

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

Unique Identifier: **240-79669677**

Alternative Reference Number: **n/a**

Area of Applicability: **Engineering**

Documentation Type: **Standard**

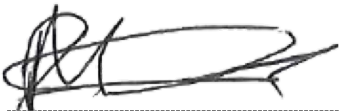
Revision: **3**

Total Pages: **28**

Next Review Date: **March 2029**

Disclosure Classification: **Controlled
Disclosure**

Compiled by



Kgomotso Manyapetsa
Chief Engineer - CATS

Date: 27/05/2024

Approved by



Judith Malinga
**Senior Manager - PTMC
SCOT Chair**

Date: 27/05/2024

Authorized by



Naresh Hari
**General Manager
Transmission Engineering**

Date: 2024-05-28

Supported by SCOT/SC



Meenal Vala
**OT Cybersecurity Study
Committee Chairperson**

Date: 27/05/2024

Content

	Page
1. Introduction	4
2. Supporting Clauses	4
2.1 Scope	4
2.1.1 Purpose	4
2.1.2 Applicability	4
2.2 Normative/Informative References.....	4
2.2.1 Normative.....	4
2.2.2 Informative	5
2.3 Definitions.....	5
2.3.1 General	5
2.3.2 Disclosure Classification	8
2.4 Abbreviations.....	8
2.5 Roles and Responsibilities	9
2.6 Process for monitoring	9
2.7 Related/Supporting Documents	9
3. OT-DMZ Design Requirements	9
3.1 DMZ Fundamentals.....	12
3.1.2 Security Zones	13
3.2 OT-DMZ architecture.....	14
3.2.1 OT-DMZ High Availability Deployment option	14
3.2.2 OT-DMZ Non-Redundant Deployment option	16
3.3 Firewall/ Next-Generation Firewall (NGFW) /Unified Threat Management (UTM)	17
3.3.1 OT-DMZ zone design guideline	18
3.3.2 OT-DMZ zone Firewall Rule Guidelines	18
3.3.3 Implementing Firewall Rules.....	19
3.4 Guidelines for configuring secure remote access	20
3.5 OT-DMZ internetworking device Hardening and configuration guidelines.....	22
3.6 OT-DMZ Device Hardening and configuration guidelines.....	23
3.7 Change Control	24
4. Authorisation.....	24
5. Revisions	25
6. Development team	25
7. Acknowledgements	25
Annex A: Power Generation and Delivery Integrated Architecture View	26
Annex B - Power Generation Reference Architecture	27
Annex C - Power Delivery Reference Architecture	28

Figures

Figure 1: Purdue Enterprise Reference Architecture	11
Figure 2: DMZ working principle	12
Figure 3: DMZ Architecture 1	15
Figure 4: DMZ Architecture 2	17

ESKOM COPYRIGHT PROTECTED

Figure 5: Remote access into DMZ	21
Figure 6: Power Generation & Delivery Integrated View	26
Figure 7: Power Station Reference Architecture	27
Figure 8: Power Substation Reference Architecture	28

Tables

Table 1: PERA Level Descriptions	9
--	---

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. It provides 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 also shielding the internal network from outside attacks. A DMZ is also called screened subnet or a perimeter network. Given the different requirements, priorities, policies, and implications of incidents between the Enterprise zone and the Industrial zone, and the desire to share data, as a result of users residing in the Enterprise zone, a DMZ must be used as a mitigation technique to provide a buffer zone between the Industrial zone and Enterprise zones. The DMZ can allow data that needs to be accessed by industrial zone and business systems to be shared securely, protecting information and accommodating the different security requirements of these zones. This 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) 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 Transmission specifically, as due to the separation requirements this document is authorised by Transmission BU and replica copies will be applicable and authorised by the respective Dx and Gx business units.

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] 240-55863502 Definition of Operational Technology (OT) and OT/IT Collaboration Accountabilities.
- [2] 240-55410927: Cyber Security Standard for Operational Technology.
- [3] 240-170000614: Cyber Security Controls Guide for Physical Security Systems.
- [4] 240-91479924: Cyber Security Configuration Guideline of Networking Equipment for Operational Technology.
- [5] 240-55863502: Definition of Operational Technology (OT) and OT/IT collaboration accountabilities.
- [6] 32-373: Information Security - IT/OT Remote Access Standard.
- [7] 240-97047595 Cyber Security Standard For Substation Automation Systems.
- [8] ANSI/ISA-95 Enterprise-Control System Integration.
- [9] IEC 62264: Enterprise-control system integration.

- [10] IEC 62443-3-2: Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design.
- [11] IEC 62443-4-1: Security for industrial automation and control systems - Part 4-1: Network security systems.

2.2.2 Informative

- [12] 240-157635971: Cybersecurity Strategy.
- [13] 32-377: Information Security – Firewall Standard.
- [14] 240-97047595 Cyber Security Standard For Substation Automation Systems.
- [15] CIS Center for Internet Security CIS Benchmarks: <https://www.cisecurity.org/cis-benchmarks>

2.3 Definitions

2.3.1 General

Definition	Description
Critical Cyber Asset	Cyber assets essential to the reliable operation of critical OT systems or critical assets.
Critical OT Systems	OT Systems that, if compromised, destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the electricity supply network.
Cyber Asset	Programmable electronic devices and communication networks including hardware, software and data that are connected to a network with a routable protocol.
Defence in depth (DiD)	is a cybersecurity strategy that uses multiple layers of defensive mechanisms to protect an organization's assets. It acknowledges vulnerabilities in hardware, software, and human factors, and aims to create a layered defence system. If one layer is compromised, additional layers are strategically implemented to prevent an attack, ensuring a resilient defence against various threat vectors. This multi-layered approach enhances a system's overall security posture and protects it against potential cybersecurity threats.
Demilitarised Zone	A perimeter network segment that is logically connected between internal and external networks that houses devices such as servers. DMZ is also referred to as a screened subnet or perimeter network.
DPI	is a method of network packet filtering that examines both the header and data components of data packets. Unlike traditional stateful packet inspection, which focuses on header information, DPI examines deeper into the metadata and content associated with each packet. This comprehensive analysis allows DPI to identify, categorize, and act on packets based on specific criteria, filtering out non-compliant data, spam, viruses, intrusions, and other defined threats. DPI can also redirect packets to alternative destinations based on its inspection results.
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. Also referred to as an Outside network
Firewall	Firewalls are devices or programs that control the flow of network traffic between networks or hosts employing differing security postures.

Definition	Description
IACS	Same as ICS
ICS	An industrial control system (ICS) is a computer-based system used to monitor and control physical processes in industries such as manufacturing, power generation & delivery, water treatment, and transportation.
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. Also referred to as an Inside network
Intrusion Detection System	An intrusion detection system (IDS) detects attacks and/or unauthorized access, verifying and characterizing threats. Its event notification and alerts inform administrators and security professionals about detected attacks.
Intrusion Prevention System	A system that identifies anomalous traffic, issues alerts and blocks traffic from proceeding further according to a defined rule base.
LAN	A local area network (LAN) is a network of devices connected in a single physical location, such as a building or office. It can range from a small industrial network with a few clients to an enterprise network with thousands of users. LANs consist of cables, access points, switches, routers, and other components that enable devices to connect to internal servers, web servers, and other LANs via wide area networks.
Layer 7	Application based inspection, with port-based flow control.
Less Critical OT Systems	Systems that rely on or connect 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
Next Generation Firewall wall	Next-generation firewalls (NGFWs) are advanced security measures that perform deep packet inspection (DPI), identify and block threats, control specific applications or services, integrate with user authentication systems, decrypt encrypted traffic, and support automation and orchestration for streamlined security management.
OSI	The OSI reference model is a layered, abstract representation created as a guideline for network protocol design and instruction. The OSI model divides the networking process into seven logical layers, each of which has unique functionality, and to which are assigned specific services and protocols. This reference model is often used to interpret the TCP/IP protocol suite.
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].
OT-DMZ	A DMZ or screened subnet is a designated network segment or subnet that acts as an intermediary between an untrusted external network, typically the internet/IT network, and a trusted internal OT network. Its primary purpose is to provide a secure landing space for external traffic. Security measures such as firewalls, VPNs, and IDS/IPS are employed to regulate and monitor traffic, safeguarding the integrity of the internal network. The DMZ architecture is essential for managing the security of OT systems accessed via the IT network or the internet. It is also referred to as an Industrial-DMZ.
OT Systems	All systems (including electronic, telecommunications, computer systems and components) that process, store or communicate operational data or information [2].

