conditions, merely perpetual and prolonged exposure to normal rainfall levels. Yet, this prolonged exposure culminated in the disruption of the power system, a duplicitous aspect of weather as a natural phenomenon.

5.7.8 Solar Output

The risk of a solar eclipse does not seem great at first glance. Still, with the increase in solar generation, an eclipse would directly impact the capacity of all power parks within the area affected.

During the solar eclipse of 2015, 80% of the sunlight was lost over Germany, with 40% of the inland generation provided by solar power [185].

In 2017, the USA was directly affected by a total eclipse. Renewable penetration was already vast, with 45 GW of installed solar generation capacity alone. With the rotational nature of the earth, sun and moon, the eclipse followed an east-west path over the continent and directly affected 14 states, affecting 1 900 power parks during the transit.

In the case of a solar eclipse, the disruption can largely be predicted, and mitigation plans can be implemented. During the 2017 eclipse, generation at solar plants was reduced in anticipation of the darkening, and the shortfall was largely replaced by more expensive generation in the form of gas-fired power stations [185].

Although eclipses are rare, they will remain a planning criterion for the future as renewable volumes continue to increase.

Cloud cover, fog, and smoke are far more common (and obvious) factors that impact solar output on the planetary surface. These factors are daily occurrences and also significantly impact solar power generation. As with rain (see section 5.7.7), power generation facilities within the same general geographic area are likely to suffer the same deleterious erosion in generation capacity simultaneously, impacting the power system.

5.7.9 External Fire

Vegetation fires are well-known disruptors of power systems. Normally, they affect networks (transmission or distribution) rather than power stations by causing power lines to trip in response to faults that develop due to the fire. However, in many cases, fires directly impact power stations, either directly or indirectly.

Vegetation fires are often naturally occurring phenomena (like veld or forest fires) or are deliberately attributed to human endeavour (like sugar cane fires as an agricultural practice). Although transmission redundancy practices (such as the (n-1)-criterion) often require duplicate power lines, power lines often share the same geographical power corridor due to servitude and cost considerations. Fires often compromise entire power corridors rather than individual power lines.

An example of vegetation fires causing an indirect multiple disruption event occurred in the morning of 19 February 2006, when heavy fog occurred in the Western Cape of South Africa. In the months before the event, there was an abundance of veld fires in the general area, causing much pollution of the insulators and bushings of transformers, power lines, HV circuit breakers and instrument transformers in HV substations. When condensation of the fog occurred on the surfaces of the insulator materials (mainly glass and ceramics at the time) in the presence of the surface pollutants, the insulation integrity was breached in various locations and over several hours, 196 HV circuit breaker operations occurred, tripping one nuclear unit at Koeberg Power Station and three gas-powered units at Acacia Power Station. The second Koeberg unit was on outage at the time, preventing it from participating in the multiple unit disruption event that would otherwise have aggravated the event considerably.

There are abundant examples of fires directly causing the tripping of power lines and the consequential loss of generating units, which will not be discussed in detail in specific case studies.

5.7.10 Extra-planetary Disruptors

The earth can hardly be considered to be a closed system. Many electric and electromagnetic phenomena are known to have their origin in space, and it can logically be deduced that such phenomena could conceivably cause disruption on Earth if sufficiently intense.

One such phenomenon is the solar wind, a stream of charged particles that flow outward from the sun into the greater solar system. The solar wind is an ongoing natural process that varies in intensity with the solar cycle. When solar surface activity is at its greatest, ejection events become more frequent and energetic, leading to a greater likelihood that such an ejection event could be directed towards the Earth.

Earth is somewhat shielded from such particles by the magnetosphere. When particles stream towards the earth, the earth's magnetic field causes the particles to enter the atmosphere at the poles. The influx of charged particles then manifests as a DC electric current that couples with the unshielded conductors comprising the power systems, typically in long-distance overhead power lines. Due to the DC nature of the phenomenon, it appears as a DC offset that causes the cyclic (normally sinusoidal) magnetisation of the magnetic cores of power transformers to cycle asymmetrically and could cause core saturation depending on the extent of the DC offset and the safety factor used in the design of the core material of the transformer.

If saturation does occur, the power frequency voltages and currents become distorted, causing protection systems to activate, either in direct response or indirectly, due to secondary effects resulting from distorted quantities.

The worst disruption of this nature, the *Quebec Storm*, occurred on 13 March 1989, when the entire Quebec power system blacked out from a power level of 21 350 MW at about 02:45. This event was caused by a massive coronal mass ejection (CME) that occurred on 10 March 1989. The specific CME event was estimated at one milliard (10^9) ton of charged particles that happened to be directed at the position where the earth was within the solar system at the time and travelling at a speed of about 1 500 000 $\text{km}\cdot\text{h}^{-1}$. The storm also caused power system disruption in the United States, with 200 related power system problems being reported and two power loss events of 150 MW and 1 410 MW, respectively, occurring at different locations. However, the power loss events did not cascade into blackout events due to the power system carrying sufficient reserves at the time [186].

However, although the *Quebec Storm* is known as the most significant event relating to power system disruption, it is certainly not the only event that disrupts power systems. The first to have been recorded to cause power system disruption is known as the *Carrington Event*. It was a particularly severe solar storm consisting of two significant CME events between 28 August 1859 and 1 September 1859. Also, it caused widespread disruption of electrical systems like telecommunication installations, although electricity was not yet the predominant form of industrial or domestic energy. The Carrington Event was believed to be the most severe solar storm on record, with strength values estimated between -800 nT to -1 750 nT [187].

On 23 July 2012, a CME event of a similar extent as the *Carrington Event* occurred but missed the earth by a mere nine days in terms of its angle relative to the earth's position at the time. Between 29 and 31 October 2003, the so-called *Halloween Storms* occurred, which caused minor power system outages. One blackout in Sweden affected 50,000 people and lasted just one hour [187].

Although South Africa did not experience any power system disruptions during the Halloween Storms, 12 major transformers of the Eskom Generation fleet were damaged, causing premature failure or pre-emptive removal from service [188].

Another interesting, yet unofficial, event occurred in the last decade of the twentieth century. In the early hours of the morning, the US president was allegedly woken up when it was falsely believed that a nuclear attack had occurred in US territory. There was a loud explosion, a bright flash and a total power blackout, all consistent with a nuclear explosion. It later transpired that a meteor exploded in the atmosphere and that the bright flash caused all the lighting in the town, operated by light-sensitive switches, to turn off. The moment the flash dissipated, all the lights simultaneously turned on, causing the local reticulation system of the town to overload and trip. This does not happen normally because the light switches do not activate at the same light level when night falls.

These events illustrate that the earth cannot and should not be considered isolated from the space environment and that events from local space could seriously disrupt power systems on a local or wide scale.

5.7.11 System Operations

An inherent feature of power systems is a *system operator* function. Such a function is needed to monitor the status of the power system, manage and control its configuration and coordinate the activities of the participants who are utilising the power system. It is, therefore, equipped with a vast and extensive information and control system spanning the entire power system. The existence of a control function that encompasses an entire power system presents a risk in itself. Such a control function could fall prey to malevolent use (e.g. cyber-attack), failure, malfunction or human error. Due to these obvious risks, special measures are taken to mitigate them.

Despite deliberate countermeasures, isolated examples exist which affect the power system in a detrimental way. One such event occurred on 22 April 2024 at about 03:30 in the morning in the South Africa power system.

It is common practice to exploit the low night-time minimum demand for electric power and pump water at the hydro pump-storage facilities to recharge the top reservoirs for utilisation during peak demand. Through instruction, the system operation function controls the pump-storage facilities to start or stop pumping. On the morning of the event, eight pump-storage units were in pumping operation at three power stations, i.e. Drakensberg, Palmiet and Ingula.

With the approaching morning peak, it was necessary to withdraw pump-storage units from pumping duty, release power consumption, used for pumping, for system-wide consumption and make the withdrawn units available for active generation when needed. Five of the units were instructed to shut down from pumping duty, but erroneously within too short a time window of only three minutes. Due to the rapid reduction in consumed power (totalling about 1 200 MW) on the power system that resulted from the collective shutting down of the five pump-storage units, the system frequency dramatically increased on the power system.

This exceptional event represents an example of a multiple contingency event resulting in an overfrequency rather than an underfrequency on the power system, and the frequency effect is shown in the following recording.

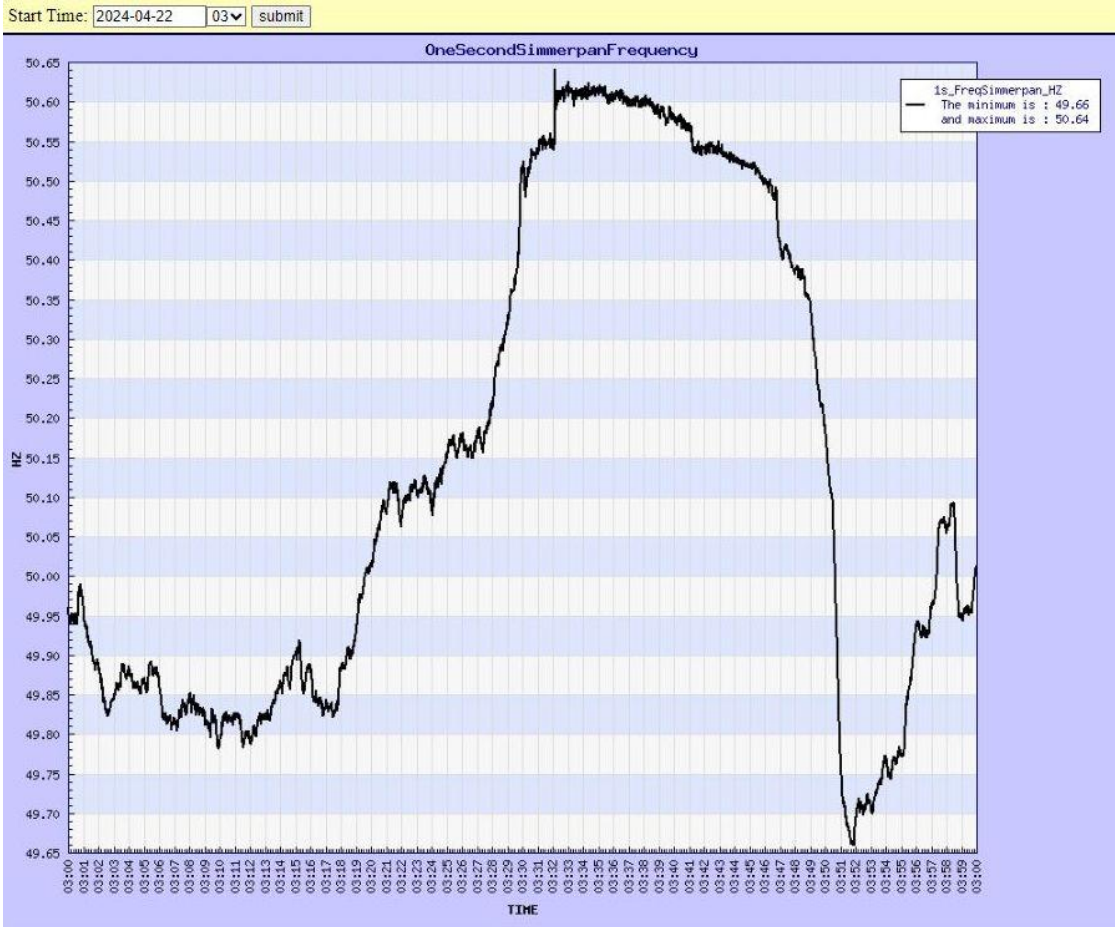


Figure 107: System frequency increase due to collective shutdown of five pump-storage units

Shutting down pump-storage units from pumping duty is a standard procedure, and the effect is readily corrected through the governing action of the generation fleet that is in service at the time. However, the ability to correct frequency through governing is limited. Still, pre-configured ramp curves within the unit control systems and the available ranges of the generating units affect the requisite correction. When individual pump-storage units are shut down, the power release is manageable for the generation fleet to correct readily, but the combined effect of five (nearly simultaneous) pump-storage units shutting down overwhelmed the ability of the generation fleet to rapidly correct for the frequency deviation caused by the abrupt surplus of power in the power system. Many units in the generating fleet were already operating at their minimum stable operating points and could not assist in the frequency correction.

Realising the effect of the five units' collective shutdown, the same pump-storage units were called back to immediately resume pumping duty once more, staggering their withdrawal from pumping duty over a more protracted period.

5.8 Disruptors

The study into cascade disruption events constantly unveils new disruptors. In the following sections, a set of disruptors is tabulated to guide an analysis and classification of events.

5.8.1 Nature

Natural attributes and events are a class of potential disruptors that affect all electricity generation technologies.

TABLE XV: NATURAL DISRUPTORS – MULTIPLE DISRUPTION EVENTS

Climatic	Temperature	High Low
	Wind	High Low
	Storms	Thunder storms Blizzards Tempests Cyclonic storms
	Precipitation	Rain (see section 5.7.7) Snow Hail and sleet
	Fog	
	Lightning	(see section 5.6.10.1)
	Solar limitation	Cloud cover Smoke Ash and soot Dust
	Drought	(see section 5.7.4)
	Pattern shifts	Wind Oceanic currents Rainfall
	Climate change	Human-induced Naturally occurring
	Paleo phenomena	Ice age Thousand-year extremes
Geographic	Waves	Tidal waves Tsunamis (see section 5.7.8)

	Flooding	
	Earthquakes	(see section 5.7.8)
	Avalanche	Snow Mudslides
	Ground movement	Subsidence Heaving
	Volcanic activity	
	Location	Proximity Commonality (e.g. coastline)
	Earth magnetic field	Variations Swapping
Fauna and Flora	Vegetation	Trees Creepers Endangered species
	Fires (see section 5.7.9)	Veld Bush Forest
	Animals	Marine (see section 5.6.7.1.2) Insects Birds and bats Reptiles Mammals Burden bearing Migration patterns
Extra-Terrestrial	Solar activity	Solar output (see section 5.7.8) Coronal mass ejection (see section 5.7.10)
	Meteors and asteroids	Impact Atmospheric explosion
	Space debris	
	Tidal phenomena	
	Seasonal variation	

5.8.2 Power System

The power system is a *de facto* commonality linking all generation facilities and a universal potential disruptor.

TABLE XVI: POWER SYSTEM-RELATED DISRUPTORS – MULTIPLE DISRUPTION EVENTS

Envelope exceedance	Voltage	High and low
	Frequency	High and low
	Quality of supply	Harmonics Power factor Phase balance
	DC offset	
	Fault level	High and low
Dynamic behaviour	Transient and sub-transient	
	Resonance	
	Oscillation and damping	
	Moment of inertia	
	Surging	
Foresight and planning	Dispatchable capacity	Conventional generation Reserve margin
	Redundancy	
	Technology mix (diversity)	
Failure and malfunction	Fire	Transformer Reactor
	Equipment	Transformer Reactor Phase shifter Feeder breaker Bus-coupler Bus-section Busbar VT or CT Isolator Capacitor bank SVC
Error and violation	Earthing	
	Work permits	

	Switching and linking	
Secondary plant	Over-tripping	
	Grading and discrimination	
	Slow clearance	
	Device compromise	Failure Malfunction
	Settings	Incorrect Not set
	Deficient design	
	Power supplies	
Lines	Sharing corridors	
	Bird proofing	
	Lightning shielding	
	Servitude integrity	
	Conductor failure	
	Pylons and structures	
	Earthing	
	Travelling waves	
Ancillary services	Voltage control	
	Frequency control	Primary Secondary
	Reserves	Generation based Customer based
System protection schemes	Out-of-step	
	Frequency	Under-frequency Over-frequency
	Transient stability	
	Voltage	
Generation collective	Fleet power flexibility	Collective floor Collective ceiling
	Fleet resilience	
	Fleet moment of inertia	
	Islanding units	
	Black-start capabilities	
	Dynamic stabilisers	

	Fault current sources	
Control centre	Skilled staff and training	
	Simulators and models	
	Overall visibility	
	Automation sufficiency	
	Backup and redundancy	
	Hierarchical delegation	
	Effective forecasting	

5.8.3 Societal

Another universal potential disruptor is the dependence upon human beings for participation in electricity generation and many disruption events originate due to this commonality.

TABLE XVII: SOCIETAL DISRUPTORS – MULTIPLE DISRUPTION EVENTS

Political	Embargos and isolation	
	Restrictive legislation	
	Tax levies	
	Strategic interdependencies	
	Equity mandates	
Malevolence	Warfare	
	Sabotage	
	Riots, strikes and intimidation	
	Theft	Infrastructure Electricity
	State capture	
	Organised crime	
	Corruption	
	Cyber-crime / attack	
Customer mobilisation	Clean energy	Pro-green Anti-conventional
	Activist behaviour	“Justified” disruption
	Irrational behaviour	Doomsday actions
	Independence	“Off the grid”

Economic	Poverty	
	Depressions and recessions	
	Inflation	

5.8.4 Operational – Generating Facility

The most vulnerable aspect of electricity generation is the power stations themselves. Such vulnerabilities require constant focus and management effort.

TABLE XVIII: POWER STATION DISRUPTORS – MULTIPLE DISRUPTION EVENTS

Systems	System compromise	Non-redundant design Prior redundancy lost Deficient design
Primary plant	Failure	Normal operational Catastrophic events
Plant configuration	Deviation from design	Non-standard (non-default) Reduced redundancy
	Design deficiency	
Plant status	Obsolescence	
	Ageing	
	Disrepair	
	Dilapidation	
Human factors	Errors and violations	
	Skill erosion	
	Management and oversight	
Support functions	OEM	
	Maintenance facilities	
	Access to market expertise	
Financial model	Cash flow	
	Funding model	Cost recovery and profit Pass through costs Feed-in tariffs
	Corruption and syndicates	Price manipulation Sabotage
	Access to credit	

5.8.5 IPS Participants

A power system is shared between many users (both in production and consumption), and their behaviour, individually and collectively, can potentially disrupt others.

TABLE XIX: IPS DISRUPTORS – MULTIPLE DISRUPTION EVENTS

Co-generators, embedded generators	Tripping	
	Dynamic behaviour	
Synchronous condensers	Tripping	
Large loads	Switching	Connection Disconnection (tripping)
	Usage	Over-use Under-use
	QOS	Harmonics Asymmetry
	Power factor	
Large power stations and units	Faults	Pole slip Switch-onto-standstill Ceiling excitation Out-of-phase connection
	Dynamic behaviour	
	Restrictive (narrow) capability	
	Degree of interdependence	
	Multiple contingencies	
Renewables	Climatic dependency	
	Harmonic pollution	
	Reduced capability	Moment of inertia Fault level contribution
	Rapid power fluctuation	
Domestic collective	Seasonal	Winter Summer
	Short term extremes	Storms Cold fronts
	Social events	*Ad hoc* Periodic (e.g. holidays)
Consumer collective	Pattern of behaviour	Rooftop solar

		Battery storage and recharge Electric vehicle adoption Shift in heating technology
Agricultural collective	Droughts	Collective pumping Water prioritisation
	Energy intensive farming	
Mining collective	Primary energy markets	Demand / price increases Primary energy scarcity
	Sectoral unrest and strikes	
	Essential resource depletion	Helium Rare-earth materials
Industrial collective	Energy-intensive manufacturing	Increase Decrease
	Sectoral economic slow-down	
	Sectoral breaks (holidays)	
	Sectoral unrest and strikes	
International in-feeds	Bulk disconnection	
	Cross border disruption	Technical / operational Social stability

5.8.6 Third-Parties

Other non-participating parties sometimes also impact generating facilities despite not being a high risk.

TABLE XX: THIRD-PARTY DISRUPTORS – MULTIPLE DISRUPTION EVENTS

Agriculture	Servitude impacts	Line damage / contact Crop burning
Road and rail	Deliveries and restock	
	Line clearance violation	
Aerial travel	Embargos	Import / export (markets) Expertise availability Spares and equipment
	Crash	Generating facility Power line or corridor Substation

Military	Strategic asset destruction	
	Employee disruption	
	Economic disruption	

5.8.7 Global

A low-likelihood but high-impact disruption class emerges from the global context – no generation facility can effectively escape global pressures.

TABLE XXI: GLOBAL DISRUPTORS – MULTIPLE DISRUPTION EVENTS

Labour markets	Skills loss and migration	
Technology	New technology direction Declining product life cycles Increased complexity	
OEM mergers	Monopolised supply chains Diminishing support	
Polarised diplomacy		

5.9 Summary

At this point, a solid understanding of the landscape of multiple-generation disruption events and their causes (disruptors) has been established. But despite the requisite context of such events, the capability to analyse, compare, and rank such events still remains elusive.

Therefore, the next section will embark on developing exactly such capabilities.

6. Event Decomposition – Disruption Metrics

Any disruption in the power generation process can potentially perturb the stability of the power system being supplied. However, it is impossible to avoid generation disruptions, and therefore, power systems are designed, maintained, and operated taking this reality into account, i.e., resilience to disruption within a given envelope.

A power system has a limit to which it can tolerate a disruption from a generation perspective. This limit depends on the specifics of the constituent generating units forming part of the power system. Typically, provision is made for a quantity of reserves that is some multiple (or percentage) of the largest connected generating unit. This limit is known as *the largest multiple contingency limit* in the South African context. It requires the power system to be tolerant to disruptions that do not exceed a power generation loss equal to three times the largest generating unit existing at a six-pack power station [1].

However, generating units generally provide various benefits to the power system, not merely electrical or energy. Therefore, a disruption in the generation profile erodes various integrity-related attributes that may adversely affect power system integrity. The most predominant ones will be discussed in the following sections to better understand the various integrity-related attributes that could become eroded during a large-scale disruption in generation.

