

Standard

Technology

Title: **NETWORK MANAGEMENT**

CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Alternative Reference Number: <n/a>

Area of Applicability: Engineering

Next Review Date: STABILISED

COE Acceptance

Richard McCurrach

/ [_____)

PTM&C Engineering Senior Manager

DBOUS Acceptance

Amelia Mtshali

DBOUS Senior Manager

Date: 23 Nov 2020 Date: 23/11/2020

This document is **STABILISED.** The technical content in this document is not expected to change because the document covers: (*Tick applicable motivation*)

1	A specific plant, project or solution X	
2	A mature and stable technical area/technology	
3	Established and accepted practices.	



Standard

Technology

Title: NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier:

240-84323647

Alternative Reference Number: <n/a>

Area of Applicability:

Engineering

Documentation Type:

Standard

Revision:

1

Total Pages:

42

Next Review Date:

March 2021

Disclosure Classification:

Controlled Disclosure

Compiled by

Matthew Taljaard

Telecommunications T&S Engineer

Date: 34/03/2016

Approved by

Cornelius Naidoo

CoE Design Manager Telecommunications T&S

Date: 24/3/2016

Authorized by

Richard McCurrach

PTM&C Senior Manager

Date: 2

Supported by SCOT/SC

Ziyaad Gydien

Telecommunications SC

Chairperson

Date: 23/03/2016

PCM Reference: 240-53458797 PCM for PTM&C

SCOT Study Committee Number/Name: Telecommunications Study Committee

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 2 of 42

Content

				Page	
1.	Intro	duction		5	
2.	Sup	porting o	clauses	5	
	2.1	Scope	9	5	
		2.1.1	Purpose	5	
		2.1.2	Applicability	5	
	2.2				
		2.2.1	Normative	6	
		2.2.2	Informative	6	
		2.2.3	General	7	
		2.2.4	Disclosure classification	8	
	2.3	Abbre	viations	8	
	2.4	Roles	and responsibilities	9	
	2.5	Proces	ss for monitoring	10	
	2.6	Relate	ed/supporting documents	10	
3.	Data	Centre	Overview	10	
Ο.	3.1		Availability		
	3.2	_	ndant Topology		
	3.3		ork Hierarchy		
	0.0	3.3.1	Core		
		3.3.2	Aggregation		
		3.3.3	Access		
	3.4		r Efficiency		
	0	3.4.1	Example A – Copper connection solution		
		3.4.2	Example B – Fibre connection solution		
		3.4.3	Benefit of PUE		
	3.5		on for Redundant Site		
	0.0	3.5.1	Latencies between the Data Centres		
		3.5.2	Maximum Theoretical Distance between the Data Centres		
		3.5.3	Co-location with Nation Control Complex		
4.	Rea	uiremer	nts for Data Centres	18	
	4.1	·			
	4.2		Security		
		4.2.1	Firewall Cluster	19	
	4.3	Storag	ge Architecture	20	
		4.3.1	Stage 1 Migration	22	
		4.3.2	Stage 2 Migration	22	
		4.3.3	Stage 3 Final		
	4.4	Data 0	Centre Infrastructure		
	4.4.1 Grounding			24	
	4.5	Cabin	ets, Racks and Cables		
		4.5.1	General requirements		
		4.5.2	Cabling Convention		
		4.5.3	Cabling Architecture	27	
			Other variants	30	

NETWORK MANAGEMENT CENTRE REDUNDANCY STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 3 of 42 4.5.5 Cabling media32 4.5.6 Standard Patch Panel Termination and Cable Dressing32 4.5.7 Testing 33 4.6 4.7.1 Energy efficiency......34 4.7.2 Standby Generators......34 4.7.3 Uninterruptable Power Supply System35 Measuring Data Centre Power and Energy Consumption.......35 Water Risk 36 4.21 Certifications and Audits41 Development team42 Acknowledgements42 **Figures** Figure 1: High Level design of an active/active data centre......11 Figure 3: High level view of NCC and NMC Co-located......17 Figure 4: TIA-942 Compliant Data Centre Showing Key Functional Areas [2]......18 Figure 8: Simple diagram of a storage design using a Fibre Channel (FC) [5]......21 Figure 12: Stage 3 Migration of FCoE23 Figure 13: Mixed cable routing under ceiling and in hollow floor24 Figure 14: Grounding Systems as a Tree Structure25

NETWORK MANAGEMENT CENTRE REDUNDANCY STANDARD

Revision:

Unique Identifier: 240-84323647

1

Page: 4 of 42 Figure 17: Tier IV Communications Cabling High-level......27 Figure 21: Top of Rack design – Saving on patch panel......31 Figure 22: Top of Rack design - Vertical Mounting31 Figure 24: Wire placement (left); Inner pairs punched (right)......33 Figure 25: Outer pairs punched (left); Minimize cable stress by not using a tight bend radius (right)33 Figure 26: Double conversion on-line UPS topology, from IEC 60240-3 block diagram showing four Figure 29: SAN Structure with Virtual Storage40 **Tables** Table 5: Power cost per year vs. PUE of copper and fibre optic.......16 Table 6: Factor and Recommendations for the 2012 NMC Feasibility Study [1]16

Table 7: Functional Area Example18

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 5 of 42

1. Introduction

Eskom's core business is to generate, transmit and distribute electricity to its core customers (i.e., industrial, mining, commercial, agriculture and residential customers and re-distributors). Electricity has become more than a luxury but a necessity. In the case of power failure, electrical devices come to a standstill. Industrial, mining, commercial and residential environments are greatly affected since they rely heavily on electricity. This translates directly in huge losses in the economy.

Continuity of supply is therefore one of Eskom's primary strategic objectives. In order to achieve this, a reliable power network that supplies power to its customers with minimal interruptions is needed. Reliably transmitting and distributing electricity requires that Eskom's power network be maintained, monitored and upgraded to meet the needs of consumers at all times. Continuity of supply also requires that faults in the grid be identified and repaired within the least amount of time. The National Control Centre (NCC) is responsible for managing and monitoring the power grid.

Eskom Telecommunications (ET) provides a telecommunication network that carries mission critical and other telecommunication products and services to support Eskom's power grid. In order for the grid to be monitored, it needs to be visible on management systems. This visibility is an example of a mission critical service and it is achieved through the use of ET's network. ET makes it possible for NCC to monitor the grid. However, just as the grid needs to be monitored and kept running at all times, ET's network also needs to be monitored and kept running because a failure in ET's network will result in visibility of the grid being lost.

The Network Management Centre (NMC) is the section that is dedicated to monitoring and managing ET's network. It is in operation 24 hours a day, 7 days a week. ET's network is required to be available 99.999% of the time, which translate to a total downtime of 5.3 minutes in a year.

The NMC data centre is the heart of NMC and full redundancy is required to ensure the products, services and availability mandated by ET are achieved. This document focuses on the NMC redundancy design.

2. Supporting clauses

2.1 Scope

The scope of this document is to provide a standard for data centre redundancy required for the Network Management Centre. The scope of the standard is the following:

- 1) Disaster recovery limitation
- 2) Instantaneous failover with no manual intervention
- 3) No downtime or loss of information
- 4) Active workloads on both data centres
- 5) Operations of the Network Management Centre

2.1.1 Purpose

This document covers the design requirements proposed for the implementation of a redundant Data Centre. This document shall be used as a standard for deriving the necessary information to create the requirements required across two data centres.

2.1.2 Applicability

This document is intended for the use by Eskom technical, planning and operations personal. This document should be used as a standard and is intended to identify risks or potential cost implications to the detail design.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **6 of 42**

2.2 Normative/informative references

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

- [1] 32 1203 Eskom Telecommunication User Requirements Specification
- [2] 32 894 Eskom Server Rooms and Data Centre Standard
- [3] 240 55410927 Cyber Security Standard for Operational Technology
- [4] 240 70732902 Fibre Optic Connector Standard

2.2.2 Informative

- [5] 240 79669677 Demilitarised Zone Designs for Operational Technology
- [6] 240-91190304 Specification for CCCTV Surveillance with Intruder Detection
- [7] R&M Data Centre Handbook R&M Convincing Cabling Solutions
- [8] PDRP_2012-39 NMC Redundancy Feasibility Study
- [9] ISO/IEC 27001 Information Security Management
- [10] ISO/IEC 27002 Code of Practice for Information Security Controls
- [11] ISO/IEC 27033 Information Technology Network Security
- [12] ISO/IEC 27005 Risk Management
- [13] ISO/IEC 38500 Governance of Information Technology for the Organization
- [14] COBIT 5 A Business Framework for the Governance and Management of Enterprise Information Technology
- [15] COSO Integrated Framework
- [16] The National Cybersecurity Policy Framework
- [17] Promotion of Access to Information Act 2 of 2000
- [18] Protection of Information Act 84 of 1982
- [19] National Key Points Act 102 of 1980
- [20] National Energy Regulator Act 40 of 2004
- [21] ISO 9001 Quality Management
- [22] ISO 14001 Environmental Management
- [23] IEC 60364-5-54 Electrical Installations of Buildings
- [24] IEC 62040-3 Uninterruptable Power Systems
- [25] EN 60529 Degrees of Protection Provided by Enclosures
- [26] EN 1627 Security and Burglary Resistance
- [27] EN 501740-2 Structure Cabling Infrastructure Guidelines
- [28] CPNI Standard
- [29] 32 727 Safety, Health, Environment and Quality Policy
- [30] Occupational Health and Safety Act (85 of 1993)
- [31] Definitions