Definition	Description
Private VLAN	A private VLAN, also known as port isolation, is a network segmentation technique used within a single VLAN to further segment traffic and enhance security. It creates sub-VLANs within a primary VLAN, restricting communication between them while still allowing communication with the outside world (typically through a device like a router or firewall).
Router	is a network device used to connect many, sometimes disparate, network segments together, combining them into an internetwork. A router can make intelligent decisions about the best way to get network data to its destination. Operates at OSI layer 3.
Stateful Firewall	A stateful firewall is a network security device that monitors the state of active connections and makes decisions based on traffic context. It maintains a table of active connections, allowing it to make intelligent decisions about allowing or blocking incoming and outgoing traffic.
System Owner	The System Owner is the authorised Eskom representative that has overall accountability for the OT system in question.
Top Secret	The classification given to information that may be used by malicious/opposing/hostile elements to neutralise 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.
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. These are networks not under the care of OT, such as corporate networks and the internet.
VLANs	is a network of end devices that behave as if they are connected to the same network segment, even though they might be physically located on different segments of a LAN. VLANs are configured through software on the switch and router. Its main objective is to reduce broadcast domains. Some important points on VLANS is that: a single VLAN is equivalent to a broadcast domain, and VLAN is equivalent to a logical network/subnet.
VPN	A virtual local area network (VLAN) is a logical group of end devices, and other network devices that are on the same LAN despite their geographical distribution. A VLAN allows a network of end devices and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to changes in network requirements and relocation of workstations and server nodes.
VPN Concentrator	A VPN concentrator is a specialized device or software application that manages and aggregates multiple VPN connections, ensuring secure communication between remote devices and a private network.

Definition	Description
WAN	A wide-area network (WAN) is a network infrastructure that connects multiple local-area networks (LANs) or other networks, to enable communication across diverse geographic areas. The Internet is the largest example of a WAN, and connections can be established through leased lines, VPNs, or IP tunnels. WANs facilitate device connectivity across different locations, making them a critical component of telecommunications network.
Zone	A zone is a collection of physically and functionally united assets that have similar security requirements. These areas are defined from the physical and functional models of the industrial system control architecture.

2.3.2 Disclosure Classification

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

2.4 Abbreviations

Abbreviation	Description
AAA	Authentication, Authorization and Accounting
CATS	Control and Automation, Technology & Support section within PTM&C
COE	Centre of Excellence
CVE	Common Vulnerabilities and Exposures
DMZ	Demilitarised Zone
DPI	Deep Packet Inspection
ECM	Engineering Change Management
WAN	Wide Area Network
ESP	Electronic Secure Perimeter
FTP	File Transfer Protocol
HTML	Hyper-Text Markup Language
IACS	Industrial Automation and Control Systems
ICMP	Internet Control Messaging Protocol
OSI	Open System Interconnect
ICS	Industrial Control System
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
NAT	Network Address Translation
NGFW	Next Generation Firewall
OEM	Original Equipment Manufacturer
OT	Operational Technology

ESKOM COPYRIGHT PROTECTED

Abbreviation	Description
PCM	Process Control Manual
PTM&C	Protection, Telecommunication, Metering and Control COE
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
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
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

Same as section 2.2 Normative/Informative References.

3. OT-DMZ Design Requirements

Operational Technology systems are best illustrated through the use of the Purdue Enterprise Reference Architecture (PERA) model. The PERA model is a reference architecture for Industrial Control Systems (ICS). It divides the ICS's into levels, which serve as distinct security zones. It is important to note that the PERA model is not cast in stone, and that it is flexible to suit the needs or requirements of a particular system in consideration. The PERA Model is important for OT security because it provides a framework for segmenting ICS networks and isolating different levels of the system. This helps to protect the ICS from cyberattacks and other threats. The Purdue Model can also be used to implement a defence-in-depth strategy for OT security. This means implementing multiple security controls at each layer of the system. This makes it more difficult for attackers to compromise the system. The summary of each level is provided on Table 1 and Figure 1.

Table 1: PERA Level Descriptions

Level	Description
Cell/Area Zone	
Level 0: Process	This level includes the physical equipment and processes. Sensors, transmitters, and other devices that collect data from the physical plant.
Level 1: Basic Control	consists of controllers that direct and manipulate the manufacturing or industrial processes. The key function of this level is to interface with the Level 0 devices (e.g., I/O,

ESKOM COPYRIGHT PROTECTED

	sensors, and actuators). The level receives data from Level 0 sensors and transmitters, makes control decisions, and sends commands to those field devices. The devices in this level are responsible for continuous control within the power utility space as opposed to batch and discrete control used in other process utilities. The interconnections are typically hardwired (this will change with the introduction of process bus and field bus based on the Ethernet-APL standard) i.e., from field device to the controllers via input/output modules. Examples of devices at these levels are PLCs, RTUs, IEDs, DCS Controllers.
Level 2: Area Supervisory Control	Level 2 applications include Servers, Operator interfaces, alarms, and control room workstations, which communicate with Level 1 controllers and share data with site level or enterprise systems via the DMZ. Examples include Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) systems and other supervisory systems are found at this level. e.g., HMI, Control room/engineering workstations, alarm servers, historians.
Level 2.5: Cell/Area Zone DMZ	The Level 2.5 Cell/Area Zone (DMZ) is a demarcation point in industrial infrastructure, ensuring secure communication between OT systems and external entities. It allows local data retrieval and processing while safeguarding critical data integrity and confidentiality. The potential use case for this is at substations where personnel is required to interact with the substation devices through the use of IT-provisioned laptops.
Industrial zone	
Level 3: Site Operations	The systems in this level provide centralized monitoring and control over various industrial processes and equipment. They collect data from Level 2 control systems and offer a higher-level view of the entire industrial operation. ICS systems are critical for overseeing and optimizing processes e.g., Engineering workstations, plant historian servers, various servers. NB: The systems and applications in Level 3 communicate with the systems in the Enterprise Zone through a DMZ. Direct communication between systems in the Industrial zone and Enterprise zones is prohibited. Also, systems in Level 3 may communicate with systems in Levels 1 and 0. The Industrial zone can function independently, regardless of connectivity status to higher levels. Level 3 is also known as Site-Wide Supervisory , as well as Site Manufacturing Operations and Control .
OT-DMZ	
Level 3.5 OT-DMZ	A DMZ or screened subnet is a designated network segment or subnet that acts as an intermediary between an untrusted external network, typically the internet/IT network, and a trusted internal OT network. Its primary purpose is to provide a secure landing space for external traffic. Security measures such as firewalls, VPNs, and IDS/IPS are employed to regulate and monitor traffic, safeguarding the integrity of the internal network. The DMZ architecture is essential for managing the security of OT systems accessed via the IT network or the internet. It is also referred to as an Industrial-DMZ .
Enterprise Zone	
Level 4: Site Business Planning and Logistics	Level 4 is an IT system level that supports core business operations such as inventory management, resource planning, and scheduling. It includes Enterprise Resource Planning (ERP) and other business software. It has security components such as IT DMZ, VPN Concentrators, firewalls, WAFs, and IDPS. These services are typically managed and operated by the IT department within the organization. Level 4 and 5 are sometimes combined into a single level depending on the size of an organization. Also the functions on this level can overlap with those at level 5.
Level 5: Enterprise Network	The Level hosts corporate IT infrastructure systems, including services such as VPN remote access and corporate Internet connectivity. Direct communication between enterprise zones and the ICS environment is discouraged due to security risks. It is recommended to manage access through a Demilitarized Zone (DMZ) and /or follow the guidelines provided on the remote access standard.