6.1 Impact – Power as an Assessment Metric

One of the most obvious and direct parameters considered in assessing the impact of a disruption on a power system is the power that was lost. This value is used even by laymen in narrative depictions of disruption events, for example, in the press or general media.

If power is lost abruptly and in sufficient quantity, it has a consequential effect on the system frequency, yet another parameter used in assessing the system's impact, but notably by the more informed audience that is schooled in power system behaviour.

The following sections will explore the role, value, and importance of lost power, considering various perspectives on this specific metric for defining the impact of disruption events on power systems.

6.1.1 Illustrative Case Studies – Methodology Application

As discussed above, an approach to systematically applying real power (MW) during disruption events will be outlined. To illustrate the practical application of each approach, actual disruption events will be applied to each of the incremental development steps that will be introduced. Although many examples can be utilised, three events were selected for demonstration purposes.

a The multiple contingency event disruption event that occurred on 6 June 2014 at Kendal Power Station when the fast transfer scheme for the station boards malfunctioned and tripped the station boards. All four units in operation at the time tripped in rapid succession, signifying a loss of 3 160 MW and a system frequency decline to 49,177 Hz (refer to section 5.6.8).

b The cascade disruption event that occurred at Kriel Power Station on 30 November 2010 when three generating units tripped due to a loss in main CW flow due to the failure of a CT in the HV yard. During this event, a total generating capacity of 1 345 MW was lost over a time window of 13 minutes, and the system frequency declined to 49,69 Hz (refer to section 5.6.7.2.1).

c The multiple contingency disruption event that occurred at Ankerlig Power Station (gas-fired) on 7 April 2013, when a human error occurred on the fuel forwarding system that caused all five generating units to trip. The MUT resulted in a total loss of 710 MW, causing a system frequency minimum of 49,31 Hz (refer to section 5.6.6).

The application of each technique that will be presented in the following sections will be illustrated using the data of these three actual case studies. Note that the case studies were deliberately selected to vary significantly in nature and have vastly dissimilar characteristics, illustrating the potential application potential for a variety of disruption events.

6.1.2 First Order – Magnitude

Any significant disruption in power generation has an adverse impact on the power system. Such an impact may be in the form of the loss of a partial unit, an entire generating unit or a multiple loss in the form of a cascade disruption event. The greater the fraction of the power loss relative to the total power in the power system, the larger the impact.

Since disruption events are often (even mostly) characterised by an abrupt nature stemming from the tripping of generation plants, the loss of power manifests as a corresponding rapid decay in system frequency.

This specific perspective has been explored in the literature survey (section 3.3.1) and is briefly repeated here.

The concept of the *magnitude* (denoted with G) has been introduced as a measure of the *impact* of an event on a power system resulting from a disruption in generation [163]. The *magnitude* was defined as the ratio between the total power being generated into the power system at the time of the event and the power being lost due to the disruption – expressed as a decibel (dB) value. Stated as a formula,

$$G = 10 \cdot log_{10}\left(\frac{P_{IPS}}{P_{event}}\right) \tag{1}$$

where

G	the *magnitude* of the disruption event expressed in dB
P_{IPS}	the total power being generated into the IPS just before the event
P_{event}	the total power being lost during the event

The following table gives value ranges of magnitude with power system consequences that have been determined empirically.

TABLE V: VALUES OF EVENT MAGNITUDE (G) IN RELATION TO POWER SYSTEM CONSEQUENCES [163]

Disruption Magnitude (G) (in dB)	**Effect on the IPS**
G > 18 dB	**Slight** – barely noticeable on the frequency of the IPS.
14 dB < G < 18 dB	**Moderate** – noticeable effect on system frequency, corrected by automatic regulating mechanisms.
10 dB < G < 14 dB	**Significant** – deliberate intervention required.
6 dB < G < 10 dB	**Threatening** – affecting most participants connected to the power system.
0 dB < G < 6 dB	**Overwhelming** –a system blackout is a likely end-state.

This approach (*magnitude*) is based on the supposition that the bulk of the power lost during the disruption event was indeed lost abruptly. If the loss in power was scattered over various time windows (or was gradual), other methods should be used, such as the event intensity I [163].

Although using the power as an indication of the *impact* of a disruption event on the power system in the form of *magnitude* (or *intensity*), it remains a one-dimensional approach in *impact* approximation. When used in conjunction with the system frequency depression, power loss provides an adequate first-order estimation of the *impact* on the power system. However, two separate metrics must be assessed.

Practically, using the first-order perspective of the event impact, the values for the three case studies listed in section 6.1.1 have been calculated and are given below.

a For the Kendal event, G=9,9 dB (using a system load of 30 600 MW)
b For the Kriel event, G=13,6 dB (using a system load of 30 949 MW)
c For the Ankerlig event, G=15,8 dB (using a system load of 28 820 MW)

This result could readily have been predicted qualitatively since the first-order assessment merely takes power loss (or gain) into account. Since the three case studies progressively increased in power loss, the *magnitude* reflects that reality in decibel values.

6.1.3 Second-Order – Event Angle

From the literature survey, it is clear that the entire basis for evaluating the extent of large-scale disruption events has been on the system frequency decay (or the increase thereof on rare occasions), and that other undesirable consequences are generally being neglected. Although the impact on system frequency is certainly the most immediate factor that needs to be handled from a system operations management perspective, it is not the only consideration.

Depending on the availability of reserves, a large generation disruption could lead to an imminent shortfall that may necessitate load shedding or other demand-side implications. Therefore, the model needs to be extended to consider the energy removed from the power system due to the disruption event and the power (frequency) impact.

The frequency impact directly results from the generated power loss [MW]. At the same time, a shortfall in energy [MW·h] causes a system cost implication in replacing through another means or ultimately in unserved energy if no replacement option exists. The impact of a cascade disruption event can be graphically represented for a given event in two dimensions, as shown in Figure 108.

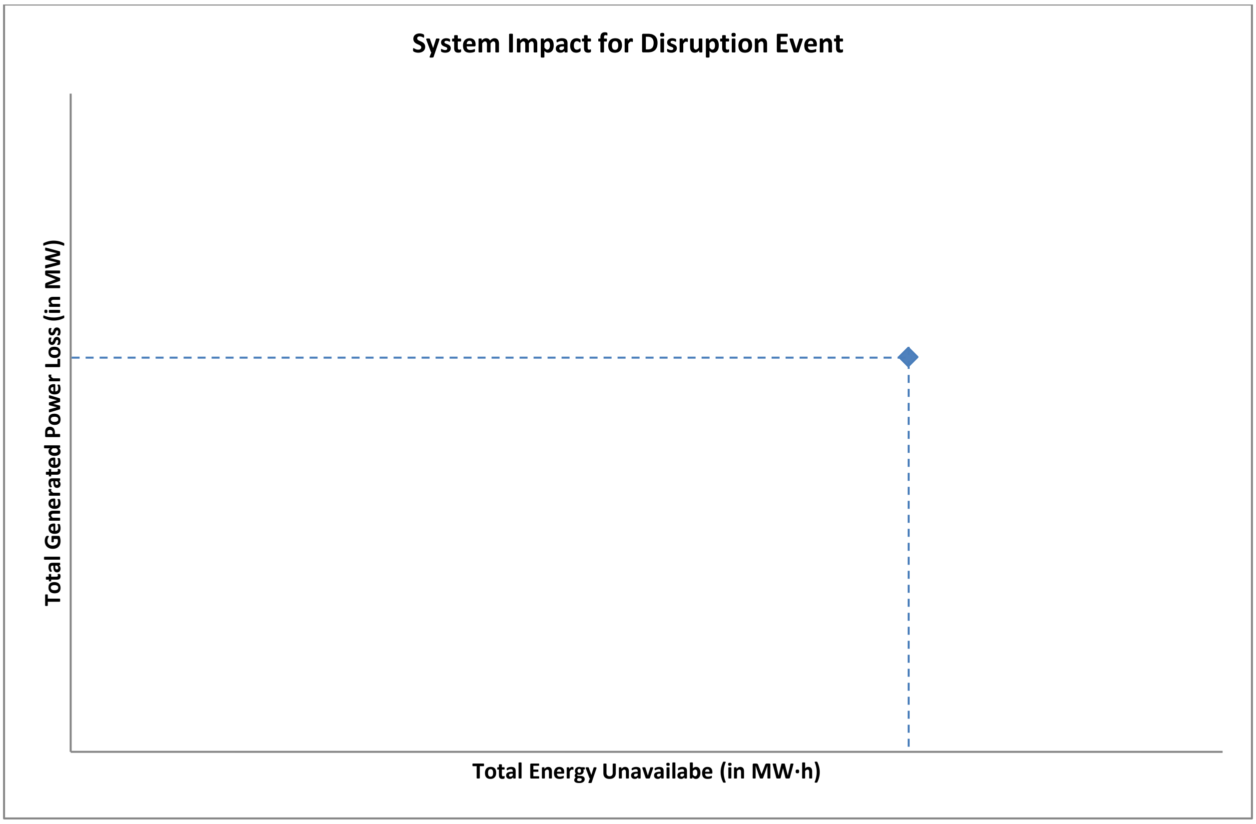


Figure 108: A disruption event expressed in two dimensions – power and energy

The graphic representation effectively visualises the relative magnitude and significance of the two dimensions in a Power-Energy plane. Moreover, different disruption events can be plotted in the same plane to compare them. Figure 109 shows two events making such a hypothetical comparison.

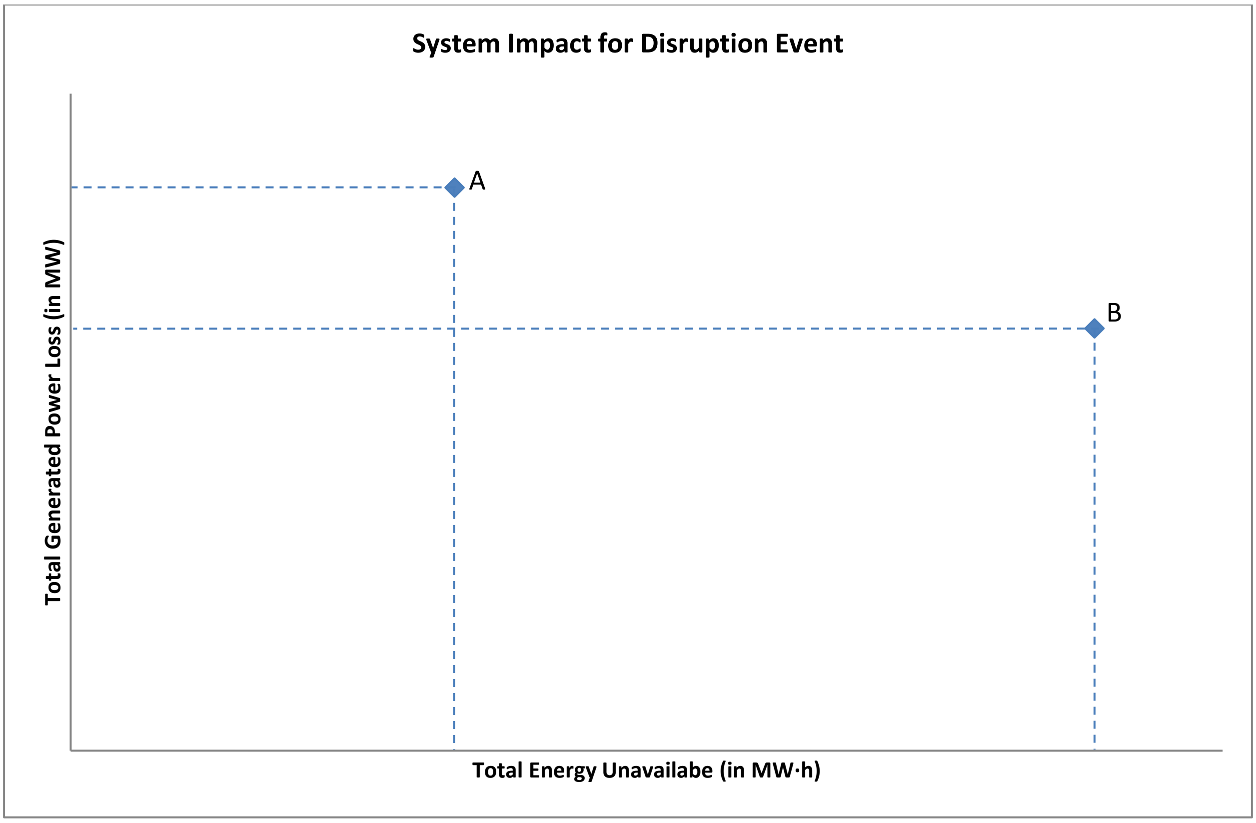


Figure 109: Example of two disruption events (A and B) in the same plane

In this example, two disruption events, A and B, are compared in the same Power-Energy plane. The two events can readily be compared this way, with Event A losing more generated power than Event B but recovering more rapidly.

It is desirable after a cascade disruption event for the units that suffered a loss in output to return to normal production soon after the event. However, this is not always readily achievable due to various factors, e.g., units that have disconnected from the power system and tripped. For them, the generation process needs to be restarted, an operation that could have an extended duration of several hours or more. To express the post-event recovery rate, the angle of the event can be measured from the origin of the Power-Energy plane, as shown in Figure 110. The angles of various events could serve as a further metric for comparing events to indicate post-event recovery rates.

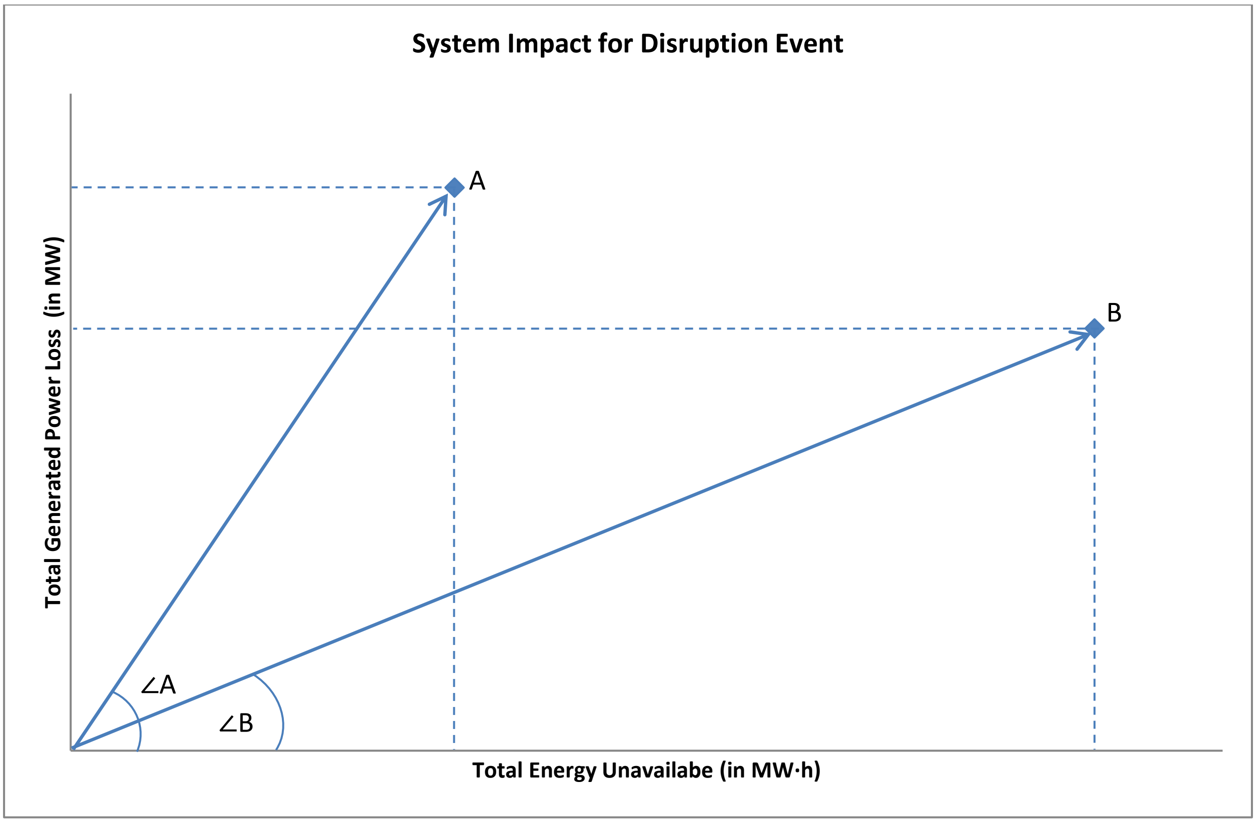


Figure 110: Event angles (∠A and $\angle B$) for two hypothetical disruption events

It can be seen that the angle associated with event A is larger than that associated with event B. The angle for a given event is given by:

$$\angle Ж = \tan^{-1}\frac{Power\ [MW]}{Energy\ [MW{\cdot}h]} = \tan^{-1}\left[\frac{P}{E}\right] \tag{6}$$

This value provides a quantitative basis for comparing two events. From a recovery performance perspective, it is desirable for the ∠Ж to be as close as possible to 90°. Small event angles signify a slow recovery after a disruption event that worsened the impact on the power system.

In the given example, Event A had a greater instantaneous impact on the power system than event B, but the larger event angle (∠A) indicates better post-event recovery than Event B. It is important to recognise that a larger loss in generating capacity leaves the power system in a more desperate need for recovery than an event with a smaller loss of generating capacity. Therefore, the larger the capacity of a generation facility becomes, the greater the need for post-event recovery and the design of power stations needs to take this necessity into account.

The South African Grid Code (SAGC) provides a regulatory standard for post-event recovery, specifically for events that result in the total blackout of a complete power station. Events of this nature are particularly detrimental to the integrity of the power system, not only from a power deficit perspective but also from a voltage support and stability perspective. The SAGC stipulates that the post-event recovery that should be achieved by a power station following the complete blackout of the power station is to be as follows [1]:

> (2) For the purposes of this code, examples of unreasonable delay in the restart of a *power station*, where the supply to the *power station* has been restored within 2 hours, are:
>
> - restart of the first *unit* that takes longer than 4 hours after restart initiation
> - restart of the second *unit* that takes longer than 2 hours after the synchronising of the first *unit*
> - restarting of all other *units* that take longer than 1 hour, one after the other, after the synchronising of the second *unit*.
> - delays not inherent in the design of the relevant start-up facilities and which could reasonably be minimised by the relevant *generator*.

These criteria were plotted in the following illustration for a typical six-pack power station.

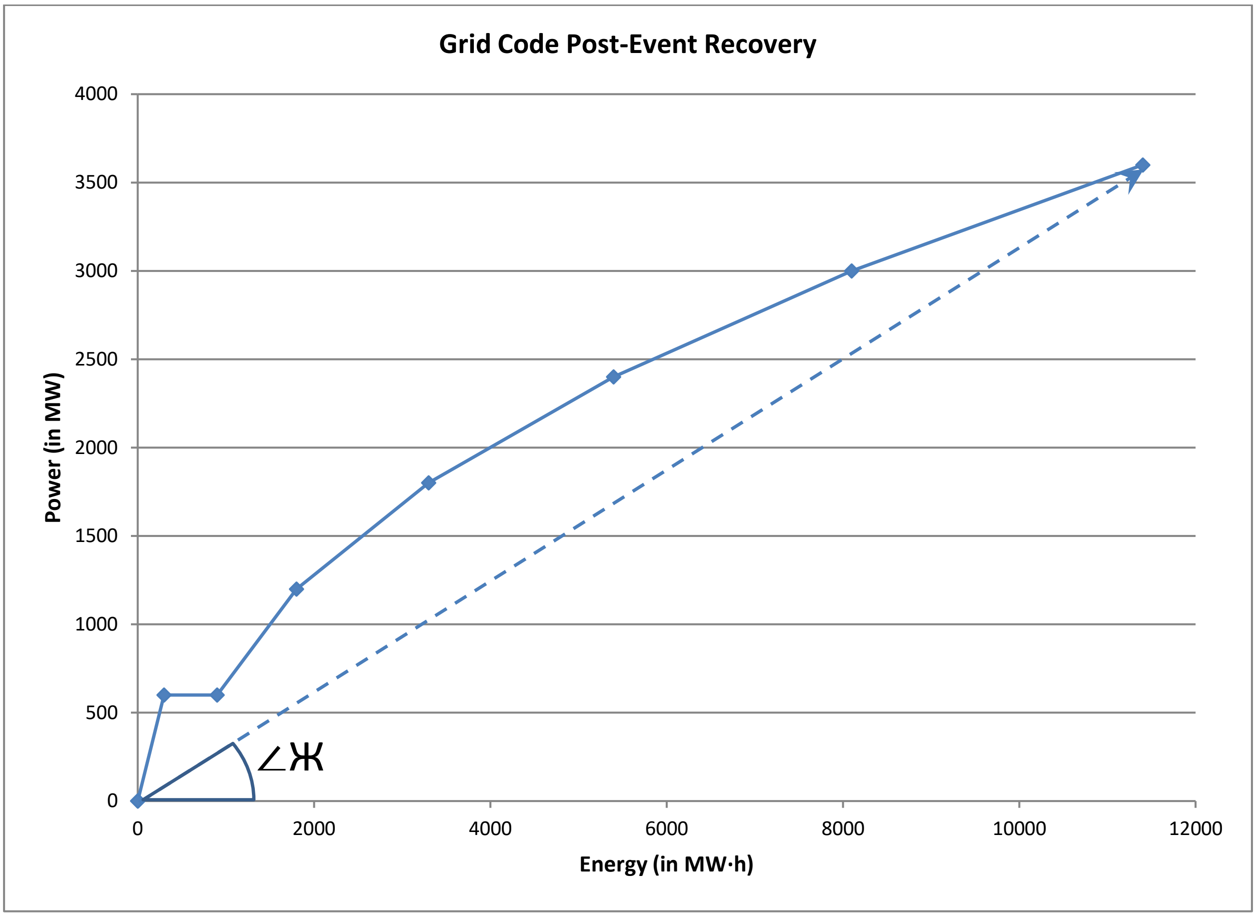


Figure 111: Event angle ∠Ж for the SAGC

In this case, the angle ∠Ж represents the event angle as derived from the stipulations of the SAGC for a six-pack power station with 600 MW units and has been calculated as:

$$\angle Ж = \tan^{-1}\frac{P}{E} = \tan^{-1}\left[\frac{3\,600}{11\,400}\right] = 17{,}5°$$

This value corresponds to the worst case tolerated by the SAGC for restoration following a complete power station blackout. It is adopted as the value for evaluating restoration performance during any cascade event where multiple losses in power generation occur.