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **7 of 42**

2.2.3 General

Definition	Description	
Active - Active	Network of independent processing systems, connected to databases kept synchronized in a geographically distributed configuration, and managed through a unified interface. Benefits of this systems is: High Utilization High Availability High Flexibility	
Co-exist	To have a system in same building as another system	
Cold Standby	A method of redundancy in which the secondary system is only called upon when the primary system fails. The system on cold standby receives scheduled data backups, but less frequently than a warm standby. Cold standby systems are used for non-critical applications or in cases where data is changed infrequently.	
Co-location	To have a system on the same site as another system	
Convergence	Convergence is the state of a set of routers that have the same topological information about the internetwork in which they operate. A state of convergence is achieved once all routing protocol-specific information has been distributed to all routers participating in the routing protocol process. Any change in the network that affects routing tables will break the convergence temporarily until this change has been successfully communicated to all other routers The convergence time is the speed at which these rules are applied to the network.	
Ethernet Ethernet is a link layer protocol in the TCP/IP stack, describing how devices can format data for transmission to other network devices on network segment, and how to put that data out on the network connection.		
Failover Switch to backup systems or alternate paths.		
Gigabit Ethernet	Gigabit Ethernet is a term describing various technologies for transmitting Ethernet frames at a rate of a gigabit per second (1,000,000,000 bits per second)	
Hot Standby	A method of redundancy in which the primary and secondary systems run simultaneously. The data is mirrored to the secondary server in real time so that both systems contain identical information.	
Link Aggregation	Applies to various methods of combining multiple network connections in parallel in order to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links should fail.	
True online double conversion system	UPS setup is similar to Standcy UPS except the primary power path is the inverter instead of the AC mains. Therefore, when AC input fails, operation is not affected as activation of a transfer switch is not needed. This is because the AC input was not the primary source, but a backup source.	
Type of Service	A field in an Internet Protocol packet (Internet Protocol Diagram) that is used for quality of service.	
Warm Standby	A method of redundancy in which the secondary system runs in the background of the primary system. Data is mirrored to the secondary server at regular intervals, which means that there are times when both servers do not contain the exact same data.	

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **8 of 42**

Definition	Description
IPsec	Internet Protocol Security is a protocol suit for secure communications by authentication and encrypting each packet of a communication session. It is seen as an end-to-end security scheme operating in the internet layer of the internet protocol suite.

2.2.4 Disclosure classification

Controlled disclosure: controlled disclosure to external parties (either enforced by law, or discretionary).

2.3 Abbreviations

Abbreviation	Description
AC	Alternating Current
ACL	Access Control List
AXT	Alien Cross Talk
BMS	Building Management System
Bpps	Billion packets per second
coso	Committee of Sponsoring Organizations of the Treadway Commission
CPNI	Centre for the Protection of the National Infrastructure
сѕѕот	Cyber Security Standard for Operational Technology
DAS	Direct Attached Storage
DDOS	Distributed Denial of Service
DoS	Denial of Service
ЕМС	Electromagnetic compatibility
FC	Fibre Channel
FCoE	Fibre Channel over Ethernet
FO	Fibre optic
Gb	Gigabit
Gbit/s	Gigabits per second
Gbps	Gigabits per second
GE	Gigabit Ethernet
HSRP	Hot Standby Routing Protocol
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
KVM	Keyboard/Video/Mouse
kW	Kilo Watts
kWh	Kilo Watt Hours

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 9 of 42

Abbreviation	Description Description
LAN	Local Area Network
MET	Main Earthing Terminal
NAS	Network Attached Storage
NCC	National Control Complex
NMC	Network Management Centre
NMS	Network Management System
PoE	Power over Ethernet
PUE	Power Usage Effectiveness
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RH	Relative Humidity
RMS	Root Mean Square
SAN	Storage Area Network
SFP Small Form-Factor Pluggable	
SFP+	enhanced Small Form-factor Pluggable
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access Controller System
TGB	Telecommunication Ground Bar
TGBB Telecommunications Ground Bonding Backbone	
TLS	Transport Layer Security
TMGB	Telecommunication Main Ground Busbar
ToR	Top of Rack
ToS	Type of Service
UPS	Uninterruptable Power Supply
UTP	Unshielded Twisted Pair
VAC	Voltage Alternating Current
VLAN	Virtual local Area Network
VoIP	Voice over Internet Protocol
vPC	Virtual PortChannel
W	Watts
WAN	Wide Area Network

2.4 Roles and responsibilities

Eskom Telecommunications and NMC personal are responsible for complying and implanting this Standard.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **10 of 42**

2.5 Process for monitoring

Annual audits will be conducted on NMC to compliance with this Standard.

2.6 Related/supporting documents

Below are documents where information and/or pictures were quoted from:

- Cisco, "Secure Data Center for Enterprise Multi Data Center Sites Deployment of Cisco ASA Clustering with FirePOWER Services Design and Implementation Guide," Cisco, America, 2015.
- A. Krone, "TIA-942 Data Centre Standards Overview," ADC Telecommunications Inc., 2008.
 [Online]. Available: http://www.herts.ac.uk/__data/assets/pdf_file/0017/45350/data-centre-standards.pdf. [Accessed 16 November 2015].
- Microsoft, "Internet Firewall Design," [Online]. Available: https://technet.microsoft.com/en-us/library/Cc700827.internalactact_big(l=en-us).gif. [Accessed 19 June 2015].
- American National Standard for Information Technology, "Fibre Channel: Backbone 5 revision 2.00," INCITS, 4 June 2009. [Online]. Available: http://www.t11.org/ftp/t11/pub/fc/bb-5/09-056v5.pdf. [Accessed 06 January 2016].
- Hubble Premise Wiring, "Augmented Category 6 Cabling Installation Guidelines," [Online].
 Available: http://www.hubbell-premise.com/Literature/10GbECablingInstallationGuidelines.pdf.
 [Accessed 11 December 2015].

3. Data Centre Overview

A data centre represents an enormous business investment. When correctly designed, a data centre can enhance business efficiency and lower operational costs. A modular or hierarchical network is composed of building blocks that are easier to replicate, redesign and grow. Each time a module is added or removed; there is no need to redesign the data centre.

By segmenting the network into small manageable elements, a business can greatly improve ease of replacing, troubleshooting, understanding and upgrading. This data centre design makes use of modular network elements.

The data centre will be company owned (enterprise data centre) which will perform all IT services for Eskom.

To ensure the data centre can meet the stringent requirements of operational technology, the data centre will be an active / active data centre as shown in Figure 1.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **11 of 42**

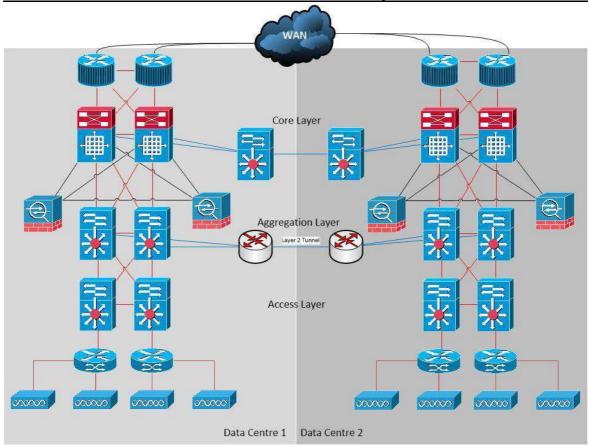


Figure 1: High Level design of an active/active data centre

3.1 High Availability

Well designed, highly available systems feature redundant hardware, redundancy software features and transparent procedures for re-converging network paths when failures occur. High available networks should not have any single points of failure on critical links or systems, and should failover in such a way that is transparent to the end user.

The design will incorporate high availability in the following manner. At layer 1, redundant links and hardware provide alternate physical paths through the network. At layer 2 and layer 3, protocols such as STP, HSRP and other dynamic routing protocols provide alternate path awareness and fast convergence. Software availability refers reliability-based protocols such as STP and HSRP as mentioned above, as well as reliable code and non-disruptive upgrades. STP, HSRP and other dynamic routing protocols provide instructions to the network and/or to components of the network on how to behave in the event of a failure.