For the levels depicted in Figure 1 and in Table 1, the Cell/Area zone is a functional area within a power Station (generating unit) or a Sub-Station. An integrated Architecture of the PERA model illustrating the integration of various plants inclusive of power generation and delivery as well as the Control centre is provided in Figure 6, in annexure A. The typical reference architectures for power generation and delivery are illustrated in Figure 7 and Figure 8 in Annexures B and C respectively. A Cell/Area zone is a set of ICS devices, that are involved in the real-time control of a functional aspect of the manufacturing or industrial process. To control the functional process, the ICS devices are all in real-time communication with each other. This zone has three levels of activity as can be seen on the Table 1 and Figure 1. It is important to note that level 0 -3, and including the OT-DMZ is under the control and domain of OT system owners. In special cases where IT is involved, these agreements must be in line with **240-55863502: Definition of Operational Technology (OT) and OT/IT collaboration accountabilities or agreed/exempted by the system owner.**

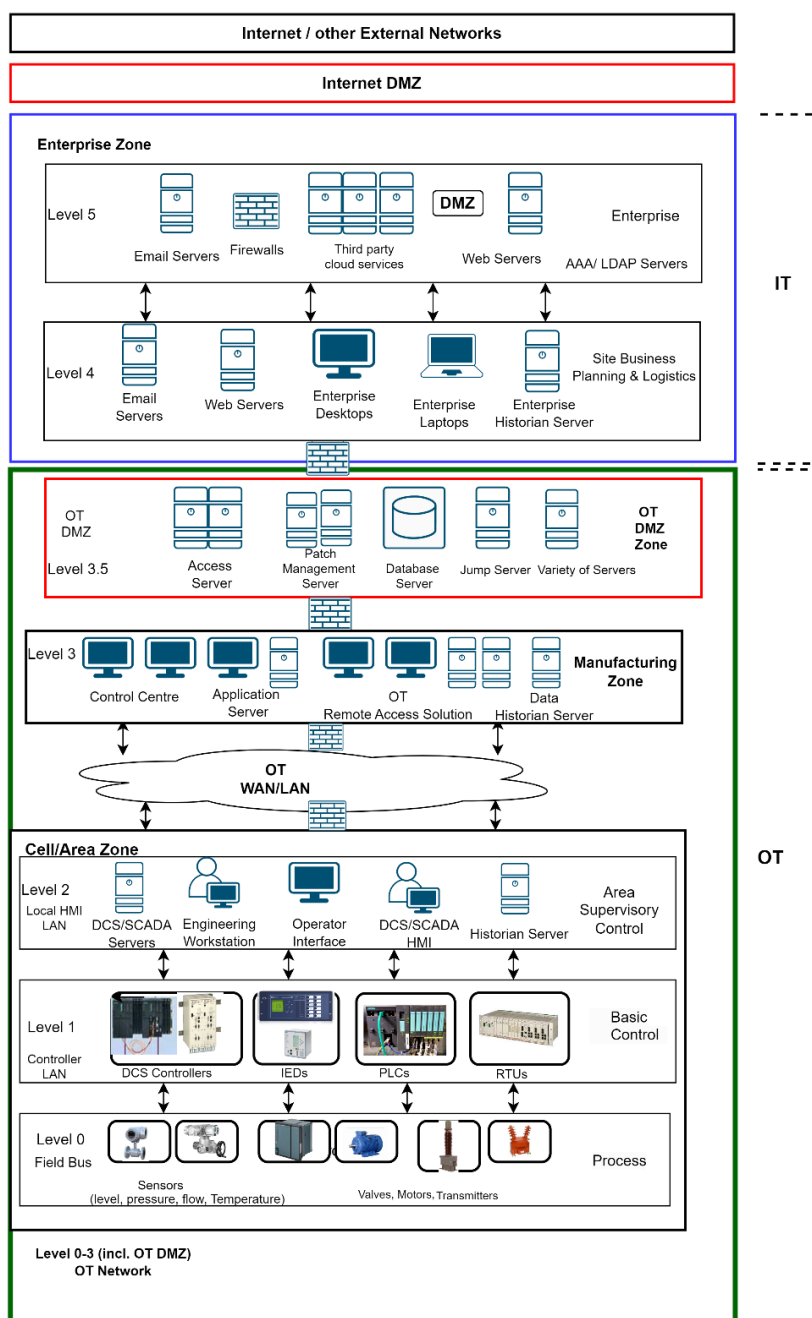


Figure 1: Purdue Enterprise Reference Architecture

ESKOM COPYRIGHT PROTECTED

3.1 DMZ Fundamentals

The Demilitarized Zone is a segregated area, either physical or logical, that acts as a barrier between an OT internal and external network, or untrusted networks, typically the Internet, however in an OT setting, IT is as close as it gets to the Internet. DMZs are sometimes referred to screened subnetworks or perimeter networks. To understand the purpose of a DMZ, consider Figure 2, in which two networks, network A & B are separated by a firewall and forming a DMZ network as depicted. The firewall has three interfaces i.e. A, B & C. Interface A connects **Network A** (the inside or internal network, which is the OT network), interface B connects **Network B** (the outside or external network), and interface C connects to the **DMZ network**. The purpose of a DMZ network in its basic form is to facilitate secure communication between Network A (internal network) & B (untrusted network) and vice versa, thereby protecting the internal network A from unauthorized access by isolating untrusted Network B from the internal network. This is achieved by hosting servers or applications that are hardened in the DMZ network that are accessible to the untrusted network B, such as web servers and other servers or services. The working principle is as follows:

a) The Firewall on interface A:

The firewall permits authorized bi-directional communication between the internal Network A (OT-Network) and the DMZ network. It explicitly denies unauthorized access between these two networks and prohibits direct communication between the internal Network A and the external Network B, in both directions.

b) The Firewall on interface B:

The firewall permits authorized access to the DMZ Network from the External Network B, and denies unauthorized access to the DMZ Network from the External network, and prohibits direct communication between Network A and Network B.

The firewall permits authorized bi-directional communication between the external Network B (IT-Network) and the DMZ network. It explicitly denies unauthorized access between these two networks and prohibits direct communication between the external Network B and the internal Network A, in both directions.

c) The Firewall on interface C

The firewall permits bi-directional authorized access to the DMZ network from both Internal and External Networks A and B respectively, while denying unauthorized bi-directional access from both Internal and External Networks A and B. Applications and/or services on the DMZ network are typically IT/Internet-facing, making them potential targets for cyberattacks. The isolation of these services in a DMZ network serves to protect the internal OT network from potential cyber threats.

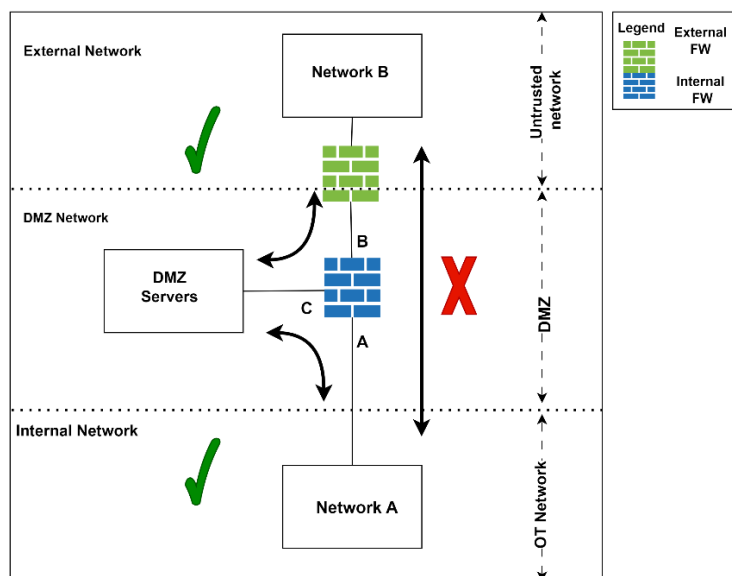


Figure 2: DMZ working principle

ESKOM COPYRIGHT PROTECTED

In summary:

- All OT network traffic from either side of the OT-DMZ terminates in the OT-DMZ, no OT network traffic directly traverses the OT-DMZ to the external network.
- All data is transient, the OT-DMZ does not store data permanently. With exceptions whereby web, file and terminal servers are utilized. These servers within the DMZ can store data permanently. Web servers frequently hold website content, user accounts, and logs. Terminal servers might store user profiles and application data.
- Functional sub-zones within the OT-DMZ are configured to segment access to OT data and network services.
- A properly designed OT-DMZ will support the capability of being unplugged if compromised, while still allowing the OT Zone to operate without disruption.

3.1.2 Security Zones

With respect to firewalls, the terms 'interface' and 'zone' can be used interchangeably, as they represent the same conceptual idea. 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 are 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 considered. 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:

- a) Trusted Zones → Internal/OT Network.
- b) DMZ Zones.
- c) Untrusted Zones→ External/ Untrusted network.

The concept of security levels for firewall zones is common across different brands, assigning relative trust values to different network segments or zones. These levels help define the default flow of traffic between zones. However, the specific numerical values used for these levels are not standardized across all firewall brands, as different vendors may use different value ranges and assign them to different security zones differently. For instance, a vendor might assign a security level of 100 to a trusted zone, 50 to a DMZ zone and 0 to an untrusted network.