It is possible, for any cascade event where multiple losses in power generation occurred, to calculate an event angle ∠Ж that can serve as a basis for comparison with other events. This measure is more representative as an indication of power system *impact* than the traditional method of merely comparing power loss [MW] of cascade events since disruptions with prolonged duration manifest significantly in the energy [MW·h] domain with undesirable consequences, such as an inability to meet demand or the activation of reserve classes that have a large cost differential over those units that suffered cascade power loss.

Note that

$$E = \int P(t) \cdot dt \tag{7}$$

where E is the (real) electrical energy in MW·h, and $P(t)$ is the power in MW.

Since electrical energy is merely the integral of power over time, the event angle is essentially a way of interpreting the power lost during the disruption event in two dimensions, thus providing a second-order approximation of the *impact* that a disruption event had on the power system.

To give practical context to the second-order assessment of the *impact* of an event, once again, consider the three case studies outlined in section 6.1.1. Using the equation (6), the event angle for the three disruption events has been calculated as being:

a For Kendal, ∠Ж=6,7° for an energy forfeiture of 26 794,7 MW·h.
b For Kriel, ∠Ж=3,4° for an energy forfeiture of 22 205,3 MW·h.
c For Ankerlig, ∠Ж=55,4° for an energy forfeiture of 490,0 MW·h.

This second-order perspective on the *impact* of each disruption event highlights the exceptionally well-executed recovery of Ankerlig, while both Kendal and Kriel had recoveries that exceeded the theoretical 17,5° angle by a significant margin. While the first-order perspective provided a rather intuitive outcome, this second-order perspective does not.

However, the model can be further refined to add yet another dimension to the concept of an event's *impact*, which will be explored in the following section.

6.1.4 Third-Order – PID

In the preceding two sections, the use of power as an approximation for the *impact* of a disruption event on the power system has been developed. As a first-order approximation, power has been introduced as a one-dimensional indicator. Thereafter, a two-dimensional approach using both power and electrical energy was suggested to be used collectively as a metric for *impact* on the system in the form of an event angle, adding a second-order evaluation.

In this final section on the topic of using power as the metric for the *impact* of a disruption event on the power system, a third dimension will be added. The main problem in using power as a metric is that it lacks the relevant context of abruptness. If, for example, an entire power station is systematically shut down over many hours, the *impact* on the power system would be entirely different than in a case when the same power station disconnects instantaneously.

To address this obvious deficiency in the *impact* model, the model should be extended to take cognisance of the rate at which power has been lost. For this reason, a third dimension to the *impact* model needs to be introduced, specifically the rate of change of power, i.e.:

$$\frac{dP(t)}{dt}$$

Such an addition to the impact model would then provide three different perspectives of power, namely power itself, the integral of power throughout the disruption and the derivative of the power loss characteristic with reference to time.

These three dimensions of power loss equate to control system theory in terms of PID, (p̲roportional, i̲ntegral and d̲erivative components), with power, $P(t)$, representing the P-component; energy, $\int P(t) \cdot dt$, representing the I-component and the rate of power loss, $\frac{dP(t)}{dt}$, representing the D-component in the PID-model.

A fundamental aspect of the *impact* model is combining the three dimensions into a single metric that would facilitate the comparison of different disruption events. In this respect, the following approach yielded a single-value metric.

The *impact* of a disruption event can be visualised as a three-dimensional cuboid that is positioned at the origin of a three-dimensional Cartesian space, with the x-coordinate being the value of $\int P(t) \cdot dt$, the y-coordinate being $P(t)$ and the z-coordinate being $\frac{dP(t)}{dt}$ – illustrated below (Figure 112).

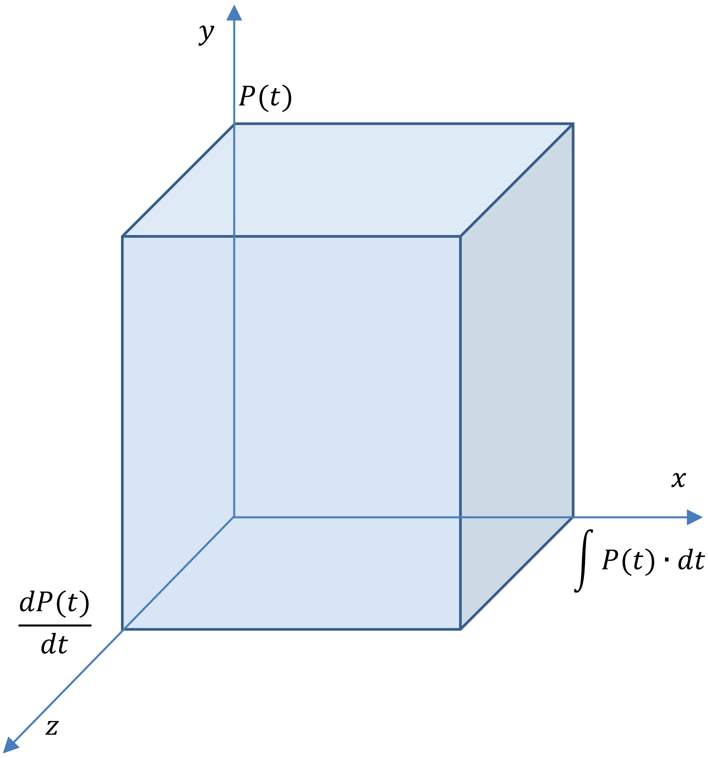


Figure 112: Three-dimensional representation of a disruption event

The *impact* of the disruption event can be considered to be the volume of the cuboid, i.e.:

$$\mathit{Impact} = P(t) \times \int P(t) \cdot dt \times \frac{dP(t)}{dt} \tag{8}$$

with

$P(t)$ being the total power that was lost in MW,

$\int P(t) \cdot dt$, being the electrical energy throughout the disruption in MW·h, and

$\frac{dP(t)}{dt}$, being the highest rate of change in power over the event in MW·h^{-1}.

Since the hour dimension cancels in the product, the impact calculation yields a unit of MW^3 – designated as *"cubic megawatt"* using the symbol P^3, and referred to as the *power cube*.

From a practical point of view, consideration needs to be given to the time value that should be used in the calculation of $\frac{dP(t)}{dt}$. This value potentially poses a significant practical challenge. To know, with a sufficient degree of certainty, what the fault clearance times were (unless specifically recorded) is not trivial or obvious. To circumvent this difficulty, a pragmatic approach is opted for, namely to use the total time for which the system frequency remains in decline as a basis for determining the derivative component of the metric. When disruption events are staggered over time, the worst (most extreme) frequency event is selected for the calculation.

The three case studies outlined in section 6.1.1 practically demonstrate the application of the power-cube metric as the third-order perspective on the *impact* of a disruption event.

Using the event information that was recorded for the three events and applying equation (8), the following values for P^3 were calculated.

a Kendal, P^3=37,9x1012 MW^3
b Kriel, P^3=4,64x1012 MW^3
c Ankerlig, P^3=15,1x10^9 MW^3

As can be seen from the above values, the third-order perspective on an event's *impact* discriminates effectively between disruption events, with Kendal being an order of magnitude greater than Kriel and Ankerlig being three orders of magnitude less. Using the *impact* model from various perspectives provides a suitable and convenient set of metrics for comparing the *impact* that disruption events have on the power system.

The power-cube metric (P^3) concludes the impact model by providing a third-order perspective on the *impact* of a disruption event on the power system.

6.2 Power System Integrity

In the preceding section, a method was developed to assess the impact of a multiple disruption event on a power system. However, the integrity of the power system depends not only on the power that was lost (in terms of the *impact*) but also on various other aspects.

During the course of a cascade disruption event, an increasing quantum of network assets and generating units (and plants) are being switched out or become disconnected from the power system. Each additional network asset or generating unit that becomes disconnected is removing capacity, functionality or services from the power system.

Since it is the collective quantum of connected power system resources (both generation facilities and network assets) that ensures the integrity of the power system, progressively disconnecting such resources in ever increasing quantities has an erosive effect on its overall integrity. The degree to which the integrity of the power system becomes eroded is not readily known and the quantification thereof is not trivial.

The following section will be devoted to gaining insight into the aspect of power system integrity erosion and ultimately develop a means for the quantification thereof.

6.2.1 Erosion Factor 1 – Power

Although power loss has been used extensively in the previous impact model, the erosion model equally recognises that power is a key erosion component when considering power system integrity.

Electrical power remains the most predominant factor that erodes the integrity of a power system. In the vast majority of cases, a disruption in electricity generation will manifest in a nearly immediate reduction in the amount of electrical power being supplied into the power system, manifesting almost instantly as a decay in the system frequency.

When the extent of the disruption is mild, the power system can readily "*rectify*" the shortfall by extracting kinetic energy from the synchronous rotating masses (see section 6.2.4.) and by increasing the power output from the remaining units connected to the power system. In more severe cases, load blocks may be required to disconnect at predetermined frequency values, implemented in dedicated protection schemes designed for this specific purpose, thus re-establishing an equilibrium between supply and demand.

Electrical power deficit (real power in MW) is the factor that directly results in a reduction in the system frequency and, therefore, the immediate quantity that needs to be replaced. This quantity, the power that is injected into the power system, is often referred to as send-out power.

The power deficit caused during the event is generally the single most significant parameter that erodes and defines a cascade disruption event, and much of what follows from the event depends on it.

6.2.2 Erosion Factor 2 –Reserve Range

The actual real power, P, is insufficient to express the erosion the power system suffered comprehensively. Closely associated with the actual send-out power of a unit that became disrupted is the range of reserve that the unit represented in the power system while in service.

Usually, units operate at a lower generation value than their maximum capacity. However, because the unit is already synchronised to the power system, it can readily increase (or decrease) its generation level. This range within which the unit could be dispatched is highly beneficial to the power system, and the benefit is lost when the unit trips.

Take, as an example, a coal-fired unit that has a maximum rating of 600 MW. Since most coal-fired units are operated as load-following units instead of peaking or base-load units, the actual output from the unit varies continuously over time. Such a unit may typically remain in stable operation down to 350 MW. But during the time that it became disrupted and disconnected, it was (for example) delivering 450 MW into the power system. Thus, the power that was lost was 450 MW, while the reserve range wherein the power output of the unit could have been varied, was 250 MW.

An additional component added to the reserve range is the unit's emergency capability. This capability enables a unit to exceed its MCR rating with a certain margin (with additional costs) but can nonetheless be dispatched if circumstances necessitate, hence the addition.

Each unit that suffers disruption is associated with a reserve range, and the total reserve range lost during a cascade disruption event is the sum of all the individual reserve ranges of those units that disconnected during the event. This collective loss in the reserve range is a second erosion factor that results from the cascade disruption event.

6.2.3 Erosion Factor 3 – Reactive Power

Reactive power, the imaginary component of apparent power required for the electrical integrity of the system, is a local phenomenon with an impact normally contained to the location where a disruption occurs. It is designated by Q and expressed with the unit *var*.

Once again, a generating unit has an actual amount of reactive power that it is either providing to the system or absorbing from the system – in both cases as a benefit to the power system.

The issue of reactive power is rather more complex than real power or energy. The point is that the phenomenon is merely local, and secondly, that generating units can disconnect in more than one way from the power system. Firstly, a unit can disconnect from the power system by merely disconnecting the generator, yet leaving its main transformers still connected – causing the reactive power needed by the transformers to be supplied by the power system or other units connected at the same electrical node. Secondly, it is equally possible for generating units to disconnect entirely from the power system, including the main transformers, thereby not requiring the supply of reactive power from other sources and, therefore, not representing a reactive power drain on the power system. Furthermore, reactive power is a value that readily manifests in two quadrants, unlike energy and power, which makes it more difficult to account for and interpret.

To circumvent the many complications presented by reactive power, it is more practical to merely consider the voltage level of the electrical nodes where the disruption occurs rather than attempting to track reactive power increases and decreases during the progression of the disruption. The reactive power nett effect can effectively be considered by taking the node voltage deviations from the nominal value, expressed as a percentage deviation.

6.2.4 Erosion Factor 4 – Inertia

When dealing with rotating bodies, such as the shaft trains of generating units, the moment of inertia, J (in kg·m^2), is analogous to the mass of a body moving in a straight line. And as the mass of a body, moving in a straight line exhibits a property known as inertia (that resists changes in the speed of movement), so too does a body rotating around an axis exhibit an inertial property resisting changes in the speed of rotation, known as the moment of inertia. The moment of inertia for an arbitrary rigid object can be expressed as,

$$J = \sum m \cdot r^2 \tag{9}$$

for each mass m (in kg) located at radius r (in m) comprising the object [189]. Thus, the moment of inertia is, in contrast with the case for linear motion, not merely a function of mass but also geometry.

Similar to linear motion, where a moving mass exhibits momentum, a rotating body has an angular momentum, L in (kg·m^2·s^{-1}), given by,

$$L = J \cdot \omega \tag{10}$$

with ω being the angular speed of the body, expressed in radians per second (rad·s^{-1}) [189].

Rotating masses synchronously connected to a power system, such as the rotors of turbines, synchronous generators, synchronous motors and rotating exciters, possess angular momentum resulting from their inherent moments of inertia, rotating at angular speed. Angular speed, ω, is directly related to the network frequency according to the following relationship [190].

$$f = \frac{P \cdot N}{120} \tag{11}$$

with

f electrical power system frequency

P number of magnetic poles of the synchronous machine

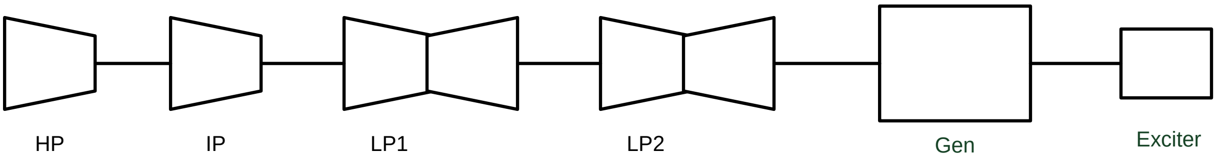
N rotating speed of the rotor in revolutions per minute (r.p.m.), which is related to the angular speed in terms of the following relationship [190],

where

$$\omega = \frac{2\pi}{60} \cdot N \tag{12}$$

Angular momentum acts to resist changes in network frequency since the frequency is directly related to the angular speed of the shaft train of the generating unit. The reason for the moment of inertia to counteract a disruption is a result of the fact that kinetic energy is stored within the rotating mass of the shaft train, which is converted into electrical energy when the network frequency decays – causing a deceleration of the shaft train until eventually, the angular speed of the shaft train will correspond to the network frequency. Conversely, a sudden rise in the network frequency will cause electrical energy to be converted into mechanical energy, accelerating the shaft train and storing energy through an increase in angular momentum. In both cases, i.e., a sudden increase and a sudden decrease in the network frequency, the conversion of energy between mechanical and electrical is resisted by the moment of inertia (a consequence of the mass and geometry) of the shaft train components.

A typical shaft train of a modern turbo-generator of a coal-fired power station is shown in the following diagram.



It shows the rotating elements of a typical steam turbine consisting of a high-pressure (HP) turbine, an intermediate-pressure (IP) turbine and two low-pressure (LP) turbines, along with the generator consisting of the rotors of the synchronous generator itself as well as the rotor of a rotating exciter. Most of the coal-fired and liquid fuel power stations make use of two pole synchronous generators that relate to rotational speeds of 3 000 r.p.m. in 50 Hz networks and 3 600 r.p.m. in 60 Hz networks, respectively.

As an illustration, typical data for the shaft train of a 600 MW coal-fired turbo-generator unit is tabulated below, featuring two low-pressure turbines and a rotating exciter.

	LP1	**LP2**	**IP**	**HP**	**Gen**	**Exciter**	**Total**
Mass (kg)	58 600	58 600	25 500	10 700	75 000	6 000	138 600
Moment of Inertia (kg·m^2)	14 000	14 000	3 500	1 000	11 000	50	43 550

In the case of hydro units, the moment of inertia is dominated by the rotor of the synchronous generator, with the water turbine typically contributing less than 10% of the total rotation train. However, the generator rotor is relatively short and features a large radius to accommodate several magnetic pole-pairs in a salient pole configuration. This difference results in a significantly larger moment of inertia as compared to steam turbo-generators used in coal-fired power stations – typically one or two orders of magnitude greater, despite the power rating of the hydro-generator being half or less of that of the generator used in a coal-fired power station.

Once again, similar to the case of linear motion, the kinetic energy stored in the moving mass can be expressed for a rotating body, using the following relationship,

$$E_k = \frac{1}{2} \cdot J \cdot \omega^2 \tag{13}$$

with E_k in joule (J) [189]. Since the joule is an impractical unit to be used in the context of power systems, the unit of preference is (MW·s) for individual shaft trains and (GW·s or TW·s) for large power systems.

Since the rotating speeds of the shaft trains may differ, the rotational speed needs to be considered when calculating the kinetic energy for the two cases contemplated above, i.e., a coal-fired and a hydro unit, respectively. The following table shows the results of such a comparison using 50 Hz in the example.

	Moment of Inertia	**Rotation Speed**	**Kinetic Energy**
	J (*kg·m^2*)	**(*r.p.m.*)**	**(*MW·s*)**
600 MW Coal	40 000	3 000	1973,9
300 MW Hydro	2 000 000	300	987,0

The above data shows that, despite the significantly greater moment of inertia of the hydro generator, the kinetic energy stored in the steam turbo-generator of a coal-fired power station is an order of magnitude greater. Although this may seem counterintuitive, it is a result of the rotational speed, which is much lower in the hydro case.

The total collective kinetic energy available to a power system due to the rotation of all the synchronous shaft trains connected to it is given by,

$$E_{k|sys} = \sum_{i=1}^{T} E_{k|i} = \tfrac{1}{2} \cdot \sum_{i=1}^{T} J_i \cdot {\omega_i}^2 \tag{14}$$

where J_i is the moment of inertia of the shaft train i in the population of all connected generating units, totalling T shaft trains, individually rotating at an angular speed ω_i [191].

Much of the integrity of a power system depends on the sufficiency of the overall, or resultant, moment of inertia connected to it. Moment of inertia provides retardation in the rate at which the frequency of the power system can rise or fall between the instance of disruption and the effects produced by the disruption. This time lag is vital since it allows for remedial action to avoid a loss in system stability or a total collapse thereof. Specifically, the rate of change of frequency (RoCoF) resulting from a disruption event is determined by two factors, i.e., the total power that was lost (either from a source or load perspective) and the total inertia that is connected to the system at the time [191].

In addition, the total moment of inertia of the system largely determines the dynamic behaviour of a power system during disturbance conditions, allowing deterministic countermeasures to be designed and brought to bear to stabilise the system that might otherwise spiral out of control into an unavoidable blackout. Moment of inertia is a significant component determining the time constants characterising a power system at a given point in time.

When generating capacity would instantaneously disconnect from the power system, a power deficit would cause the frequency to decay. The frequency decay would, however, not occur immediately but rather reduce at a gradient due to the collective angular momentum of the synchronised rotation trains that release energy into the power system as angular deceleration occurs.

During a disruption event, successive units become compromised and disconnect from the power system. The time constants also change (typically reduce) from one disconnection to the next, and the time durations between the disruptions and their effects reduce as a result. This condition becomes ever more critical as the disruption event runs its course, threatening eventual system collapse if not arrested.

Although the concept of inertia constants (so-called H-values) is widely used in power system studies and models, such values are, however, not an ideal metric to express the level of erosion of the operability (or integrity) of the power system. The reason for this is that an H-

value is calculated as a normalised version of the actual moment of inertia of the rotating mass comprising the turbo-generator shaft train – denoted by J and measured in ($kg \cdot m^2$). However, the actual value of the moment of inertia is equally not an ideal metric in terms of the quantity of system integrity that becomes eroded during a disruption event since the moment of inertia is independent of rotational speed – a parameter directly related to system frequency. Therefore, the only plausible value that can be used is the kinetic energy stored in the synchronised rotation train.

Although the moment of inertia does not vary due to operating conditions, the kinetic energy does indeed. In most power systems, the generators would not all rotate at the same angular velocity due mainly to technological differences that underlie the power generation process at various power stations.

6.2.5 Erosion Factor 5 – Automatic Frequency Control

The power system constantly strives to balance the real-time load demand with the generated infeed. This balance is not a coincidental condition but a constantly controlled process.

The demand is essentially dictated to the system through the collective requirements of the individual loads or customer demand. This demand is not a constant value but rather changes gradually in a pattern that represents the combined behaviour of the domestic, commercial and industrial sectors throughout a day, a week and a year. It is further affected by social and socio-economic behaviours normally superimposed upon the demand patterns mentioned before. However, the pattern normally represents gradual increases and decreases in the total system demand.

As the demand changes continuously, so must the total generated supply change in a lockstep fashion with the demand. This continuous matching of generation to a changing demand requires real-time control of the collective power system input. The control is achieved through various means, but the most direct real-time method relies on continuously changing the control set-points of the individual generating units in service. The control variable for the system is the network frequency, which is 50 Hz in the SAPP, with a 150 mHz dead-band symmetrically around it, wherein no control adjustment is required.