Failure in this case could be a power outage, hardware failure, software corruption, or a disconnected cable. These protocols provide rules to reroute packets and reconfigure paths. The speed at which these rules are applied is called convergence. A converged network is one that, from a user standpoint, has recovered from a failure and can now process instructions.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **12 of 42**

The data centre shall be company owned and have an availability of at least 99.999% as per the Eskom Telecommunications User Requirement Specification. This implies the data centre shall:

- 1) Have planned activity/maintenance that does not disrupt critical load and the data centre can sustain at least one worst-case unplanned event with no critical load impact
- 2) Multiple active power and cooling distribution paths that includes redundant components of 2(N+1) redundancy
- 3) Annual down time of less than 24 minutes or 0.4 hours
- 4) Uninterrupted OT operations
- 5) 24/7 availability, 24/7 monitoring, 24/7 access
- 6) Short response times for upgrades and extensions
- 7) Low latencies

3.2 Redundant Topology

This standard complies with the highest level methodology of providing high levels of reliability by providing most of the reliability through redundancy in the network topology rather than primarily within the network devices themselves.

In this type of network design, there is a backup for every link and every network device in the path between the client and server. This approach to network reliability has a number of potential advantages.

The network elements providing redundancy need not be kept together in the same location with primary network elements. This reduces the probability that problems with physical environment failure will interrupt services.

Problems with software bugs/upgrades or configuration errors/changes can often be dealt with separately in the primary and secondary forwarding paths without completely interrupting service. Therefore, network-level redundancy can also reduce the impact of non-hardware failure mechanisms.

With the redundancy provided by the network, each network device no longer needs to be configured for the ultimate in standalone fault tolerance. Device-level fault tolerance can be concentrated in the core and distribution layers of the network where a hardware failure would be expected to affect a large number of users and services.

With appropriate resiliency features, plus careful design and configuration, the traffic load between the respective layers of the network topology (e.g. access layer to distribution) can be shared between the primary and secondary forwarding paths. Therefore, network-level redundancy can also provide increased aggregated performance and capacity, which in turn helps to reduce the incremental cost of a redundant network.

Redundant networks can be configured to transparently fail-over from primary to secondary facilities without operator intervention. The duration of service interruption is equal to the time it takes for failover to occur. Failover times of a few second are achievable.

Designing a cost-effective network that supports business objectives for high availability of network services and communication services requires the right mix of networking technologies including:

- 1) Device-level fault tolerance
- 2) Network-level redundancy
- 3) Complementary operational procedures

In many cases, a successful implementation of a high availability network project will include a balanced combination of the above mentioned considerations.

In order for redundancy to be possible, the data centre at peak load shall not exceed 50%. This is required as if data centre 1 goes down, then data centre 2 can take over the load without compromising the performance for applications and services.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **13 of 42**

3.3 Network Hierarchy

A data centre can be divided into discrete layers. Each of these layers provides functions within the overall network. This separation allows the data centre to become modular which results in the following advantages:

- Scalability
- Redundancy
- Performance
- Security
- Ease of administration
- Maintainability

Figure 2 shows the Three Tier Network that consists of a core, aggregation/distribution and access layer.

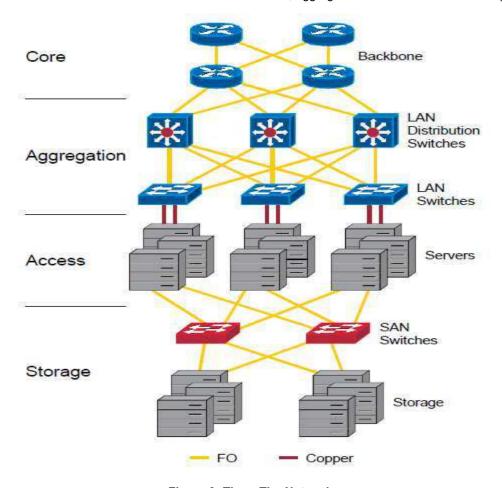


Figure 2: Three Tier Network

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **14 of 42**

3.3.1 Core

The core layer is the high-speed "backbone" of the network as it responsible for forwarding large volumes of data. This layer is critical for connectivity between the devices in the aggregation layer and therefore must have high availability and redundancy. The core area can be connected to internet resources.

Core switches are responsible for handling most data in a switched LAN. As a result, forwarding rate is the most important criteria when selecting these devices. Due to the performance demand of core switches, they generate significant heat and sufficient cooling is required for core switches.

QoS is an essential service component for core switches. Time critical data requires higher QoS guarantees and this may be resolved by using a software based solution for data prioritization. Where additional bandwidth in the core layer may fail, a cost-effective option for data prioritization using core switches allows for use of existing bandwidth in an optimal and diverse manner.

3.3.2 Aggregation

The aggregation (also known as distribution) layer in which switching centres combine and protect (e.g. firewalls) all data between the core and access layer. The primary purpose is to combine data that was received from the switches in the access layer before they are forwarded to the core layer to be routed.

This layer controls the flow of network data with the help of guidelines and establishes the broadcast domains by carrying out the routing functions between VLANs that are defined in the access layer. Aggregation switches therefore relieve the core switches of the need to carry out his routing function as core switches are already used to forward large volumes of traffic. The data on a switch can be subdivided into separate sub-networks through VLANs.

Aggregation Switches shall support ACLs which allows the switch to reject or accept specific types of data. This allows the aggregation switch to control which network devices may communicate in the network. Aggregation switches have high performance requirements to enforce ACLs as each packet must be examined to determine whether it corresponds to one of the ACL rules defined for the switch.

Link aggregation (also known as combining or trunking) will be applied for all links in this layer to prevent bottleneck and increase throughput. Example: 8 x 10 Gbit/s aggregated will give 80 Gbit/s of throughput.

Aggregation switches are severely loaded in the data centre environment and will be implemented in pairs for redundancy to ensure availability. The aggregation switch pair must run at no higher than 50% of its maximum capacity to ensure that when one goes down, the redundant switch can handle the load without compromising performance.

3.3.3 Access

This layer creates the connection to terminal devices and arranges access to the remainder of the network. The access layer can include bridges, desktops, hubs, switches, servers, storage resources and wireless access points. The primary purpose of the access layer is to provide a mechanism which controls how devices are connected to the network and which devices are allowed to communication in the network.

Where large access is required, multiple access switches shall be stacked with one another into one virtual switch which can be managed and configured through one master device.

3.4 Power Efficiency

Data centres require huge amounts of power and therefore, efficient power reducing techniques are required to bring the cost of operations down for the data centre.

The data centre shall be able to measure its power efficiency.

The PUE shall be used to measure the data centre power usage and is the ratio of total power consumed by the data centre to the power consumed by the IT equipment alone.

$$PUE = \frac{Total\ Facility\ Energy}{IT\ Equipment\ Energy}$$

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **15 of 42**

3.4.1 Example A – Copper connection solution

Energy requirement when using a 10 Gbit/s switch chassis:

Table 1: Energy requirement for copper connection

336 copper connections	Power
7 modules with 48 copper ports at 6W*	2016 W
Total ventilation	188 W
NMS Module	89 W
10 Gb fibre uplink	587 W
Total	2.88 kW

^{*}Average based on manufacturer specifications

Total Consumption:

Table 2: Power consumption of copper switch

Power Consumption – Copper Switch	2.88 kW
DC/DC conversion	0.52 kW
AC/DC conversion	0.89 kW
Power distribution	0.12 kW
Uninterrupted power supply	0.4 kW
Cooling	3.08 kW
Switchgear in energy distribution	0.29 kW
Total power requirement	8.12 kW

3.4.2 Example B – Fibre connection solution

Energy requirement when using a 10 Gbit/s switch chassis:

Table 3: Energy requirement of fibre optic connection

336 fibre optic connections	Power
7 modules with 48 FO ports at 2W*	672 W
Total ventilation	188 W
NMS Module	89 W
10 Gb fibre uplink	587 W
Total	1.536 kW

^{*}Average based on manufacturer specifications

Total Consumption:

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **16 of 42**

Table 4: Power consumption of fibre optic switch

Power Consumption – FO Switch	1.536 kW
DC/DC conversion	0.28 kW
AC/DC conversion	0.48 kW
Power distribution	0.06 kW
Uninterrupted power supply	0.22 kW
Cooling	1.65 kW
Switchgear in energy distribution	0.15 kW
Total power requirement	4.376 kW

3.4.3 Benefit of PUE

Table 5: Power cost per year vs. PUE of copper and fibre optic

Power Costs for Switching Hardware	Copper Switch	Fibre Optic Switch	
Power consumption	8.12 kW	4.376 kW	
Hours per year	24h * 30.5days * 12 Months = 8784h	24h * 30.5days * 12 Months = 8784h	
Power consumption per year	71326.08 kWh	38.438.784	
Power cost per kWh	160c/kwh	160c/kwh	
Power costs per year	R113,121.72	R61,502.06	
Energy costs by energy efficiency			
PUE factor = 3.0	R339,365.16 / year	R184,506.17 / year	
PUE factor = 2.2	R248,867.75 / year	R135,304.52 / year	
PUE factor = 1.6	R180,994.76 / year	R98,403.29 / year	

It is important to note how much the PUE factor shows the cost in the long run of operating a data centre. Therefore the data centre shall have a PUE factor of less than 2.0.

