Eskom	Standard	Technology

Title: **DEMILITARISED ZONE (DMZ) DESIGNS FOR OPERATIONAL TECHNOLOGY**

Unique Identifier:	**240-79669677**
Alternative Reference Number:	**<n/a>**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**Draft 1.1**
Total Pages:	**12**
Next Review Date:	**March 2023**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	**Approved by**	**Authorized by**
Billy Petzer	**Richard McCurrach**	**Willy Majola**
Engineer, PTM&C	**Senior Manager – PTM&C CoE**	**SGM Engineering**
Date:	Date:	Date:

Supported by SCOT/SC

Prathaban Moodley

Smart Grid Technology Study Committee Chairperson

Date:

PCM Reference: **<xxxxxx>**

SCOT Study Committee Number/Name: **<Number or name>**

Content

Figures

1. Introduction

A Demilitarised Zone (DMZ) is a common limited network of servers joining two or more zones for the purpose of controlling data flow between zones [3]. The purpose of a DMZ is to provide network segregation with the intent of isolating network traffic. It enforces a network's internal policy for external information exchange and provides external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks.

The proceeding document details the standard for Demilitarised Zone designs within the Eskom Operational Technology (OT) environment. The user of this document must consider the environment within which the DMZ will be deployed when choosing the applicable design. The security zones, firewall /UTM rules, guidelines and principles (Section 3.2 to 3.9) will apply to all DMZ designs whilst considering the OT environment of implementation.

2. Supporting Clauses

2.1 Scope

The scope of this document includes the definition of a DMZ within the Eskom OT environment.

2.1.1 Purpose

The purpose of this document is to provide controls that are to be implemented in the Eskom OT environment. This is to prevent cyber related attacks on OT systems from affecting Information Technology (IT) systems as well as to prevent cyber related attacks from the Eskom IT environment affecting the Eskom OT environment

2.1.2 Applicability

This document shall apply to the OT environments throughout Eskom Holdings SOC Ltd.

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] ISO 9001 Quality Management Systems.

[2] 240-55410927: Cyber Security Standard for Operational Technology

2.2.2 Informative

[3] BS IEC 62443-3-3 : 2013 : Industrial communication networks - Network and system security

[4] 240-55863502: Definition of Operational Technology (OT) and OT/IT collaboration accountabilities

[5] 32-373: Information Security - IT/OT and Third Party Remote Access Standard

[6] 32-377: Information Security – Firewall Standard

2.3 Definitions

2.3.1 General

Definition	Description
Critical Cyber Asset	Cyber assets essential to the reliable operation of critical assets.
Critical OT Systems	OT Systems that include critical cyber assets [2].
Cyber Asset	Programmable electronic devices and communication networks including hardware, software and data that are connected to a network with a routable protocol.
Demilitarised Zone	A perimeter network segment that is logically inserted between internal and external networks.
External Network	A network that is not the primary focus of protection, but which requires information exchange with the network that is the primary focus of protection (the internal network). The external network is viewed as untrusted.
Firewall	Firewalls are devices or programs that control the flow of network traffic between networks or hosts employing differing security postures.
GREEN Interface	Eskom's Operational Technology network (Internal).
Internal Network	In the context of industrial automation and control systems, the term internal network refers to the segment of the network that is the primary focus of protection. The internal network is viewed as trusted.
Intrusion Prevention System	Identifies anomalous traffic, issues alerts and blocks traffic from proceeding further according to a rule base defined.
Layer 7	Application based inspection, with port based flow control.
Less Critical OT Systems	Systems that rely on or connected to critical OT systems that has limited control and impact on the Eskom power system, or the information stored on the system is not classified as secret or top secret
Operational Technology (OT)	OT is the technology that is used to operate, monitor and control the power system. For a more specific definition refer to the OT Practice Note [4].
ORANGE Interface	Demilitarised Zone (DMZ).
OT Systems	Are all systems (including electronic, telecommunications, computer systems and components) which process, store or communicate operational data or information [2].
RED Interface	Eskom's Business network or IT enterprise network.
Secret	The classification given to information that may be used by malicious/opposing/hostile elements to disrupt the objectives and functions of Eskom Holdings SOC Limited.
System Owner	The System Owner is the authorised Eskom representative that has overall accountability for the OT system.
Top Secret	The classification given to information that may be used by malicious/opposing/hostile elements to **neutralize** the objectives and functions of Eskom Holdings SOC Limited.
Trusted	The internal network with the highest security posture. The trusted network contains systems (e.g. critical cyber assets) that require protection from the threats posed by external networks.