Under normal system conditions, system frequency control is achieved through two independent control functions, namely:

- Primary frequency control (governing) – commonly known as AGC (Automatic Generation Control)
- Secondary frequency control (regulation) – commonly known as Frequency Bias

The purpose of both primary and secondary control is to achieve an equilibrium between generated and consumed power for the power system. Primary frequency control is a turbine speed control function that restores turbine speed to nominal when deviations occur. Each unit is equipped with control functionality to provide frequency control, which forms part of the unit's overall process control system.

Secondary frequency control is a centralised control function physically located at National Control (in the South African context). It issues commands to specific units in the power system to incrementally change their load control set-points up or down.

6.2.6 Erosion Factor 6 – Specific Functions

In the above five sections, some of the most significant aspects that cause the integrity of a power system to become eroded during disruption events were discussed. There are, however, various other services or functions that power stations (or generating units) may provide to a power system and that may become unavailable when the unit or power station is compromised. Many, but not all, additional functions can be classified as ancillary services, although not all of these functions may be formally recognised as such. For this reason, the term quasi-ancillary services will be used to denote these additional functions. The following list serves as a collection of examples of what may be included as aspects that add to the overall erosion of a power system. However, the list does not cover all conceivable quasi-ancillary services that might be considered erosion factors.

a Excitation ceiling capability
b Power system stabiliser functionality
c Unit islanding capability
d Black-start, self-start or nuclear off-site supply capabilities
e Automatic under-frequency starting capability
f Automatic tripping from pump mode of operation (in pumped storage schemes)
g Synchronous condenser operation functionality
h Pumping capability
i Reactive power range
j Voltage range
k Mandatory governing
l Unit ramp rate
m Rapid call-up capability
n Generator transformer tap changer availability and tapping range
o Fault level

It is more or less self-evident, for example, that if a unit with islanding capability is lost during a disruption event, the overall power system is left with one less unit that has such capability. Thus, the power system's integrity is eroded due to the loss. Each item on the list above has similar undesirable results if compromised. Also, the list is not comprehensive, and various other functionalities could be conceived that, in its own right, would represent an aspect that would erode the power system integrity when lost.

6.2.7 Other Erosion Factors

The six erosion factors of the preceding sections do not represent a definitive list. Power systems are not the same, and it is entirely possible that other factors could be considered to be erosive to the power system in its own right.

Consider, for example, power systems containing significant HVDC systems. Such a system may well require other erosion factors to be considered that are not listed above.

It needs to be understood that the list above represents the more typical erosion factors but that other factors may be added to the list. The methodology derived later would readily be extended to incorporate other erosion factors. Also, some items grouped together in *Erosion Factor 6 – Specific Functions* (section 6.2.6. above) could be considered as entirely separate erosion factors if deemed to be specifically significant in the case being considered. The methodology being developed is entirely insensitive to the number, or grouping, of the erosion factors that would ultimately be decided upon.

6.3 Quantifying Disruption Severity

During the preceding sections, six erosion factors were identified, each representing an aspect of power system integrity that could be adversely impacted when a disruption occurs. A disruption event typically manifests as a combination of multiple erosion factors that collectively detract from the integrity of the power system. However, disruption events will differ in terms of which (and the extent) erosion factors are being manifested during a given event, depending on the nature and specifics of that event.

In understanding, analysing and trending disruption events, it is necessary to differentiate between the severity of different events. Determining the severity of an event is not a trivial matter. Disruption events cannot be reduced to binary manifestations of grid integrity erosion since cascade events evolve as more and more generating plants become compromised. Using the most severe level of erosion in system integrity (that occurred during a disruption event) to represent the overall severity of the entire event is an oversimplification that would fail to provide adequate understanding and analysis of the event.

The severity of a disruption event is essentially an expression of the combined erosive effect that detracts from the integrity of the power system due to the event. The erosion that a cascade event inflicts on the integrity of a power system typically progresses as a stepwise deterioration in the system integrity. At each step in the progression, the level to which the integrity of the system became eroded tends to increase until the progression of the disruption ceases, plateauing at a certain level.

In the following sections, a methodology will be developed for determining event severity, a measure that could be applied in the analysis, quantification, and management of cascade disruption events.

6.3.1 Event Progression and Severity

As stated above, every cascade disruption event propagates through a series of progression steps. At each step of the progression, more generation capacity becomes compromised. Hence, the progression step is associated with a further increase in the degree to which the integrity of the power system has been eroded. In other words, each step i in the progression of the cascade event is characterised by a differential in erosion level from the previous step in the progression, $\Delta Э_i$.

The integrity of the power system becomes increasingly eroded with each subsequent step $Э_i$, with $Э_0$ being the level of power system integrity before the first progression step $Э_1$ of the cascade disruption event. To standardise event severity calculations, the convention is used that $Э_0 = 0$. As an illustration, consider a five-step disruption event with erosion values shown in Figure 113 (numerical erosion values are arbitrary).

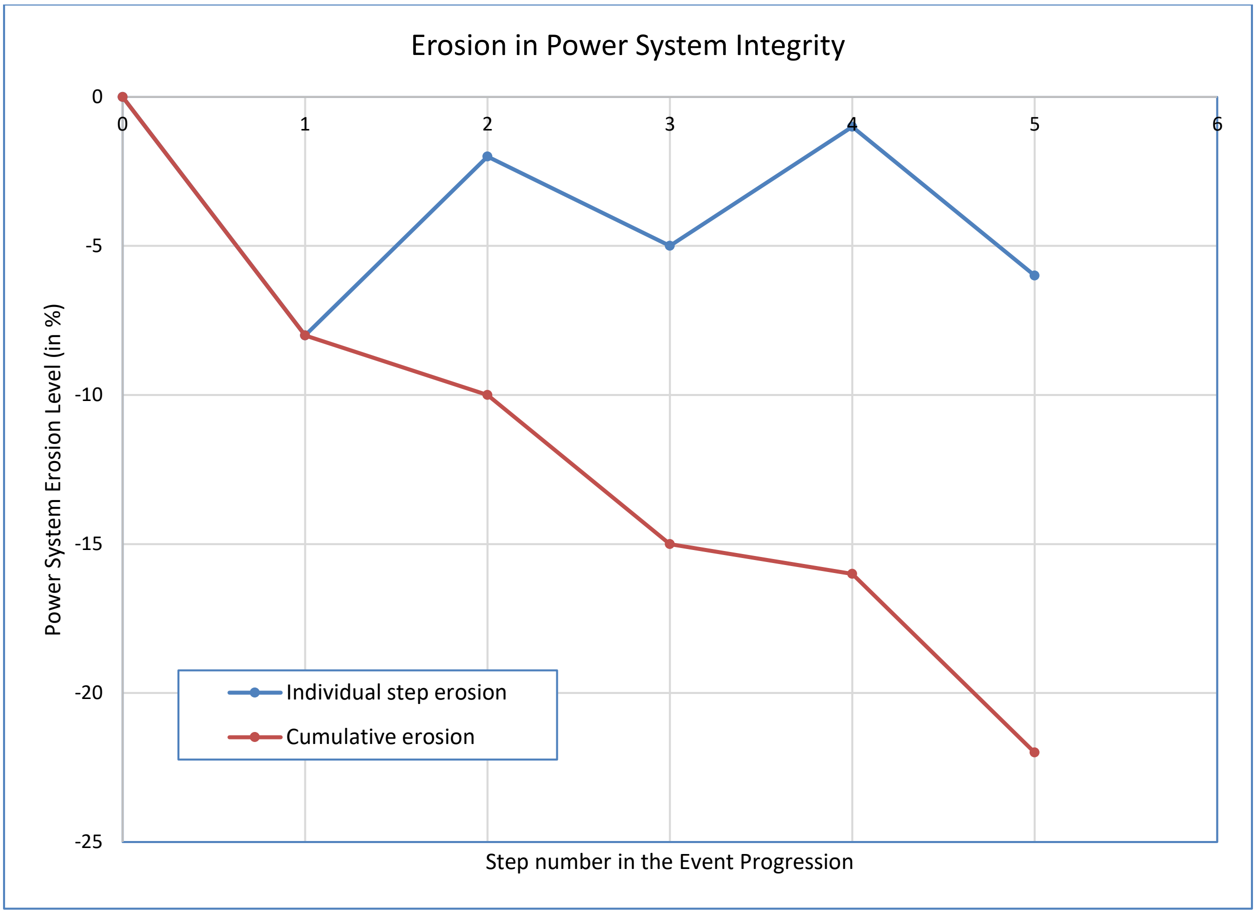


Figure 113: Example of a disruption event with five progression steps

Note that the erosion values are negative since the erosion detracts from the integrity of the power system. The blue line indicates the incremental erosion of each step in the event progression $Э_i$, while the red line indicates the cumulative value to which the integrity of the power system became eroded – the cumulative erosion (red line) is referred to as the erosion trajectory, $Э(t)$ – a piecewise function of time.

Conversely, full or partial restoration of the integrity of a power system is also normally achieved stepwise, usually by re-establishing or improving the balance between the production and consumption of electrical power. Restoration (i.e., counteraction to the erosive effects of the cascade disruption event) is denoted by $Я$, with $ΔЯ_i$ being the restoration differential that occurred in step i of the event progression. Figure 114 shows the same example as above, with the addition of an illustrative restoration occurring during the event's progression. Similar to the erosion trajectory, the restoration trajectory is taken for conventional purposes as $Я_0 = 0$.

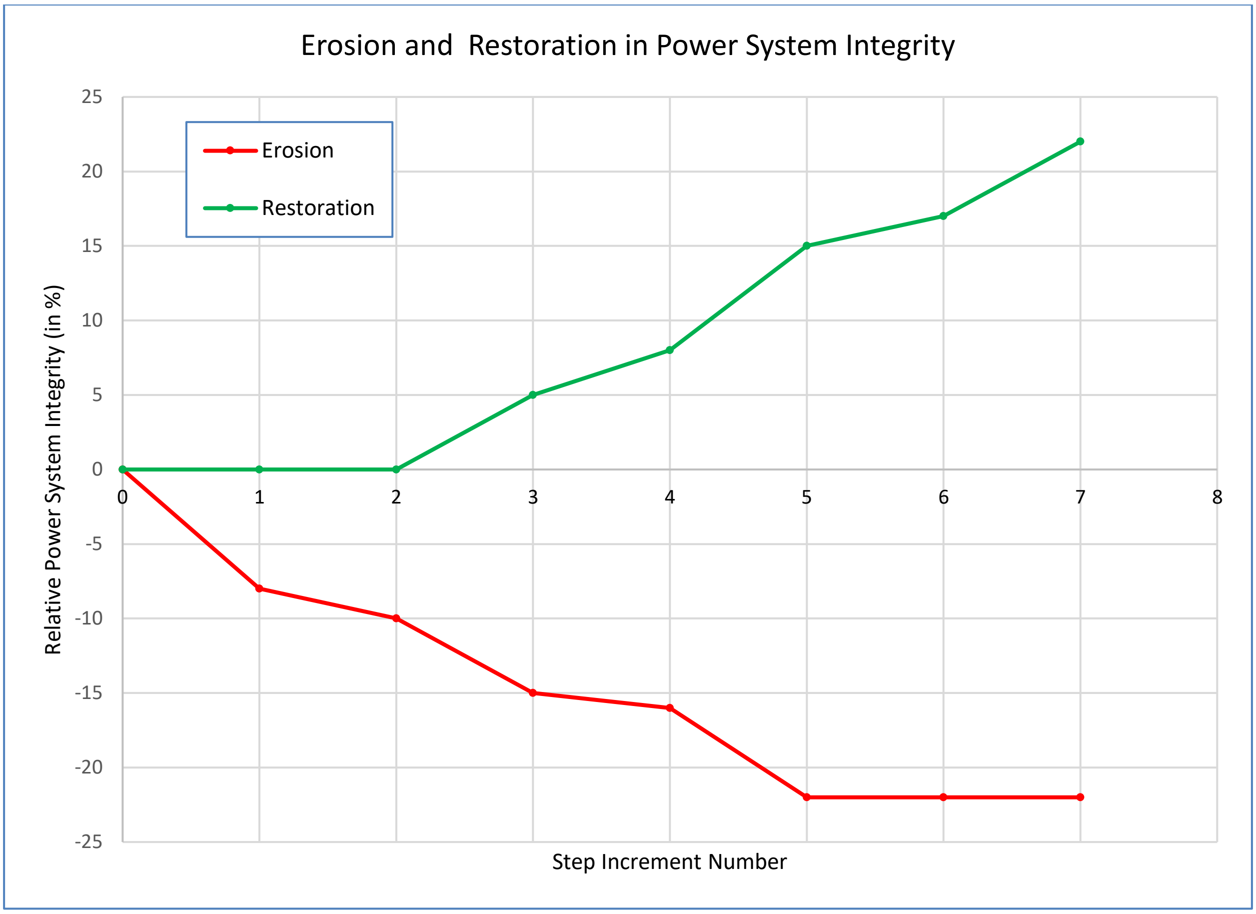


Figure 114: Example of a disruption event with progression steps for erosion and restoration

Unlike the erosion steps, $Э_i$, that are negative, the restoration steps, $Я_i$, are indicated as positive values (in green) – known as the restoration trajectory, $Я(t)$ – a piecewise function of time.

Adding the two trajectories of erosion and restoration together, a new characteristic for the disruption event is derived, known as the event trajectory with progression steps, $Ɛ_i$. Once again, the event trajectory, $Ɛ(t)$ is a piecewise function of time. Expressed mathematically,

$$Ɛ(t) = Э(t) + Я(t) \tag{15}$$

for the overall characteristic describing the entire event, or discrete as,

$$Ɛ_i = Э_i + Я_i \tag{16}$$

for each step i in the progression of the disruption event. Note that although the individual sections of the three piecewise functions (the erosion, restoration and event trajectories) are normally represented by straight lines, actual calculated or sampled data can be used, if available.

Figure 115 shows all three trajectories for the same fictitious example used above.

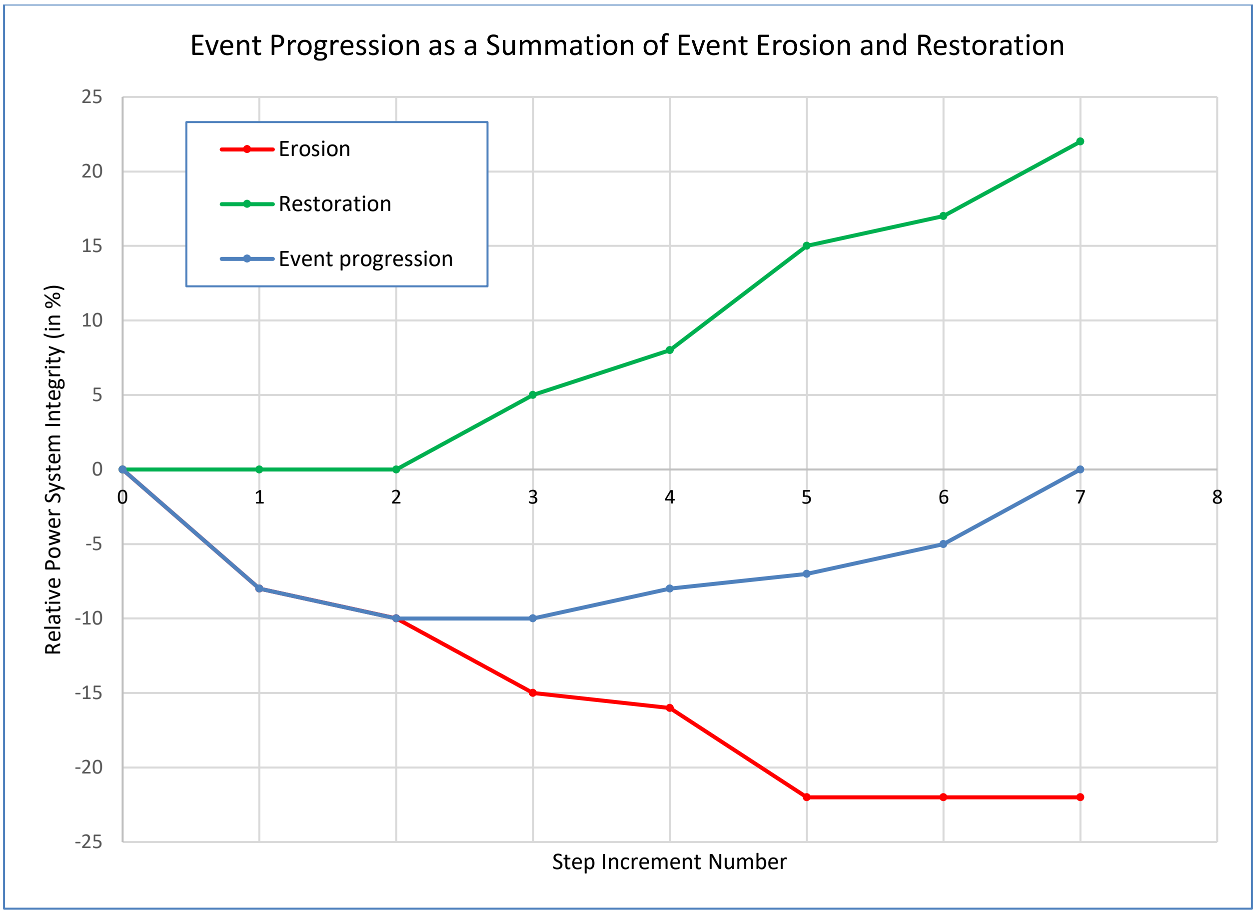


Figure 115: Example of deriving the event trajectory

Note that the event trajectory ends when the erosive effect of the disruption event has been neutralised (or cancelled out) through restoration steps. The severity, Ƨ, of the cascade disruption event can hence be calculated as the integral of the event trajectory. For practical purposes, the severity is expressed as a positive value. Expressed mathematically,

$$\text{Ƨ} = \int_{t=0}^{t=r} |\text{Ɛ}(t)| \cdot dt = \int_{t=0}^{t=r} |[\, \text{Э}(t) + \text{Я}(t)\,]| \cdot dt \qquad (17)$$

for an event starting at $t = 0$, and with a total of r steps in the overall event progression.

Note that the relative power system integrity in the graphs contained in this section is merely the degree to which the state of the power system has been affected by the erosion steps of the disruption event as well as the restoration steps taken to recover from the disruption steps that occurred during the event.

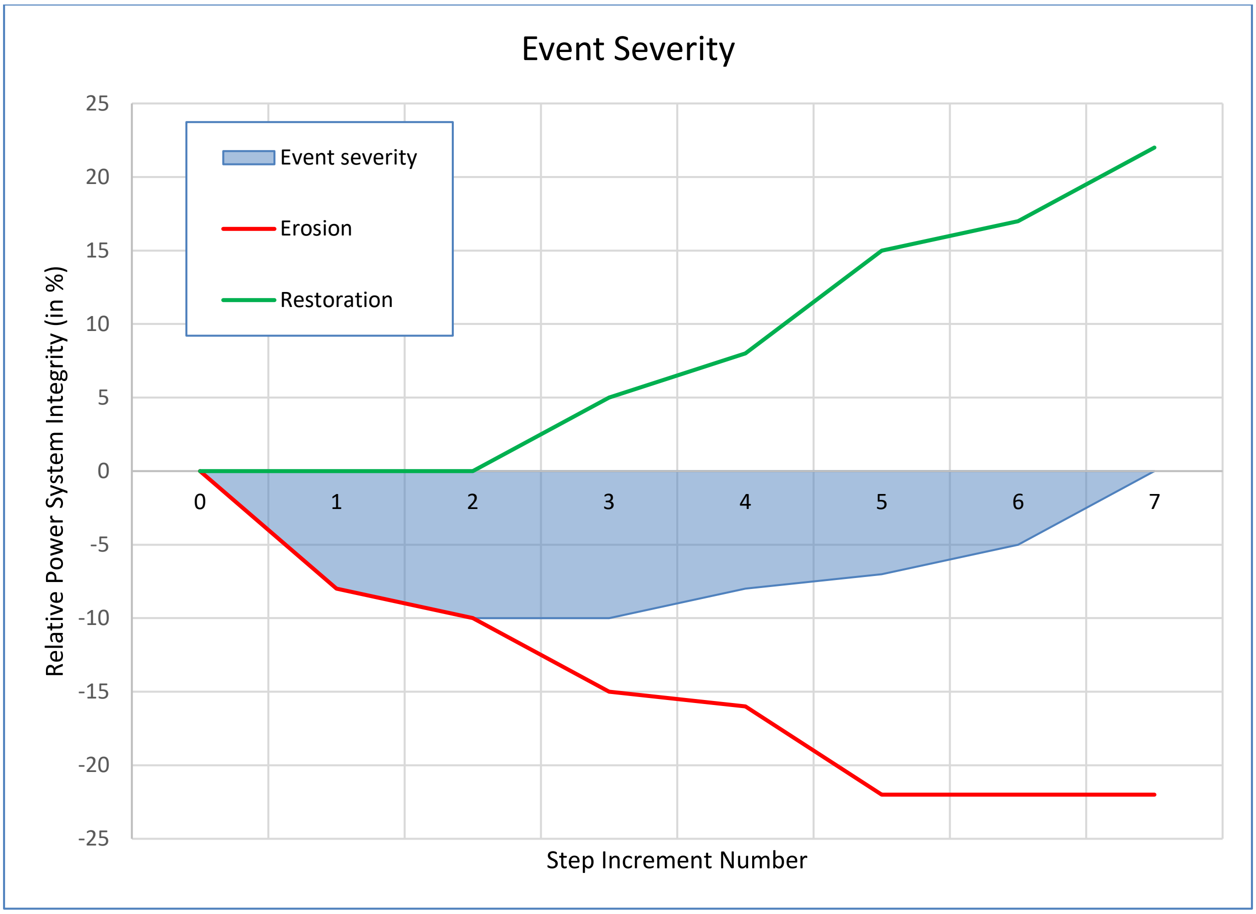


Figure 116: Example showing the event severity (as a shaded region)

The shaded area above graphically shows the severity of the event, albeit as a negative quantity.