3.5 Location for Redundant Site

The redundant site must be geographically separated as to not be susceptible to the same hazards.

In 2013, a feasibility study (PDRP_2012-39) was done to determine the best site location for a redundant data centre. The factors affecting data centre physical location and the recommendations are as follows:

Table 6: Factor and Recommendations for the 2012 NMC Feasibility Study [1]

Factor	Recommendation
Earthquake	48 km
Tornado	48 km
Asteroid / Meteor	112.84 km
Atomic Bomb	160 km

The recommended physical location from a geographical perspective for the data centre would be outside the range of an atomic bomb of 160km

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **17 of 42**

In general the data centre should be outside of flood-risk areas, dangerous production sites, airports, power plants and other high-risk zones. If there is a risk, proper mitigation steps must be in place to prevent and recover from the risk.

3.5.1 Latencies between the Data Centres

An active / active data centre requires latency between the data centres of less than 10ms.

3.5.2 Maximum Theoretical Distance between the Data Centres

With a dedicated fibre, it is possible to achieve the required latency with a fibre span of 160km.

3.5.3 Co-location with Nation Control Complex

The NMC data centre should be co-located with the NCC data centre but not co-existing with NCC data centre as shown in Figure 3 below. This should apply to the redundant site as well.

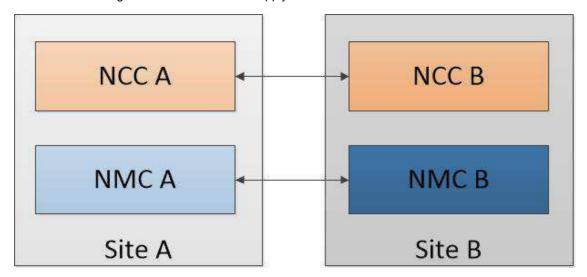


Figure 3: High level view of NCC and NMC Co-located

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **18 of 42**

4. Requirements for Data Centres

4.1 Functional Area Segregation

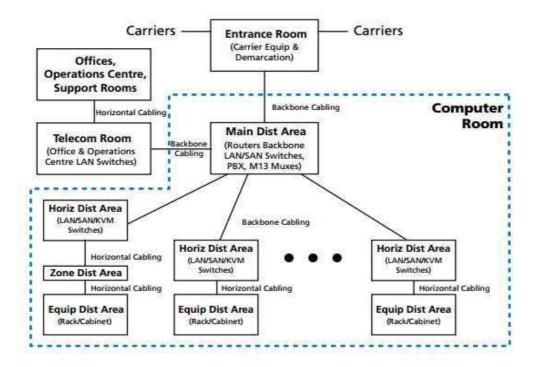


Figure 4: TIA-942 Compliant Data Centre Showing Key Functional Areas [2]

Figure 4 above shows the key functional area segregation that should be applied in a data centre.

The physical access into the data centre shall be analysed and classified into different areas. As you approach the data centre, the level of the security zone increases and the level of access required increases.

These zones are also known as functional areas and an example and Figure 5 below is given:

Table 7: Functional Area Example

Security Zones	Function	Marking
1	Site	White
2	Semi-public area, office spaces	Green
3	Operating area	Yellow
4	Technical Systems	Blue
5	IT and network Infrastructure	Red

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **19 of 42**

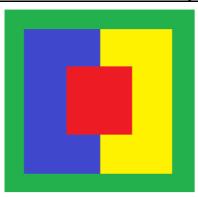


Figure 5: Functional Area Example

The security zones shall provide guidance on where technical systems equipment should be kept to prevent sabotage to the data centre. For example, a 3rd party maintenance technician for air conditioning systems should only have access to the blue area for maintenance and not the red area where the infrastructure is located.

Physical access to data centre shall be restricted to essential personal only. The data centre will be housing cyber assets that will be classed as a Critical Cyber Asset and shall comply with "Physical Security of Critical Cyber Assets" in the CSSOT in that regard.

4.2 Cyber Security

The data shall have methods in place to implement security. This includes:

- 1) DoS and DDOS prevention methods
- 2) Encryption, decryption and secure protocols
- 3) Deep pack inspection
- 4) Authentication, Authorization and Accounting (RADIUS, TACACS, etc)
- 5) Layer 2 (e.g. port security), Layer 3 (e.g. IPsec) and Layer 4 (TLS) security
- 6) Inbound and Outbound traffic controls
- 7) Management tools for monitoring the data centre

The data centre is considered a critical asset and all critical cyber assets in the data centre shall comply to the "Requirements for OT Cyber Security Management" detailed in the CSSOT.

4.2.1 Firewall Cluster

Two Firewalls will be used per data centre. All four of these firewalls will be clustered together. The WAN routers would advertise the same IP prefix to the outside world, attract the traffic and pass the traffic through the nearest firewall. The inside routers will take care of proper traffic distribution. The active/active firewalls would exchange flow information and will solve asymmetrical flow problems as seen in Figure 6. Clustered firewalls allow configurations on one firewall to be mirrored on all firewalls in the cluster and can be geographically separated. All four firewalls will be active as seen in the figure below and traffic will be load balanced across all of these firewalls. The firewalls must have a high bandwidth and low latency requirement.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 20 of 42

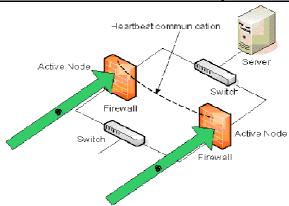


Figure 6: Active / Active Firewall configuration [3]

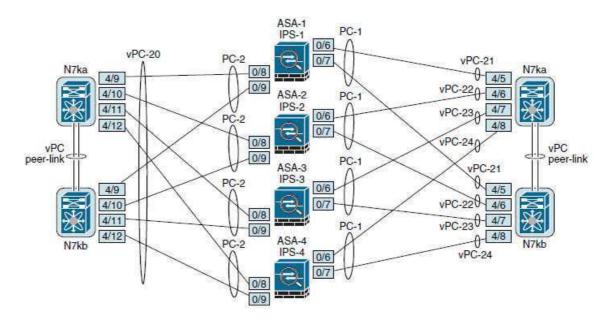


Figure 7: Cluster firewall layout example from Cisco [4]

Figure 7 above shows a more detailed setup of a cluster firewall combination. All the distribution switches will have a connection to each of the firewalls. The firewalls will have a vPC between the distributed switches.

4.3 Storage Architecture

The storage architecture should have a storage-consolidated environment as shown in Figure 8. This means that a storage network is installed for servers to store data. The advantages are:

- 1) Better manageability
- 2) High availability
- 3) Extended functions like cloning, mirroring, etc.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **21 of 42**

Fibre Channel SAN technology should be used as the storage-consolidated environment. DAS and NAS may be considered as a redundant technology as backup storage for the data centre.

An EMC storage solution and FC will connect the infrastructure in both data centres for virtualization and storage.

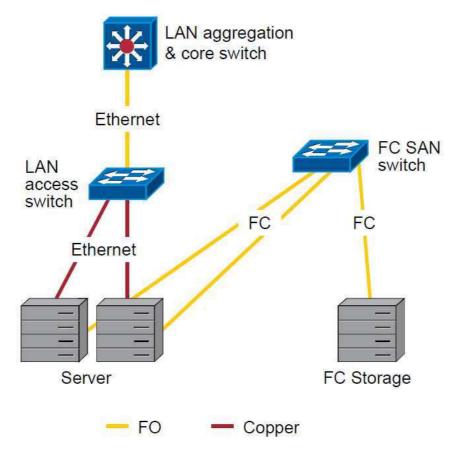


Figure 8: Simple diagram of a storage design using a Fibre Channel (FC) [5]

In order to use existing Ethernet storage, FCoE, shown in Figure 9, will be required to allow both Ethernet servers (using LAN protocols) and FC storages (using SAN protocols) to operate together [6]. This can be done as follows:



Figure 9: Summary of FCoE

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 22 of 42

4.3.1 Stage 1 Migration

A Convergence Network Switch is introduced that allows existing hard to be reused. SPF+ shall be used as the transceiver interface and this is shown in Figure 10.

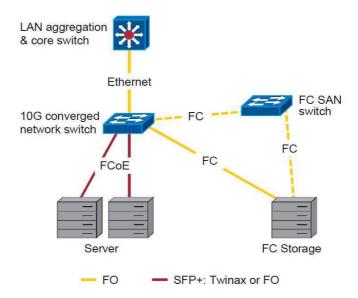


Figure 10: Stage 1 Migration to FCoE

4.3.2 Stage 2 Migration

The Convergence Switch is upgraded with an FCoE uplink and connected to FCoE in the backbone and is shown in Figure 11.

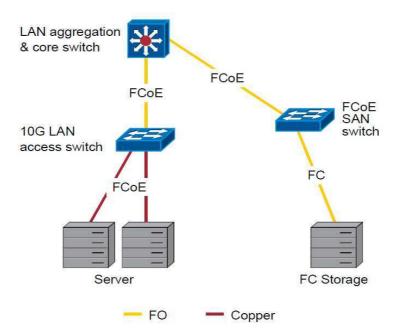


Figure 11: Stage 2 Migration for FCoE

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 23 of 42

4.3.3 Stage 3 Final

The final FCoE solution is connected directly to the core network. FC as an independent protocol has disappeared from the network. All data centres will end with a design shown in Figure 12. This allows network (IP) and storage (SAN) data traffic can be consolidated using a single network.

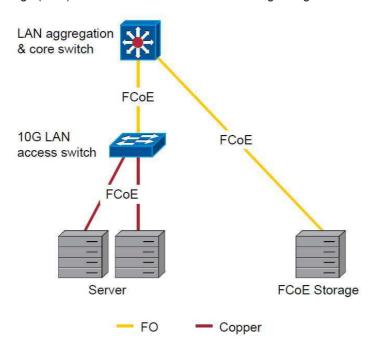


Figure 12: Stage 3 Migration of FCoE

4.4 Data Centre Infrastructure

- Data centres access doors shall be at least 1 meter wide and 2.1 meters high, lockable and have no thresholds.
- The data centre room shall have a head room of at least 2.6 meters, as seen in Figure 13, from the floor to the lowest installations and a loading capacity of more than 750 kg/m².
- A maximum filling level or 40% shall be estimated when dimensioning the cable tray
- Aisles shall have sufficient spacing of at least 1.2 meters to install and dismantle active components.
- If a raised floor is used, cabinet rows should be placed so that at least one side of the cabinets is
 flushed with the grid of the bas tiles and that at least one row of base tiles per passageway can be
 opened.
- Data centre shall be rectangular or square to provide consistent boundaries for elements such as air handlers, power distribution units and server rows.
- The external shell of the data centre must insulate the room from undesirable external conditions.
 This includes no windows or transparent walls
- New data centres shall use low energy lighting systems (such as timers or motion-active/zoned lighting). Existing data centres shall use energy efficient lighting to reduce heat.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 24 of 42

No external doors shall be used in the data centre. External meaning no doors leading directly to
the outside. If an external door is required due to fire regulations, it may only be used for exit. The
external door is required to only open from the inside and an alarm to deploy when the door is
used.

All interior finishes with in the data centre shall be static and dust-free surfaces.

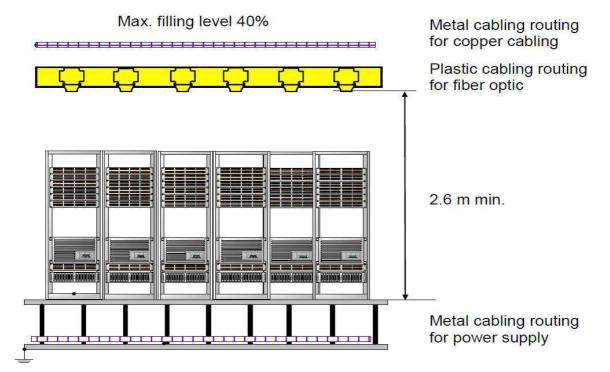


Figure 13: Mixed cable routing under ceiling and in hollow floor

4.4.1 Grounding

Ideally, low and high frequency potential equalization for EMC is meshed as tightly as possible between all metal masses, machine, racks and system components. The following applies:

- All patch panels must be grounded individually (no daisy chains)
- Patch panels must be grounded to the cabinet
- Cabinet itself must be bonded or grounded to the TMGB or TGB
- A minimal of conductor of 4-6 mm² shall be used for earthing
- Local regulations regarding grounding shall be followed
- International standard IEC 60364-5-54 shall be followed

A grounding tree structure shall be used to avoid ground loops and reduce interference from low frequency interference voltages. As seen in Figure 14 below, the individual grounding conductors are connecting with one another at a central grounding point. A high level view is seen in Figure 15

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **25 of 42**

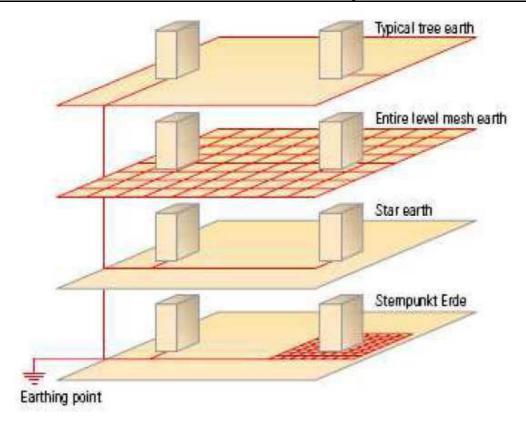


Figure 14: Grounding Systems as a Tree Structure

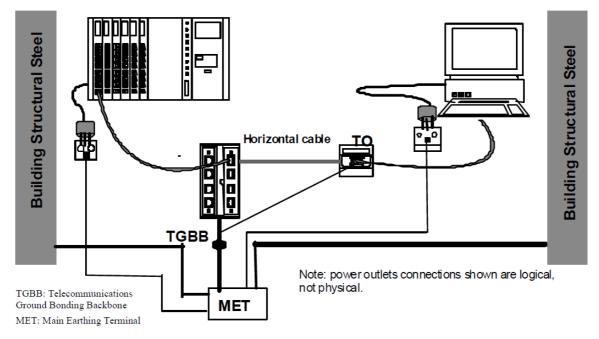


Figure 15: Simple High level Grounding Tree System Drawing

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **26 of 42**

4.5 Cabinets, Racks and Cables

4.5.1 General requirements

- 1) All cabinets and server racks shall conform to the EIA-310-D standard.
- 2) The data centre shall be designed with separate racks and pathways each by media type. Power and communication cables must be placed in separate pathways or separated by a physical barrier. Adequate space must be provided within and between cabinets and racks and in pathways for better cable management, bend radius protection and access.
- 3) Where the risk is identified, racks that require locks must be locked at all times. Only authorized employees may unlock the rack and must lock again when leaving the rack. Unsupervised unlocked racks are prohibited.
- 4) A labelling scheme is required for all racks, cabinets, patch panels, patch cords and cables.
- 5) Only approved cables as mentioned in 4.5.5 shall be used in the data centre.
- 6) Cables must be cut to length.
- 7) Cables must be labelled.
- 8) Cables must satisfy cabling requirements so that no losses in performance occurs
- 9) Cables must be tidy and hidden to prevent a tripping hazard or an accidental disconnect.
- 10) Cables entering the rack from ladder, tray or conduit shall have at least 0.15m space to form a large bend radius as shown in Figure 16 below.
- 11) Large cables groups shall be divided into multiple random bundles to prevent AXT effects.





Figure 16: Spacing to allow natural curvature of the cable

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **27 of 42**

4.5.2 Cabling Convention

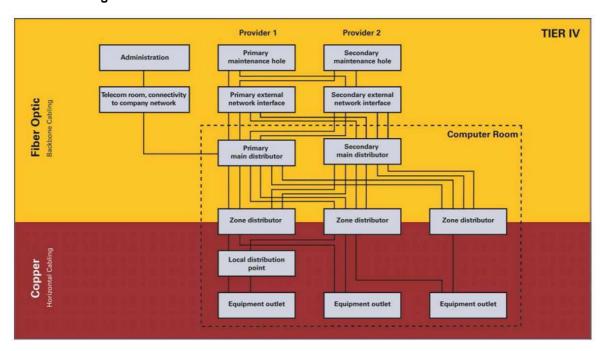


Figure 17: Tier IV Communications Cabling High-level

In Figure 17 above, the backbone cabling and all active components such as servers, switches, etc. as well as the uninterruptable power supply and the emergency power generator are redundant 2 * (N+1) which implies that two independent paths with redundancy are used to complete the task [7]. Horizontal cabling may also be redundant.

Uninterrupted systems and network functions must be ensured 24/7. This tier level ensures the design is completely fault tolerant. Maintenance and repair work can be performed without interrupting operations. There is no single point of failure.