3.2 OT-DMZ architecture

With reference to the PERA model in Table 1 and Figure 1, the OT-DMZ (level 3.5) is a network that separates the Enterprise and Industrial zones, allowing them to share data and access systems. This zone protects information and accommodates different security requirements. All traffic should terminate in the DMZ, eliminating direct traffic flow between the two zones. An OT-DMZ acts as a buffer between an enterprise network and industrial control system (ICS) network environments. It isolates systems exposed to the Corporate network (IT) and the internet, such as remote access VPN and corporate internet access services. In terms of communication from the enterprise zone to the industrial zone, systems and applications in the enterprise zone can communicate with systems in the industrial zone through the DMZ. This communication is typically managed and controlled by stateful inspection firewalls. The firewall inspects the traffic between the zones and allows only authorized connections to pass through. It is important to note that, direct communication between the enterprise zone and the industrial zone is prohibited. Similarly, in terms of communication from the industrial zone to the enterprise zone, systems in the industrial zone can communicate with systems in the enterprise zone through the OT-DMZ. The stateful firewall in the OT-DMZ inspects the traffic and allows only authorized bi-directional connections between the respective zones to pass through and denies the rest. It is important to note that direct communication between systems in the industrial zone and enterprise zones is discouraged and must be denied. The use of the DMZ adds an extra layer of security by enforcing controlled and monitored communication between these zones. The stateful firewalls in the OT-DMZ network can provide Authentication, Authorization, and Accounting (AAA) (if not available in the OT network) services and can be installed with an Intrusion Detection/Prevention System for intrusion detection and protection. It is important to note that the direct connection of the OT and IT networks with a firewall without a DMZ network (i.e., DMZ servers) is not allowed at this level as it weakens the defence-in-depth and other security approaches. Therefore, the following is recommended:

- a) ICS systems that need to be accessed by the enterprise network or users should be placed in a DMZ, which is a separate network segment that is isolated from the internal network.
- b) All connections between the ICS systems and the enterprise network must pass through a stateful inspection firewall, which will only allow authorized connections.
- c) The firewall should follow a "deny all" or "explicit deny" policy, which means that any connection that is not explicitly allowed will be blocked. This approach helps to protect the ICS systems from unauthorized access and cyberattacks.

3.2.1 OT-DMZ High Availability Deployment option

OT Systems within the power utility (i.e. level 0-3) covers systems in the power Generation and Delivery systems. These systems are typically comprised of industrial control systems such as Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLC), Intelligent Electronic Devices (IEDs) etc. as depicted on both Figure 1 and Figure 3.

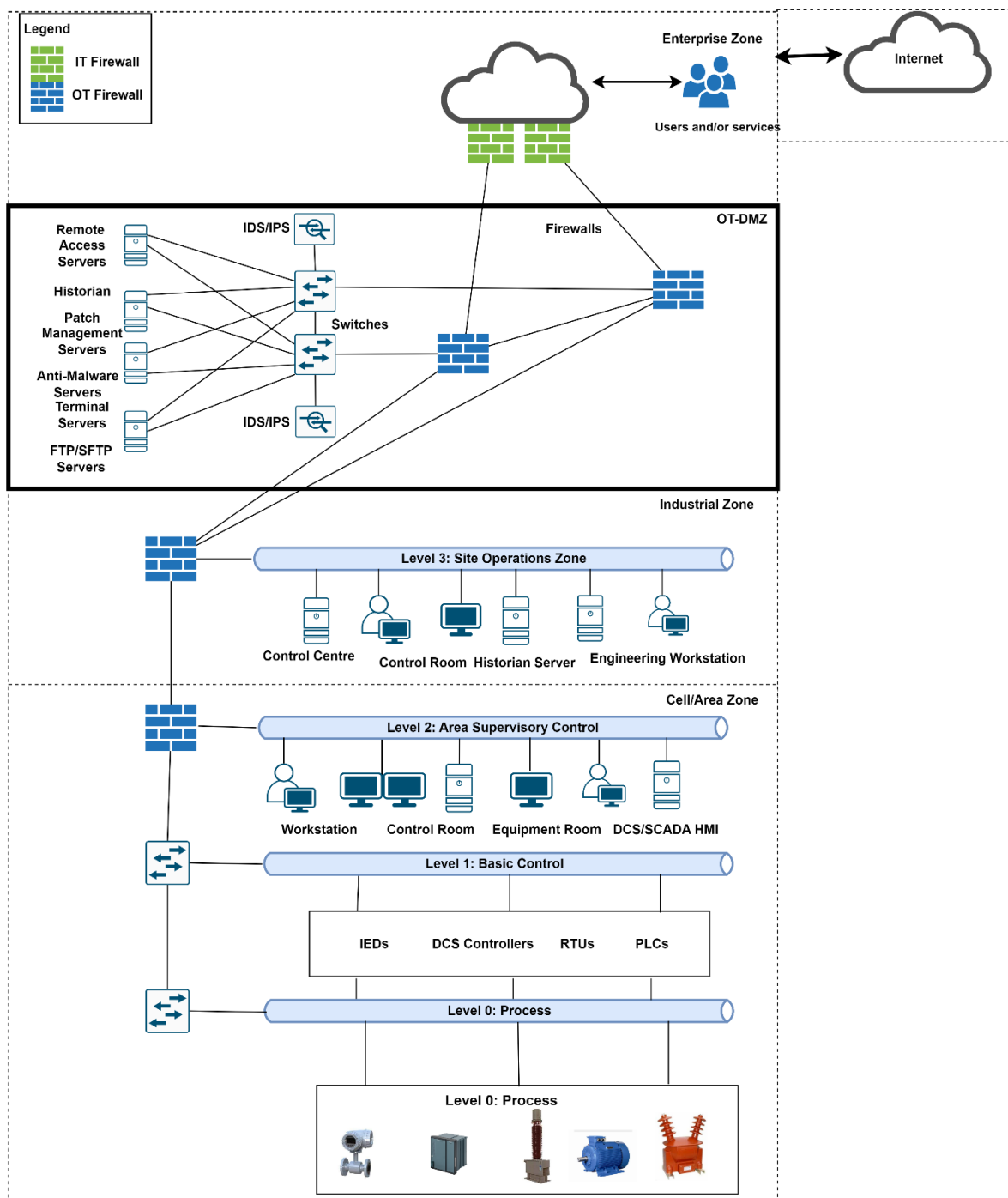


Figure 3: DMZ Architecture 1

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.

To ensure the security of interconnection between the Industrial Control Systems (ICS)/OT and Information Technology (IT) networks, it is recommended that the entry points into the ICS environment be minimized. This safeguard helps limit potential attack vectors for intruders. For a high availability deployment scenario, consider Figure 3, a DMZ is established between the Enterprise (Corporate) and OT environments using two pairs of firewalls, one of which belongs to Group IT and the other is owned by OT. Within the OT-DMZ zone, the interfaces between the enterprise and OT-DMZ zones of the pair of firewalls (for redundancy) prevents inbound attacks from corporate network targeting ICS systems, scrutinizing traffic in and out of the OT-DMZ zone. The firewall on the interfaces between the DMZ and industrial zone, manages traffic to and from the ICS environment, containing attacks originating within the ICS network. This firewall setup improves security by introducing additional layers of defence that must be breached to compromise ICS systems. Improved security is achieved by employing firewalls from different manufacturers, introducing diverse vulnerabilities. To compromise both sets of firewalls, an attacker would need to exploit vulnerabilities common to both sets of devices. Additionally, the dual firewall pair architecture facilitates separation of duties, allowing the IT department to manage one set of firewalls while the OT department oversees the other pair. However, this firewall deployment type of using different vendors' firewalls is not strictly enforced, and it is being reviewed at an organizational level especially on Group IT side for its viability given the changing technological landscape. It is vital to recognize that while the interruption of OT-DMZ connectivity does not impact the industrial zone operations, it can significantly affect diagnostic functions reliant on accessing plant data. Given that ICS data is collected and transferred to a business system in the Enterprise zone, a disruption in the OT-DMZ connectivity may hinder the flow of data. Despite the ICS application and network not depending on the OT-DMZ for availability, aspects such as inter-connectivity to the Enterprise and functions such as remote access, Historian data access, SIEM and SOC solutions are dependent on OT-DMZ functionality. To ensure continued availability, implementing redundant firewalls is essential, especially for critical OT systems. Based on Figure 3, the component of an OT-DMZ comprises of:

- a) Firewalls to provide the strong segmentation between the zones,
- b) DMZ switches to provide inter-connectivity between any servers and the firewalls,
- c) Servers to run any application mirrors or store data to be shared,
- d) Firewall and security management software to manage the firewall, which may optionally reside in the DMZ network zone.

Furthermore, for Critical OT systems that have the capability to send control signals to the plant in the Eskom OT environment, the following configuration shall be used:

The Layer 7 UTM and IPS functionality or NGFW may be on a single security appliance and the IPS rules shall be implemented on all its interfaces, ideally it should be redundant. The rules on OT UTMs or NGFW shall be set up to filter according to the security postures of their different interfaces. In the event of a compromise due to a 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. Provision is made for a DMZ for IT-related applications on the external facing OT UTM.

3.2.2 OT-DMZ Non-Redundant Deployment option

Another toned down architecture is shown with single usage of firewalls, switches and servers. This architecture is well suited for 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 IDS/IPS or NGFW may be a single device and the IPS or access control rules shall be implemented on all interfaces.