6.3.2 Incremental Step Assessment

In the preceding section, recognition was given to a cascade disruption event's incremental (step-wise) nature. It follows that events are characterised by event trajectories, piecewise functions that account for erosion and restoration steps during the progression of the event. Finally, a quantitative value was derived to signify the severity of a disruption event as a strictly positive integral of the piecewise function (the event trajectory).

However, the respective values of erosion and restoration that are used to construct the event trajectory, have been adopted without explanation of how such values are to be obtained. If the event severity would be used as a metric to analyse and rank cascade disruption events, then values of erosion and restoration need to be scientific and cannot merely be assumed or guessed. Instead, such values should be based on actual data or high-accuracy inferences based on an in-depth understanding of the system components and their behaviours.

On the other hand, it should also be noted that the data and information required for a conclusive study of cascade disruption events are often scant, uncertain or lacking. This lack of conclusive evidential information has often been the reason not to pursue systematic analysis or event recording – ultimately failing to fathom and explore disruption events systematically and thus providing the very foundation that would underpin proper planning, strategy and enhanced power system resilience.

Therefore, it is necessary to use the best information available for an event while not rendering the method useless whenever important data or information cannot be obtained. The following methodology aims to balance sound event information without faltering when key information is unobtainable. Uncertainty and inexactness are, after all, part of most engineering problems and are all too common when the unplanned and the unexpected occur.

The following sections will develop a suggested method for obtaining meaningful values for constructing the event trajectory,

$$\text{Ɛ}(t) \;=\; \text{Э}(t) + \text{Я}(t) \tag{15}$$

that will form the basis for calculating the event severity, Ƨ.

6.3.3 Progression Vectors

In the preceding sections, six categories of so-called erosion factors were discussed – aspects that cause the integrity of a power system to become eroded. These erosion factors are:

F_1 – Power output lost from a unit or generation facility

F_2 – Operational reserve range that was lost

F_3 – Reactive Power disruption at the node in the power system

F_4 – Inertia lost from a unit or generation facility

F_5 – Automatic frequency control

F_6 – Specific power system support functions

Assuming that each of these erosion factors can be expressed as a single numerical scalar value for a given increment in the event progression, then it is possible to express the erosion (or restoration) at the given increment as a vector containing the individual erosion factors associated with that increment, as

$$\overline{\text{ꟼ}}_{t=i} \;=\; \left(F_{1|t=i},\, F_{2|t=i},\, F_{3|t=i},\, F_{4|t=i},\, F_{5|t=i},\, F_{6|t=i}\right) \tag{18}$$

for time increment i in the event progression – with $\overline{q}_{t=i}$ being the progression vector.

Every increment in the progression of a cascade disruption event can similarly be expressed with a specific progression vector associated with that specific increment of the event.

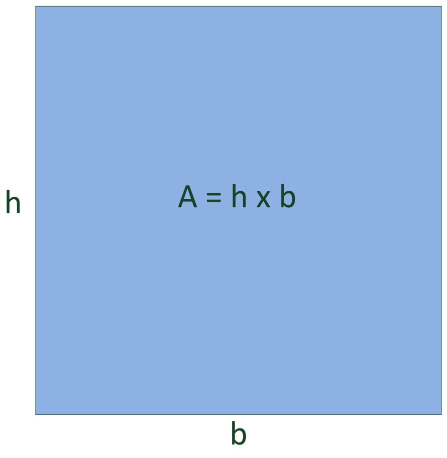
To be able to eventually compare different disruption events with one another, it is necessary to introduce the convention that all erosion factors are zero at the start of the disruption or

$$\overline{q}_{t=0} = (0, 0, 0, 0, 0, 0).$$

6.3.4 Vector Reduction

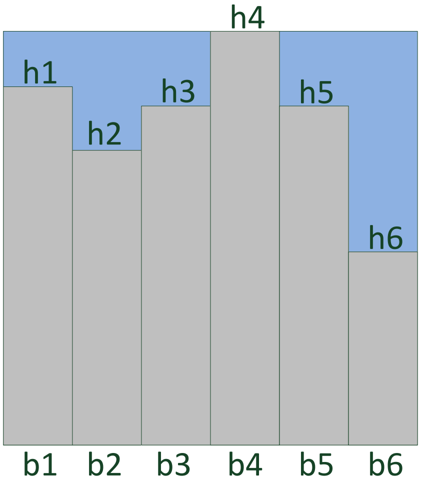
Although the progression vector, $\overline{q}_{t=i}$, is a comprehensive expression of the erosion in power system integrity at time increment i of the disruption event, the extent of the erosion is not readily apparent when comparing the vectors at two separate increments. Therefore, it is necessary to simplify the vector expression of erosion.

It is possible to visualise the integrity of a power system as a channel through which electricity is to be transmitted between various participants, not unlike a pipe through which liquid could be transported. Assuming that the channel is rectangular (or square) in shape, the cross-sectional area of the channel can readily be calculated, visually represented below.



This channel can be conceptualised as the integrity of the power system before the start of a cascade disruption event. The throughput of a hypothetical liquid through an imaginary conduit is a maximum when none of the conduit's boundaries are being encroached upon.

When a disruption event occurs, the integrity of the power system would become eroded, similar to the throughput capacity of a conduit of which the cross-sectional area is reduced. Because there are six erosion factors listed above, they could correspond to six individual sections of the channel that reduce in dimension, as illustrated below.



The rectangular channel has been reduced in size – each of the six sections into which the channel has been divided has been reduced to a different extent, yielding six sets of h and b values that can be used to calculate a new effective cross-sectional area as

$$A_i = h_{1|i} \times b_{1|i} + h_{2|i} \times b_{2|i} + h_{3|i} \times b_{3|i} + h_{4|i} \times b_{4|i} + h_{5|i} \times b_{5|i} + h_{6|i} \times b_{6|i}$$

for increment i of the event progression. Because the breadth, b, of the channel has been divided into equispaced sections, the equation can be reduced to

$$A_i = b_i \cdot (h_{1|i} + h_{2|i} + h_{3|i} + h_{4|i} + h_{5|i} + h_{6|i})$$

with

$$b_i = b_1 = b_2 = b_3 = b_4 = b_5 = b_6.$$

In this way, each increment i in the progression of the disruption event can be quantified to an equivalent cross-sectional area, A_i, that are based on the progression vector, $\overline{q}_i$, associated with that specific increment.

In this way, the values of A_i become the values used to construct the event trajectory $\text{Ɛ}(t)$. This means that,

$$\text{Ɛ}_i = A_i$$

but

$$\text{Ɛ}_i = \text{Э}_i + \text{Я}_i$$

$$\therefore\ A_i = \text{Э}_i + \text{Я}_i$$

But using this technique, the severity, Ƨ, of the event can readily be determined.

Note that the breadth associated with any of the erosion factors may be increased relative to others, thereby increasing the weight of such an erosion factor over others (if deemed appropriate) – the appropriate variations need to be made in the calculation to accommodate such an approach.

6.3.5 Incomplete Progression Vectors

Complete and accurate data for scientific and engineering calculations have always been the holy grail of analytic study. To this end, experiments are designed and planned to provide data with sufficient accuracy to enable subsequent analysis. Disruption events are not experiments conducted in laboratories under controlled circumstances where parameter variation can be limited or controlled, thus allowing for repeatable results.

The absence of complete and accurate data is often the reason for not endeavouring to analyse real-life occurrences, being inherently bereft of data with the desired level of integrity. And cascade failure events are no exception. These events are plagued by large gaps in data and often do not have the certainty that would guarantee reasonable assurance in a calculated outcome.

Unlike science itself, engineering is often less exact and generally relies on reasonable assumptions, thus avoiding the stalemate of being unable to derive an answer or solution. Although such assumptions have often proved most valuable, the question remains: How to deal with situations where assumption and estimation are entirely nonsensical?

This exact question is a recurring phenomenon in the analysis of disruption events. Every increment in the progression of the event requires six elements in its 1×6 progression vector to definitively describe the increment, but due to the nature of disruption events, it is often found that elements of the progression vector are unknown or highly uncertain, sometimes defying the possibility of reasonable assumption or estimation.

This dilemma often prohibits any endeavour to analyse disruption events, thus failing to properly study these events to establish an empirical knowledge base that could inform long-term strategy and operational mitigation tactics. To breach this barrier of lacking data elements, a deliberate workaround needs to be introduced in the methodology.

To circumvent the problem of lacking data elements in a progression vector, $\overline{\mathcal{q}_i}$, for a given step in the event progression, the data element is merely omitted from the vector, thus changing the vector from a 1×6 vector to a 1×5 vector. However, this change in the order of the vector needs to be compensated for during the vector reduction described above. For an 1×6 progression vector each element of the vector will be weighted at $\frac{1}{6}$ while a fraction of $\frac{1}{5}$ would apply to a 1×5 progression vector, signifying a 20% increase in the relative weight of the individual elements of the progression vector towards the overall value of the reduced vector.

6.3.6 Time Series Spacing

It is customary and even desirable when using statistical methods that the intervals selected on the x-axis of a graph or function are equispaced. Although such an equispaced distribution of data points is analytically ideal, the nature of cascade disruption events seldom allows for such a uniform distribution.

In the case of disruption events, the x-axis is typically a time-axis. Some of the many factors that present obstacles in the spacing of the time series include:

- Differing recording devices and technologies
- Lack of time synchronisation across recording and logging devices
- Different time resolution of various recording and logging devices
- Unpredictable, random and uncoordinated nature of event progression
- Vastly different time scales for events and restoration, often many orders of magnitude
- Data uncertainty during inter-incremental time durations
- Gaps and losses in the continuity of data sets due to device interruption and malfunction
- Conflicting data across various data platforms and devices

One of the initial objectives for developing a *severity* measure is that the method should be rigorous and not falter due to imperfect and sub-ideal circumstances. Therefore, the x-axis spacing (time increment spacing) is accepted to be non-uniform. This means that the time spacing between the inflexion points (or knee-points) of the event trajectory, $\mathcal{E}(t)$, are to be non-uniform. This implies that the event trajectory would be evaluated only at every point of interest as the event unfolded – typically at those points where abrupt changes occurred, such as tripping or switching events.

This has significance during the calculation of the severity, Ƨ, since it involves calculating the area of trapezoidal surfaces. The non-uniformity of the time-axis spacing requires that the base dimension of each trapezium need to be accounted for while calculating the value of Ƨ.

6.3.7 Case Study – Severity

To illustrate the method detailed above using a real event, the severity will now be calculated for an actual case study of a disturbance event that occurred on 19 April 2022. A high-level event log is provided in Annexure 1. The reason for choosing this example is that the entire event plays out during a one-hour interval, making it an ideal case study from a demonstration point of view.

At about 17:00, with the evening peak approaching, various gas turbine peaking units were being called up from the cold reserve. The specific units being dispatched were from two Eskom power stations, Ankerlig and Gourikwa Power Stations, and from two IPP Power Stations, Avon and Dedisa Power Stations. For industrial gas turbine units, the unit start-up time typically ranges between 10 minutes and 20 minutes, depending on various factors.

At 17:01:20, unit 4 at Lethabo Power Station tripped, causing the frequency to decay from 50,17 Hz to 49,79 Hz. However, due to a prior call-up of gas turbine units, two Gourikwa units synchronised in short succession thereafter, one at 17:03 and the next at 17:06.

At 17:07, unit 5 of Medupi Power Stations tripped due to an unrelated cause, resulting in a low frequency of 49,5 Hz. From 17:08 to 17:21, seven gas turbine units synchronise to the power system. However, at 17:24, Lethabo 3 trips due to the same initiating event of unit 4 earlier, with a resulting frequency minimum of 49,63 Hz. Seven more gas turbine units synchronised to the power system for the remainder of the hour (until 18:00).

The total power sent out on the power system during the hour of this event is shown in the following recording.

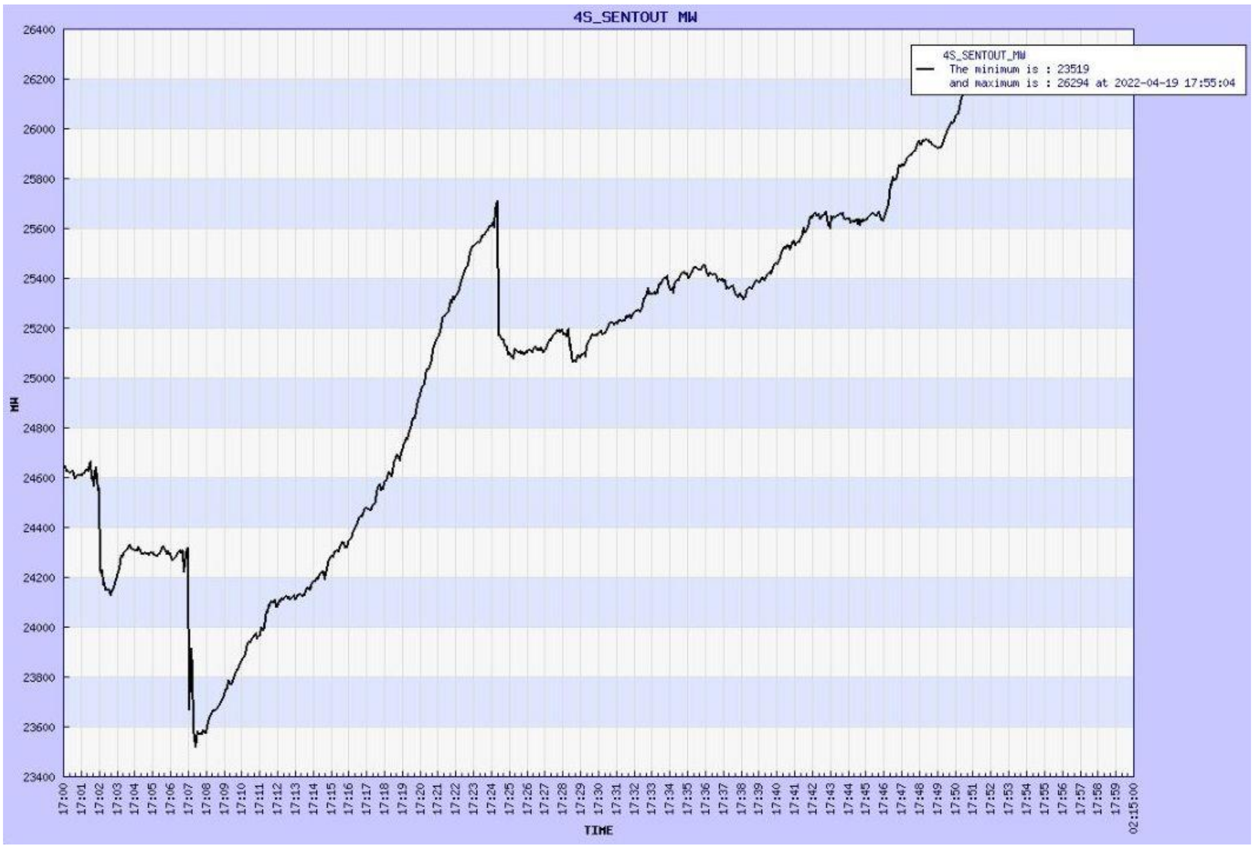


Figure 117: Total power system power send out for the Lethabo event of 19 April 2022

As a means of illustrating the method of determining the severity of the event, Ɛ, the significant points that occurred during the event's progression are taken to be every trip and every synchronisation of a unit. In addition, the actual frequency minima were used as additional data points for analysis purposes, since significant frequency decays occurred following each unit that tripped.

Since the case study example is relatively simple (from a power system perspective), only the two most significant erosion factors, the total generation capacity of the synchronised fleet of generating units and the total kinetic energy of the synchronised fleet, have been used for analysis.

This approach resulted in two-dimensional progression vectors at each point of interest. The following graph shows the progression of the two erosion factors over the one-hour window of analysis, i.e., from 17:00 to 18:00.

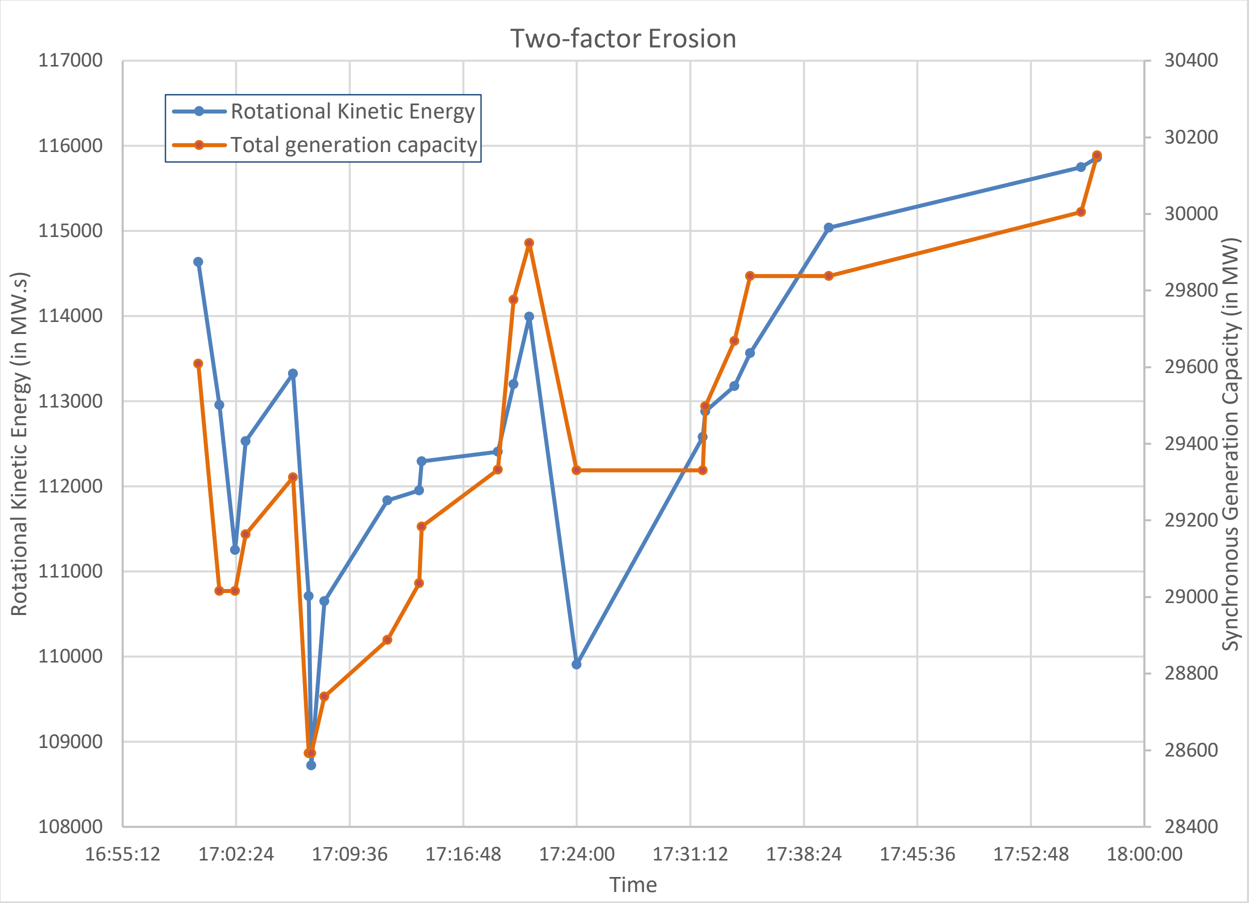


Figure 118: Kinetic energy and total generation capacity for the Lethabo event of 19 April 2022

Using 22 data points (points of interest) during the progression of the event, erosion values were determined for both the rotational kinetic energy and the total generation capacity that was synchronised to the power system. Both losses from the coal-fired units and gains from the gas turbine units were quantified. Using equal weighting for these two erosion factors, the erosion in system integrity was calculated incrementally at each point of interest, yielding the event trajectory shown in the following graph.