Definition	Description
Unified Threat Management	Security features that protect a system against viruses, malicious threats, cyber-attacks, spyware, Trojans and zero day attacks.
Untrusted	An external network with a different security posture than the trusted network. The untrusted network is viewed as unsecure and the potential source of cyberattacks on the trusted network.

2.3.2 Disclosure Classification

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

2.4 Abbreviations

Abbreviation	Description
CVE	Common Vulnerabilities and Exposures
DMZ	Demilitarised Zone
ESP	Electronic Secure Perimeter
FTP	File Transfer Protocol
HTML	HyperText Markup Language
ICMP	Internet Control Messaging Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
NAT	Network Address Translation
OEM	Original Equipment Manufacturer
OT	Operational Technology
SIEM	Security Incident and Event Monitoring
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
TCP	Transmission Control Protocol
UTM	Unified Threat Management
XSS	Cross- Site Scripting

2.5 Roles and Responsibilities

The implementation of this standard is the accountability of the Eskom OT System owners. The Eskom OT System owners may delegate the responsibility of the implementation, management and support of the devices defined in this standard.

2.6 Process for monitoring

This document will be revised from time to time as required, as the review of Eskom's corporate strategy and as functional IT, OT, Technology and Smart Grid strategies evolve, and will ultimately be superseded by revisions of the relevant policy and procedure documents.

2.7 Related/Supporting Documents

Not applicable.

3. DMZ Design Requirements

When designing the DMZ interface:

a) The external facing OT firewall shall be a Layer 7 UTM (Unified Threat Management with IPS (Intrusion Prevention System) functionality. The layer 7 UTM and IPS can be on the same security appliance, or be separate security appliances.

b) No critical data shall pass through the OT Layer 7 Unified Threat Management (UTM) connected to the IT business network.

c) It should be possible to disconnect the OT system from this firewall if an attack is taking place, while the OT system is still functioning.

d) If there are multiple machines in the DMZ performing different functions, the DMZ should be virtually divided into multiple DMZ's, to limit the damage if a server is compromised.

e) Any hosts in a DMZ should be hardened from attacks from the untrusted zone, as well as from other compromised hosts within the DMZ.

It should be noted that the following configuration diagrams do not illustrate system redundancy that may be required for high availability applications.

3.1 Security Zones

Network security zones operate on the concept of "trust". Each zone is assigned a level of trust, and trust increases from the outer most layers to the inner most layer where OT systems are located. Any systems that receive traffic from untrusted networks is at risk of being compromised. A DMZ is designed with the assumption that any DMZ host may be compromised, therefore the DMZ is designed to contain the compromise and prevent it from spreading to trusted networks.

Communication may only occur between adjacent zones and may not jump a zone. Traffic directionality between zones must be taken into account.

All security zones shall be implemented based on the system requirements and the identified risk mitigation. Networks have different security requirements relative to each other. From the perspective of the OT network, the IT network can be viewed as Untrusted, and from the perspective of the IT network, the OT network can be viewed as untrusted. Protection from the OT perspective is divided into the following zones:

- Trusted Zones
- DMZ Zones
- Untrusted Zones

3.2 DMZ Interface with ot systems

3.2.1 Critical OT Systems

For Critical OT systems [2] that have the capability to send controls to plant in the Eskom OT environment, the following configuration shall be used:

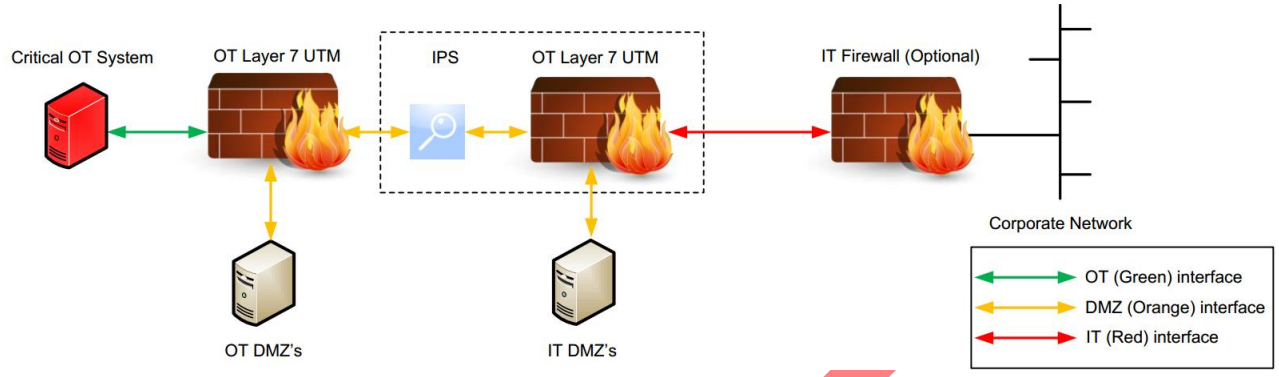

Figure 1: Configuration of Critical OT system

The Layer 7 UTM and IPS functionality may be on a single security appliance and the IPS rules shall be implemented on all its interfaces. The rules on both OT UTMs shall be set up to filter according to the security postures of their different interfaces. In the event of a compromise due to firewall failure, a dual OT-firewall DMZ requires two firewall failures before the trusted network is exposed, increasing the security for critical OT systems.

The IT firewall should be provisioned by Eskom Group IT according to the requirements set out in Eskom Group IT standards [6]. Provision is made for a DMZ for IT-related applications on the external facing OT UTM. Should no IT DMZ be implemented, it is still necessary to have two UTMs.

3.2.2 Less critical OT systems

If the OT system has limited control and impact on the Eskom power system, or the information stored on the system is not classified as secret or top secret, the following configuration may be used to reduce cost.

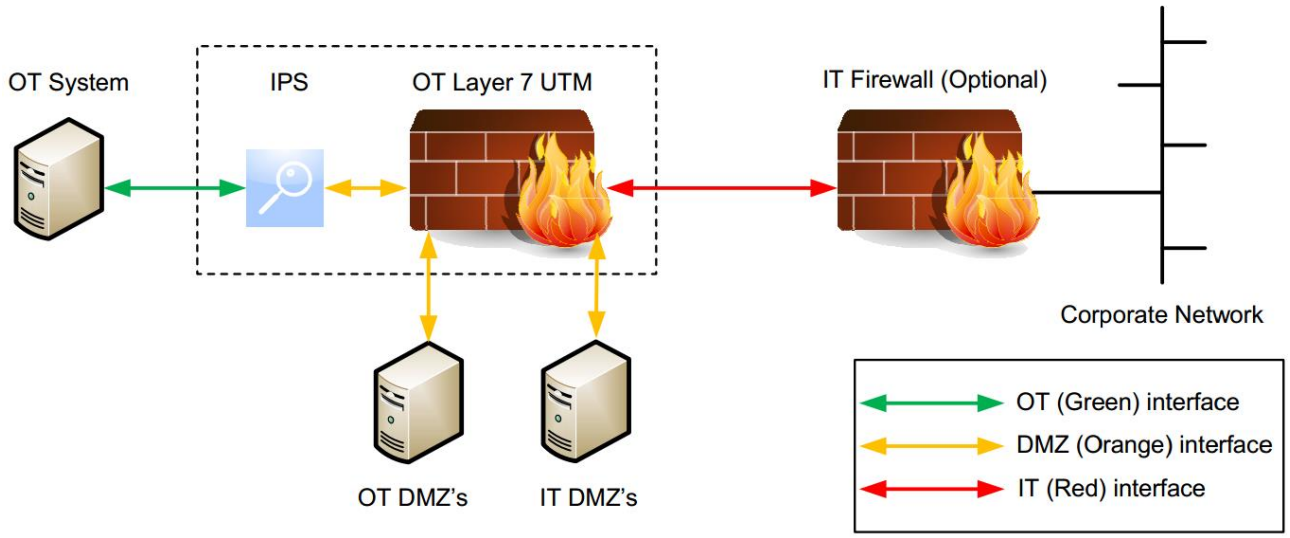

Figure 2: Less critical OT Systems

If possible, the OT system should only push data out to the DMZ, with no inbound connections allowed. The Layer 7 UTM and IPS may be a single device and the IPS rules shall be implemented on all interfaces.

3.2.3 OT/IT Interface

Where no incoming connections are required, and data is only pushed out of the OT zone into the IT zone, a configuration that uses unidirectional security gateways (e.g. network diodes, etc.) similar to Figure 3 below may be used:

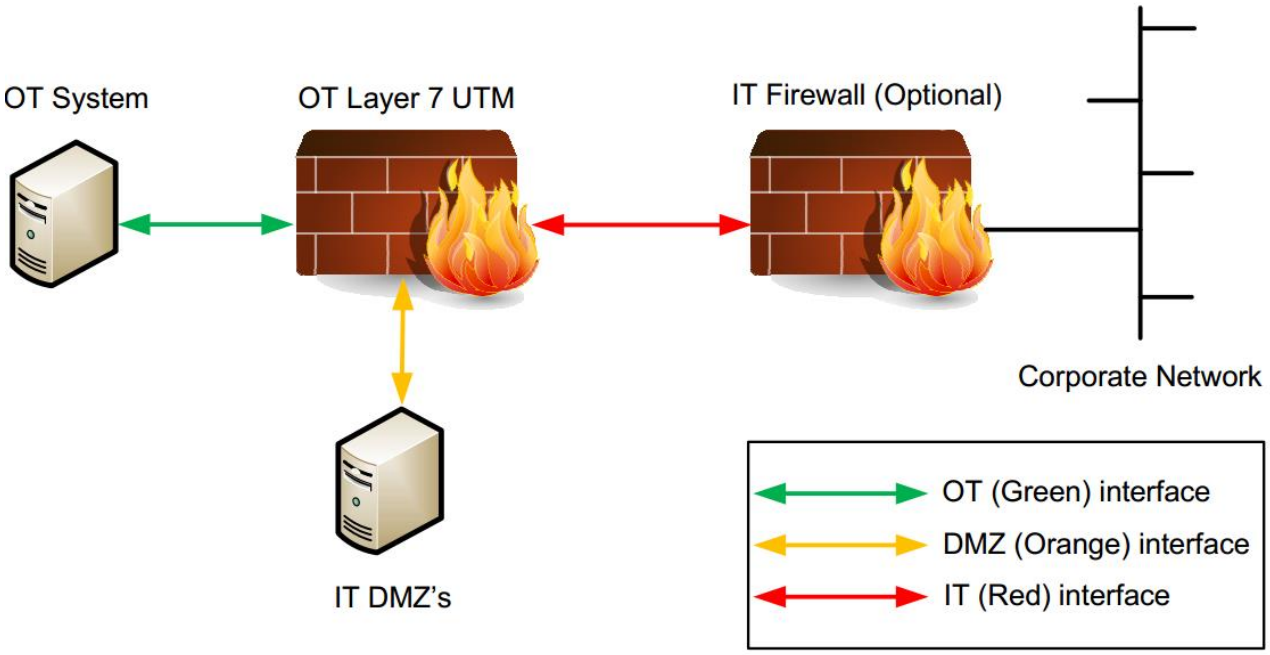

Figure 3: OT/IT Interface - unidirectional

3.3 UTM / Firewall Management

3.3.1 Connections from RED (external) Interface:

No connection initiated from the RED interface shall connect directly into the GREEN (OT) network zone. Only RED to ORANGE (DMZ) connections are allowed. The following RED to ORANGE principles apply:

a) Read Access:

This access is applicable when external users or systems will browse, read or consume information or for systems within the DMZ. i.e. read only access. No risk exists to integrity of internal data sources or systems.

b) Write Access:

This access is applicable when external users or systems will upload, write, update or alter data, information or systems within the DMZ but not the DMZ infrastructure. i.e. read/write access. Possible integrity risk exists to internal data sources or systems, controls shall be in place to provide assurance to integrity of data.