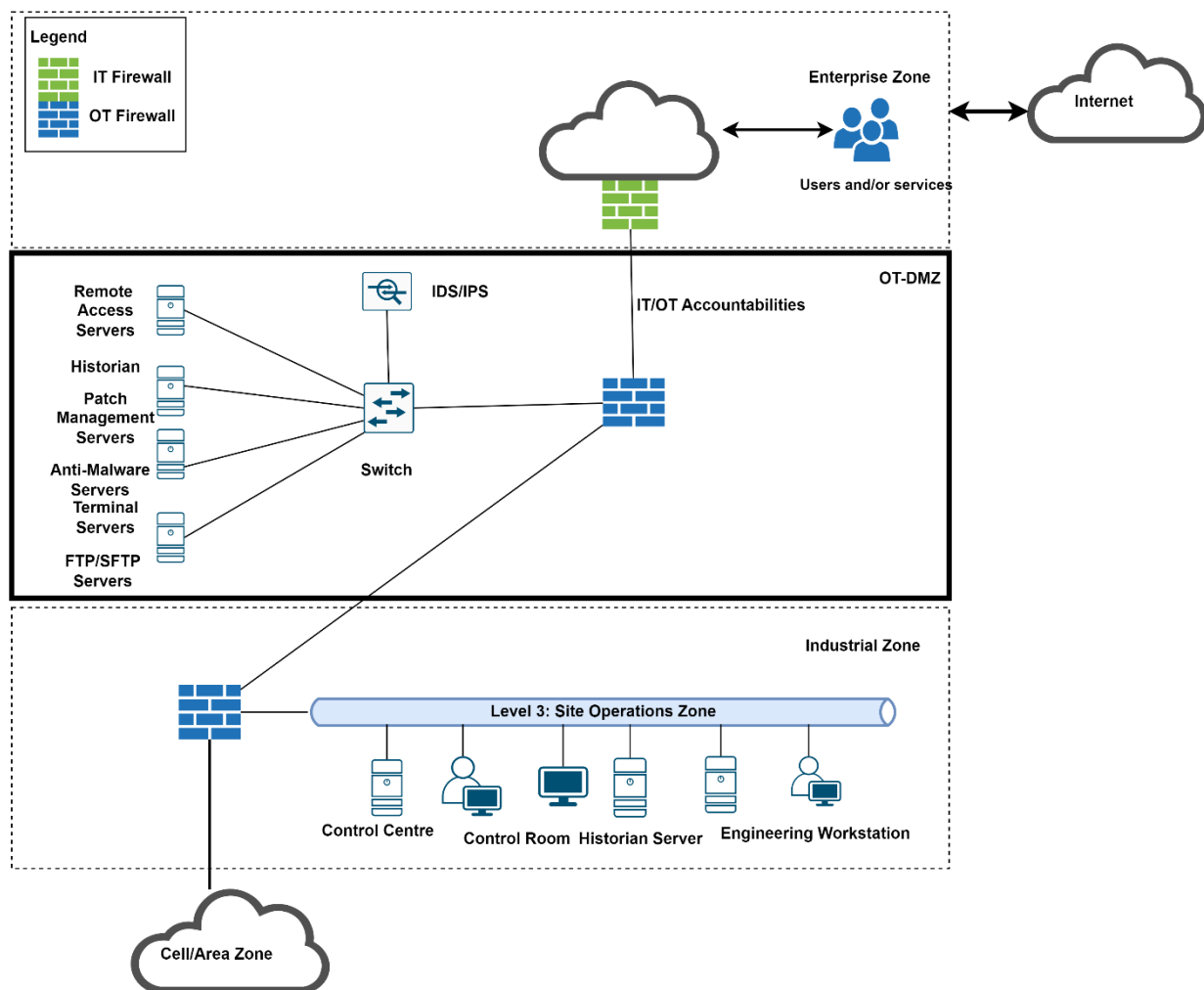


Figure 4: DMZ Architecture 2

3.3 Firewall/ Next-Generation Firewall (NGFW) /Unified Threat Management (UTM)

The OT-DMZ (level 3.5) itself is a security key aspect of the defence-in-depth security stance. The firewall is critical to the security of the industrial zone and the ICS systems that it contains. Therefore, the following features should be considered for the firewall appliances, taking into consideration the services or functionalities that are required for the specific OT environment:

- a) Stateful packet inspection and access control support to manage traffic flows,
- b) Content security,
- c) Malware detection,
- d) VPN technology,
- e) Intrusion protection and detection services,
- f) Modular policy support,
- g) Authentication (AAA) enforcement and ability to setup local authentication,
- h) Web portal, support for remote desktop and other proxy services,
- i) NAT(incl. PAT) services,
- j) Support for SSH, HTTPS, and SNMPv3.

ESKOM COPYRIGHT PROTECTED

3.3.1 OT-DMZ zone design guideline

When designing the DMZ interface/s:

- a) The external facing OT firewall shall be a Layer 7 UTM (Unified Threat Management with IPS (Intrusion Prevention System) or NGFW functionality. The layer 7 UTM/IPS or NGFW can be on the same security appliance or be separate security appliances, dependent upon the business case.
- b) No critical data shall pass through the OT Layer 7 Unified Threat Management (UTM) or NGFW connected to the corporate/IT business network.
- c) It should be possible to isolate the OT system from the DMZ if an attack is taking place, while the OT system is still functioning.
- d) If there are multiple servers/systems in the DMZ performing different functions, the DMZ should be virtually divided into multiple zones based on the functionality of the systems to limit the damage if one or more servers are compromised. Segmentation should be considered.
- 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.
- f) It should be possible to isolate the DMZ from the IT systems if an attack is taking place, while the DMZ and OT system is still functioning.

3.3.2 OT-DMZ zone Firewall Rule Guidelines

Before a firewall rule can be created, a security risk analysis (i.e. an assessment of the likelihood that a threat vector will exploit a vulnerability to produce an impact adverse to the system design specifications) shall be performed on the applications that will traverse the firewall and the services associated with the application. The following should be considered as recommended practice for general firewall rule sets and can be tailored for a specific OT environment:

- a) The base rule set should be deny all, permit none.
- b) Ports and services between the control network environment and the corporate network should be enabled and permissions granted on a specific case-by-case basis. There should be a documented business justification with risk analysis and a responsible person for each permitted incoming or outgoing data flow.
- c) All "permit" rules should be both IP address and TCP/UDP port specific, and stateful if appropriate.
- d) All rules should restrict traffic to a specific IP address or range of addresses.
- e) All firewall management traffic should be carried on either a separate, secured management network (e.g., out of band) or over an encrypted network with multi-factor authentication. Traffic should also be restricted by IP address to specific management stations.
- f) All firewall policies should be tested periodically and/or after changes to rules are implemented.
- g) All firewalls should be backed up immediately prior to commissioning.
- h) Identification of network applications deemed necessary.
- i) Identification of vulnerabilities associated with the applications.
- j) Creation of application traffic matrix showing protection method; and
- k) Creation of firewall rules based on applications traffic matrix.
- l) Consideration for assuring confidentiality and the implications of a potential breach (breach impact, containment, etc.)
- m) Consideration for assuring data integrity and the implications of a potential breach (breach impact, containment, etc.)
- n) Consideration for assuring availability and the implications of a potential breach (breach impact, business continuity, preventative measures, etc.)

ESKOM COPYRIGHT PROTECTED

3.3.3 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 use 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:
 - 1) The source 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).
 - 2) 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).
 - 3) 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.
 - 4) Characteristics of the Layer 4 communication session – the protocol such as TCP or UDP.
 - 5) The destination ports of the sessions; source and destination ports shall be configured, software applications using port hopping is not recommended.
 - 6) 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 traverse the firewall.
- f) All firewall rule sets shall contain the following two rules:
 - 1) A “stealth” rule which drops all connections to the firewall system itself.
 - 2) A “drop” or “deny” rule as the last rule which shall drop/deny all connections not matched by the preceding rules.
- g) The firewall rule set shall always block the following types of traffic:
 - 1) 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.
 - 2) 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.
 - 3) Inbound traffic containing ICMP traffic.
 - 4) Inbound traffic from a non-authenticated source system containing SNMP traffic.
 - 5) Inbound traffic containing IP Source Routing information.
 - 6) 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.
 - 7) Inbound or outbound network traffic containing a source or destination address of 0.0.0.0.
 - 8) Inbound or outbound traffic containing directed broadcast addresses. A directed broadcast attack is a form of Denial of Service.
- h) 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.
- i) Inbound network traffic shall terminate in a DMZ and may not traverse two firewalls.