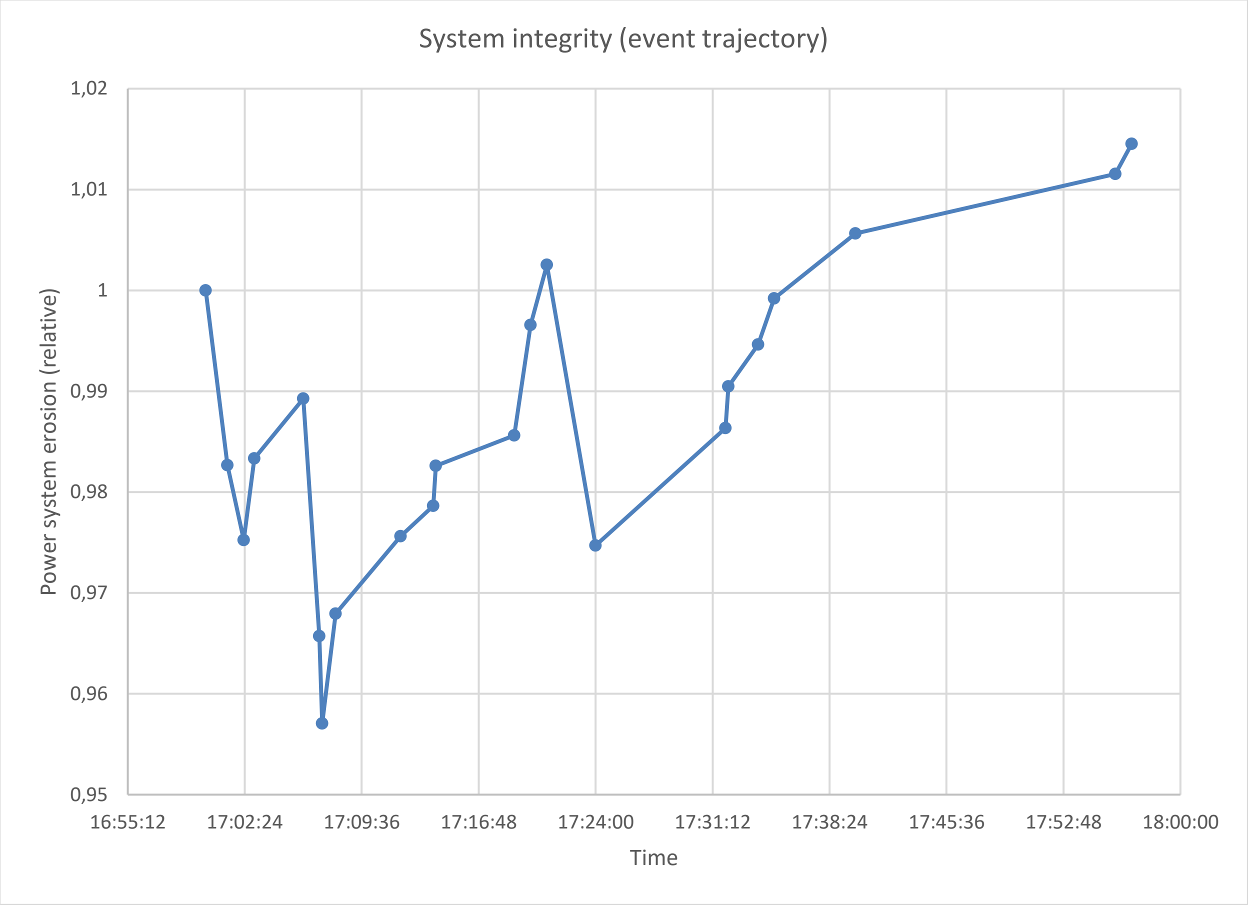


Figure 119: Erosion (and recovery) in power system integrity for the Lethabo event of 19 April 2022

In the event trajectory shown above, the y-axis value of 1 is used as the base integrity at time zero, used as the reference point for all erosion and restoration calculations throughout the hour of the event. In terms of multiple disruption events, this event is not significant, neither from a time or an intensity perspective. This is also evident from the event trajectory above that the most severe erosion level occurred at 17:07:10 following the trip of Medupi 5. The kinetic energy and the total generation capacity were at their respective minima, yielding an erosion in integrity of 4,3%.

After having determined each coordinate of the event trajectory, the severity could be calculated using:

$$\text{Ƨ} = \int_{t=0}^{t=r} |\mathcal{E}(t)| \cdot dt = \int_{t=0}^{t=r} |[\, \text{Э}(t) + \text{Я}(t) \,]| \cdot dt \qquad (17)$$

from section 6.3.1. Applying the trapezoidal rule for numerical integration, the overall event severity was calculated as [192]:

$$\text{Ƨ} = 36{,}9$$

Note that the number of erosion factors used to construct the progression vectors may vary, hence the unit of Ƨ vary between cases. Therefore, it is merely stated as *erosion-minutes*, or a variant thereof (e.g. *erosion-hours*, *erosion-days*, etc.). In this example, the severity of the event is $\text{Ƨ}=36,9$ erosion-seconds.

Time denotation is important for scaling when comparing different events. As a refinement to the notation used, a left-hand subscript and superscript are introduced, indicating the maximum and minimum number of erosion factors used in the *severity* assessment over the event progression. For this example, using the convention of this notation, the *severity* of the event is stated as ${}^{2}_{2}\text{Ƨ}=39,9$ erosion-seconds, using two erosion factors consistently in all 22 progression vectors. In other words, the combination of the subscript and superscript indicates the consistency and depth to which the assessment of *severity* has been undertaken.

6.4 Positive Yield

Large-scale disruption events are highly undesirable, and their avoidance consumes considerable resources internationally. Therefore, it is not apparent how such events can be regarded as making any positive contribution.

However, despite the risk and adversity associated with large-scale cascade disruption events, it represents one of the most valuable treasures of information that cannot be obtained through any other means.

As illustrated thus far, the field of disruption events is vast, and the number of measures required to mitigate such risks is extensive. It is nigh impossible to exhaustively validate such mitigation measures despite efforts to perform testing, conduct simulations using extensive models, conduct inspections and surveys, monitor vast arrays of real-time parameters, etc. Section 3.1 showed that the blackout events occurring internationally are not declining. Indications are that the blackout incidence rate is increasing despite the abovementioned measures.

If the measures that are mentioned above were effective, the incidence rate for blackouts should decline – it does not. Therefore, the only logical deduction that can be drawn is that the measures that are intended to provide assurance and that are the culmination of recommendations obtained out of the investigations into a great many blackout events from all over the world are not effective and fail to provide acceptable (and believable) assurance levels.

Therefore, another means should be obtained to provide insight into the threat of power system blackout events. Large-scale disruption events present a unique opportunity to determine the effectiveness of countermeasures, mitigation strategies, operational tactics, and contingency planning [193].

Large-scale disruption events are nothing less than data eruptions – events spewing out vast quantities of data from which a wealth of highly relevant information can be extracted. But, tests, simulated modelling, plant audits and surveys, etc., all have a fundamental weakness – "*how representative are the results to an actual event?*" Large-scale disruption events do not suffer from that specific weakness. It is an actual event. And although the scale may be different, results are inherently authentic.

Tests can never genuinely represent actual events; some obvious reasons are listed below.

- Plants subjected to testing are carefully prepared to be in an optimal state of readiness with all redundancies available.
- Tests are often carried out shortly after the process control has undergone optimisation and ensure a near-ideal response from the process and the control systems.
- Staffing is meticulously selected to be of the highest competency level.
- Staffing numbers are increased for the purpose of testing as a contingency measure.
- Emergency systems are verified to be available and on standby prior to a test.
- The plant that will be subjected to the test is isolated from other (sometimes adjacent) plants to ensure that the extent of the ramifications is minimised even if the test fails.
- The time of the test is selected so that the impact of a failed result will have minimal impact on the rest of the power system, e.g., ensuring sufficient reserves.
- Tests are initiated from a stable condition of operation (both the unit and the power system), avoiding exposure to a dynamic or transient condition.

When large-scale disruption events are treated as information capsules, rather than a mere nuisance that need to be recovered from so that normal operations can resume, much value can be extracted, specifically regarding strategic improvements for future planning.

The potential benefit that could be derived from large-scale disruption events are vast, should an approach of systematic extraction of information be adopted as an assurance and validation framework. Some of the areas that can benefit from such an approach is contained in Annexure 3.

Large-scale disruption events should be viewed as a most valuable resource in the management of power systems – the value of which cannot be overemphasised…

6.5 Summary

The disruption space in which multiple-generation disruption events feature is largely devoid of suitable metrics to aid in quantification and subsequent comparison across events. The reason for this is complex and has been discussed earlier in various sections.

Consider, for example, that two earthquakes could readily be compared with one another using the Richter scale, regardless of spatial or temporal considerations. However, for large scale disruption events, comparison is less trivial where events occurred in different geographic regions or when events occurred several decades apart – or both.

Suitable metrics are lacking and therefore had to be developed. In this section, two methods have been developed, both entirely independent of the nature of the power system where the event occurred. Firstly, a means was developed to assess the *impact* of an event, and this method was extended to provide three different metrics (first, second, and third-order) that can be elected, depending on the purpose intended.

Secondly, a method was developed for assessing the *severity* of an event based on the degree to which the event eroded the integrity of the power system and the countermeasures taken to recover from it. The *severity* of an event could potentially be used to analyse any event using the state of the power system just before event inception as a baseline against which the event starts to erode the integrity of the power system.

Both methods for *impact* and *severity* are fundamentally normalisations, evaluating each event relative to the specific power system at the time when the even occurred. Therefore, these metrics remain applicable regardless of the size of the power system or any other factors that normally would be regarded as limitations.

Ultimately, the fact that large-scale disruption events can be utilised as a highly beneficial aid in developing more resilient power systems in the future should not be disregarded.

7. Conclusion

Events, where multiple generation resources are compromised, may lead to disruptions of entire interconnected power systems. However, as a specific class of power system disturbances, multiple generation disruption events are not internationally recognised as being a special class of event. However, since power stations and power generating units are distinctly different from transmission and distribution systems, investigating their disruptions requires a completely different approach, tools and methods, different forms of analysis and different expertise.

In concluding this work, salient material will be synoptically emphasised, and unique contributions to this specific field of study will be accentuated.

7.1 Contextualisation

In introducing a specific branch of study that does not enjoy universal recognition, sufficient context needs to be provided. The context has followed a systematic approach in elucidating specific perspectives that have bearing on multiple generation disruption events, which are listed below.

a Early manifestations of power system disruptions caused by cascading losses in power generation.
b The evolution of power systems and power stations from the inception of electricity as a separate and unique technology, to their current incarnations.
c The South African electricity industry is typical in many respects of its counterparts globally. It is highly equivalent to most of the larger power systems.
d How various power generation technologies contribute to, and becomes disrupted by, cascade failure events.
e The regulatory landscapes from many international power systems.
f African grid codes in terms of their regulatory requirements.
g Major power system disturbances and blackout events across the world.
h Analysis of a typical large-scale power system blackout in the United States, focusing on the contributions of the power generation base.
i Functional composition and vulnerabilities of power station systems.
j Introduction of redundancy and commonality within power stations.
k. Generation plant hierarchical classification and design approach.

Eventually, having established a fundamental context for the practice and historical background of power stations, the *system concept* was introduced, with the system as the fundamental building block of power stations in general. Subsequently, the concept of *process* as an ongoing and continuous activity was explored.

Various systems were also contextualised through descriptive narrative and graphic representations. System vulnerabilities were outlined, and examples of disruptions were provided.

An important distinction was introduced, namely that some disruptions are inherently contained locally within the boundaries of individual power stations, while others escalate to affect multiple power stations collectively. The disruptors were contextualised using further industry examples.

Once sufficient context was presented, a method was developed to generate suitable disruption metrics to aid in analysing and managing the cascade generation disruption threat.

7.2 Unique Contributions

Various contributions expanded the field of power station practice and the study of power generation disruptions. The contributions are outlined below.

a Power stations could be classified based on their design philosophies and the incorporation of redundancy and resilience principles. To embody this approach, the concept of generations of power stations was introduced, with five generations identified and outlined. The concept of power station generation has facilitated the contextualisation of the evolution of power stations for more than a century.

b The risk of coincidental tripping of multiple generating units through unrelated causes has traditionally not been considered due to an absence of supporting empirical evidence. However, as more such examples started to mount, the question of whether such a risk had legitimate merit was analysed.

Using an extensive event record of unit trip data from the South African power system, the probability density function could be determined as a specific gamma function that was not recognised before.

$$y = f(x|\alpha,\beta) = \frac{1}{\beta^{\alpha}\Gamma(\alpha)} x^{\alpha-1} e^{\frac{-x}{\beta}} \quad \forall x \in [0,\infty)$$

with α and β, within a 99% confidence interval and with a log-likelihood of -56130, estimated at:

	Estimate	**Standard Error**
$\boldsymbol{\alpha}$	0,627	0,009
$\boldsymbol{\beta}$	2 287,4	47,970

With this new insight, the extent to which the mean time between units becomes unavailable due to failure could be quantified in the South African power system, data that is useful for risk assessment and planning purposes.

c Recognising and separating multiple generation disruption events into two main categories, namely intra-station and inter-station escalation events, demonstrating the different disruption modes with actual case study evidence. Both categories were contextualised and the differences in their nature was illustrated using case study information of actual events.

d Contextualising system commonalities that expose power stations, and therefore the power system, to disruption and providing copious examples of actual disruption events for each case. Although all large scale cascade disruption events are inherently undesirable, those that exceeds the grid code limitations have been shown to pose the greatest risk to the power system.

e Identifying the threat of distributed intelligence in modern power systems and power stations as a specific and unique class of disruption not associated with the electrical, mechanical or process dynamics or transient characteristics. Suitable terminology was introduced to distinguish between aberrant event branching and the deterministic cascading mechanisms.

f In a specific and distinct field of study, suitable metrics for analysis were devoid, so various metrics were developed.

  i The introduction of a second-order metric for the *impact* of an event, using the concept of an *event angle* ∠Ж. This metric could be applied directly to different disruption events for comparison purposes. It was shown that the value could be used directly to assess grid code compliance when an entire power station was blacked out.

ii Developing a third-order metric for the *impact* of an event – referred to as the PID of the event. This method combines the power lost during an event, the rate at which the power loss occurred and the integral of the power loss throughout the event into a single number, the power cube (P^3). This metric is considered more comprehensive and encompassing than the event angle, although grid code compliance cannot be derived forthwith from the third-order value.

iii A method was developed and illustrated to determine the *severity* of a disruption event. It hinges on the concept that each generating unit that is compromised and trips during a disruption event causes the integrity of the power system to become eroded. The method provides a means of quantifying the erosion in practical terms and ultimately provides a single value for the *severity*, Ƨ.

g The erosion in power system integrity was condensed into six main erosion factors. Such erosion factors are ultimately used to construct various event identity curves known as trajectories. The *erosion trajectory* $\text{Э}(t)$, the *restoration trajectory* $\text{Я}(t)$ and the *event trajectory* $\text{Ɛ}(t)$, with:

$$\text{Ɛ}(t) \;=\; \text{Э}(t) + \;\text{Я}(t)$$

h Recognition has been given to incomplete and inaccurate data for disruption events. The method has been deliberately conceived for practical application in sub-ideal circumstances, wherein major generation disruption events invariably occur. To this end, the method tolerates the following practical imperfections that traditionally plague event analysis.

i Non-uniform time-axis data spacing
ii Variations in the number of known (or estimable) event parameters
iii Differences from one data point to another throughout the event progression

i Annexure 2 provides an investigation framework based on practical experience accumulated over decades of investigating major generation disruption events.

j Identifying areas that should be analysed after events to serve as a record for comparison against future and historical events in Annexure 3.

k Recognising that large-scale disruption events, detrimental as they are, present the very essence of gaining understanding and guiding the evolution toward resilient power systems of the future.

7.3 Further Research

Although this research laid the initial foundation for a systematic approach to the investigation of large scale power system disruption events, this field is largely untouched and unmapped in industry. As such there exists much scope for future research. Certain obvious topics that could benefit from further research include.

a. The effects of markets and regulatory landscapes on the resilience and vulnerability of interconnected power systems.

b. How the summary adoption of global narratives, like global climate change, impact on the electricity industry (including cost implications to industry), and

c. The development of a mitigation framework for the threat posed by pervasive distributed intelligent devices in modern power systems and generation facilities.

7.4 Concluding Remarks

The threat of large-scale power system disruptions will remain a reality and will likely increase over time. This risk category must receive greater attention from power station operators, power system operators, industry organisations (e.g., Cigré), and academia globally.

In terms of the specific threat category of multiple generation disruption and cascading failure, very little exists internationally in terms of:

a Investigation frameworks

b Metrics employed for benchmarking

c Management systems and techniques

d Event databases

e Trending and monitoring of both local and global events

f Pier involvement and collaboration

g Global information sharing

h Identifying emerging risk

i Industry standards

j Regulatory and technical guidance

As a major power system risk category, it suffers globally from:

a A lack of recognition as being a specific class of threat

b Regulatory content to govern the risk of multiple-contingency events

c Resources and management systems for capture, analysis and trending

d Research programs to contribute and develop the level of understanding

e International platforms and coordination

f Practitioner base having skill and capability to contribute

g Strategic roadmaps towards greater resilience and diminishing risk

Much development and research are required, and power utilities, independent power producers, universities, power system operators, industry support organisations, and industry regulators must commit a great deal of time and effort to that end. Failing which, economic disruption and the resulting erosion of human well-being will continue unabated…

8. References

[1] National Energy Regulator of South Africa, *The South African Grid Code: The Network Code*, version 10.1, National Energy Regulator of South Africa, 2022.

[2] S.R. Conradie and L.J.M. Messerschmidt, *A Symphony of Power – The Eskom Story*, Eskom, 2000.

[3] Eskom, *Eskom Heritage Site*, http://heritage.eskom.co.za/, Eskom, 2022, accessed 2023.

[4] Electricity Supply Commission, *Report of the Commission covering the period 1st March to 31st December, 1923, with a brief review of its activities up to 9th August 1924*, Radford, Adlington, LTD., 1924.

[5] Electricity Supply Commission, *Second Annual Report of the Commission for the year ended 31st December, 1924 with a brief review of its activities up to 30th September 1925*, Radford, Adlington, LTD., 1925.

[6] Electricity Supply Commission, *Third Annual Report of the Commission for the year ended 31st December, 1925 with a brief review of its activities up to 30th September 1926*, Radford, Adlington, LTD., 1926.

[7] Electricity Supply Commission, *Fourth Annual Report of the Commission for the year ended 31st December, 1926 with a brief review of its activities up to 30th September 1927*, Radford, Adlington, LTD., 1927.

[8] Electricity Supply Commission, *Fifth Annual Report of the Commission for the year ended 31st December, 1927 with a brief review of its activities up to 30th June 1928*, Radford, Adlington, LTD., 1928.

[9] Electricity Supply Commission, *Sixth Annual Report of the Commission for the year ended 31st December, 1928 with a brief review of its activities up to 30th June 1929*, Radford, Adlington, LTD., 1929.

[10] Electricity Supply Commission, *Seventh Annual Report of the Commission for the year ended 31st December, 1929 with a brief review of its activities up to 30th April 1930*, Radford, Adlington, LTD., 1930.

[11] Electricity Supply Commission, *Eighth Annual Report of the Commission for the year ended 31st December, 1930 with a brief review of its activities up to 30th April 1931*, Radford, Adlington, LTD., 1931.

[12] Electricity Supply Commission, *Ninth Annual Report of the Commission for the year ended 31st December, 1931 with a brief review of its activities up to May 1932*, Radford, Adlington, LTD., 1932.

[13] Electricity Supply Commission, *Tenth Annual Report of the Commission for the year ended 31st December, 1932 with a brief review of its activities up to 30th April 1933*, Radford, Adlington, LTD., 1933.

[14] Electricity Supply Commission, *Eleventh Annual Report of the Commission for the year ended 31st December, 1933 with a brief review of its activities up to 31st May 1934*, Radford, Adlington, LTD., 1934.

[15] Electricity Supply Commission, *Twelfth Annual Report of the Commission for the year ended 31st December, 1934 with a brief review of its activities up to 31st May 1935*, Radford, Adlington, LTD., 1935.

[16] Electricity Supply Commission, *Thirteenth Annual Report of the Commission for the year ended 31st December, 1935 with a brief review of its activities up to 31st May 1936*, Radford, Adlington, LTD., 1936.

[17] Electricity Supply Commission, *Fourteenth Annual Report of the Commission for the year ended 31st December, 1936 with a brief review of its activities up to 31st March 1937*, Radford, Adlington, LTD., 1937.

[18] Electricity Supply Commission, *Fifteenth Annual Report of the Commission for the year ended 31st December, 1937 with a brief review of its activities up to 31st March 1938*, Radford, Adlington, LTD., 1938.

[19] Electricity Supply Commission, *Sixteenth Annual Report of the Commission for the year ended 31st December, 1938 with a brief review of its activities up to 31st March 1939*, Radford, Adlington, LTD., 1939.

[20] Electricity Supply Commission, *Seventeenth Annual Report of the Commission for the year ended 31st December, 1939 with a brief review of its activities up to 31st March 1940*, Electricity Supply Commission of South Africa, 1940.

[21] Electricity Supply Commission, *Seventeenth Annual Report of the Commission for the year ended 31st December, 1940 together with a brief review of its activities up to 31st March 1941*, Electricity Supply Commission of South Africa, 1941.

[22] Electricity Supply Commission, *Nineteenth Annual Report of the Commission for the year ended 31st December, 1941*, Electricity Supply Commission of South Africa, 1942.

[23] Electricity Supply Commission, *Twentieth Annual Report of the Commission for the year ended 31st December, 1942*, Electricity Supply Commission of South Africa, 1943.

[24] Electricity Supply Commission, *Twenty-first Annual Report of the Commission for the year ended 31st December, 1943 with a brief review of its activities up to 30th April 1944*, Electricity Supply Commission of South Africa, 1944.

[25] Electricity Supply Commission, *Twenty-second Annual Report of the Commission for the year ended 31st December, 1944 with a brief review of its activities up to 30th April 1945*, Electricity Supply Commission of South Africa, 1945.

[26] Electricity Supply Commission, *Twenty-third Annual Report of the Commission for the year ended 31st December, 1945 with a brief review of its activities up to 30th April 1946*, Electricity Supply Commission of South Africa, 1946.

[27] Electricity Supply Commission, *Twenty-fourth Annual Report of the Commission for the year ended 31st December, 1946 with a brief review of its activities up to 30th April 1947*, Electricity Supply Commission of South Africa, 1947.

[28] Electricity Supply Commission, *Twenty-fifth Annual Report of the Commission for the year ended 31st December, 1947 with a brief review of its activities up to 30th April 1948*, Electricity Supply Commission of South Africa, 1948.

[29] Electricity Supply Commission, *Twenty-sixth Annual Report of the Commission for the year ended 31st December, 1948 with a brief review of its activities up to 30th April 1949*, Electricity Supply Commission of South Africa, 1949.