It is advisable to use different DMZ's for read only access and read/write access requirements.

3.3.2 Connections from GREEN (OT) Interface:

No connection initiated from the GREEN (OT) interface shall connect directly into the RED network zone. Only GREEN to ORANGE (DMZ) connections are allowed.

Connections are allowed from GREEN to ORANGE when data or information should be placed, altered or updated on the ORANGE side of the firewall.

a) Read Access:

This access is when internal users or systems will browse, read or consume information or systems within the DMZ. i.e. read only access. No risk exists to the integrity of internal data sources or systems.

b) Write Access:

This access is when internal users or systems will upload, write, update or alter data, information or systems in the destination network. Possible integrity risk exists to internal data sources or systems. Controls should be in place to provide assurance to integrity, e.g. Proxy server, Application server, Web Method, etc.

3.4 Threat Management

In the event of a cyber- attack, if the firewalls can be physically accessed, the firewalls shall be disconnected. Otherwise, the firewall shall be remotely accessed and all relevant interfaces on the firewall, besides the management interface, shall be shut down.

3.5 Firewall Rule Guidelines

Before a firewall rule can be created, a risk analysis shall be performed on the applications that will traverse the firewall and the services associated with the application.

The steps involved in creating firewall rules shall be as follows:

a) Identification of network applications deemed necessary;

b) Identification of vulnerabilities associated with applications;

c) Creation of application traffic matrix showing protection method; and

d) Creation of firewall rules based on applications traffic matrix.

e) Consideration for assuring **confidentiality** and the implications of a potential breach (breach impact, containment, etc.)

f) Consideration for assuring **data integrity** and the implications of a potential breach (breach impact, containment, etc.)

g) Consideration for assuring **availability** and the implications of a potential breach (breach impact, business continuity, preventative measures, etc.)

3.6 Implementing Firewall Rules

a) The default rule for the firewall for handling inbound and outbound traffic shall be to drop all packets and connections unless the traffic type and connections have been specifically permitted.

b) No firewall rule shall be defined with an “any” source or destination address or service.

c) Firewall platforms shall utilise rules as their mechanism for implementing security controls. The contents of these rules determine the actual functionality of a firewall. As a minimum, all rules shall contain the following fields:

- The source address of the packet, i.e. the Layer 3 address of the computer or device the network packet originated from (e.g. an IP or network address);
- The destination address of the packet, i.e. the Layer 3 address of the computer or device the network packet is destined to (e.g. an IP or network address);
- The type of traffic, i.e. the specific network protocol being used to communicate between the source and destination systems or devices – often Ethernet at Layer 2 and IP at Layer 3;
- Characteristics of the Layer 4 communication session – the protocol such as TCP;
- The destination ports of the sessions; source and destination ports shall be configured, software applications using port hopping is not recommended.

- An action, such as “Deny” or “Permit” the packet, or “Drop” the packet that does not return a response to the packet’s sender.

d) Firewall rules shall be built to be as specific as possible with regards to the network traffic control.

e) Rules shall be kept as simple as possible, so as not to accidentally introduce “holes” in the firewall that might allow unauthorised or unwanted traffic to transverse the firewall.

f) All firewall rule sets shall contain the following two rules:

- A “stealth rule” which drops all connections to the firewall system itself;
- A “drop rule” as the last rule which shall drop all connections not matched by the preceding rules.

g) The firewall rule set shall always block the following types of traffic:

- Inbound traffic from a non-authenticated source system with the destination address of the firewall system itself. This type of traffic normally represents some type of probe or attack against the firewall.
- Inbound traffic with a source address indicating that the packet originated on a network behind the firewall. This type of packet likely represents some type of spoofing.
- Inbound traffic containing ICMP traffic.
- Inbound traffic from a non-authenticated source system containing SNMP traffic.
- Inbound traffic containing IP Source Routing information.
- Inbound or outbound network traffic containing a source or destination address of 127.0.0.1 (local host). Such traffic is usually some type of attack against the firewall system itself.
- Inbound or outbound network traffic containing a source or destination address of 0.0.0.0.
- Inbound or outbound traffic containing directed broadcast addresses. A directed broadcast attack is a form of Denial of Service.