- j) Inbound network traffic should traverse via at least 1 Layer 7 firewall (UTM) with deep packet inspection capabilities to detect and prevent Cross-site Scripting (XSS), SQL Injection, HTML5 attacks, CVE exploits, etc.
- k) Firewall rules shall be reviewed on a bi-annual basis and all rules that are unused shall be deleted. This excludes the default “drop/deny” rule (see point f), which should always remain in place. Any changes shall follow the Engineering Change Management process.
- l) 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.
- m) Firewalls must be configured to prevent the initialization of administrative protocols from inside the DMZ (e.g. Telnet, FTP, SSH).

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

3.4 Guidelines for configuring secure remote access

Remote access to the OT environment requires strong security measures and should be controlled by two-factor authentication. A Virtual Private Network (VPN) gateway, positioned in the Enterprise zone DMZ, serves as a critical entry point. Users requesting access must establish an encrypted VPN tunnel to the Eskom's VPN gateway, where authentication involves a valid username-password combination and a second form of authentication, typically a one-time password (OTP) from a token device. The VPN gateway acts as the authenticator, forwarding authentication requests to an external user database within the Enterprise Zone. Upon successful authentication, users are authorized to access a remote access server in the OT-DMZ and following the principle of least privilege. Further access into the OT environment requires connecting to a remote access server in the DMZ. This connection must be encrypted to prevent the transmission of sensitive data in plain text. Successful authentication at this stage mandates a valid username-password combination and a second form of authentication under the OT environment. Once authenticated, users are only authorized to access specific systems within the OT environment necessary for their designated job functions. This multi-layered approach ensures a stringent and secure remote access framework for the ICS environment. Figure 5 summarizes the steps typically undertaken for remote access:

Steps	Description
1	Encrypted VPN connection between (Remote User/Vendor) and VPN concentrator in the Enterprise DMZ
2	Encrypted Authentication request/response between the VPN concentrator and AAA database server
3	Encrypted connection between (Remote User/Vendor) and Remote Access Server in the OT-DMZ
4	Encrypted connection between the Remote Access Server and the OT/ICS Environment

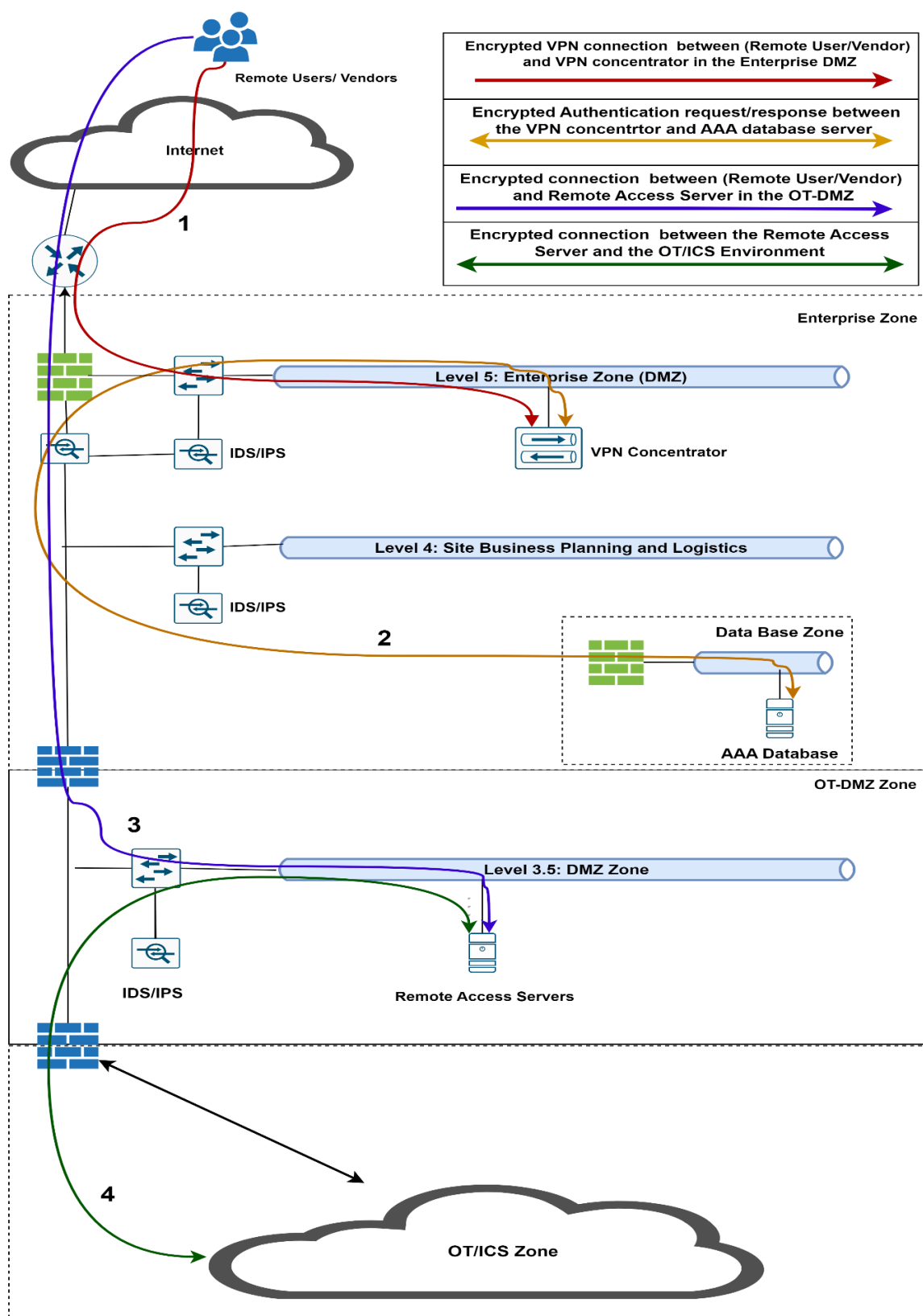


Figure 5: Remote access into DMZ

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.

Follow these guidelines for configuring a secure remote access VPN:

- a) Implement VPN technology to support remote access to OT networks by remote clients over the Internet and secure communications between sites across public networks.
- b) Select a VPN protocol that gives the most effective security while also being supported by the OT servers and client devices.
- c) Install the VPN concentrator to the network edge by using a secure firewall configuration to prevent compromise.
- d) Develop a remote access policy to ensure only authorized users can connect and ensure that the network is not compromised by remote clients with weak security configurations.

For more on the remote standard, it recommended to consult **32-373: Information Security - IT/OT Remote Access Standard** and **240-55863502 Definition of Operational Technology (OT) and OT/IT Collaboration Accountabilities**.

3.5 OT-DMZ internetworking device Hardening and configuration guidelines

Network Device Hardening guidelines:

- a) Change default credentials: Avoid guessable usernames and passwords.
- b) Upgrade firmware: Regularly update operating system, applications, and firmware.
- c) Patch and Update: Apply patches and updates to operating system, applications, and firmware.
- d) Disable Unneeded Network Services: Reduce attack surface.
- e) Use Secure Protocols: opt for secure protocols over insecure ones.
- f) Secure SNMP: Use SNMP Version 3, providing encryption and enhanced security features.
- g) Generate New Keys/Credentials: Rotate important credentials regularly and practice responsible encryption key management.
- h) Disable Unneeded Switch Ports: Shut down unused switch ports to prevent unauthorized access.
- i) Ensure Spanning Tree Protections: Implement STP protections.
- j) Enable DHCP Snooping: Prevent rogue DHCP servers and DHCP pool exhaustion attacks.
- k) Use VLAN Segmentation: Protect systems from accidental or malicious attacks.
- l) Use Port Security: Lock switch ports to MAC addresses.
- m) Use Router Advertisement (RA) Guard: Protect against attacks in IPv6 environments.
- n) Use Dynamic ARP Inspection (DAI): Guard against MAC address spoofing.
- o) Use Control Plane Policing (CoPP): Control the rate of packets to and from the control plane.
- p) Use Private VLANs: Seg networks for specialized deployments.
- q) Change Default VLAN: Alter the default VLAN to reduce risk of exploitation.
- r) Use Access Control Lists (ACLs): Strengthen security, especially for protecting internal web servers.
- s) Use Role-Based Access: Create groups or roles on network devices, mapping them to different permission levels.

For more, consult **240-91479924: Cyber Security Configuration Guideline of Networking Equipment for Operational Technology**.

3.6 OT-DMZ Device Hardening and configuration guidelines

The devices within the OT-DMZ network comprises of hardware and software elements such as workstations, servers, operating systems, applications all of which must be secured and hardened. Also note that, Virtualization platforms, hypervisors, and VMs are software products with flaws and vulnerabilities, hence their basic security recommendations are also similar to those for operating systems and applications.

Follow these guidelines for device hardening within the OT-DMZ zone, this can be tailored for the specific OT environment:

- a) Physical Security: Lock down physical ports and restrict access to server rooms.
- b) Change default device credentials on installation and ensure that accounts are secured with strong passwords.
- c) Use only secure channels for administration traffic or any other protocol where credentials need to be submitted.
- d) Configure services according to the device's baseline and disable any services which are not required. Consider setting up alerting mechanisms to detect service configuration changes.
- e) Ensure that only the necessary IP ports (TCP and UDP ports) to run permitted services are open and that access to a port is controlled by a firewall ACL if appropriate.
- f) Ensure any physical ports on a device that could be used to attach unauthorized USB or network devices are protected by secure access (in a locked room or cabinet).
- g) If a device is decommissioned, ensure that encryption keys stored on that device are archived (if appropriate) and then securely deleted from the device storage.
- h) Change encryption keys used to access servers and appliances when employees with credentials to access these devices leave the company or change job roles.
- i) Operating System Security: Minimal Installation, Regular Patching, Hardening Guidelines, Network Segmentation, Antivirus/Antimalware, Logging and Monitoring, User Access Controls, Data Encryption, Backup and Recovery, Incident Response Plan, and Training Personnel.

BIOS and UEFI Security Measures:

- a) Password Protection: Use strong passwords for BIOS/UEFI interfaces.
- b) Password Policy: Enforce strict password policy, regular updates, and prevent reuse of passwords.
- c) Disable Unnecessary Features: Disable unnecessary BIOS/UEFI features like USB boot, CD/DVD boot, etc.
- d) Secure Boot: Enable Secure Boot in UEFI to load only signed and authenticated firmware and operating system components.
- e) Firmware Updates: Regularly update BIOS/UEFI firmware to patch vulnerabilities and enhance security.

Virtualization Security Measures:

- a) Implement good patch/service pack/update management procedures for both hosts and users.
- b) Remove applications with known vulnerabilities or histories.
- c) Test and apply virtual platform security patches.
- d) Harden the host device by implementing file and folder permissions, controlling users and groups, and configuring logging and time synchronization.
- e) Secure communication links between the host and network users using SSH, SSL, and IPSec.
- f) Secure endpoint devices connected within the hypervisor using L2 switching controls.
- g) Create security between VMs and the underlying host by turning off unnecessary services.

ESKOM COPYRIGHT PROTECTED

3.7 Change Control

A change control process shall be implemented on all firewalls, routers, and switches within the OT-DMZ. All changes need to be logged and the current configuration shall be archived. The change control process shall be adhered to as per the Cyber Security Standard for OT, other related standards and follow the Engineering Change Management (ECM) PCM (Process Control Manual).

4. Authorisation

This document has been seen and accepted by:

Name and surname	Designation
Anita Oommen	Smart Grid Technology Study Committee Chairperson
Alison Maseko	Senior Manager – Eskom Telecommunications
Christopher Kohlmeyer	Acting Senior Manager – Control and Instrumentation
Comfort Masike	Senior Manager – System Operator, Technical Operations
Ezzard De Lange	Senior Manager –Operational Technology
Judith Malinga	Senior Manager – PTM&C Engineering
Malcolm Van Harte	Senior Manager – Smart Grids
Sithembile Songo	Senior Manager – Information Security
Zwelandile Mbebe	Corporate Specialist Telecommunications
Andre De La Guerre	Middle Manager – Protection, Metering, and DC
Cornelius Naidoo	Middle Manager – Telecommunications Technology and Support
Mpumelelo Mathe	Middle Manager – Control and Automation Technology and Support
Pitso Sekhoto	Middle Manager – Substation Automation and Integration
Andre Kotze	Chief Engineer – Asset management
Bongani Shezi	Chief Engineer – Telecommunications Technology and Support
Craig Boesack	Chief Engineer – Control and Instrumentation
Craig Moran	Chief Advisor IT Architecture
George Nunes	Chief Engineer – Control and Instrumentation
Johan Botha	Senior Consultant – System Operator
Johan Pieterse	Chief Engineer – Electrical
Kenneth Brown	Chief Engineer – Electrical
Kholofelo Halefose	TX Cyber Security chair
Meenal Vala	OT Cyber Security Chair
Mondli Dlamini	Chief Engineer – Security Division
Vonani Mathebula	Chief Engineer – Electrical
Mziwakhe Macina	Snr Advisor Security Cybersecurity

5. Revisions

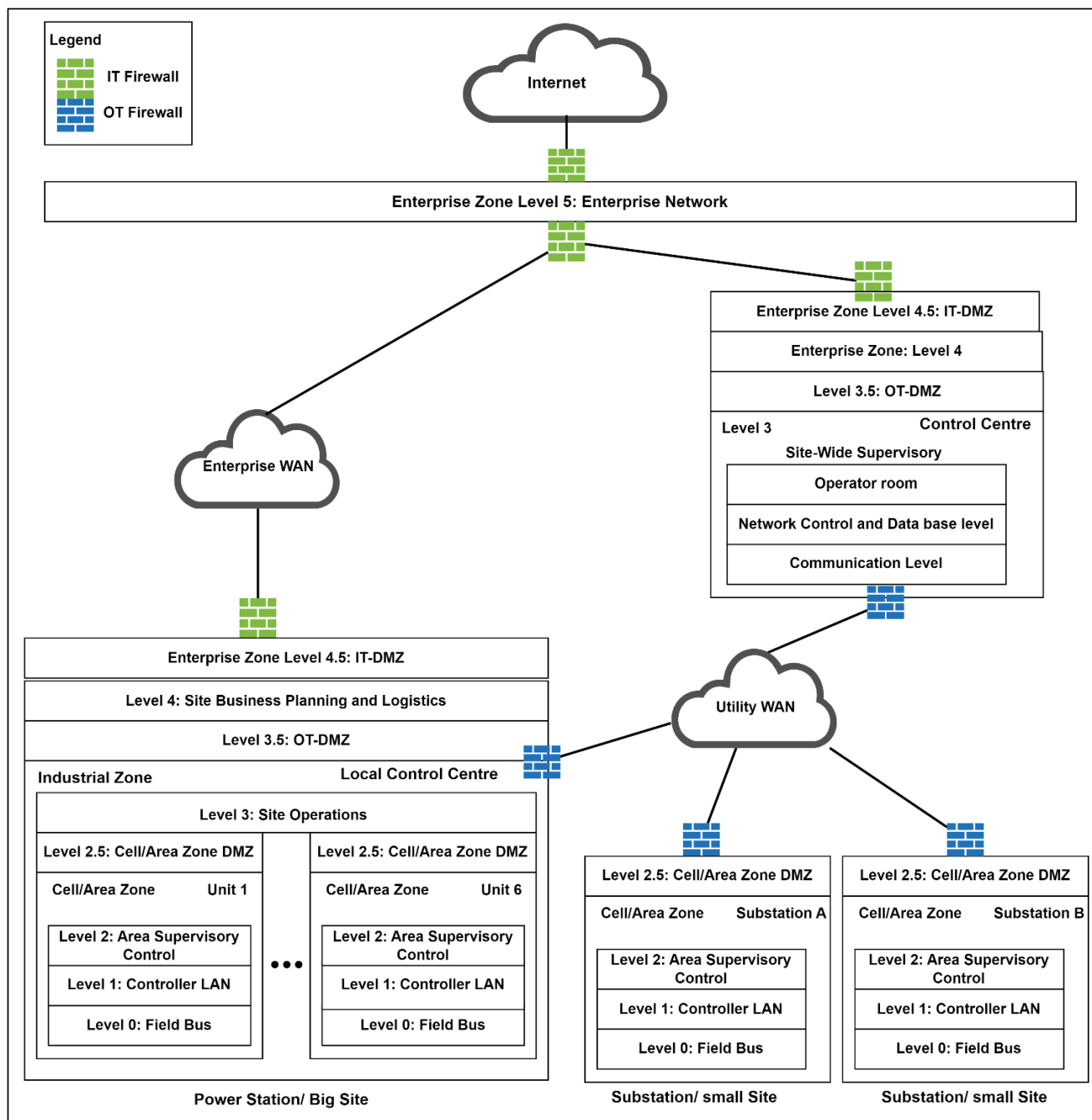
Date	Rev	Compiler	Remarks
March 2024	3	Kgomotso Manyapetsa	On the Third issue, the document has been amended to capture the current trends and practices. In Section 2, more normative, informative references were added, definitions and abbreviations added. In section 3, the Purdue Enterprise Reference architecture is introduced and its associated supporting diagrams, the fundamentals of DMZ introduced, deployment options are refined, and the schematics are refreshed. Introduced guidelines for configuring remote access within the OT environment with the associated diagram given that remote access is possible via the DMZ, guidelines on hardening all devices within the DMZ is provided.
Feb 2019	2	Billy Petzer	Requirement for dual-Layer 7 UTM's from different OEMs amended for critical OT systems. Section on security zones expanded.
Jan 2015	1	Johan Botha	First Issue

6. Development team

Not applicable.

7. Acknowledgements

Not applicable.

Annex A: Power Generation and Delivery Integrated Architecture View**Figure 6: Power Generation & Delivery Integrated View****ESKOM COPYRIGHT PROTECTED**

Annex B - Power Generation Reference Architecture

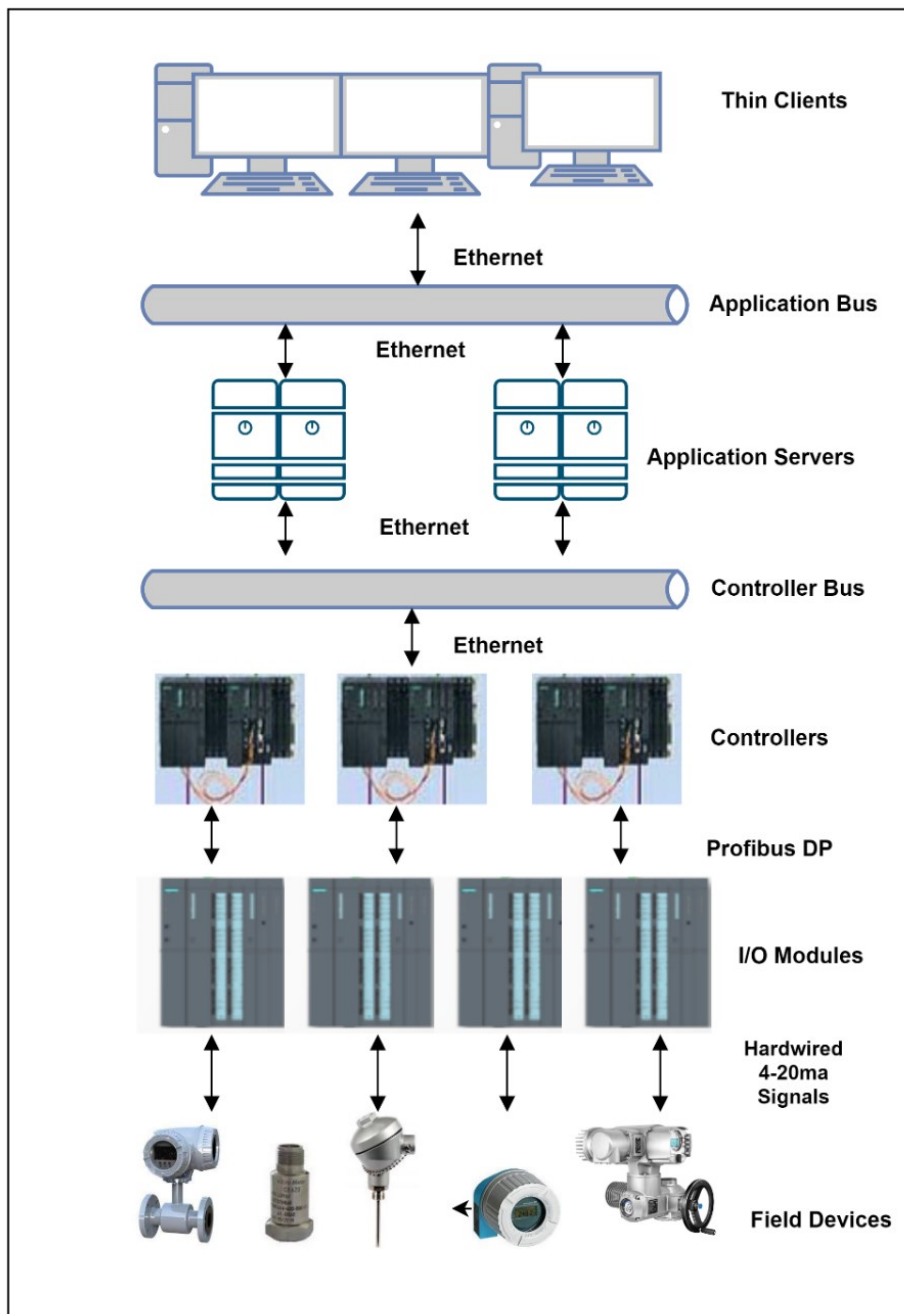


Figure 7: Power Station Reference Architecture

ESKOM COPYRIGHT PROTECTED

Annex C - Power Delivery Reference Architecture

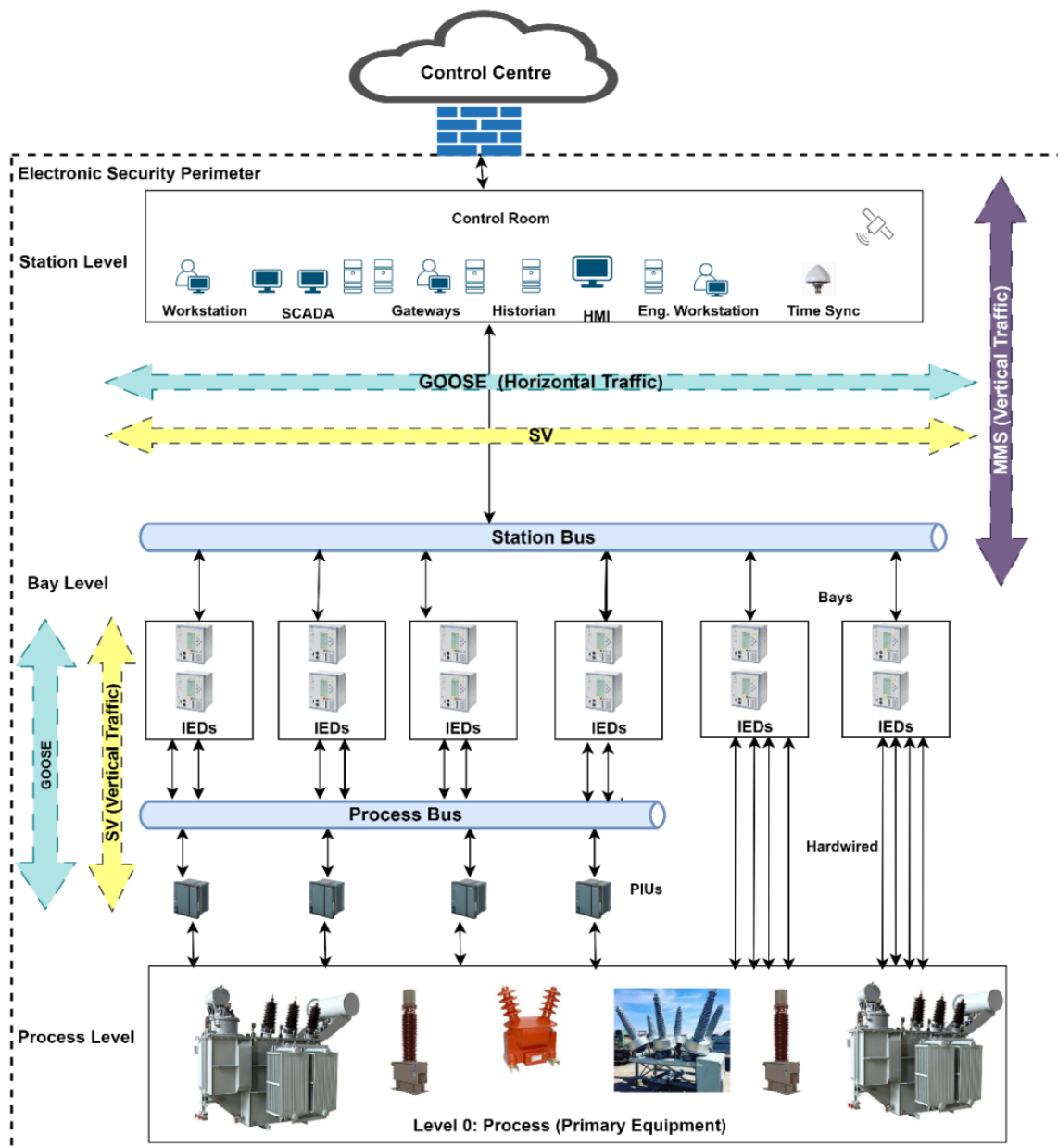


Figure 8: Power Substation Reference Architecture

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.