[30] Electricity Supply Commission, *Twenty-seventh Annual Report of the Commission for the year ended 31st December, 1949 with a brief review of its activities up to 30th April 1950*, Electricity Supply Commission of South Africa, 1950.

[31] Electricity Supply Commission, *Twenty-eighth Annual Report of the Commission for the year ended 31st December, 1950 with a brief review of its activities up to 30th April 1951*, Electricity Supply Commission of South Africa, 1951.

[32] Electricity Supply Commission, *Twenty-ninth Annual Report of the Commission for the year ended 31st December, 1951 with a brief review of its activities up to 30th April 1952*, Electricity Supply Commission of South Africa, 1952.

[33] Electricity Supply Commission, *Thirtieth Annual Report of the Commission for the year ended 31st December, 1952 with a brief review of its activities up to 30th April 1953*, Electricity Supply Commission of South Africa, 1953.

[34] Electricity Supply Commission, *Thirty-first Annual Report of the Commission for the year ended 31st December, 1953 with a brief review of its activities up to 30th April 1954*, Electricity Supply Commission of South Africa, 1954.

[35] Electricity Supply Commission, *Thirty-second Annual Report of the Commission for the year ended 31st December, 1954 together with brief references to important events up to 30th April 1955*, Electricity Supply Commission of South Africa, 1955.

[36] Electricity Supply Commission, *Thirty-third Annual Report of the Commission for the year ended 31st December, 1955 including brief comments on important developments up to the 30th April 1956*, Electricity Supply Commission of South Africa, 1956.

[37] Electricity Supply Commission, *34th Annual Report of the Commission for the year ended 31st December, 1956 and includes brief comments on important developments up to the 30th April 1957*, Electricity Supply Commission of South Africa, 1957.

[38] Electricity Supply Commission, *Thirty-fifth Annual Report of the Commission for the year ended 31st December, 1957*, Electricity Supply Commission of South Africa, 1958.

[39] Electricity Supply Commission, *Thirty-sixth Annual Report and the Accounts covering its work during the financial year ended at the 31st December, 1958*, Electricity Supply Commission of South Africa, 1959.

[40] Electricity Supply Commission, *Thirty-seventh Annual Report and the Accounts covering its work during the financial year ended at the 31st December, 1959*, Electricity Supply Commission of South Africa, 1960.

[41] Electricity Supply Commission, *Thirty-eighth Annual Report and the Accounts covering its work during the financial year ended at the 31st December, 1960*, Electricity Supply Commission of South Africa, 1961.

[42] Electricity Supply Commission, *Thirty-ninth Annual Report and the Accounts covering its work during the financial year ended at the 31st December, 1961*, Electricity Supply Commission of South Africa, 1962.

[43] Electricity Supply Commission, *Fortieth Annual Report and the Accounts covering its work during the financial year ended at the 31st December, 1962*, Electricity Supply Commission of South Africa, 1963.

[44] Electricity Supply Commission, *Forty-first Annual Report and the Accounts covering its work during the financial year ended at the 31st December 1963*, Electricity Supply Commission of South Africa, 1964.

[45] Electricity Supply Commission, *Forty-second Annual Report and the Accounts covering its work during the financial year ended at the 31st December, 1964*, Electricity Supply Commission of South Africa, 1965.

[46] Electricity Supply Commission, *Forty-third Annual Report and the Accounts covering its work during the financial year ended at the 31st December, 1965*, Electricity Supply Commission of South Africa, 1966.

[47] Electricity Supply Commission, *Forty-fourth Annual Report and the Accounts covering its work during the financial year ended at the 31st December, 1966*, Electricity Supply Commission of South Africa, 1967.

[48] Electricity Supply Commission, *Forty-fifth Annual Report and the Accounts covering its work during the financial year ended at the 31st December, 1967*, Electricity Supply Commission of South Africa, 1968.

[49] Electricity Supply Commission, *Forty-sixth Annual Report and the Accounts covering its work during the financial year ended at the 31st December, 1968*, Electricity Supply Commission of South Africa, 1969.

[50] Electricity Supply Commission, *Forty-seventh Annual Report and the Accounts covering its work during the financial year ended at the 31st December, 1969*, Electricity Supply Commission of South Africa, 1970.

[51] Electricity Supply Commission, *Forty-eighth Annual Report and the Accounts covering its work during the financial year ended at the 31st December, 1970*, Electricity Supply Commission of South Africa, 1971.

[52] Electricity Supply Commission, *Forty-ninth Annual Report and the Accounts covering its work during the financial year ended at the 31st December, 1971*, Electricity Supply Commission of South Africa, 1972.

[53] Electricity Supply Commission, *ANNUAL REPORT for the year ended 31st December, 1972 with a review of activities to April 1973*, Electricity Supply Commission of South Africa, 1973.

[54] Electricity Supply Commission, *Fifty-first Annual Report and the Accounts covering its work during the financial year ended 31st December, 1973*, Electricity Supply Commission of South Africa, 1974.

[55] Electricity Supply Commission, *Fifty-second Annual Report and the Accounts covering its work during the financial year ended 31st December, 1974*, Electricity Supply Commission of South Africa, 1975.

[56] Electricity Supply Commission, *Fifty-third Annual Report and the Accounts covering its work during the financial year ended 31st December, 1975*, Electricity Supply Commission of South Africa, 1976.

[57] Electricity Supply Commission, *Fifty-fourth Annual Report and Financial Statements covering its work during the financial year ended 31st December, 1976*, Electricity Supply Commission of South Africa, 1977.

[58] Electricity Supply Commission, *Fifty-fifth Annual Report and Financial Statements covering its work during the financial year ended 31st December, 1977*, Electricity Supply Commission of South Africa, 1978.

[59] Electricity Supply Commission, *Fifty-sixth Annual Report and Financial Statements covering its work during the financial year ended 31st December, 1978*, Electricity Supply Commission of South Africa, 1979.

[60] Electricity Supply Commission, *Fifty-seventh Annual Report and Financial Statements covering its work during the financial year ended 31st December, 1979*, Electricity Supply Commission of South Africa, 1980.

[61] Electricity Supply Commission, *Fifty-eighth Annual Report and Financial Statements covering its work during the financial year ended 31st December, 1980*, Electricity Supply Commission of South Africa, 1981.

[62] Electricity Supply Commission, *Fifty-ninth Annual Report and Financial Statements covering its work during the financial year ended 31st December, 1981*, Electricity Supply Commission of South Africa, 1982.

[63] Electricity Supply Commission, *Sixtieth Annual Report and Financial Statements covering its work during the financial year ended 31st December, 1982*, Electricity Supply Commission of South Africa, 1983.

[64] Electricity Supply Commission, *Sixty-first Annual Report of the Electricity Supply Commission for the year ending 31 December 1983,* Electricity Supply Commission of South Africa, 1984.

[65] Electricity Supply Commission, *Sixty-second Annual Report and Financial Statements covering its work during the financial year ended 31 December, 1984*, Electricity Supply Commission of South Africa, 1985.

[66] Escom, *Escom Annual Report 1985*, Escom, 1986.

[67] Escom, *Escom Statistical Yearbook 1985*, Escom, 1986.

[68] Escom, *Escom Annual Report 1986*, Escom, 1987.

[69] Escom, *Escom Statistical Yearbook 1986*, Escom, 1987.

[70] Eskom, *Eskom Annual Report 1987*, Eskom, 1988.

[71] Eskom, *Eskom Statistical Yearbook 1987*, Eskom, 1988.

[72] Eskom, *Eskom Annual Report 1988*, Eskom, 1989.

[73] Eskom, *Eskom Statistical Yearbook 1988*, Eskom, 1989.

[74] Eskom, *Eskom Annual Report 1989*, Eskom, 1990.

[75] Eskom, *Eskom Statistical Yearbook 1989*, Eskom, 1990.

[76] Eskom, *Eskom Annual Report 1990*, Eskom, 1991.

[77] Eskom, *Eskom Statistical Yearbook 1990*, Eskom, 1991.

[78] Eskom, *Eskom Annual Report 1991*, Eskom, 1992.

[79] Eskom, *Eskom Statistical Yearbook 1991*, Eskom, 1992.

[80] Eskom, *Eskom Annual Report 1992*, Eskom, 1993.

[81] Eskom, *Eskom Statistical Yearbook 1992*, Eskom, 1993.

[82] Eskom, *Eskom Annual Report 1993*, Eskom, 1994.

[83] Eskom, *Eskom Statistical Yearbook 1993*, Eskom, 1994.

[84] Eskom, *Eskom Annual Report 1994*, Eskom, 1995.

[85] Eskom, *Eskom Statistical Yearbook 1994*, Eskom, 1995.

[86] Eskom, *Eskom Annual Report 1995*, Eskom, 1996.

[87] Eskom, *Eskom Statistical Yearbook 1995*, Eskom, 1996.

[88] Eskom, *Eskom Annual Report 1996*, Eskom, 1997.

[89] Eskom, *Eskom Statistical Yearbook 1996*, Eskom, 1997.

[90] Eskom, *Eskom Annual Report 1997*, Eskom, 1998.

[91] Eskom, *Eskom Annual Report 1998*, Eskom, 1999.

[92] Eskom, *Eskom Annual Report 1999*, Eskom, 2000.

[93] Eskom, *Eskom Annual Report 2000*, Eskom, 2001.

[94] Eskom, *Eskom Annual Report 2001*, Eskom, 2002.

[95] Eskom, *Eskom Annual Report 2002*, Eskom, 2003.

[96] Eskom, *Eskom Annual Report 2003*, Eskom, 2004.

[97] Eskom, *Eskom Annual Report 2005*, Eskom, 2005.

[98] Eskom, *Eskom Annual Report 2006*, Eskom, 2006.

[99] Eskom, *Eskom Annual Report 2007*, Eskom, 2007.

[100] Eskom, *Eskom Annual Report 2008*, Eskom, 2008.

[101] Eskom, *Eskom Annual Report 2009*, Eskom, 2009.

[102] Eskom, *Eskom Integrated Report 2010*, Eskom, 2010.

[103] Eskom, *Eskom Integrated Report 2011*, Eskom, 2011.

[104] Eskom, *Eskom Integrated Report 2012*, Eskom, 2012.

[105] Eskom, *Eskom Integrated Report 2013*, Eskom, 2013.

[106] Eskom, *Eskom Integrated Report 2014*, Eskom, 2014.

[107] Eskom, *Eskom Integrated Report 2015*, Eskom, 2015.

[108] Eskom, *Eskom Integrated Report 2016*, Eskom, 2016.

[109] Eskom, *Eskom Integrated Report 2017*, Eskom, 2017.

[110] Eskom, *Eskom Integrated Report 2018*, Eskom, 2018.

[111] Eskom, *Eskom Integrated Report 2019*, Eskom, 2019.

[112] Eskom, *Eskom Integrated Report 2020*, Eskom, 2020.

[113] Eskom, *Eskom Integrated Report 2021*, Eskom, 2021.

[114] Eskom, *Eskom Integrated Report 2022*, Eskom, 2022.

[115] R.G. Farmer and E.H. Allen, *Power System Dynamic Performance Advancement from History of North American Blackouts*, PSCE, 2006.

[116] O.I. Elgerd, *Electric Energy Systems Theory: An Introduction*, second edition, McGraw-Hill International Book Company, 1983.

[117] F.H.D. Conradie and A.C. Paterson, *Major Disturbances on the ESCOM Power System since 1975: Causes and Remedial Action,* SAIEE, 1979.

[118] L. Saribulut, G. Ok and A. Ameen, *A Case Study on National Electricity Blackout of Turkey*, Energies MDPI, 2023.

[119] M. Adibi, *Restoration in Sweden and Experience Gained from the Blackout of 1983*, Power, Energy, & Industry Applications, 2000.

[120] P. Gomes; A.C.S. de Lima and A. de Padua Guarini, *Guidelines for Power System Restoration in the Brazilian System*, IEEE Transactions on Power Systems, 2004.

[121] T. Ohno and S. Imai, *The 1987 Tokyo Blackout*, IEEE PSCE, 2006.

[122] U. Hain and I. Schweitzer, *Analysis of the Power Blackout of June 8, 1995 in the Israel Electric Corporation*, IEEE Transactions on Power Systems, 1997.

[123] O.P. Veloza and R.H. Cespedes, *Vulnerability of the Colombian Electric System to Blackouts and Possible Remedial Actions*, IEEE Power Engineering Society General Meeting, 2006.

[124] J.D. McCalley, *Operational Defence of Power System Cascading Outages*, IEEE PES T&D Conference and Exposition, 2006.

[125] M. Sanaye-Pasand, *Scrutiny of the Iranian National Grid*, IEEE Power and Energy Magazine, 2006.

[126] G. Andersson, P. Donalek; R. Farmer, N. Hatziargyriou, I. Kamwa; P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor and V. Vittal, *Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance*, IEEE Transactions on Power Systems, 2005.

[127] S. Corsi and C. Sabelli, *General Blackout in Italy Sunday September 28, 2003, h. 03:28:00*, IEEE Xplore.

[128] M. El-Werfelli, R. Dunn, M. Redfern and J. Brooks, *Analysis of the national 8th November 2003 Libyan blackout*, UPEC, 2008.

[129] C.D. Vournas, V.C. Nikolaidis and A.A. Tassoulis, *Postmortem Analysis and Data Validation in the Wake of the 2004 Athens Blackout*, IEEE Transactions on Power Systems, 2006.

[130] C.A. Ruiz, N.J. Orrego and J.F. Gutierrez, *The Colombian 2007 Black Out*, IEEE Power Engineering Society General Meeting, 2006.

[131] D.N. Efimov and N.I. Voropai, *Blackouts Analysis and Generalization*, 3rd Int. Workshop "Liberalization and Modernization of Power Systems; Risk Assessment and Optimization for Asset Management", Irkutsk, Russia, 2006.

[132] M.W. Younas and S.A. Qureshi, *Analysis of Blackout of National Grid System of Pakistan in 2006 and the Application of PSS and FACTS Controllers as Remedial Measures,* International Conference Electrical Engineering, 2007.

[133] C. Li, Y. Sun and X. Chen, *Analysis of the blackout in Europe on November 4, 2006*, International Power Engineering Conference, 2007.

[134] X. Chen, C. Deng, Y. Chen and C. Li, *Blackout prevention: Anatomy of the blackout in Europe*, International Power Engineering Conference, 2007.

[135] https://en.wikipedia.org/wiki/List_of_major_power_outages, accessed 2024.

[136] I.C. Decker, M.N. Agostini, A.S.E. Silva and D. Dotta, *Monitoring of a large scale event in the Brazilian Power System by WAMS*, Bulk Power System Dynamics and Control Symposium, 2010.

[137] H. Pidd, *India blackouts leave 700 million without power*, The Guardian, http://www.guardian.co.uk/world/2012/jul/31/india-blackout-electricity-power-cuts, 2012, accessed 2020.

[138] A.L. Jazeera, '*Countrywide blackout' plunges Pakistan into darkness*, Pakistan News, 2021.

[139] New York Independent System Operator, *Blackout August 14, 2003, Final Report*, NYISO, 2005.

[140] G.I. Maldonado, *The Performance of North American Nuclear Power Plants during the Electric Power Blackout of August 14, 2003*, IEEE, 2004.

[141] Clarion Energy Content Directors, *13 Years After: The Northeast Blackout of 2003 Changed Grid Industry, Still Causes Fear for Future,* https://www.power-grid.com/executive-insight/13-years-after-the-northeast-black-of-2003-changed-grid-industry-still-causes-fear-for-future/#gref, Power Grid International, 2016, accessed 2022.

[142] The State of Western Australia, *Electricity Access Network Codes*, 2004.

[143] The Irish Government, *EirGrid Grid Code*, 2011.

[144] National Grid Electricity Transmission plc, *The Grid Code*, 2012.

[145] Verband der Netzbetreiber - VDN – e.V. beim VDEW, *Network and System Rules of the German Transmission System Operators*, 2007.

[146] DIE ENERGIEKAMER VAN DIE NEDERLANDSE MEDEDINGINGSOUTORITEIT, *Systeemcode Elektriciteit*, 2012.

[147] Die Energiekamer van die Nederlandse Mededingingsoutoriteit, *Netcode Elektriciteit*, 2012.

[148] The Italian Authority for Electricity and Gas, Grid Code, 2012.

[149] The Hashemite Kingdom of Jordan National Electric Power Company, *NEPCO Transmission Grid Code*, 2004.

[150] NEPRA, *NEPRA Grid Code*, 2002.

[151] Southern African Power Pool, SAPP, https://www.sapp.co.zw, SAPP, 2021, accessed 2021.

[152] National Energy Regulator of South Africa, *The South African Grid Code: The System Operation Code*, 2022.

[153] Electricity Control Board, *Transmission Grid Code: Electricity Act 2007*, 2018.

[154] Zimbabwe Electricity Regulatory Commission, Zimbabwe Grid Code, 2005.

[155] Zambia Energy Regulation Board, *The Zambian Grid Code*, 2006.

[156] Southern African Development Community, *Southern African Power Pool Operating Guidelines*, 2011.

[157] Sudan Electricity Regulatory Authority, *Sudan Grid Code*, 2011.

[158] Rwanda Utilities Regulatory Agency, *The Rwanda Grid Code*, 2012.

[159] Uganda Electricity Regulatory Authority, *Statutory Instruments 2003 NO. 24: The Electricity (Primary Grid Code) Regulations*, 2003.

[160] Kenya Energy Regulatory Commission, *Kenya Electricity Grid Code*, 2008.

[161] Nigeria Electricity Regulatory Authority, *The Grid Code for the Nigeria Electricity Transmission System*.

[162] National Energy Regulator of South Africa, *The South African Grid Code: Governance Code*, 2022.

[163] M. Viljoen, *'n Omvattende nasionale bestuursraamwerk vir kragsteselbelemmering deur aaneengeskakelde ontwrigting van kragontwikkeling in Suid-Afrika*, North-West University, 2013.

[164] I. Miller and J.E. Freund, *Probability and Statistics for Engineers*, Prentice-Hall International Editions, 1985.

[165] L. Chizhova and B. Whitmore, *Ghosts of Russia's 'Kursk' Disaster Haunt Dam Accident*, RadioFreeEurope RadioLiberty, 2009.

[166] P.S. Neporozhny, *ТЕХНИЧЕСКОГО РАССЛЕДОВАНИЯ ПРИЧИН АВАРИИ, ПРОИСШЕДШЕЙ 17 АВГУСТА 2009 ГОДА*, RusHydro - Sayano-Shushenskaya HPP. 2009.

[167] R.P. Randall, *Precautions against Overspeeding of Turbo-Generators*, The Transactions of the SAIEE, SAIEE, 1965.

[168] Anonymous, *Generator Accident in Africa*, MassEngineers, 2003.

[169] *INSAG-7 The Chernobyl Accident: Updating of INSAG-1*, International Atomic Energy Agency, 1992.

[170] Google Earth, https://earth.google.com/web/, Google, 2021, accessed 2021.

[171] *Lethabo – phoenix of the nineties – Technical Information,* Eskom Communication Department, 1995 (revised).

[172] T.E. Carter, *Studies on motor bus transfer challenges for the ancillary equipment of a large thermal power station*, North-West University, 2021.

[173] *Degrees of protection provided by enclosures (IP code)*, IEC 60529 ED. 2.2, 2013.

[174] H.J. van Staden, *Benchmarking power station voltage dip performance to meet the grid code requirements*, North-West University, 2018.

[175] G.P. Tilly and W. Sage, *The Interaction of Particle and Material Behaviours in Erosion Processes*, Wear, 1970.

[176] R.D. Shandu, *Experimental Investigation of Erosion caused by Gas-Bourne Ash Particles*, University of the Witwatersrand, 2007.

[177] C.A. Berry, *Russia's gas shutoff is forcing Germany's energy giant Uniper to fire up a mothballed coal-fuelled power plant*, Reuters, 2023.

[178] J. Watts, *Brazil's worst drought in history prompts protests and blackouts*, The Guardian, https://www.theguardian.com/world/2015/jan/23/brazil-worst-drought-history, 2015, accessed 2022.

[179] *Drought behind worsening power outages in Malawi,* Bizcommunity, https://www.bizcommunity.com/Article/129/704/171119.html, 2017, accessed 2021.

[180] J. Thompson, *Zimbabwe gets 10-hour electricity cuts as drought hits hydropower*, Sunday Times – Times LIVE, https://www.timeslive.co.za/news/africa/2019-05-12-zimbabwe-gets-10-hour-electricity-cuts-as-drought-hits-hydro-power/, 2019, accessed 2022.

[181] *Japan earthquake: Evacuations ordered as fears grow of radiation leak at nuclear plant*, news.com.au, https://www.news.com.au/world/japan-earthquake-evacuations-ordered-as-fears-grow-of-radiation-leak-at-nuclear-plant/news-story/7b5b54c597afc3cfe093f066dab3a965, 2011, accessed 2022.

[182] W. Freebairn, *Nuclear plants in Carolinas brace for Hurricane Florence, may shut in advance*, S&P Global, 2018.

[183] E. Simoes, *Brazil blackout blamed on storm, grid in spotlight*, Reuters, 2009.

[184] M. Viljoen and J.A. de Kock, *Determining Vulnerability Parameters for Power Generation Fleets to Adverse Environmental Conditions*, Cigré, 2021.

[185] A. Choi, Solar eclipse 2017: *how the solar power industry is prepping for a huge blip*, Solar eclipse 2017: how the solar power industry is prepping for a huge blip - Vox, Vox, 2017, accessed 2023.

[186] S. Odenwald, *The day the sun brought darkness*, NASA, https://www.nasa.gov/topics/earth/features/sun_darkness.html, 2009, accessed 2023.

[187] *Solar storm risk to the North American electric grid*, Lloyd's and Atmospheric and Environmental Research, Inc., 2013.