h) Address ranges (numbering) should be clearly (visibly) different between different network zones and should be able to identify what is public, private, DMZ, etc.

i) Under no circumstances is inbound traffic allowed to any OT server that is not in a DMZ.

j) Under no circumstances will original / actual internal IP addresses be exposed to networks external to the Electronic Security Perimeter (ESP) of the system [2]. To the internet/intranet, Network Address Translation (NAT) shall be used where exposure is required.

k) Inbound network traffic shall terminate in a DMZ and may not traverse two firewalls.

l) Inbound network traffic should traverse via at least 1 Layer 7 firewall (UTM) with deep packet inspection capabilities (IPS) to detect and prevent Cross-site Scripting (XSS), SQL Injection, HTML5 attacks, CVE exploits.

m) Firewall rules shall be reviewed on a bi-annual basis and all rules that are unused shall be deleted. Any changes shall follow the Engineering Change Control process.

n) The IPS shall be placed behind at least one Layer 4 firewall to reduce attack surface of the IPS and to improve accuracy of actual attacks on only exposed ports.

o) IPS and UTM signatures shall be updated on a regular basis or when critical signatures have been released by the OEM.

p) Time or period of use of rules shall be implemented as much as possible, e.g. an application might only require gaining access through the firewall for 10 minutes every day after 03h00.

q) Firewalls must be configured to prevent the initialization of administrative protocols from inside the DMZ (e.g. Telnet, FTP, SSH).

r) IPS shall fail closed so that when they fail they do not forward any packets whatsoever.

3.7 Firewall / UTM Access Logs

The following shall be adhered to:

a) Firewall / UTM logs shall be sent to a log server within the ESP (DMZ/private network).

b) All interactive sessions originating from a lower security zone shall be logged.

c) Attempts to access a service that is denied shall be logged.

d) All management connections to the firewall shall be logged. Management of the firewall should only be allowed from specified hosts that reside in the higher security interface of the firewall, or a dedicated management network.

A Security Incident and Event Monitoring (SIEM) system is recommended to analyse events and alert the monitoring team of any incidents identified via correlation rules.

3.8 Change Control

Change control needs to be implemented on all firewalls, routers, and switches within the DMZ. All changes need to be logged and the current configuration shall be archived. Change control process shall be adhered to as per the Cyber Security Standard for OT [2] and follow the ECM PCM.

4. Authorisation

This document has been seen and accepted by:

Name and surname	Designation
Prudence Madiba	Senior Manager – Control and Instrumentation
Richard McCurrach	Senior Manager – PTM&C Engineering
Lloyd Chego	Senior Manager – Security Division
Alison Maseko	Senior Manager – Eskom Telecommunications
Cornelius Naidoo	Middle Manager – Telecommunications Technology and Support
Steven Papadopoulos	Middle Manager – Control and Automation Technology and Support
Amelia Mtshali	Senior Manager – Metering, DC and Security Technology and Support
Prathaban Moodley	Chief Engineer – Research
Rosalette Botha	Corporate Specialist – System Operator
Johan Botha	Senior Consultant – System Operator
Geoffrey Ive	Chief Engineer – System Operator
Reshin Moodley	Chief Engineer – Security Division
Craig Boesack	Chief Engineer – Control and Instrumentation
Zameka Qabaka	Senior Technologist – Koeberg Power Station
Rishi Hariram	Chief Engineer – Control and Automation Technology
Ian Naicker	Chief Engineer – Control and Automation Technology
Tertius Hyman	Senior Engineer – Western Cape Operating Unit
Marius van Rensburg	Transmission Grid Representative

5. Revisions

Date	Rev	Compiler	Remarks
March 2018	Draft 1.1	Billy Petzer	Requirement for dual-Layer 7 UTM's from different OEMs removed for critical OT systems. Section on security zones expanded.
Jan 2015	1	Johan Botha	First Issue

6. Development team

- Billy Petzer
- Matthew Taljaard
- Tertius Hyman
- Jason Hector
- Michelle Govender
- Johan Botha

7. Acknowledgements

Not applicable.