4.5.3 Cabling Architecture

Placement of network components shall be placed in an area that has high potential for optimization. The ToR concept shall be applied. ToR advantages are:

- Little to no horizontal cabling
- Reduced installation costs
- Suitable for high server density
- Easy to add additional servers

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 28 of 42

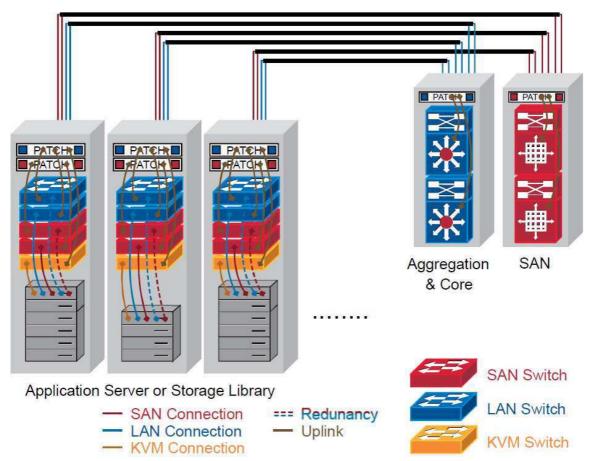


Figure 18: Top of Rack design 1

Figure 18 above shows the principle of cabling architecture. Cables are patched through to the patch panel, then to the relevant switch and then to the application server or storage library. The switches take priority nearest to the patch panel, and then followed by the application server or storage library. The KVM switch should be located nearest to the application server or storage library as shown above.

Application servers will start from the bottom. A redundant line to the KVM switch and a redundant KVM switch is not required as it does not affect the operations of the data centre. The KVM switch is used for configuration management and monitoring of devices.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 29 of 42

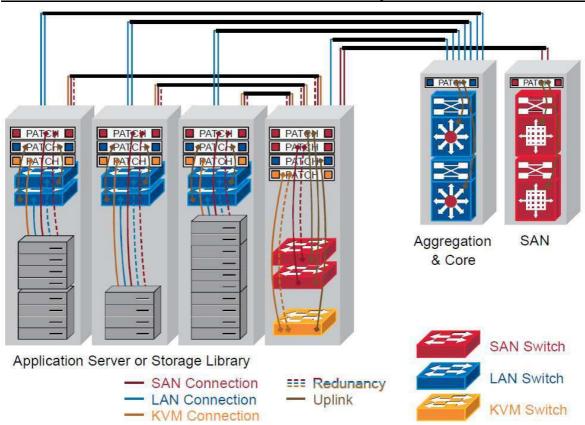


Figure 19: Top of Rack design 2

Figure 19 above shows a top of rack design to reduce the number of switches. In this example, a dedicated cabinet is used for the KVM and SAN switches which removes the need to put these switches in every cabinet. Important to note that no horizontal cabling is done, all cabling enters and leaves the cabinets through the designated path.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 30 of 42

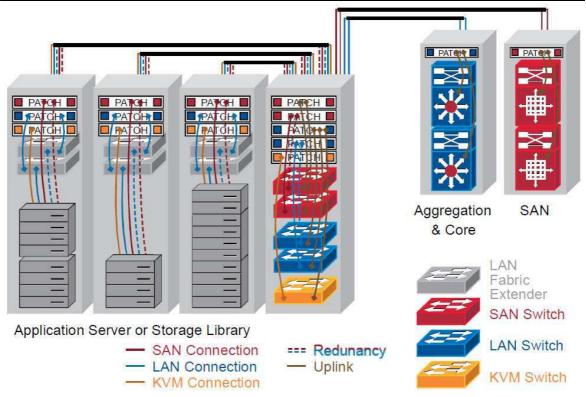


Figure 20: Top of Rack design 3

Figure 20 above shows a Cisco version where the LAN switch is also moved to a separate cabinet. A LAN fabric extender sits in each cabinet to provide LAN to the application server or storage library.

NOTE: The Top of Rack design convention is for cabinets where cabling is above the cabinet. In the event that the cabling convention is done underneath (under-floor installation) of the data centre, the above still holds true but in reverse. Example: Cabling from floors will patch to the patch panel located at the bottom of the cabinet. The switches will be located at the bottom after patch panels in the relevant order and the application server or storage library will start at the top of the cabinet.

Under-floor installations shall:

- 1) Have a minimum floor plenum depth of 800 mm.
- 2) Restrictions running across the airflow must be restricted to less than 20% of the plenum depth.
- 3) Restrictions shall run parallel with the air flow where possible.

4.5.4 Other variants

Depending on the cabinet, the other variants can be considered, as long as they follow the overall ToR convention.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 31 of 42

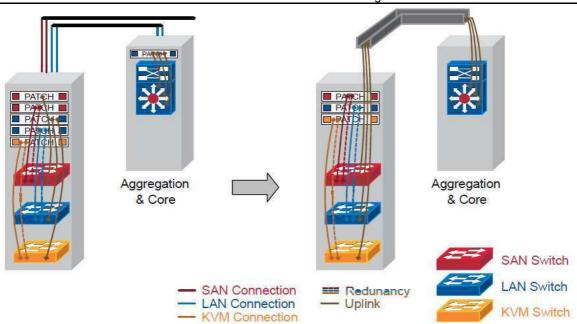


Figure 21: Top of Rack design - Saving on patch panel

Figure 21 shows a possible method of saving on patch panel and can be considered if the distance is small and few ports are required.

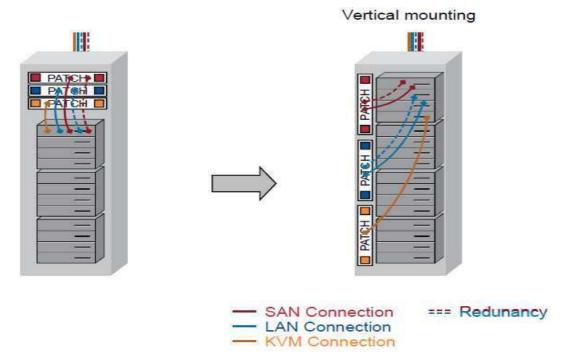


Figure 22: Top of Rack design - Vertical Mounting

Figure 22 above shows a translation from horizontal mounting to vertical mounting.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 32 of 42

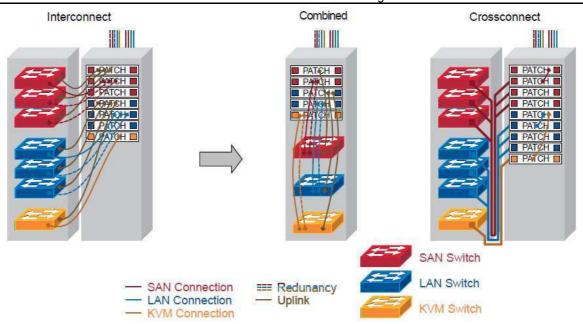


Figure 23: Top of Rack design - Crossconnect

In the case where two cabinets must be connected together, the ToR design must be followed. The result is either to use the combined or crossconnect approach as seen above in Figure 23.

4.5.5 Cabling media

The following telecommunication cabling system provides specifications for the following cabling media:

- 1) Standard single mode fibre
- 2) 50µm multimode fibre
- 3) Laser-optimised 50µm multimode fibre
- 4) 75-ohm coaxial cable
- 5) 4-pair Augmented Category 6 (CAT6A) UTP cable

4.5.6 Standard Patch Panel Termination and Cable Dressing

- Strip approximately 50 mm of cable jacket and cut off pair separator and ripcord flush to the jacket.
- Position the cable perpendicular to the panel.
- Centre cable closely behind the termination posts between the green and orange positions as seen in Figure 24.
- Patch the inner pairs first as seen in Figure 24
- Patch the outer pairs as seen in Figure 25
- The exposed points length must be minimized
- To minimize cable stress at termination a large bend radius shall be applied as seen in Figure 25.

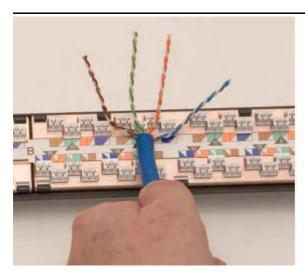
NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 33 of 42



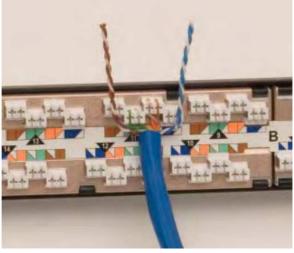
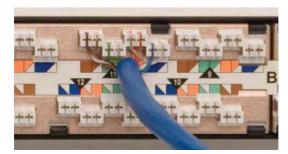


Figure 24: Wire placement (left); Inner pairs punched (right)



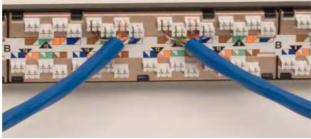


Figure 25: Outer pairs punched (left); Minimize cable stress by not using a tight bend radius (right)

4.5.7 Fibre Connections

Single mode fibre shall be used in the data centre to future proof the connection and ensure distance is not an issue. The fibre shall comply with the 240-70732902 - Fibre Optical Connector Standard.