[188] C.T. Gaunt and G.J. Coetzee, *Transformer Failures in Regions Incorrectly Considered to have Low GIC-Risk*, IEEE Lausanne, 2007.

[189] F.W. Sears, M.W. Zemansky and H.D. Young, *University Physics*, sixth edition, Addison-Wesley Publishing Company, 1982.

[190] G. McPherson and R.D. Laramore, *An introduction to electrical machines and transformers*, John Wiley & Sons, 1990.

[191] E. Ørum et.al., *Future system inertia*, European Network of Transmission System Operators for Electricity, 2019.

[192] S.C. Chapra and R.P. Canale, "*Numerical methods for engineers with personal computer applications*", McGraw-Hill, 1985.

[193] M. Viljoen and J.A. de Kock, *"Cascade Disruption of Generation: The Hidden Gift of Failure*", IEEE Power and Energy Society Conference and Exposition in Africa: Intelligent Grid Integration of Renewable Energy Resources (PowerAfrica), 2012.

[194] M. Viljoen, *"Cascade Disruption of Generation – Using Adversity for Learning & Improvement*", IEEE Xplore (Eurocon), 2011.

[195] M. Viljoen and J.A. de Kock, *"A Special Focus on African Grid Vulnerabilities*", IEEE Xplore (Africon), 2011.

[195] M. Viljoen and J.A. de Kock, *"Exploiting Cascade Failure for the Calibration of Planning Assumptions & Operational Improvement*", CIGRE Proceedings, 2019.

9. Annexures

9.1 Annexure 1 – Disruption Event Example Log

17:02		**GX EVENTS**: SOUTHERN LETHABO UNIT 04 MW: 550 MW FREQUENCY: 50,13 Hz - 49,73 Hz UNIT TRIPPED DUE TO LOSS OF 380 V UNIT DIESEL BOARD.
17:03	00:14	**EL1 CALLUP**: WESTERN GOURIKWA UNIT 11 / 00:14 MW: 148 MW OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.
17:06	00:08	**EL1 CALLUP**: WESTERN GOURIKWA UNIT 22 / 00:08 MW: 148 MW OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.
17:07	17:19	**GX EVENTS**: NORTHERN MEDUPI UNIT 03 / 17:19 MW: 720 MW FREQUENCY: 50,15 Hz - 49,50 Hz UNIT TRIPPED DUE TO TURBINE VIBRATIONS. UNDER INVESTIGATION.
17:07	17:19	**INSTANTANEOUS DEMAND RESPONSE**: NORTHERN MW: 889 MW FREQUENCY: 49,50 Hz - 50,04 Hz INSTANTANEOUS DEMAND RESPONSE OPERATED DUE TO MEDUPI UNIT 03 TRIP.
17:08	00:02	**EL1 CALLUP**: WESTERN GOURIKWA UNIT 12 17:42 / 00:02

		MW: 148 MW OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.
17:11		**EL1 CALLUP**: NATIONAL NEIGHBOURING COUNTRIES: MOZAL SUBSTATION MW: 447 MW MOZAL WARNED OF A POSSIBLE LOAD REDUCTION BETWEEN 17:10 - 21:00.
17:12	23:50	**EL1 CALLUP**: WESTERN ANKERLIG UNIT 42 / 23:50 MW: 148 MW OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.
17:14	00:20	**EL1 CALLUP**: WESTERN GOURIKWA UNIT 13 / 00:20 MW: 148 MW OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.
17:14	23:44	**EL1 CALLUP**: WESTERN ANKERLIG UNIT 32 / 23:44 MW: 148 MW OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.
17:19	23:38	**EL1 CALLUP**: WESTERN ANKERLIG UNIT 21 / 23:38 MW: 148 MW OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.
17:20	23:14	**EL1 CALLUP**: WESTERN ANKERLIG UNIT 43 / 23:14 MW: 148 MW OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.
17:20	23:17	**EL1 CALLUP**: WESTERN ANKERLIG UNIT 31 / 23:17 MW: 148 MW

		OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.					
17:20	23:14	**EL1 CALLUP**: WESTERN					
		ANKERLIG UNIT 41				/	23:14
		MW: 148 MW					
		OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.					
17:21	23:37	**EL1 CALLUP**: WESTERN					
		ANKERLIG UNIT 22				/	23:37
		MW: 148 MW					
		OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.					
17:24	22:15	**GX EVENTS**: SOUTHERN					
		LETHABO UNIT 03				/	22:15
		MW: 593 MW					
		FREQUENCY: 50,19 Hz - 49,63 Hz					
		UNIT TRIPPED DUE TO LOSS OF 380 V UNIT DIESEL BOARD.					
17:28	18:38	**EL1 CALLUP**: NATIONAL					
		MW: 447 MW					
		MOZAL, POTLINE 2 UTILISED TO ARREST FREQUENCY DECAY.					
		REQUESTED					
		INTERRUPTABLE LOAD: ILS	447 MW	17:28	18:38		
		REQUESTED TOTAL:	447 MW				
17:32	23:19	**EL1 CALLUP**: WESTERN					
		ANKERLIG UNIT 11				/	23:19
		MW: 148 MW					
		OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.					
17:32	22:24	**INDEPENDENT POWER PRODUCER**: SOUTHERN					
		DEDISA UNIT 01				/	22:24
		MW: 167 MW					
		IPP OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.					
17:34	22:53	**INDEPENDENT POWER PRODUCER**: EAST					

		AVON UNIT 02 MW: 170 MW IPP OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.	/	22:53
17:35		**INDEPENDENT POWER PRODUCER**: EAST AVON UNIT 03 MW: 170 MW IPP OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.	/	22:53
17:40		**GX EVENTS**: NORTH EAST ARNOT UNIT 02 MW: 370 MW UNIT SYNCHRONISED ON LOAD AFTER BOILER TUBE LEAK REPAIRS.		
17:56	22:24	**INDEPENDENT POWER PRODUCER**: SOUTHERN DEDISA UNIT 02 MW: 167 MW IPP OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.	/	22:24
17:57	23:45	**EL1 CALLUP**: WESTERN ANKERLIG UNIT 12 MW: 148 MW OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.	/	23:45
18:26	22:36	**INDEPENDENT POWER PRODUCER**: EAST AVON UNIT 01 MW: 170 MW IPP OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.	/	22:36
18:26	22:36	**INDEPENDENT POWER PRODUCER**: EAST AVON UNIT 04 MW: 170 MW IPP OCGT IN GEN MODE DUE TO SHORTAGE OF GENERATION.	/	22:36

9.2 Annexure 2 – Multiple Generation Event: Data Capture Framework

To enable for the exhaustive analysis of multiple-generation contingency events, comprehensive data collection and recording is necessary. Since much information and data are typically neglected during the initial investigation, later analysis is often impossible.

In general, the following framework needs to be observed as a general guideline for managerial focus following an event.

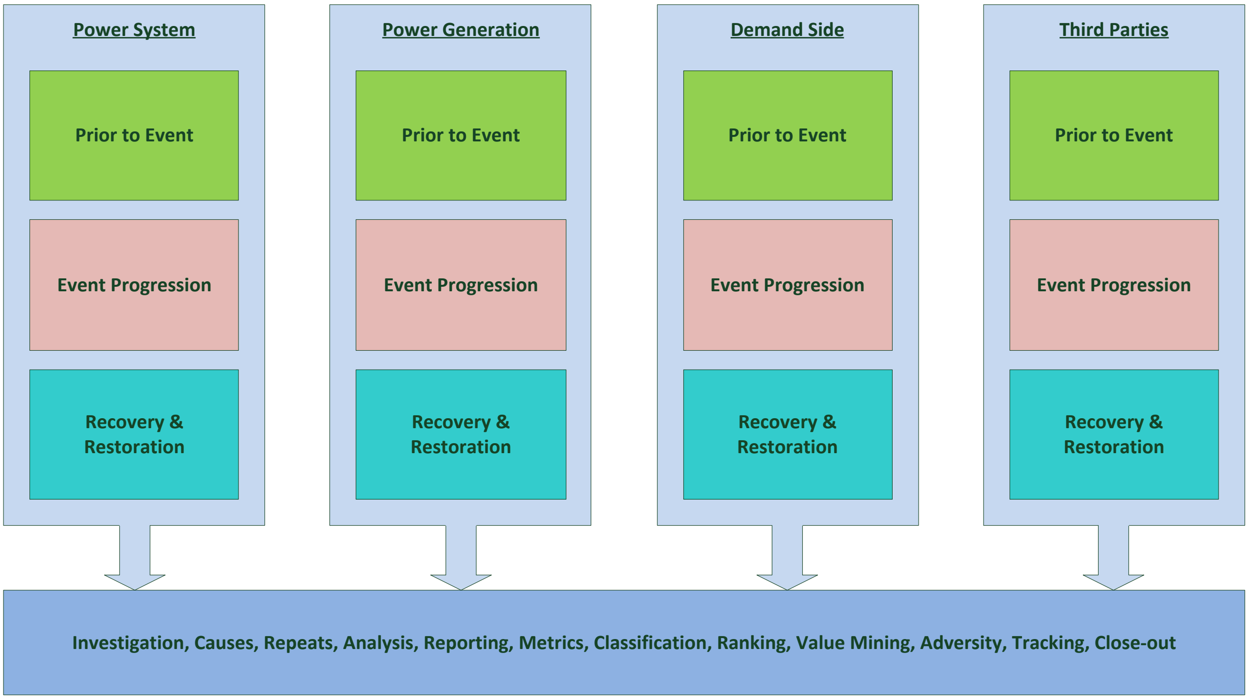


Figure 120: Data gathering and event mining structure

Essentially, every multiple disruption event impacts a fixed set of parties – exceptions do occur but are infrequent. Each event has some impact on the power system, the generation base, the user (or customer) base, and often third parties. Third parties include cross-border parties (like international participants (power stations, customers, etc.) or cross-boundary parties (like municipal participants such as embedded generators or customers).

Each of the four parties mentioned above needs to be assessed in terms of three high-level categories: the state before the event, the event itself as it unfolded, and the recovery or restoration after the event has played out. When this set of information has been obtained for all parties, the actual investigation, analysis and reporting should follow, involving:

a Investigation and inquisition
b Sequence of events
c Redundancy analysis (backup and standby system, emergency system performance)

- d Protection performance
- e Human performance
- f Dynamic and transient performance (including automated systems)
- g Data systems and recording system performance
- h Determining causes
- i Barrier analysis
- j Determining triggers and initiating events
- k Determining cascading branches
- l Assessing and determining the following
  - i What could (reasonably) have been the worst outcome or extent of the event
  - ii Why did the worst-case outcome not present itself
  - iii What caused the event to stop
  - iv Which units (systems, etc.) should reasonably have tripped but did not. Why?
  - v Which units (systems, etc.) should reasonably not have tripped but did. Why?
- m Determining defects
- n Damage and losses
- o Malicious and criminal aspects
- p Weighing and ranking the event
- q Produce metrics for long-term study
- r Recommendations

After the investigation, when sufficient facts have been obtained, evaluation of the event is required. This requires a number of assessments, some of which are shared below.

- a Assessing barrier sufficiency
- b Resilience
- c Identifying deficiencies
- d Assessing functional contribution and performance
  - i Operating
  - ii Maintenance
  - iii Engineering
  - iv Management
  - v Organisational
  - vi Industry norms
- e Recovery performance
- f Grid code compliance
- g Benchmarking with previous events (and international if possible)
- h Risk of recurrence

- i Contingency plan performance
- j Deficiency identification
  - i Design
  - ii Barriers
  - iii Protection
  - iv Data and information
  - v Recovery preparedness
  - vi Philosophies and strategies
  - vii Contingency planning
- k Non-scientific
  - i Eureka insights
  - ii Luck and bad-luck aspects
- l Anti-fragile possibilities

Here is a set of information that was empirically found to be required to perform an analysis for a deeper understanding of events that are often required.

9.2.1 Basic Information

- a Power station name
- b Number of units that became disrupted
- c Number of units that tripped
- d Specific units affected (e.g. units 1, 3 and 8 tripped / unit 2 de-loaded to ½ load)
- e Status of unaffected units (e.g. unit 4 off on maintenance / unit 5, 6 and 7 unaffected)
- f Date and time of the event
- g Date and time of the initiating event (often preceding the main event)
- h Operating points of the all units before the event (typically power send out in MW)
- i Was the power station blacked out (were any units still in service following the event?)
- j What was the status of the units (e.g. generating, off, SCO, pumping, ½-load, etc.)
- k Etc.

9.2.2 Basic Specifications

- a MCR rating of the units
- b EL1 rating of the units
- c Minimum generation floor of the units
- d Moment of inertia of the shaft trains of the units
- e Ceiling excitation values of the units
- f Capability diagram limitations (generator and other unit systems and components)

g Tap changer range
h Etc.

9.2.3 Basic Philosophies

a Number of mills required
b Fuel oil support strategies
c CW operational strategies
d Feedpump duties
e Etc.

9.2.4 Basic Actuals (event inception)

a Plant defects
b Plant abnormalities
c Deviations from defaults, norms and standards
d Limping plant or systems
e Unit loading (voltage and power)
f System frequency
g Automated systems not operating in automatic mode
h Emergency, standby and backup plant status
i Automatic modes active (e.g. frequency control, AVR, load control, etc.)
j Tap changer position
k Mill configuration
l Load losses in force
m Maintenance being executed and permits issued
n Staff compliment
o Level of unit optimisation
p Etc.

9.2.5 Common and Shared Systems

a Fuel oil and propane plant status (pumps, heating, levels, loading, etc.)
b Compressed air plant (compressors, receivers, loading, marginality of installation, etc.)
c Cooling systems (temperatures, pumps, etc.)
d Coal and ash (redundancy, levels, usage rates, etc.)
e Etc.

9.2.6 Functionality Statuses (active or inactive)

a Primary frequency control
b Secondary frequency control
c Mandatory frequency control
d Power system stabiliser
e Islanding capability
f Etc.

9.2.7 Redundancies, Backup, Standby and Fall-back plant and systems

a Boiler feed pumps
b Boiler circulating pumps
c Mills
d AVR channels
e Protection schemes (HV and MV)
f Diesel generators and other diesel plant
g DC and battery banks
h UPS channels
i Station supply and loop supply
j Etc.

9.2.8 Out-of-Normal, Temporary Alterations, Non-default Configurations

a Electrical reticulation systems
b DC and UPS systems
c Diesel generators
d Station supply
e Loop supply
f Mills, feeders and burners
g Draught groups
h Boiler feed pumps and circulating pumps
i Etc.

9.2.9 Stock Levels

a Raw water
b Demin water
c Coal levels (bunkers, silos, coal stockyard)

d Fuel oil and propane

e Diesel fuel

f Production gasses (H_2, CO_2, etc.)

g Lubricant

h Consumables (chemicals, grinding media, etc.)

i Etc.

9.2.10 Protection Performance

a Functions operated

b Failures and malfunctions

c Protection deficiencies found

d Unexpected, unpredicted, unintentional operations

e Etc.

9.2.11 Power System Information

a System frequency

b Frequency extremes and oscillations

c Frequency recovery time

d $\frac{df}{dt}$ behaviour during the incremental steps of the disruption

e Total number of synchronous unit connected

f Total moment of inertia

g Total power served through the power system

h Tie-line power (before, during and after the event)

i Demand side management options implemented

j Support from non-market participants

k Primary and secondary frequency control performance

l Renewable energy (before, during and after the event)

m Peaking options implemented (before, during and after the event)

n Etc.

9.2.12 Event Information

a Initiating event

b Failed defences (physical, procedural, human, etc.)

c Cascading event branches

d Identifying systems that failed

e Disruption jumps – from one system to another

f Actual loss (actual power, collective unit capacity, moment of inertia, reserve range)
g Commonality
h Etc.

9.2.13 Causal Factors

a Failure
b Malfunction
c Fault
d Error
e Violation
f Malicious action
g Competence and proficiency
h Oversight and supervision
i Interruption
j Lack or absence
k Fatigue
l Overloading
m Deficiency
n Functional allocation
o Configuration management
p Optimisation
q Operational envelope
r Abnormal
  i. Operating
  ii. Configuration
  iii. Condition
s Neglect
t Risk underestimated
u Lack of redundancy
v Etc.

9.2.14 Recovery Information

a Duration before each unit loaded to contract once more
b Cost (raw or precise) – at station level and within the power system
c Resources consumed
d Energy forfeited – at station level and within the power system

e Damage that occurred
f Etc.

9.2.15 Event Statistics

a Total number of protection functions activated
b Total number of breaker operations
c Number of discrete disruption steps
d Number of discrete steps to counter and restore
e Calculated metrics
f Etc.

9.2.16 Specific Interest

a What should also have tripped, but did not – and why?
b What should not have tripped, but did – and why?
c Worst potential loss (if units that were off, were also in service)
d Was the event sudden and unforeseen – or predictable?
e What caused the disruption to cease – not cascading further
f Is the defensive framework sufficient?

9.3 Annexure 3 – Areas for Post-Event Assessment and Validation

As illustrated in section 6.4, much value can be derived from the data gathered and investigation into large-scale disruption events. This section shares some of the questions and relevant information that should be explored in an event mining framework.

It is first important to realise that information assessment and evaluation should be conducted in terms of various categories, namely Figure 120. In other words, every functional area in an event needs to be considered, e.g., generation, system operator, etc. For every functional area, there should be three perspectives: before the event, the event itself, and following the event (recovery).

9.3.1 Generation – Utility and IPP

9.3.1.1 Prior to the Event

a Did consumable stock levels comply with standards and regulations?
b Was the nature, plant or system recorded in the MUT risk register of the power station?
c Was the possibility of a potential disruption event foreseen and identified as a risk?
d Was the risk of a potential disruption event form part of a risk assessment?
e Was the risk assessment adequate / and effective?
f Was the likelihood of the disruption risk correctly evaluated?
g Were the risk mitigation measures adequate, and were they all implemented?
h Were abnormal (non-default) plant configurations recognised as a risk?
i Were unavailable plant and systems recognised as a risk?
j Station supply availability
k Were there warning signs that could have prevented the disruption event?
    i Previous similar events
    ii Staff warnings
    iii Alarms
    iv Condition monitoring
    v Obvious conditions
l Were non-routine maintenance and operating risks identified and assessed?
m Were actions from previous similar events implemented?
n Total fleet overview – all units
    i In service, outages, cold reserve, etc.
    ii Total load losses
    iii Pumping and SCO

    - iv Total reserves (all reserve classes)
    - v Total moment of inertia
    - vi Black-starting status

9.3.1.2 Event Progression (power station level)

- a Did all systems (primary and auxiliary) perform as expected?
- b Secondary system evaluation
    - i Process control (static and dynamic)
    - ii HMI and mimics
    - iii Data acquisition and archiving
    - iv Excitation control
    - v Protection
    - vi Fault recording
    - vii Alarm systems
    - viii Automated functions – all controllers in automatic mode
    - ix Automatic chop-over systems
- c Staffing evaluation
- d What caused the cascade to cease?
- e Which units should have tripped, but did not? Why?
- f Emergency isolation, draining, venting, boxing up, cut off, lock out performance
- g Aberrant behaviour

9.3.1.3 Post-Event

- a Islanding and trip-to-houseload performance
- b Plant damage assessment
- c Reticulation system reconfiguration
- d Recovery performance
- e Resource mobilisation
- f Contingency plan performance
- g Procedural adherence, non-adherence and contravention
- h Communication system performance and sufficiency
    - i Radios
    - ii Telephones
    - iii Satellite phones
    - iv Public address systems and sirens
    - v Pagers
    - vi Data communication links

i Diesel, pneumatic and DC plant performance

j Nuclear off-site performance

k Synchronising installation performance

l Total fleet overview – all units

    i In service, outages, cold reserve, etc.

    ii Total load losses

    iii Pumping and SCO

    iv Total reserves (all reserve classes)

    v Total moment of inertia

    vi Black-starting status

9.3.1.4 Generation Collective Fleet Level

a High-frequency performance

    i Governing (primary frequency control)

    ii AGC (secondary frequency control)

    iii Mandatory governing

    iv Overfrequency protection

b Islanding performance

c Black-start performance

d Recovery and restoration timelines

9.3.2 Transmission and Distribution

9.3.2.1 Prior to the Event

a Redundancies (e.g. (n-1))

b Tie-lines

c Loading levels

d Abnormal configurations

e Weather

f Event trigger

9.3.2.2 Event Progression

a Reserves performance and adequacy

b Asset trips and switch-backs

c Protection system performance

d Network island formation

e Data logging capability performance

f DC system performance

g Staffing evaluation
h Aberrant behaviour

9.3.2.3 Post-Event

a Restoration performance
b Plant damage assessment
c Resource mobilisation
d Contingency plan performance
e Procedural adherence, non-adherence and contravention
f Communication system performance and sufficiency

9.3.3 System Operator

9.3.3.1 Prior to the Event

a Reserves levels and adequacy
b Islanding units adequacy
c Black-start facilities adequacy
d Total system overview – all participants
    i Generation resources and status
    ii Transmission system status
    iii Demand side resources (loads and generation)
    iv Power pool interconnections
    v Telecommunication system status

9.3.3.2 Event Progression

a Reserves performance
b Islanded states
c System frequency response and containment
d Voltage stability performance
e Oscillatory events
f Power surges
g Information system performance
h Communication system performance and adequacy
i Emergency power supply and DC system performance
j Staffing evaluation

9.3.3.3 Post-Event

a Black-start performance
b Islanding unit returns
c Islanded network reconnection
d Recovery timelines
e Contingency plan performance
f Total system overview – all participants
    i Generation resources and status
    ii Transmission system status
    iii Distribution system status
    iv Control centres
    v Demand side resources (loads and generation)
    vi Power pool interconnections
    vii Telecommunication system status