Information is required to evaluate the maturity and suitability of Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) for deployment within NTCSA's Operational Technology (OT) environment.

List of Abbreviations

Abbreviation	Description
BOM	Bill of Materials
BSS	Business Support System
CPU	Central Processing Unit
HDD	Hard Disk Drive
IP	Internet Protocol
MPLS	Multiprotocol Label Switching
NBI	North Bound Interfaces
NFV	Network Function Visualisation
NTCSA	National Transmission Company South Africa
OSS	Operational Support Systems
OT	Operational Technology
PDH	Plesiochronous Digital Hierarchy
PoC	Proof of Concept
QoS	Quality of Service
RAM	Random Access Memory
RBAC	Role-based Access Control
RFI	Request For Information
RTO	Recovery Time Objective
SDH	Synchronous Digital Hierarchy

SDN	**Software Defined Networks**
SSD	**Solid State Drive**
TCO	**Total Cost of Ownership**
TDM	**Time Division Multiplexing**
TSN	**Time-sensitive Networking**
VNF	**Visualised Network Function**

1. Background

The introduction of Software-Defined Networking (SDN) into modern communication networks allegedly provides significant advantages by decoupling the control plane from the data plane. In traditional network architectures, each network device independently performs both decision-making (control plane) and packet forwarding (data plane), resulting in distributed complexity, limited flexibility, and difficult management. SDN addresses these challenges by centralising the control plane within a logically centralised controller, while network devices operate as simple forwarding elements.

This separation enables a global view of the network, allowing for more intelligent and optimised routing decisions based on real-time conditions such as congestion, latency, and application requirements. Furthermore, SDN introduces programmability through software-based control, enabling rapid network configuration, automation, and dynamic policy enforcement without the need for manual device-level intervention. This can reportedly improve operational efficiency, reduce configuration errors, and lower operational costs. In large-scale telecommunication networks such as those operated by NTCSA, this technology can be particularly useful for improving scalability, simplifying network management, and enhancing overall network performance. In addition, the integration of Network Functions Virtualization (NFV) reportedly further simplifies the telecommunications network by enabling critical functions such as firewalls, routing, and load balancing to operate as virtualized services on standard hardware.

A key consideration is whether NTCSA can leverage SDN and NFV to establish redundant paths for mission critical or high-priority traffic. Accordingly, NTCSA seeks to understand how these technologies can be used to simplify network management and how redundancy mechanisms can be implemented through their integration. In particular, the focus is on how SDN and NFV can work together to dynamically create and manage resilient, redundant links that ensure high availability (99.999%) and continuity of service for mission-critical traffic.

Traditional network architectures, such as those used by NTCSA, face several operational and maintenance challenges, including complex and time-consuming device-level management, slow fault detection and recovery, limited scalability when expanding the network, high operational and maintenance costs due to reliance on specialised hardware, and inconsistent security policy enforcement. Additionally, these networks lack flexibility and real-time adaptability, making it cumbersome to efficiently manage traffic and maintain high availability for critical services.

To address these challenges, NTCSA is seeking detailed information on SDN and NFV. This should include how these technologies can be effectively integrated into existing networks including the Wide Area Network (WAN), data centre environments, and substation Local Area Networks (LAN). This detail must be accompanied with suitable migration mechanisms from traditional architectures, and the frameworks and standards to follow when designing and implementing SDN/NFV-based networks. In addition, NTCSA requires guidance on interoperability with legacy systems, scalability considerations, cybersecurity implications, redundancy and high-availability strategies, performance management, and the operational skills and tools required to support and maintain such a network.

NTCSA intends to use the information received through this RFI to gain a comprehensive understanding of how SDN and NFV technologies are implemented within Electrical Power Utilities' (EPUs) private OT environment. The objective is to identify the best practices, frameworks, and standards to follow when designing and deploying different types of SDN/NFV architectures, while also understanding the potential cyber threats associated with these technologies. Furthermore, NTCSA seeks insights into how SDN/NFV solutions can be leveraged to enhance network management, improve operational efficiency, enable dynamic traffic control, and ensure high availability and redundancy for critical services across its extensive and distributed network infrastructure. This information will support informed decision-making for future network modernisation initiatives.