4.6 Testing

Changes to the Date Centre shall first be tested on one section of the data centre (example Site A data centre) before rolling out to the whole data centre system. Therefore, if an error occurs, Site B data centre can take over and even provide a rollback configuration with no down time.

The redundancy of the data centre shall be tested every six months to ensure correct operations in event of a failure.

4.7 Power and UPS

- 1) The data centre must be supplied with sufficient electrical power to cope 'day-1' demands and foreseeable expansion plans.
- 2) A minimum 32 amp, 230V single phase feed shall be in all data centres. At least two feeds shall be required for redundancy and backup purposes.
- 3) Higher power ratings require more than 7 kW shall use either more 32 amp feeds or a three-phase supply, which should provide around 22 kW

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Revision: 1

Unique Identifier: 240-84323647

Page: **34 of 42**

- 4) The voltage for single phase shall be 220 240 VAC RMS
- 5) The voltage for three phases shall be 380 400 VAC RMS.
- 6) Where possible, equipment shall be dual powered.
- 7) All equipment within the data centre shall be protected against electrical disturbances such as electrical storms, fluctuations within the facility, utility low voltage (brown outs, sags, etc.), variations in voltage frequency, etc.
- 8) Data centres shall have:
 - Dedicated powers distributions systems
 - Power conditioning equipment
 - Over and Under voltage protection
 - Lightning arrester's and grounding system
 - UPS
- 9) The maximum consumption per cabinet to be designed for is 27kW per cabinet.
- High power density equipment shall be spaced throughout the data centre in a balanced manner to deduce the power and cooling requirements.
- 11) Rows or zones within a data centre that are to be deployed in the future shall be planned as high density value and primary feed wiring and piping must be installed up-front. Actual selection of power and cooling equipment shall be deferred until the deployment plans are defined.
- 12) Circuit protection shall be one per machine.
- 13) Circuit breaks shall not operate above 80% of their RMS current ratings.
- 14) Distribution boards shall be clearly marked.
- 15) Circuits and distribution boards shall be monitored for overloading.
- 16) Certificate of compliance should be issued with all new installations.

4.7.1 Energy efficiency

- 1) Where possible and financial feasible, energy efficiency techniques shall be applied to achieve a PUE less than 2.0
- 2) Optimizing power distribution by minimizing the conversions required in the data centre.

4.7.2 Standby Generators

A generator shall be installed to supply power with enough fuel for at least 2 weeks and is kept securely onsite.

Generators shall be tested once every two months under load for 30 minutes.

The data centre shall have an independent standby power supply.

The generator shall be capable of handling full load, including the air-conditioners.

The generator shall start automatically within 30 seconds of power failure.

The generator shall be capable of operating at least 24 hours without refuel.

The generator shall be equipped with an emergency override switch that allows the user to start the generator manually in the event of a control system failure.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **35 of 42**

4.7.3 Uninterruptable Power Supply System

- 1) The data centre shall operate 24 hours per day, 365 days per year without any interruption in the power supply.
- 2) The UPS shall operate automatically in the event of a mains power failure. The data centre shall be unaffected [7].
- 3) A UPS system must be in place to operate the data centre for 12 hours.
- 4) The UPS shall be capable of handling the full data centre load for a period of 30 minutes.
- 5) The UPS shall be a double conversion on-line system as shown in Figure 26.
- 6) The UPS shall be capable of recharging the standby batteries within 4 hours after a full discharge.
- 7) The UPS shall have 100% parallel redundant.
- 8) The UPS shall be tested once every 3 months.
- 9) The UPS shall be on a service contract.
- 10) The UPS must have a remote alarm panel and remotely monitored with an alarm facility.
- 11) The load on the UPS must be balanced

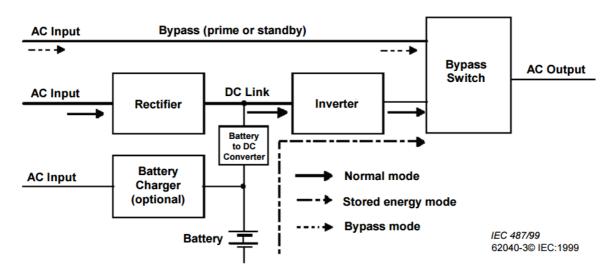


Figure 26: Double conversion on-line UPS topology, from IEC 60240-3 block diagram showing four converter blocks

4.7.4 Measuring Data Centre Power and Energy Consumption

The power and energy consumption for all data centres within Eskom shall be measured at the data centre level (utility meter), sub-system level (hardware load at the plug) as well as at hardware compute load level (server and networking equipment level).

4.8 Fire Detection and Suppression Systems

- 1) An independent zoned fire detection and fire suppression system shall be installed complete with detectors, siren, bell and lock off until in all data centres.
- 2) A sufficient quantity of optical smoke detection (EFD) as well as air-sampling or carbon dioxide / monoxide sensors shall be deployed in data centres.
- 3) One potential free contact for the shutdown of the air-conditioning system shall be supplied.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Revision: 1

Page: **36 of 42**

Unique Identifier: 240-84323647

4) Data centres shall have portable fire extinguishers mounted in key locations around the data centres

- 5) All firefighting equipment shall have an independent battery supply.
- 6) All firefighting equipment shall be serviced and inspected as per local bylaws.
- 7) An automatic detection and suppression system shall be installed opposite to where the electrical outlets are located. (If electrical outlets are above, the system shall be installed under the raised floor.)
- 8) The data centre shall use a gas extinguisher to prevent damage to the equipment.
- 9) The extinguishing system shall be designed redundantly to prevent false alarms.
- 10) The data centre shall shut down all electrical power before activating the fire suppression systems.
- 11) Schematic diagram of all fire detectors and nozzles shall be available.
- 12) All safety signs and colour-coding shall be done as per building regulations as well as local by-laws.

4.8.1 Fire Risk outside the data centre

Due to the systems and preventative measures placed inside the data centre, it is more likely for a data centre to be damaged from outside fires than internal fires. It is therefore essential that the surrounding area has adequate fire preventative measures to protect the physical location of the data centre and its internal equipment.

4.9 Water Risk

The data centre should have limited to no use and storage of water/liquids inside the data centre. The data centre shall be water tight to prevent water leakage from the outside. The most likely case of flooding is water extinguishing systems from outside the data centre could compromise the data centre. Water tightness must be certified with EN-60529 compliance.

4.10 Smoke Risk

Smoke with harmful particles, like burning plastics that release hydrochloric acid gas, can corrode equipment. Therefore, the data centre shall have a protection class of IP56 (Internal Protection Marking).

4.11 Unauthorized Access Risk

- 1) Access to all entry points into and within the data centre shall be protected by electronic access and control systems with different access levels (see 4.14)
- 2) The physical security shall comply with burglar protection in accordance with EN 1627 with resistance class III or equivalent.
- All data centres shall have integrated a video camera system that complies to the Specification for CCCTV Surveillance with Intruder Detection.
- 4) The surveillance system shall monitor both internal and external areas of the data centre.
- 5) The data centres' security system shall be functional at all times, complete with uninterruptable power supply for ensuring its continuous operation.
- 6) Scheduled and unscheduled security, fire and safety inspection shall be done as per policy requirements.
- 7) The access control security system shall be serviced and inspected as per local bylaws.
- 8) An anti-pass back system shall be included to prevent a cardholder from passing their card to a second person to gain entry into the same control area (example: finger print.)

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **37 of 42**

9) The access door shall not be blocked open without approval by the system owner and shall be monitored by an authorized employee for the full duration of the exception.

- 10) All processes shall be monitored and documented as per the CSSOT.
- 11) Where possible, the air-conditioning systems, electrical equipment and extinguishing equipment shall be physically separated from the server room as to allow the systems to be serviced from the outside.
- Only authorized Eskom employees shall have physical access to the data centre. Any unauthorized person shall be accompanied by an authorized employee at all times.
- 13) Under no circumstance shall an unauthorized person be left unattended in the data centre.
- 14) If any evidence (pictures, recordings, etc.) are taken by an unauthorized person, they shall be authorized before any evidence can be taken and final product must be approved on site before the unauthorized personal may leave the site to prevent compromising evidence leaving the data centre.

4.12 Building Management System

- 1) The data centre or server room shall have a temperature and humidification recorders.
- 2) An alarm shall be raised if the temperature and humidification levels are out of specified ranges.
- 3) All environmental alarm conditions shall be escalated to carious users.
- 4) A monthly inspection sheet shall be available and executed.
- 5) The BMS shall be able to send remote alarm signals.
- 6) The BMS shall be able to assist service staff with relevant information. (Trends, graphs, etc.)
- 7) The BMS shall monitor air-conditioners, cooling, power, generator, fire system, UPS and doors at cabinet level.
- 8) Under-floor water detection shall be installed at all Eskom data centres
- 9) The BMS shall be able to integrate on an enterprise wide facilities monitoring and management system.

4.13 Explosion Risk

This risk of attacks or other catastrophes which could trigger an explosion must be factored in the design of the data centre. The data centre shall undergo an explosion test in accordance with the CPNI Standard.

4.14 Security Zones

4.15 Maintenance

- 1) All hardware in the data centre will have a maintenance strategy that shall be adhered to.
- 2) The maintenance strategy will also detail the number of spares that shall be located at each data centre at all times.
- 3) These spares shall be securely stored in a manner that the equipment can be replaced at any time.
- 4) The necessary tools to make these changes shall also be stored securely in the same manner.

4.16 Cooling

- 1) A raised-floor system shall be used for adequate and flexible cooling.
- 2) The cooling system shall be designed to operate 24 hours per day, 365 days per year.
- 3) The cooling system shall be capable of handling 40% more than the current heat load.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 38 of 42

- 4) Air conditioning equipment filters must have a minimum rating of 45%.
- 5) The following shall be monitored: air filtration, cooling and dehumidification, humidification and reheating.
- 6) Cabinets and racks should be arranged in an alternating pattern to create 'hot' and 'cold' aisles.
- 7) Closed-circuit air condition or any other method can be used to implement the raised-floor cooling system as shown in Figure 27.
- 8) The cold aisle shall be between 18° C and 27° C with a target of 23° C.
- 9) A maximum temperature fluctuation of 5° C per hour in the aisles.
- 10) The server room air humidity shall be between 40% and 60% RH without condensation.
- 11) The server room air humidity maximum rate of change shall not exceed 6% RH per hour.
- 12) Cabinets and racks with gaps must be blocked to ensure the air flow integrity.
- 13) The raised floor shall be at least 0.8 meters in height.
- 14) Data and power supply cables must be separated in accordance with EN 50174-2.
- 15) If under ceiling cabling is used, distance between the power and data cables must also comply with EN 50174-2.
- 16) Under ceiling cabling must not obstruct lighting, security sensors and fire extinguishing systems.

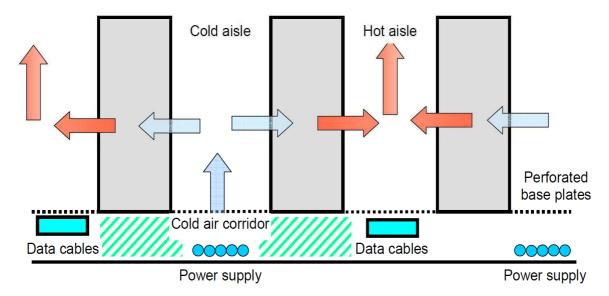


Figure 27: Hot Aisle / Cold Aisle Cooling of under-floor installations

Perforated tiles in the raised floor of the cold aisles allow cold air to be drawn into the face of the equipment. This cold air washes over the equipment and is expelled out the back into the hot aisle. There are no perforated tiles in the hot aisle which prevents hot air from mingling with the cold air. This can be seen in Figure 27 and Figure 28.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 39 of 42

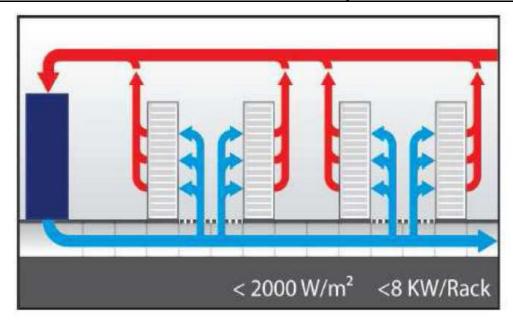


Figure 28: Air conditioning via raised floor with racks arranged in cold/hot aisles

Other considerations for cooling include the following:

- 1) Increasing airflow by clocking unnecessary air escapes and/or increasing the height of raised floor.
- 2) Spread equipment out over unused portions of the raised floor.
- 3) Use open racks instead of cabinets when security is not a concern (e.g. No USBs that could be removed.), or use cabinets with mesh fronts and backs.
- 4) Use perforated tiles with larger openings.
- 5) Free cooling shall be considered to maximise efficiency gains in cooling. Free cooling uses the outside air and/or water to cool the data centre.

4.17 Virtualization

The data centre will utilize virtualization on a software level (e.g. VMware).

This will allow the following benefits:

- 1) Less server hardware required.
- 2) Reduced energy requirements
- 3) Resource management is simplified.
- 4) Recovery simplified
- 5) Application flexibility across data centres
- 6) Reduced operation costs

The data centre shall comply to Figure 29 that shows a basic SAN structure with virtual storage. The data shall be stored in a "cloud" where the actual location is unimportant.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: 40 of 42

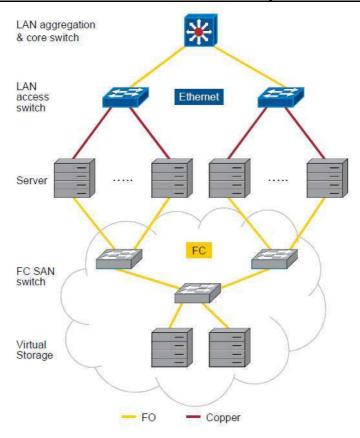


Figure 29: SAN Structure with Virtual Storage

4.18 Decommissioning of Assets

All assets must be physically destroyed to prevent any form of data harvesting. The assets must be destroyed before leaving the physical security perimeter or given to a 3rd party.

4.19 Remote Connections

No remote connections into the data centre production network or management network is allowed. All configurations shall be done locally at the data centre site. If a remote connect is required, it shall follow the exception process and must follow the

4.20 Maintaining the Data Centre Environment

- 1) All data centre sites shall adhere to the Safety, Health, Environment and Quality Policy (32-727), ISO 14001 and all regulations as per the Occupational Health and Safety Act (85 of 1993).
- 2) A safety representative shall be appointed at each site.
- 3) Monthly safety reports shall be sent to the safety coordinator at head office.
- 4) The safety coordinator and the electrical "competent" officer shall do a yearly safety audit.
- 5) Monthly checklists shall be available and kept for reference.
- 6) All safety signs and procedures shall be installed and made available.

NETWORK MANAGEMENT CENTRE REDUNDANCY

STANDARD

Unique Identifier: 240-84323647

Revision: 1

Page: **41 of 42**

- 7) Daily walkthrough inspections shall be conducted.
- 8) Any failure or abnormal conditions shall be reported to the landlord immediately.
- 9) The site shall be clean and neat at all times.
- 10) Change control procedures shall be followed.
- 11) Access control shall be monitored.
- 12) No flammable items shall be stored in the server room.
- 13) Data centre log book shall be signed by all personal including visitors.
- 14) No electric tools shall be plugged into dedicated power points.
- 15) Doors shall be kept closed at all times except where authorized work prohibits this.
- 16) No smoking or eating in the server room.
- No equipment shall be removed from the data centre and server room without the explicit permission of the system owner or a delegated representative.
- 18) No changes to any equipment or electrical settings are permitted. E.g. Air conditioner, electrical distribution board.
- 19) All work related debris and tools shall be removed immediately.

4.21 Certifications and Audits

The data centre shall obtain certifications to reduce the possibility of security weaknesses, increase reliability and promote an efficient data centre.

At minimum, the major certification and audits that the data centre shall comply to are:

- 1. ISO 27001 Information Security Management Systems
- 2. ISO 27001 Basic IT Protection
- 3. ISO 9001 Quality Management
- 4. ISO 14001 Environmental Management

5. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Danie Du Plessis	Senior Manager – Grids
Paul Grobler	Chief Engineer – TX
Sikelela Mkhabela	Senior Manager – DX
Prudence Madiba	Senior Manager – GX
Joe Manyisa	Senior Manager - Eskom Telecommunications (Acting)
Sean Maritz	Senior Manager – GIT

6. Revisions

Date	Rev	Compiler	Remarks
March 2015	1	M Taljaard	First issue

NETWORK MANAGEMENT CENTRE REDUNDANCY Unique Identifier: 240-84323647

STANDARD

Revision: 1

Page: **42 of 42**

7. Development team

The following people were involved in the development of this document:

Matthew Taljaard

8. Acknowledgements

- Bongani Shezi
- Chris Van Wyk
- Eddie Langford