2. NTCSA User Requirements

Respondents must provide details addressing the following core areas:

2.1 General Requirements:

a) For the supplier to clearly state all open standard communication protocols if the proposed SDN/NFV solution requires integration with existing/current NTCSA Telecoms OSS/BSS systems.

- Give full description of the North Bound Interfaces (NBI) available for integration with Telecoms OSS/BSS.

b) The communication protocols between the VNFs and VNFs-to-SDN controller shall be secured.

c) The solution shall support all EPU protocols.

d) Multi-factor authentication shall be required for access to SDN/NFV infrastructure, including SDN controller software and VNFs.

e) The solution shall implement role-based access control (RBAC) to manage access to SDN/NFV infrastructure, including SDN controller software and VNFs.

f) The solution must guarantee zero data loss and achieve a Recovery Time Objective (RTO) of 8 to 24 hours.

g) The solution should implement an active-active (hot) disaster recovery architecture.

h) The solution shall provide real-time and historical performance monitoring capabilities, including but not limited to packet loss, latency, jitter, and other relevant network performance metrics.

i) The proposed SDN/NFV architecture shall demonstrate the implementation of Quality of Service (QoS) mechanisms to ensure efficient traffic prioritisation and performance.

j) The supplier shall provide detailed specifications for the recommended computing resources, storage resources, and VNFs:

- Computing resources: CPU, Processor, RAM capacity, and virtualization support.
- Storage resources: storage type Solid State Drive (SSD) or Hard Disk Drive (HDD), capacity, redundancy mechanisms, and scalability options
- VNF specifications: type of VNFs, functional description, resource requirements (CPU, memory, storage), and performance capabilities

k) Supplier must provide SDN/NFV architecture management policies, including but not limited to:

- Software and firmware lifecycle and update management.
- Bug and vulnerability assessment, identification, and mitigation strategies for the SDN/NFV environment.

2.2 Use Case Requirements:

a) The supplier shall provide evidence of successful implementation of SDN/NFV-based architecture in an Operational Technology (OT) environment. The solution shall demonstrate, at a minimum, implementation of:

i. Grid monitoring and control services (SCADA functionality)

ii. Logging of errors and faults based on SDN/NFV network elements examination

iii. QoS enforcement and bandwidth management

iv. Failover and disaster recovery capabilities

v. High availability and redundancy mechanisms for critical grid control services.

b) The supplier shall identify and describe the expected improvements and potential challenges observed in the organisation's network following the successful deployment of an SDN/NFV solution. Key aspects for the supplier to comment on include but not limited to:

vi. Network agility, scalability, cost reduction, and network visibility

vii. Network vulnerabilities

viii. Complexity of the network

ix. Required skill set for operating and managing SDN/NFV network architecture.

2.3 Management System Requirements:

a) The supplier to provide licence management policy that at minimum covers how the licenses are generated, stored and distributed.

b) The solution shall incorporate real-time monitoring (graphic visualisation) of SDN/NFV components to enable timely detection and identification of network faults as they occur.

c) The solution shall support automation of monthly service performance reports with an option to include out-of-service maintenance window.

2.4 Maturity Requirements

a) The proposed technologies shall be proven in production environments and not limited to laboratory, prototype or pilot implementations.

b) The proposed technologies shall demonstrate industry adoption, including:

- Multiple operational deployments
- Use in critical infrastructure environments
- Availability of reference installations.

c) The proposed technologies shall be well understood from an operational perspective, with available documentation, support, and established maintenance practices.

d) The proposed technologies shall support secure deployment in OT environments and align with recognized cybersecurity practices for critical infrastructure.

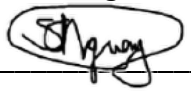
e) The proposed technologies shall comply with applicable IEC, IEEE, IETF, or equivalent industry standards relevant to power utility and OT environments.

f) The proposed technologies shall be practically deployed within power utility OT environments, considering latency, availability, reliability, and operational constraints.

Yours faithfully

Name: Oscar Ngwenya

Designation: Chief Engineer Prof Engin

Signature: 

Name: Khehla Gumede

Designation: Learner Intern Grad Engin

Signature: