

Title: **NTCSA CYBER SECURITY
ARCHITECTURE AND
DESIGN PRINCIPLES**

Unique Identifier: **240-171000271**

Alternative Reference Number: **240-146054527**

Area of Applicability: **National Transmission
Company South Africa**

Documentation Type: **Standard**

Revision: **1**

Total Pages: **65**

Next Review Date: **March 2030**

Disclosure Classification: **Controlled Disclosure**

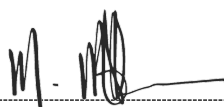
Compiled by



Pieter Mocke

**Chief Advisor: Information
and Cybersecurity**

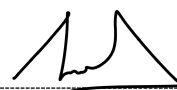
Functional Responsibility



Mervin Mottian

**Middle Manager: Information
and Cybersecurity**

Authorised by



Richard McCurrach

**Chairperson: NTCSA
Information & Technology
Steerco**

Date: 17/03/2025

Date: 18/03/2025

Date: 18/3/2025

Content

	Page
Executive Summary.....	5
1. Introduction.....	6
2. Supporting clauses	6
2.1 Scope	6
2.1.1 Purpose	6
2.1.2 Applicability	7
2.2 Normative/informative references	7
2.2.1 Normative.....	7
2.2.2 Informative	7
2.3 Definitions.....	8
2.3.1 General	8
2.3.2 Disclosure classification.....	9
2.4 Abbreviations.....	9
2.5 Roles and Responsibilities	11
2.6 Process for Monitoring	11
2.7 Related/supporting documents.	11
3. Cyber Security Design Principles and Architecture.....	12
3.1 Design Principles.....	12
3.1.1 Saltzer and Schroeder Design Principles	12
3.1.2 ISO Standard Design Principles	14
3.1.3 Defence in Depth	15
3.2 Zero Trust.....	19
3.2.1 Core Principles.....	19
3.2.2 Logical Components of Zero Trust Architecture	20
3.2.3 Zero Trust Objectives.....	22
3.2.4 Building Zero Trust.....	22
3.3 NTCSA Network Zero Trust Security landscape and Architecture	24
3.3.1 Reference Architectures for Zero Trust	24
3.3.2 Reference Architecture Development: Starting with the Purdue Model	25
3.3.3 Reference Architecture and Profiles	27
3.3.4 Reference Architecture for NTCSA.....	27
3.3.5 Zero Trust Security Architecture for NTCSA.....	32
3.3.6 Zero Trust Architecture in single OT site.	33
3.4 Secure Areas, Security Zones and Electronic Security Perimeters	34
3.4.1 ICT Network Security Framework Secure Areas in Reference to the Security Architecture for NTCSA.	35
3.4.2 Operational Technology Areas (Area 1 and Area 2).....	37
3.4.3 Centralised IT / OT Demilitarised Zone	38
3.4.4 Function and Purpose of Operational Technology Secure Areas	39
3.4.5 Information Technology Secure Areas (Area 3 and Area 4).....	39
3.4.6 Function of Information Technology Secure Areas.....	40
3.4.7 IT Segregation and Site VPN.....	41
3.4.8 Information Technology Centralised Demilitarised Zone	41
3.4.9 External Service (Secure Area 6)	43
3.4.10 External Control Centers (Secure Area 7)	44

CONTROLLED DISCLOSURE

3.4.11 Independent Power Producers (IPP) and Independent Transmission providers (ITP) (Secure Area 8).....	45
3.4.12 Industrial Internet of Things (IIoT) (Secure Area 9)	46
4. Authorization.....	47
5. Revisions	47
6. Development team	47
7. Acknowledgements	48
Annex A – Zero Trust Architecture in OT	49
Annex B – Secure Area Attributes.....	59
Annex C – NTCSA Security Design checklist.....	63

Figures

Figure 1: System Attack landscape	13
Figure 2: Cross Authenticated	13
Figure 3: Network Segments Authenticate	14
Figure 4: Defence in Depth Solution.....	15
Figure 5: Cybersecurity management plan.....	18
Figure 6: Cybersecurity life cycle.....	18
Figure 7: Core Zero Trust Logical Components	21
Figure 8: Transition from Network to Segment Perimeter	22
Figure 9: NTCSA Reference Cyber Security Architecture.....	28
Figure 10: Regional Utility-Scale DER Profile	30
Figure 11: Control Centre Profile	31
Figure 12: Control Centre Profile with Multiple Physical Zone Assets	31
Figure 13: Zero Trust Architecture in Single OT site	33
Figure 14: ICT Network Security Strategy Framework.....	35
Figure 15: Security Zone / Electronic Security Perimeter and Secure Areas.....	36
Figure 16: Logical Connection of Secure Area 1, Secure Area 2, OT/IT DMZ and WAN	37
Figure 17: IT / OT exchanging data over a Central DMZ	38
Figure 18: Logical Connection of the IT Secure Areas.....	40
Figure 19: Information Technology Site-to-site Virtual Private Network.....	41
Figure 20: Secure Area 5.....	42
Figure 21: Guidelines for Planning an TC Security Operations Center, by G. Rasche, December 2013, EPRI	43
Figure 22: Threat Centric Secure Operations Centre: Hybrid Framework	43
Figure 23: Secure Area 6.....	44
Figure 24: External Control Centers (Secure Area 7)	44
Figure 25: IPPs and ITPs (Secure Area 8)	45
Figure 26: Industrial Internet of Things (Secure Area 9)	46

CONTROLLED DISCLOSURE

Tables

Table 1 - Secure Area Attributes59

Table 2- Design Principles Related to Cyber Resiliency63

Table 3- Operational Principles Related to Cyber Resiliency.....65

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

Executive Summary

This document provides a reference security architecture for establishing secure Operational Technology (OT), Industrial Control Systems (ICS) and Information Technology (IT) within National Transmission Company South Africa SOC Ltd (NTCSA). These OT and IT systems, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) are vital to the operation of NTCSA critical infrastructures and are highly interconnected and mutually dependent systems. This document provides a Cyber Security architecture of the OT/IT ICS topologies and design Principles.

Initially, OT had little resemblance to traditional information technology (IT) systems in that OT were isolated systems running proprietary control protocols using specialized hardware and software. Many OT components were in physically secured areas and the components were not connected to IT networks or systems. Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cybersecurity vulnerabilities and incidents. As NTCSA transitions to adopting IP-based solutions to enhance corporate business systems connectivity and enable remote access capabilities, these solutions are increasingly being designed and implemented using industry-standard computers, operating systems (OS), and network protocols. Consequently, they are beginning to closely resemble traditional IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for OT from the outside world than predecessor systems, creating a greater need to secure these systems via a good reference cyber security architecture.

The increasing use of wireless unlicensed spectrum networking also places OT implementations at greater risk from adversaries who are in relatively close physical proximity but do not have direct physical access to the equipment. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to the OT environments. In some cases, new security solutions are needed that are tailored to the OT environment.

OT cybersecurity programs should be part of the broader OT/IT safety and reliability programs at both substation level and enterprise cybersecurity programs because cybersecurity is essential to the safe and reliable operation of modern electric utility processes. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters as well as malicious or accidental actions by insiders. NTCSA OT/IT cyber security objectives follow the priority of Safety, Availability and Integrity, followed by Confidentiality.

CONTROLLED DISCLOSURE

1. Introduction

The purpose of designing a cyber security architecture is to ensure security requirements are properly implemented in systems. Further, the architecture helps prevent or respond to attempts to compromise availability, integrity or confidentiality. NTCSA must build security into the design, implementation, and management of new and existing systems. This enables safe operation that reasonably and appropriately manages risk associated with affected systems and the data classification and categorization of said systems.

There are three main types of network providers to NTCSA; these are **Eskom Group Technology** (which provides Corporate LAN and IT MPLS WAN country-wide links), **NTCSA Telecommunications** (TT) (which provides Operational Technology LAN and OT MPLS WAN country-wide links), and other **3rd Party Telecommunications Service Providers** (which provide LAN/WAN/APN/Radio/Satellite/Internet links to both Eskom Group Technology and NTCSA Telecommunications). Some networks in the NTCSA environment are segregated with no interconnectivity and are known as “air-gapped” or “islanded” networks. These networks may also require connectivity soon.

Cyber security architecture design principles need to apply to both systems and the network infrastructure. Security architecture design is based on one or more risk assessments. It's important that the security architect / planner understand the risk associated with the data and critical systems involved. Architecture design must also include all statutory and regulatory compliance requirements and must be appropriate and based on the business's operational environment.

The future NTCSA network should incorporate the safety, confidentiality, integrity, and availability (SCIA) requirements for all NTCSA's services. It is therefore important that cybersecurity principles are embedded in the framework, architecture, and design of future ICT/ OT and IT networks.

According to the official International Information System Security Certification Consortium (ISC²) Guide to the CISSP Common Body of Knowledge reference, *“Success in security architecture is much more likely when one is aligned with the business and taking a risk management approach to security architecture”*.

2. Supporting clauses

2.1 Scope

The scope of this document is to assist planners in designing systems and networks with cybersecurity architecture design principles by looking at the elements of a high-level design standard of the future NTCSA ICT network security estate. The Standard will assist NTCSA in aligning with relevant legislative acts. The document covers the intended use of the ICT and OT network security and how it aims to achieve the challenges NTCSA experiences.

Network aspects will be included in relevant network frameworks, roadmaps, architecture, and/or other documents.

2.1.1 Purpose

The purpose of this document is to give a high-level understanding of the following:

CONTROLLED DISCLOSURE

- 1) Clear cybersecurity design principles for use in NTCSA OT/IT networks and system planning.
- 2) Define a Network Security Framework for NTCSA.
- 3) Assist in addressing current and future Cybersecurity demands and challenges of the electric power utility network.
- 4) Alignment of ICT Network Security Framework with Cybersecurity requirements.
- 5) Identify the key role players for IT/OT network security and their responsibility to the business.

2.1.2 Applicability

This document shall apply throughout National Transmission Company South Africa 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] 32-373: Information Security - IT/OT Remote Access Standard
- [3] 240-79669677: DMZ designs for Operational Technology
- [4] Critical Infrastructure Protection Act 8 of 2019
- [5] 32-143 Handling of classified items standard
- [6] 240-180100065: TX Cybersecurity Strategy
- [7] 240-55863502 Definition of Operational Technology (OT) and OT/IT Collaboration Accountabilities.

2.2.2 Informative

- [1] 240-170001061: Transmission Cyber Security Standard for Operational Technology
- [2] 240-91479924: Cyber Security Configuration Guideline of Networking Equipment for Operational Technology
- [3] 32-644: Eskom document management standard
- [4] 204-53114002: Engineering Change Management Procedure
- [5] Minimum Information Security Standard (MISS) – South African National document
- [6] 240-56355910 Management of Plant Software Standard
- [7] 240-131313815 – Critical Cyber Assets List.

CONTROLLED DISCLOSURE

2.3 Definitions

2.3.1 General

Definition	Description
Critical Asset	Facilities, systems, and equipment which if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the electric power utility network. Criteria for a critical asset is defined in 240-170001061 "Transmission cyber security standard for operational technology".
Cyber Security	Cyber Security is the process of safeguarding critical cyber assets from attack, through the implementation of policy, standards and procedures for cyber risk mitigation.
Data Centre	A data centre is a repository that houses computing facilities like servers, routers, switches, and firewalls, as well as supporting components like backup equipment, fire suppression facilities, and air conditioning. A data centre may be a dedicated building, or a room known as a data room. A data centre may be private or shared.
Defence in depth	Defence in depth is a concept used in Information security in which multiple layers of security controls are placed throughout an information technology system.
Electronic Security Perimeter	An electronic security perimeter (ESP) is a logical fencing of a system. The term ESP is introduced when a system has multiple secure zones. An example is a data centre with geographically separate sites for redundancy. At a minimum, this data centre will have two secure zones (one for site A and one for site B). Still collectively they will reside together under one ESP (e.g. data centre X ESP) to create a high-availability data centre.
Hardening	The process of securing a system by reducing its surface of vulnerability.
Information and Communication Technology	Information and Communication Technology (ICT) is an umbrella term for the collective NTCSA and Group Information Technology network.
Information Technology	Information Technology (IT) is a common term to describe the entire spectrum of technologies used for corporate information processing including software, hardware and related services. It involves the electronic representation of business information that is processed by a computer or sent over digital communications (e.g. IP network). In NTCSA, the Group Information Technology (GIT) business unit represents IT.
IT-OT Convergence	The trend that: The underlying platforms and technologies used in IT and OT are increasingly the same. The underlying platforms are increasingly using some shared infrastructure, standard and approaches. The shifting from proprietary and hardware-based technology to open and software-based technology. The evolution of new risks due to the above. Those companies are increasingly leveraging these trends for increased business value and efficient monetary spending.
Jump Server	A jump server is a device that spans two dissimilar security zones (such as a DMZ and a zone residing in a secure area) and provides a controlled means of access between them. A hardened jump server can be used for critical areas of the business such as connections into Secure Area 1.

CONTROLLED DISCLOSURE

Definition	Description
Open Systems Interconnection Model	Open System Interconnection (OSI) model is a conceptual model that standardises the communication functions of a telecommunication or computing system without regard to the underlying internal structure and technology. The model uses layers and is defined as such: Physical Layer – Transmission and reception of raw bit streams over a physical medium. Data Link Layer – Reliable transmission of data frames between two nodes connected by a physical layer. Network Layer – Structuring and managing a multi-node network, including addressing routing and traffic control. Transport Layer – Reliable transmission of data segments between points on a network including segmentation, acknowledgement, and multiplexing. Session Layer – Managing communication sessions. Presentation Layer – Translation of data between a networking service and an application. Application Layer – High-level application programming interface.
Operational Technology	Technology used to control, monitor, or operate the electrical grid is considered Operational Technology (OT). This is considered NTCSA's core business.
Secure Area	A secure area is a term used to secure a service both on-site and in transport. Secure areas are setup in a manner that prevents the propagation of a threat from one secure area to another. When a secure area is defined in an organisation, those classed services must be segregated from services outside that secure area. Segregation can be in the following: Physical insulation, protocol insulation and firewall insulation.
Security Zone	A security zone is defined as a grouping of logical or physical assets that share common security requirements. A security zone is a segregated zone in a network. A security zone is limited to the physical infrastructure that creates that zone. Once the data leaves that segregation device (e.g. firewall), it is in another zone. Examples can be a control zone for production equipment, a demilitarised zone for sharing information between networks, an enterprise zone for the corporate side of the business, etc.
Zero trust (ZT)	Zero Trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per request access decisions in information systems and services in the face of a network viewed as compromised
Zero trust architecture (ZTA)	Zero trust architecture is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
API	Application Programming Interface
ASR	Attack surface reduction
BYOD	Bring Your Own Device

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

CCA	Critical Cyber Assets
CDM	Continuous Diagnostics and Mitigation
CIA	Confidentiality, Integrity and Availability
CSMS	Cybersecurity Management Systems
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DoS	Denial of Service
EAAB	Enterprise Architecture Advisory Board
ESP	Electronic Security Perimeter
ET	Eskom Telecommunications
G2B	Government to Business (private industry)
G2G	Government to Government
HMI	Human Machine Interface
ICT	Information and Communications Technology
IED	Intelligent Electronic Device
IP/MPLS	Internet Protocol / Multiprotocol Label Switching
IS	Information Security
IT	Information Technology
LAN/WAN	Local Area Network / Wide Area Network
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
OSI	Open System Interconnection
OT	Operational Technology
PA	Policy Administrator
PDP	Policy Decision Point
PE	Policy Engine
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PSP	Physical Security Perimeter
RMF	NIST Risk Management Framework
SCADA	Supervisory Control and Data Acquisition
SCOT	Steering Committee of Technologies
SDN	Software Defined Network
SDP	Software Defined Perimeter
SIEM	Security Information and Event Monitoring

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

TIC	Trusted Internet Connections
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
ZT	Zero Trust
ZTA	Zero Trust Architecture

2.5 Roles and Responsibilities

The following are roles and responsibilities for the implementation of this document:

- 1) Planners are responsible for assessing the requirements against this standard on a per-project basis and performing the detailed design based on the site-specific requirements.
- 2) System Owners shall participate in the standards and process development through approved committees and architecture forums and project implementation through design review governance.

2.6 Process for Monitoring

These design standards and architecture are to be used during design governing processes to standardize the approach from NTCSA with regards to cyber security. The standard is to provide guidance for key role players to update their documentation and designs going forward.

The relevant committees as per the roles and responsibilities above shall review this standard design principles.

The standard should provide the ability to measure risk and improve cyber security.

The framework maps back to COBIT, ISO, NIST, CIS. IEC etc.

2.7 Related/supporting documents.

Not applicable

CONTROLLED DISCLOSURE

3. Cyber Security Design Principles and Architecture

Building cyber security into a system instead of adding it later is less expensive. It also enables security between system components. Cyber Security isn't just about keeping people honest. It's also about controlling what internal and external non-human entities can access.

The two overarching principles are: (1) security functions must be implemented in a way that prevents bypass, circumvention, or tampering, and (2) security functions must be initiated whenever necessary to enforce one or more security requirements

The sets of design principles below are the design principles as defined by Saltzer and Schroeder or the *protection of information in computer systems principles* and the concept of *Defense in depth* with *Zero Trust*.

This section outlines key principles to consider when designing secure cyber architecture. These are guiding principles, and while projects should evaluate their designs against these principles, adherence is not a strict requirement. It incorporates three foundational concepts:

1. **Saltzer and Schroeder Design Principles:** These principles focus on minimizing complexity, enforcing access controls, and assuming eventual compromise.
2. **ISO Standard Design Principles:** These principles build upon Saltzer and Schroeder's concepts, adding elements like domain separation, layering, and redundancy.
3. **Defense in Depth:** This approach emphasizes layering security controls to create multiple barriers against attackers.

3.1 Design Principles

3.1.1 Saltzer and Schroeder Design Principles

These principles provide a foundational framework for secure design and are essential for ensuring that all NTCSA systems are effectively integrated into the design and implementation process. Planners may use these principles to evaluate systems from a cybersecurity perspective throughout the project lifecycle:

1. **Economy of Mechanism:** Keep security features per NTCSA system simple and manageable.
2. **Fail-Safe Defaults:** Deny access by default, explicitly granting permissions to any NTCSA resources.
3. **Complete Mediation:** Every access attempt requires authorization checks.

CONTROLLED DISCLOSURE

This graphic below (Figure 1) shows a high-level view of a system's attack surface. The architecture design must address authentication and authorization at each layer or surface.

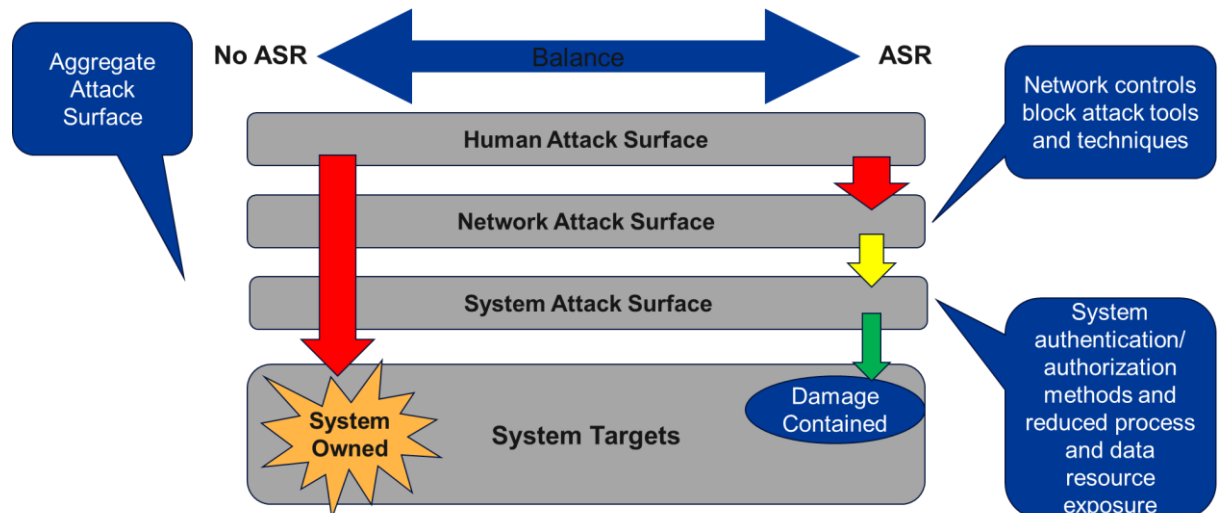


Figure 1: System Attack landscape

Once a system is accessed, use of any process must also be authenticated. This includes one process accessing other processes or services (Figure 2).

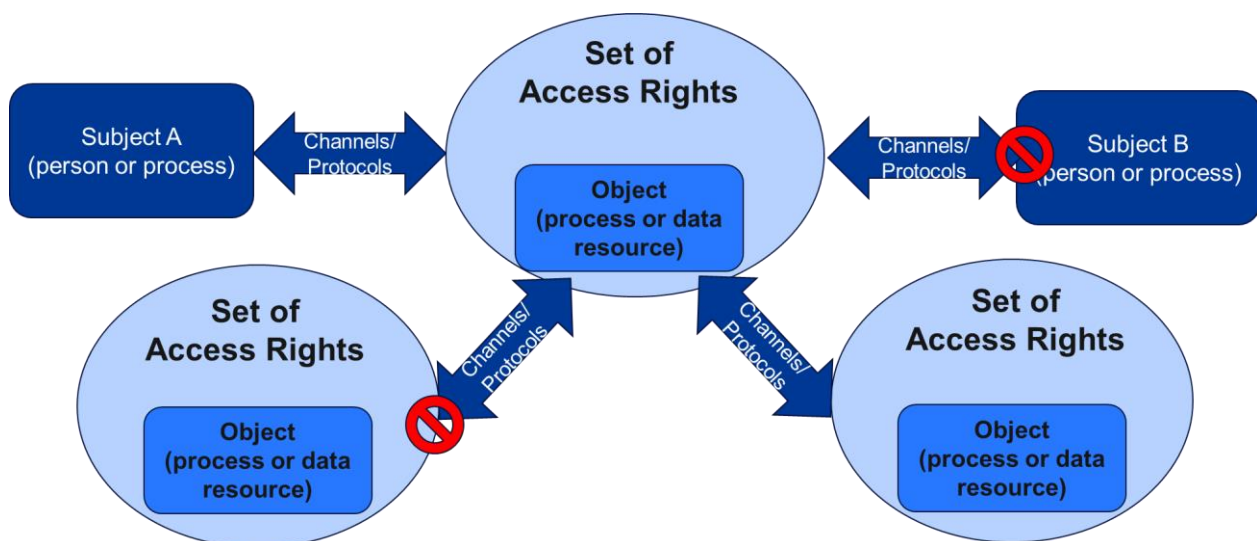


Figure 2: Cross Authenticated

4. **Open Design:** Cybersecurity relies on robust design rather than the secrecy of implementation. It must be thoroughly documented and aligned with the appropriate document classification standards.
5. **Separation of Privilege:** Sensitive operations should require the involvement of multiple actors.
6. **Least Privilege:** Grant only the minimum level of access necessary to perform tasks.
7. **Least Common Mechanism:** Limit shared components to minimize trust boundaries.

CONTROLLED DISCLOSURE

8. **Psychological Acceptability:** Design controls that are user-friendly and easy to work with.
9. **Work Factor:** Ensure that attacks require significant effort and resources, deterring potential attackers.
10. **Compromise Recording:** Assume breaches will occur and implement detection mechanisms at every level of the architecture.

3.1.2 ISO Standard Design Principles

The ISO standard expands on these principles with a focus on architecture:

- **Architectural Principles:**
 - **Domain Separation:** Isolate systems based on trust levels between IT and OT. The Active Directory (AD) for Group Technology should be separate from the AD for Telecoms, System Operations, and OT, with each being isolated as distinct entities.
 - **Layering:** Implement security checks at each system layer. In the example below (Figure 3), a user is attempting to access an application. Once on the application, the application must access the database. At each layer, the entity attempting access must authenticate. In addition, the system elements are separated by network segments. At each segment border, the traffic is checked to determine if it is allowed.

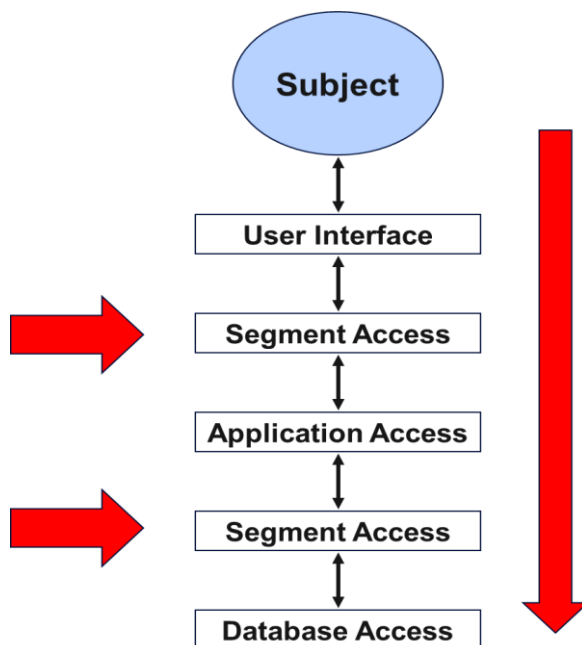


Figure 3: Network Segments Authenticate

- **Encapsulation:** Systems need to control access to object functionalities.
- **Redundancy:** Planners need to eliminate any single points of failure in priority 1 and 2 systems.
- **Virtualization:** Utilize virtualization for efficient resource management and redundancy design.
- **Design Principles:**
 - **Least Privilege:** Minimize access rights for users, applications, and services to only what is necessary for performing required tasks.

CONTROLLED DISCLOSURE

- **System Attack Surface:** Reduce exposed points of entry by disabling unused services and validating inputs.
- **Centralized Parameter Validation:** Implement robust input validation mechanisms to prevent malicious attacks and ensure data integrity.
- **Centralized General Security Services:** Centralize the management of critical security activities, such as authentication and logging, using an IAM system.
- **Errors and Exception Handling:** Design systems to detect, log, and respond to unexpected behaviour.

3.1.3 Defence in Depth

This approach utilizes multiple layers of security controls to create a comprehensive defence. It is crucial for planners to be thorough and meticulous when enhancing the cybersecurity framework of a system by adding multiple layers of defence. Defence in depth reduce the probability that an intruder can succeed to penetrate the system. Defence in depth can also help to identify intruders who attempt to access the system. If an intruder gains access to a system, defence in depth reduce the harmful impact and gives administrators and engineers time to update countermeasures and prevent future attacks. The different layers of this defence in depth are listed in Figure 4.



Figure 4: Defence in Depth Solution

Utilizing a combination of active and passive cybersecurity techniques can effectively strengthen the overall security posture of the system:

- **Concept:** No single control is foolproof. Layered defences slow attackers and provide redundancy.
- **Elements:**
 - **Administrative Controls:** Policies, procedures, and training to promote secure practices.
 - **Physical Controls:** Physical barriers and access restrictions to both IT and OT infrastructure.

CONTROLLED DISCLOSURE

- **Technical Controls:** Firewalls, intrusion detection/ prevention systems, authentication mechanisms, and endpoint security software.
- **Behavioural Analysis:** Monitoring user and system activity for anomalies, including SIEM.

3.1.3.1 Network Segmentation

It is required to segments the network in zones separated by firewalls as it will offer more security because if an intruder compromise the perimeter zone, he must first penetrate the firewall to compromise the other zones behind it to get control of physical equipment. Section 3.4 provides details on the implementation of secure areas and security zones.

3.1.3.2 Firewalls

Firewall must be configured to authorise only needed services or protocols for communication between the segmented zones. These will obscure the network structure and devices from external view and establish the boundary between security zones.

3.1.3.3 Secure Protocols

All unsecure protocol or clear text protocols must be disabled because data such as username and password are transferred without encryption and a simple sniffing tool can get them. NTCSA must use only the secure versions for example. For the network management the use of Simple Network Management Protocol V3 (SNMPv3) instead of SNMPv1 or v2. For file transfer the use of Secure File Transfer Protocol SFTP instead of FTP. For web server the use of the Secure Hypertext Transfer Protocol HTTPS instead of HTTP. For device configuration the use of SSH Secure Shell instead of Telnet.

3.1.3.4 Hardening Devices

One of best solution against internal attack is hardening devices. Hardening devices mean that all unused ports, protocols, or services in a device must be disabled. For each equipment in the architecture the following actions needs to be taken.

Switches: The first action is to disable the default admin account and create new account with complex password. The second action is to disable unused ports for communication. The third action is to enable secure protocol and disable unsecure protocols such as HTTP, FTP and Telnet. Besides, ware supported NTCSA needs to associate ports with media access control (MAC) address for all devices. In this case, If the intruder tries to connect a device into a port that is assigned to MAC address the port will be disabled preventing access to the network.

Computers: Gateways and HMI are industrial computers that are running on windows operating system. The **first** action is to be sure that the operating system is installed from a trusted and certified CD/ source because engineers often install windows from materials downloaded from the internet, so these materials could be infected or have some vulnerabilities. The **second** action is to install the latest updates from the operating system provider that correct all vulnerabilities detected in previous version. The **third** Action is to disable all USB ports as malwares and virus can be injected via USB key drivers. Action **four** is to disable all unused services, application, or ports in the computer.

IED: For the bay controllers or numeric protective relays, the default username and password must be deleted, and more complex password must be used. Integrating with an Identity and Access Management (IAM) system that uses Role-Based Access Control (RBAC) is advisable as it enhances security and simplifies user management. IAM systems manage identities and enforce policies, while RBAC ensures that users have access only to the resources necessary for their roles.

CONTROLLED DISCLOSURE

3.1.3.5 Access Control Management

Another solution for protection against internal threats can be done by using access control management. For this aim we are to apply the recommendation of part 8 from IEC62351, which is Role based access control (RBAC). For every device in the substation and control centre (Level 3 to Level 0) the RBAC must be deployed on new installations, so for every user access should be granted only for object concerning this user operation. For example, some operator will have access only to open or close primary equipment but will not have access to change setting of relay settings. The RBAC allows to divide access by areas of expertise which prevent from unintentional operation fault and from disgruntled employees. For computers based on windows operating system, to use of a domain controller to secure authentication requests are required.

3.1.3.6 Monitor Traffic

The Monitoring of logging activities and unsuccessful login attempts can give an idea about the way users are operating. The system owners need to deploy a logs system manager which will collect logs from all devices using Syslog protocol following standard RFC3164 and RFC 5424. It can also be feed to a SIEM with OT awareness. This will give the possibility to create historical audit trails of individual user account and system access activity.

3.1.3.7 Whitelisting

In addition to the antivirus that must be installed on computer its recommended to add/ enable a whitelisting program, this will allow only trusted applications and services declared in the list to be executed, which will Blocks any malicious software, even if it is unknown. In the mostly static environments like OT, it is recommended.

3.1.3.8 Backup & Restore

One way to enhance the security from equipment's failure is to have a backup and restore policy. A purpose-built backup process needs to be in place for all the systems. The backup and restore of computers using VM's need to be automatic using dedicated software. In the case IED setting are stored in their internal memory, so the backup will be manually by taking a copy of the last known validated settings. In the case of an equipment failure, for example, a computer or a IED damaged due to an overvoltage in the auxiliary power supply, the maintenance team can change the equipment and inject the backup setting which will offer them better time in comparison to the case if they don't have a backup and should configure it from zero.

3.1.3.9 Cybersecurity Management

Cyber security is an ongoing process that encompasses procedures, policies, software, and hardware. Implementing a plan for managing incidence response in case of any external or internal vulnerability reported from the vendor on any device needs to be developed/ implemented and tested. Figure 5 presents the Cybersecurity management plan.

CONTROLLED DISCLOSURE

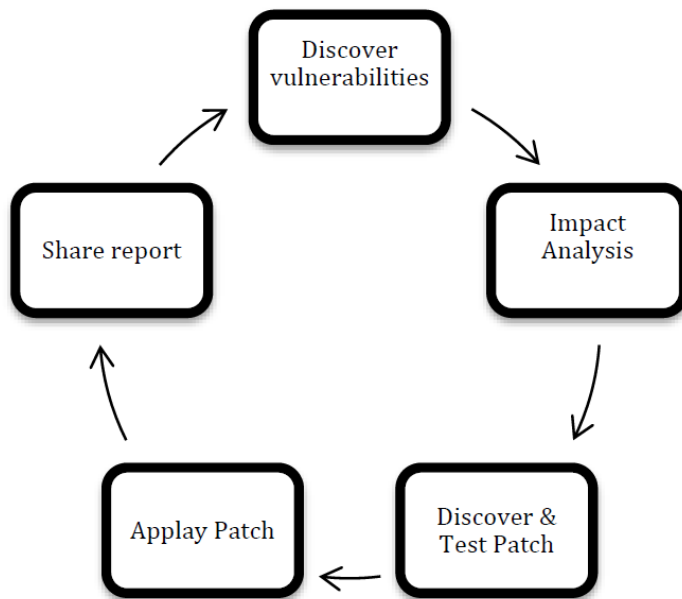


Figure 5: Cybersecurity management plan

First, if a detection of a vulnerability occurs, an impact analysis on the system should be conducted. Then, a Patch to fix the vulnerability should be found and evaluated and tested before being applied. Finally, a report about the vulnerability should be shared with other stakeholders. Cybersecurity procedures and policies should be applied in early phase of projects following the cyber security life cycle presented in Figure 6.

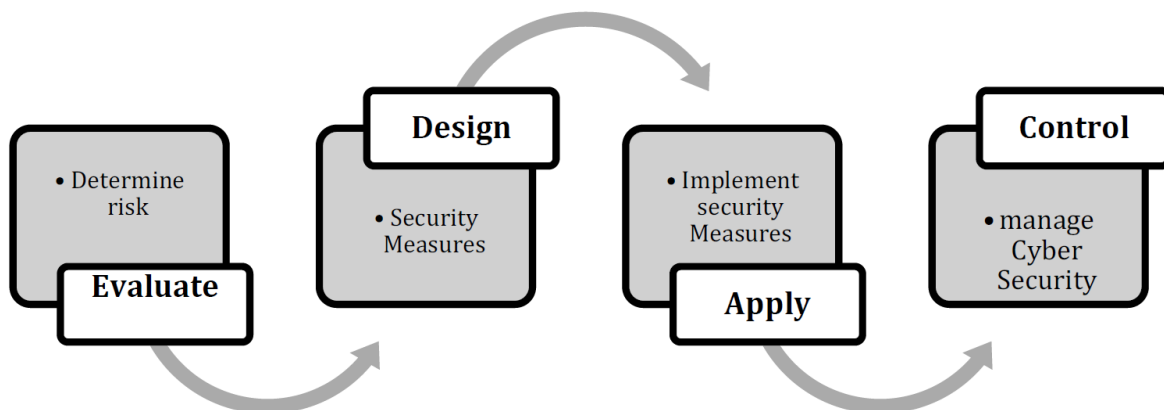


Figure 6: Cybersecurity life cycle

The first step is to determine baseline risk and security levels. The second step is to design the system using the appropriate security measurements as per the standard. The third step is to implement the security measurements and procedures with the purpose to obtain the minimal impact on the operation of substation. Finally, the cybersecurity risk should be managed by an incidence response plan.

CONTROLLED DISCLOSURE

Although the fact that the defence in depth comes into sight to be a complex and fatiguing solution to implement in grid automation systems, it is mandatory to apply it on power grids because the cyberattacks become dangerous to substations; also, the multiple layers of security is an efficient way to prevent from external attacks and especially from internal treats that are hard to be detected or prevented as the major element in internal treats are human whether attacks are intended or unintentional wrong operations. By following these principles and employing defence in depth, NTCSA can significantly improve our overall cybersecurity posture.

3.2 Zero Trust

3.2.1 Core Principles

This section outlines the key principles of Zero Trust to consider when designing secure cyber architecture. These are guiding principles, and while projects should evaluate their designs against these principles, adherence is not a strict requirement. Zero Trust is a security paradigm that assumes no user, device, or network segment is inherently trustworthy. All access requests require continuous verification, authorization, and encryption.

Key principles include:

- **Never Trust, Always Verify:** Every access attempt necessitates strict identity verification, regardless of location.
- **Least Privilege:** Users and devices are granted only the minimum access permissions needed for their tasks.
- **Continuous Monitoring:** Access requests and user activity are constantly monitored for suspicious behaviour.
- **Micro segmentation:** The network is segmented into smaller, more secure zones to limit the impact of potential breaches.

Benefits:

- Improved security posture.
- Reduced blast radius of breaches.

Challenges:

- Integration complexity.
- Users experience considerations.

3.2.1.1 Zero Trust Basics

Zero Trust focuses on resource protection and continuous evaluation of trust. Planners need to emphasize on the following during a system design:

- Identity and access management (IAM system per level of the perdue model)
- Operations classification (OT vs IT)
- Endpoints identification (All data generating devices)
- Hosting environments (virtualization and bare metal)
- Interconnecting infrastructure (OT to OT and OT to IT)

Initial Focus: A thorough review of all IT systems, OT systems, and cloud resources (if applicable) must be conducted to guarantee alignment with the following security standards.

CONTROLLED DISCLOSURE

- Restrict resources to those with a need to access.
- Grant only minimum privileges (read, write, delete).
- Eliminate implicit trust based on location or authentication.

3.2.1.2 Tenets of Zero Trust

NTCSA must adhere to the following tenets:

1. All data sources and computing services are to be seen as resources.
2. All communication needs to be secured regardless of network location.
3. Access to individual NTCSA resources is granted on a per-session basis and determined by dynamic policy based on:
 - User identity
 - Application/service
 - Requesting asset
 - Behavioural and environmental attributes
4. All owned and associated assets are continuously monitored for compliance to the security posture.
5. All resource authentication and authorization are dynamic and strictly enforced.
6. NTCSA collects data (via SIEM / SOC) to improve security posture through policy creation and enforcement.

3.2.1.3 NTCSA Zero Trust Implementation

NTCSA needs to implement Zero Trust principles incrementally through:

- **Process Changes:** Redesign workflows to incorporate Zero Trust controls.
- **Technology Solutions:** Implement tools for authentication, authorization, and micro segmentation.
- **Use Case Approach:** Prioritize Zero Trust implementation for critical use cases.

3.2.2 Logical Components of Zero Trust Architecture

There are numerous logical components that make up a ZTA deployment. These components should be operated as an on-premises service. The conceptual framework model in Figure 7 shows the basic relationship between the components and their interactions. *Note, that this is an ideal model showing logical components and their interactions.* From Figure 7, the policy decision point (PDP) is broken down into two logical components: the policy engine and the policy administrator (defined below). The ZTA logical components use a separate control plane to communicate, while application data is communicated on a data plane.

CONTROLLED DISCLOSURE

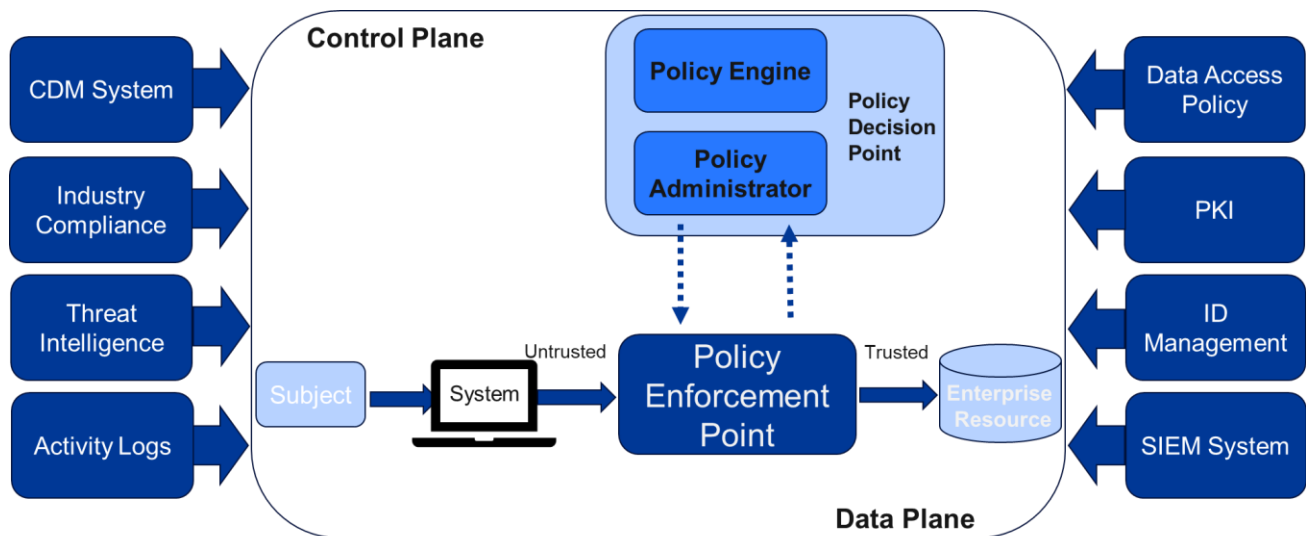


Figure 7: Core Zero Trust Logical Components

- **Policy Engine (PE):** Makes access decisions based on policy and external sources (e.g., threat intelligence).
- **Policy Administrator (PA):** Establishes and manages communication paths between subjects and resources.
- **Policy Enforcement Point (PEP):** Enables, monitors, and terminates connections.

Network/Environment Components

- **Control Plane:** Used for network control communication and access decisions.
- **Data Plane:** Used for actual communication between software and end device components.

Key Requirements:

- NTCSA needs to distinguish between owned/managed assets and their security posture.
- NTCSA needs to observe all network traffic.
- All NTCSA resources are not reachable without a PEP.
- Data and control planes are logically separate.
- NTCSA assets can reach the PEP component(s) and are isolated by it.
- The PEP is the only component that accesses the policy administrator.
- The ZTA access decision process infrastructure is scalable.
- NTCSA assets may not reach certain PEPs due to policy or security factors.

Broad principles that must be adhered to as a best practice:

- Eliminate implicit trust.
- Verify all data flows/sessions.
- Limit the blast radius with micro-segmentation and defence in depth.
- Implement role-based and context-aware access.
- Grant least privileged access.
- Utilize dynamic and adaptive policies.

CONTROLLED DISCLOSURE

- Protect data with encryption and other techniques.
- Maintain continuous logging and monitoring for suspicious activity.

3.2.3 Zero Trust Objectives

3.2.3.1 The Challenge

Shifting from traditional network perimeters to resource-centric security presents a significant challenge. Zero Trust advocates for securing each resource within its own security zone (Figure 8). While achieving this ideal state may not be immediately feasible for all NTCSA environments, it should serve as the guiding principle for cyber security design. Additionally, the security posture required for each resource will vary based on its classification and categorization. Figure 8 illustrates the transition from Network to Segment Perimeter.

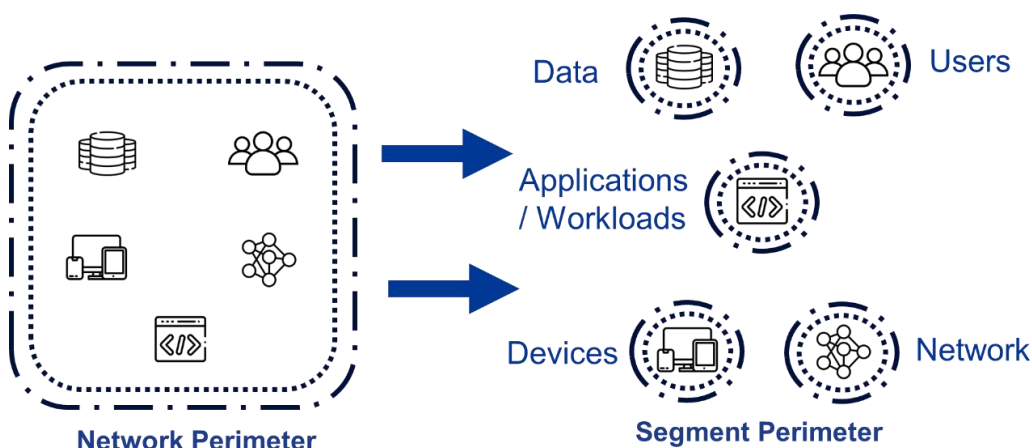


Figure 8: Transition from Network to Segment Perimeter

3.2.3.2 Security Zones

The concept of security zones, though not always explicitly named, has been used for years. VLAN segments with access control lists (ACLs) exemplify this approach. Traditionally, access to resources within a zone was granted after a single point of authentication for a user, application, and device combination (subject). Subsequent access to devices within the zone often relied on the same initial authentication and authorization, potentially granting access for extended periods. Zero Trust, however, necessitates a more granular approach and needs authentication for every new request.

3.2.4 Building Zero Trust

The objectives for NTCSA's Zero Trust implementation are aligned with the recommendations outlined in NIST Special Publication 800-207, Zero Trust Architecture <https://csrc.nist.gov/pubs/sp/800/207/final>. These core principles are:

1. **All resources:** All data sources and computing services are considered resources within NTCSA's security domain.
2. **Secure communication:** All communication channels, regardless of network location (Internal NTCSA network or via third-party ISP's) must be secured.
3. **Per-session access:** Access to individual NTCSA resources is granted on a per-session basis.

CONTROLLED DISCLOSURE

4. **Dynamic policy:** Access control decisions are made based on dynamic policies that consider various factors including Subject identity (user, application, device), Subject behaviour, Time of access, Geographic location of the subject, Classification/categorization of the resource being accessed.
5. **Security posture monitoring:** NTCSA need to continuously monitors and assesses the security posture of all owned and associated assets.
6. **Strict authorization:** All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. **Data collection and risk adjustment:** NTCSA gathers comprehensive data about the current state of assets, subjects, network infrastructure, and communications to dynamically adjust session-based risk assessments.

Core Assumption: NTCSA needs to operate under the assumption that all devices on the network, including those connected remotely, are potentially compromised until analysis proves otherwise.

3.2.4.1 The Basics

Any attempt by a subject to access a resource triggers a real-time risk assessment to determine the associated risk of that specific session. Prior successful access to the same resource is irrelevant; each session is evaluated independently.

The risk assessment needs to consider various session characteristics:

- Subject identity (user, application, device).
- Subject behaviour.
- Time of access.
- Geographic location of the subject.
- Classification/categorization of the resource being accessed.

Implementing a Zero Trust solution allows NTCSA to achieve these objectives. While specific solutions may vary, they all provide the following core functionalities:

- **Policy Decision Point (PDP):** Determines if a subject falls within an acceptable risk threshold based on administrator-defined parameters. The PDP utilizes two components:
 - **Policy Engine (PE):** Analyses data from various sources to make access decisions, including:
 - Continuous Diagnostics and Mitigation (CDM) system for subject device health assessment (patch level, installed software).
 - Industry Compliance System for enforcing regulatory or industry-specific requirements.
 - Threat intelligence feeds.
 - Security Information and Event Management (SIEM).
 - Data access policies set by the administrator.
 - Public Key Infrastructure (PKI) for issuing and validating subject certificates.
 - Identity and Access Management (IAM) system for subject authentication.
 - User and subject behavior data.
 - **Policy Administrator (PA):** Configures sessions based on the PE's decision.

CONTROLLED DISCLOSURE

- **Policy Enforcement Point (PEP):** Establishes and terminates sessions based on instructions from the Policy Administrator. The PEP can be a software agent on devices, a hardware appliance, or both.

Configuring the infrastructure to enable zero trust is a function of the solution one selects and our network's existing infrastructure. Implementation does not have to be all or nothing. NTCSA has already segmented our networks for security reasons. Even though strict zero-trust focuses on protecting individual applications, it can also be used to control access to existing resource clusters on VLANs or other segments, segments protected based on the associated risk.

Zero Trust Architecture is a business enabler. It encompasses people, processes, technology, and an architecture framework. That said, inherent risks do exist. Managing those risks is a multi-dimensional endeavour. Managing this risk to business requires designing and building access policies and deploying enforcement at various points. Implement such a change in paradigm, requires organizational culture change, buy-in from all business stakeholders, planning, developing asset inventory, mapping complex data flow, and micro-segmenting networks to limit blast radius. Security controls are required to check users, devices, systems, and processes to interact with business data, and then effectively manage the associated risks. In practice, given the diverse set of solutions available, system owners may choose additional tools and third-party solutions to secure their environment.

3.3 NTCSA Network Zero Trust Security landscape and Architecture

3.3.1 Reference Architectures for Zero Trust

This section explains the reference architectures within the context of Zero Trust (ZT) security for NTCSA ICT networks.

Definition and Purpose

The term "reference architecture" has various interpretations. One definition, provided by the European Innovation Partnership on Smart Cities and Communities, states:

"Reference architecture is defined as an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions."

For this document, we adopt the following working definition:

- A reference architecture establishes a common communication platform through a system of classification (taxonomy).
- It typically encompasses common architectural principles, patterns, building blocks, and relevant standards.

Reference architectures are prevalent across numerous industries. They often serve as a foundation for system design. By studying a relevant reference architecture, designers can gain insights into essential components for their specific system, avoiding the need to start from scratch. This approach accelerates the design process and fosters improved outcomes.

In the cybersecurity domain, reference architectures provide a starting point for security implementations. They establish a common ground for security discussions surrounding new systems, facilitating efficient communication between stakeholders (including original equipment manufacturers [OEMs] and system owners/operators [SOOs]). These architectures guide discussions that appropriately consider security features and controls.

Shared reference architectures offer several benefits aligned with NTCSA cybersecurity strategy:

CONTROLLED DISCLOSURE

- **Risk-Based Approach:** They promote a risk-based approach to cybersecurity, aligning with NTCSA's overall security strategy.
- **Reduced Duplication:** Reference architectures minimize redundant efforts by establishing best practices.
- **Continuous Improvement:** They can be continually updated to reflect evolving security landscapes.
- **Standardized Baselines:** SOOs can leverage these baselines for short- and long-term design and engineering practices.
- **OEM Guidance:** They provide a starting point for secure design considerations by OEMs.

Within this document, reference architectures provide value in two keyways, assuming a collection addressing various aspects of electric grid cybersecurity:

1. **Identifying Security Design Gaps:** Comparing a specific system's security architecture with an applicable reference architecture can reveal missing security controls that can be incorporated into the design.
2. **Identifying Standards Gaps:** Reference architectures can expose gaps within the existing set of cybersecurity standards applicable to the electric grid. Mapping these standards onto reference architectures can identify areas not adequately addressed by standards. These gaps represent potential vulnerabilities that require collaborative efforts from grid stakeholders to address through security design solutions.

This document establishes a reference architecture and accompanying profiles to deliver these benefits. It begins with the "Reference Architecture for Electric Energy OT," from which domain-specific applications, referred to as profiles, are derived. The domain-specific reference architectures include:

- Substation
- Distributed Energy Resources (DER)
- Regional Utility-Scale DER
- Control Centre

3.3.2 Reference Architecture Development: Starting with the Purdue Model

The Purdue Enterprise Reference Architecture, often called the "Purdue Model," was developed to define segmentation between enterprise networks and ICS networks. While the Purdue Model was not designed to be a cybersecurity reference architecture, it does provide a framework for discussing, analysing, and designing security for ICSs, particularly the touchpoints between OT networks and IT networks.

The Purdue Model has been utilized in the industrial and manufacturing sectors, and thus the levels and zones represent these sectors. NTCSA will leverage the model but adapt some of the zone and level naming that would be more familiar to an electricity subsector OT system engineer. It is also acknowledged that the Purdue Model will have challenges as the OT systems evolve and advance (for instance, through the incorporation of virtualization technology and SDN). We will focus on the typical OT system installed or the digital OT systems that are state of the art today. The cloud-based OT systems in development are an identified gap that will require the adaption or development of a new reference architecture.

CONTROLLED DISCLOSURE

The Purdue Model for ICS Security is a framework that can help us secure our IT and OT environments. It is divided into multiple levels to manage and protect various aspects. Each level has its own set of security challenges and requirements, and the Purdue Model helps implement security controls at each level to safeguard our IT and OT processes from cyber threats. It serves as a valuable framework for maintaining the availability, integrity and confidentiality of OT environments, ensuring the safe and reliable operation of critical infrastructure systems.

The Purdue Model divides the ICS/OT architecture into different zones/levels to ensure power utility level security. These zones are organized in a hierarchical manner from top to bottom, with each level having specific security considerations:

- **Level 0**

Field Devices Zone: This is where physical processes occur. This includes physical equipment such as transformers, and circuit breakers, or in another way, where the physical system meets the cyber system, through sensors, transmitters, and other final control elements etc. Security at this level focuses on device integrity.

- **Level 1**

Process Control Zone: Control systems that manage the field devices. At this level, there are controllers, which is where they collect information from sensors and transmitters at Level 0, formulate control decisions, and issue instructions to them. This level handles ongoing control tasks, and the connections are usually established through physical wiring, such as the use of PLCs, IEDs, and DCS controllers. However, that is changing because of the introduction of the process bus. Security here involves ensuring the reliability and safety of these control systems.

- **Level 2**

Supervisory Control Zone: This zone involves supervisory control and data acquisition (SCADA) systems. It focuses on managing and controlling Level 1 processes. Security measures here aim to prevent unauthorized access and manipulation of HMIs, engineering and operator workstation data.

- **Level 3**

Grid Operations Zone: Concerned with managing the overall grid process. At this level, you get the SCADA master, Remote access servers, central Physical security management etc. Security includes data integrity, availability and process protection.

- **Level 3.5**

OT or Industrial DMZ zone: A specified network segment or subnet known as a "DMZ" or "screened subnet" serves as a bridge between our trusted internal OT network and an untrusted external network, most commonly the internet or IT network. Its main objective is to give outside traffic a safe place to land. Security mechanisms such as firewalls, VPNs, and IDS/IPS are utilized to control and observe network traffic, protecting the internal network's integrity. For controlling the security of OT systems accessed over the internet or the IT network, the DMZ design is essential.

- **Level 4**

Business Planning and Logistics: At this level, business systems interact indirectly via the DMZ (level 3.5) with the ICS or OT system. It includes corporate networks and enterprise systems. Security measures involve protecting against cyber threats and ensuring data confidentiality.

CONTROLLED DISCLOSURE

- **Level 5**

Internet/ Cloud Level: The DMZ acts as a buffer between the corporate network and external networks, like the internet. Security measures in the DMZ protect against external threats.

To achieve power utility level security, NTCSA must implement appropriate security controls, including firewalls / PEP appliances, intrusion detection systems, access controls, and regular security assessments, across these levels to safeguard our critical infrastructure.

3.3.3 Reference Architecture and Profiles

As stated above, this document refers to domain-specific reference architecture applications as profiles. Besides addressing the shortcomings of the Purdue Model, the profiles presented here include new conceptual elements: security features and participating parties assigned to each of the levels of the model. Security features are controls recommended for the level or zone to which they are attached. Participating parties are humans that are either a part of a level or interact with elements found within that level (for instance, an OT manager at the substation level).

3.3.4 Reference Architecture for NTCSA

The Reference Architecture for NTCSA (referred to below as the Reference Architecture) serves as a baseline for the profiles. Compared to the profiles, it most resembles the Purdue Model. The Reference Architecture introduces elements common to all the profiles, such as the five columns that cut across all levels:

- Security level/name
- Typical device examples
- Function
- Security features
- Participating parties.

As shown in Figure 9, the Reference Architecture includes security levels spread across six zones: Physical Assets, OT network, Operations, Enterprise, and Public. Zones or levels are separated by demilitarized zones (DMZ), network segments typically located between two firewalls.

CONTROLLED DISCLOSURE

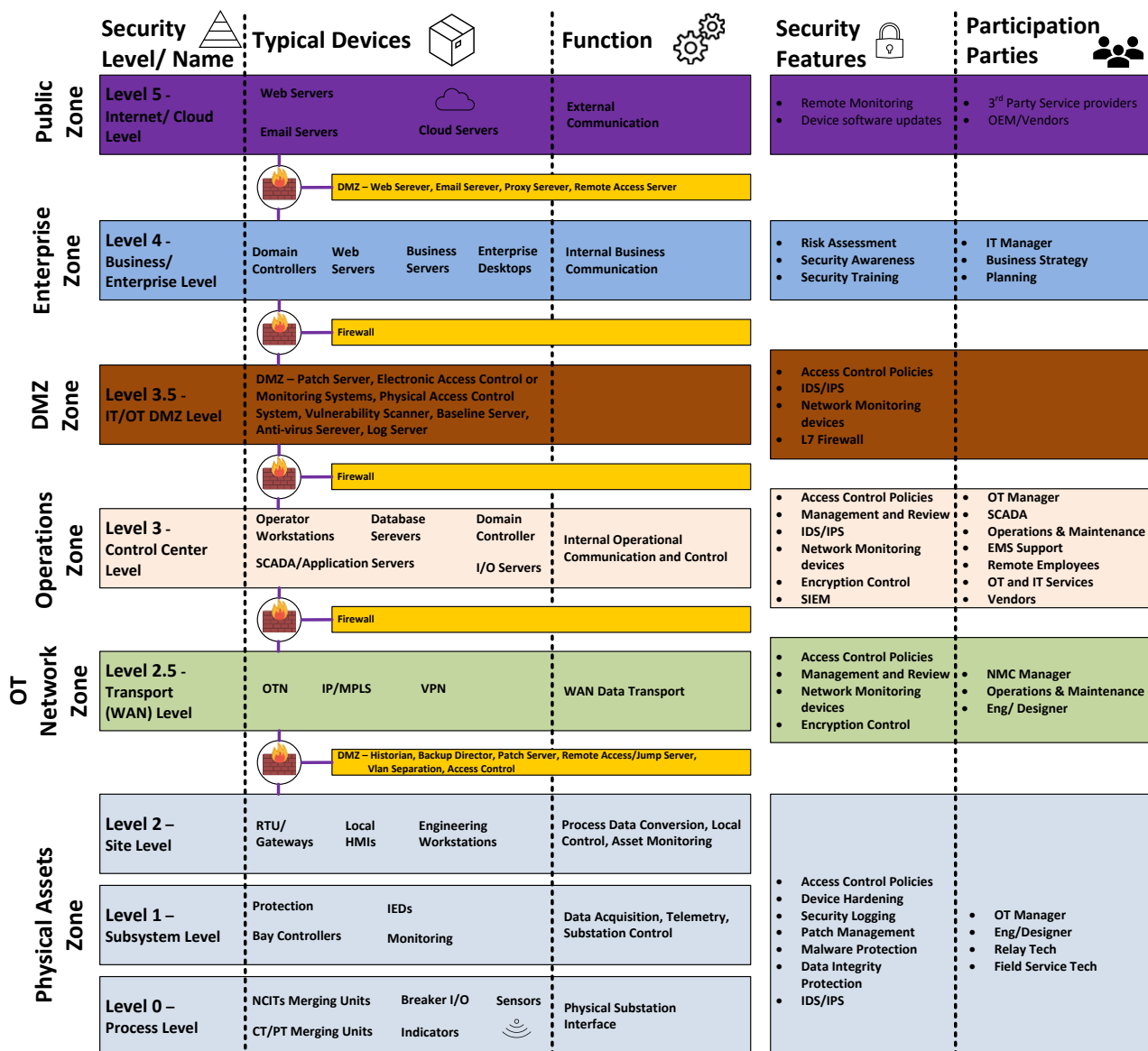


Figure 9: NTCSA Reference Cyber Security Architecture

The Reference Architecture makes no assumptions about the location of processes in Level 0. In an actual grid, you would expect breakers, current transformers, potential transformers, and other Level 0 devices to be spread across a wide geographic area. Likewise, devices all the way up to Level 2 may be distributed among remote substations or local control stations.

The following list examines the contents of the security features in detail:

- **Level 5**
 - **Remote monitoring:** Securing the touchpoints between the Group Technology facility and external resources (e.g., cloud-based applications).
 - **Device software updates:** Updating software and firmware for devices and systems. Updates might be delivered via an Internet connection with the device, requiring some security validation (e.g., checking hashes on the update files).

CONTROLLED DISCLOSURE

- **Level 4**

- **Risk assessment:** Identifying critical assets, vulnerabilities, threats, and potential impact that might result from a cyberattack.
- **Security awareness:** Knowledge that utility staff possesses about physical assets, information assets, and their protection (e.g., establishing topological, behavioural, and configuration baselines).
- **Security training:** Educating utility staff regarding issues of security awareness, as well as specific skills they may need to enforce security.

- **Level 3**

- **Access control policies:** The policies that determine who have access to various devices, information, and systems.
- **Management and review:** The activity of reviewing the cybersecurity logging against policy and adjusting any access or security settings as needed.
- **Intrusion detection system (IDS)/intrusion prevention system (IPS):** Those functions that identify a cyberattack in progress and (in the case of IPS), take some action in response to the attack.
- **Network monitoring devices:** Tools for tracking activity on a network.
- **Encryption control:** The inclusion of a cryptographic system to protect data.
- **Security information and event management:** Tools for managing data about system behaviour and observed events that may prove helpful in identifying cyber incidents.

- **Levels 2-0**

- **Access control policies:** The policies that determine access to various devices, information, and systems.
- **Device hardening:** Setting configurations, turning off unused services, and other actions that reduce the vulnerability or attack surface of a device.
- **Security logging:** Collecting data useful for identifying security events, either in real-time or after the fact.
- **Patch management:** The ongoing process of keeping software and firmware up to date as new versions are released.
- **Malware protection:** Defences against malicious software.
- **Data integrity protection:** Security controls that prevent the unauthorized injection, modification, or deletion of data.
- **IDS/IPS:** Those functions that identify a cyberattack in progress and (in the case of IPS) take some action in response to the attack.

Note that there is not a one-to-one correspondence between security features and participating parties that might contribute to their implementation. For instance, the security feature “risk assessment” might be a joint effort between participating parties’ “IT managers” and “business strategy” personnel. Likewise, an “OT manager” might contribute to “access control policies,” “device hardening,” “patch management,” and other security features. Also, job titles vary. Therefore, the “participating parties” entries should be treated as job descriptions (rather than literal job titles).

CONTROLLED DISCLOSURE

Profiles can be developed for subsystems within the substation profile. For instance, the physical assets zone of the substation profile may contain multiple subsystems.

3.3.4.1 Regional Utility-Scale Profiles

The regional utility-scale profile emphasizes the parallel control structures that may be present in an environment of heterogeneous DER technologies (solar, wind, etc.). Figure 10 illustrates this point, with multiple DER installations controlled from the same Levels 4 and 5. Security features and participating parties are not given for this profile, as they are like those in the DER profile for each level.

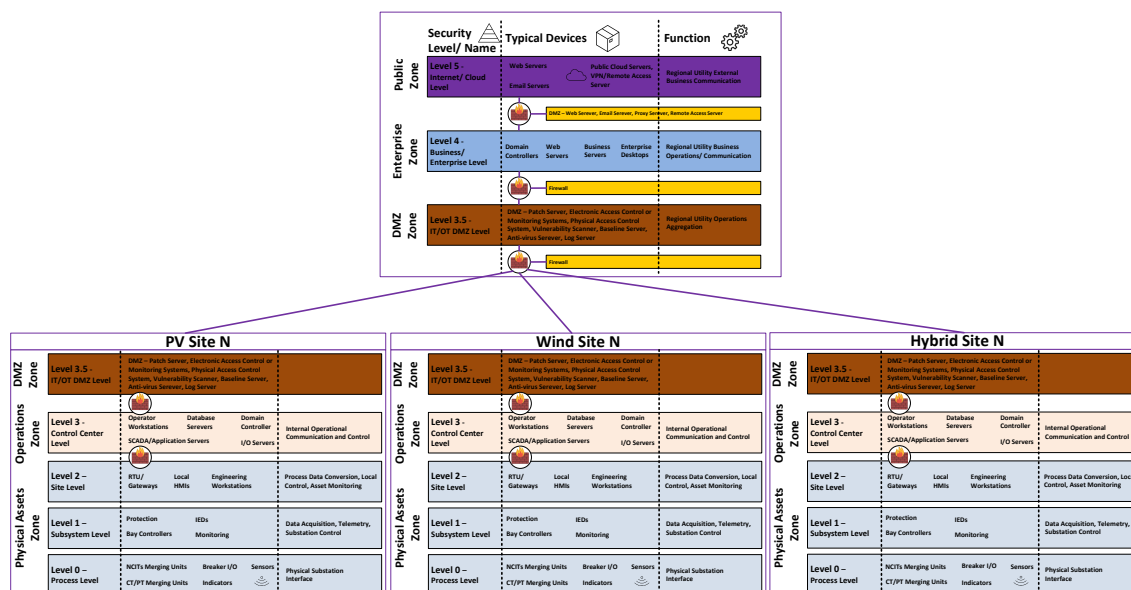


Figure 10: Regional Utility-Scale DER Profile

3.3.4.2 Control Centre Profile

The control centre profile, as shown in Figure 11, focuses on Levels 3-5.

CONTROLLED DISCLOSURE

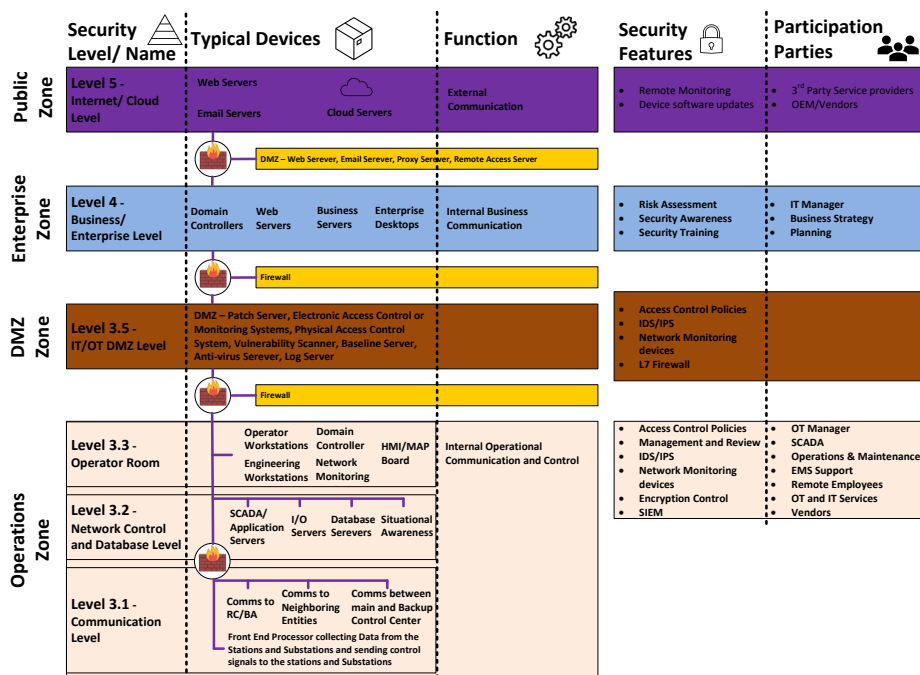


Figure 11: Control Centre Profile

Figure 12 shows how the control centre profile needs to connect to different physical asset zone implementations.

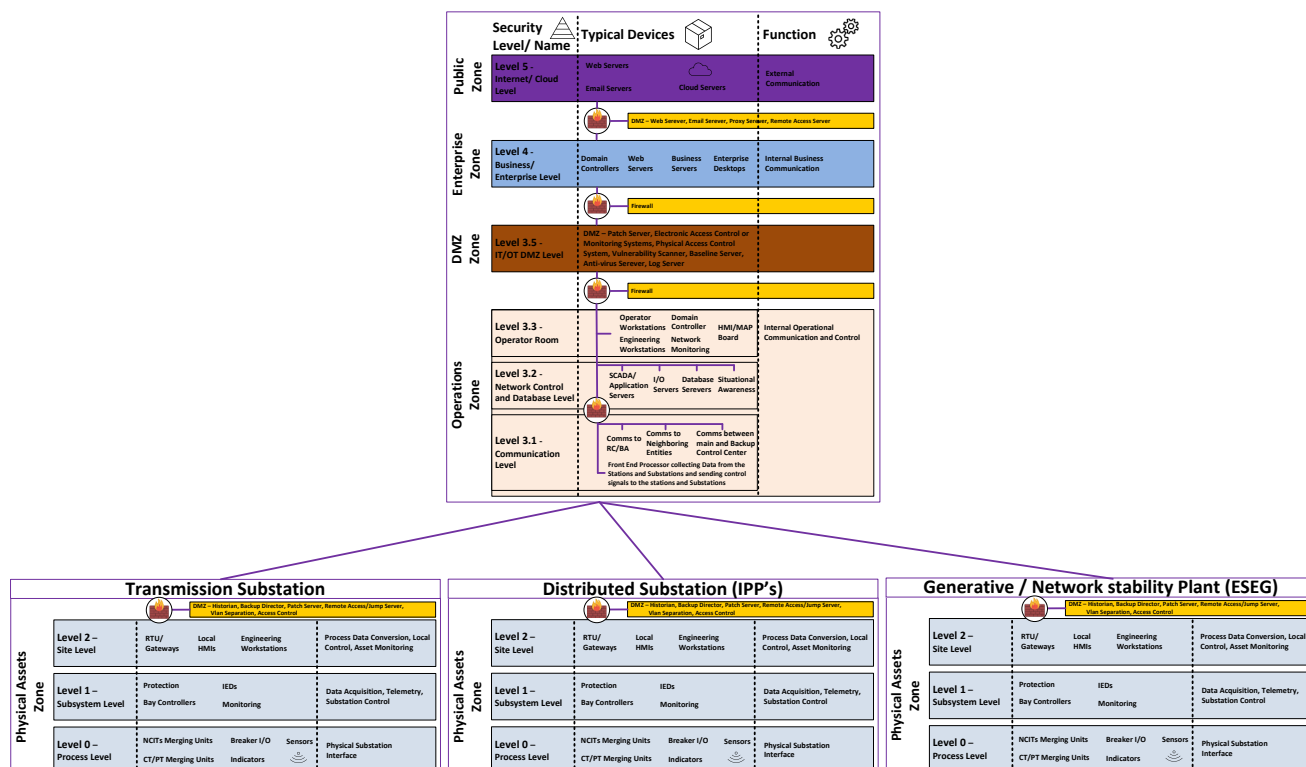


Figure 12: Control Centre Profile with Multiple Physical Zone Assets

CONTROLLED DISCLOSURE

3.3.5 Zero Trust Security Architecture for NTCSA.

This section will overlay the zero trust principles onto the Security Architecture. It will highlight where the policy enforcement point (PEP) needs to be located and the Policy Administrator and the Policy engine. There are also references to the IAM and external access control.

Below will be examples of the following scenarios:

- Zero Trust Architecture in single OT site (Figure 13)
- Zero Trust Architecture in OT with multiple sites (Annexure A.2)
- Zero Trust Architecture in OT Scenario 1: Data Flow (Annexure A.3)
- Zero Trust Architecture in OT Scenario 2: Remote Access and IAM (Annexure A.4)

CONTROLLED DISCLOSURE

3.3.6 Zero Trust Architecture in single OT site.

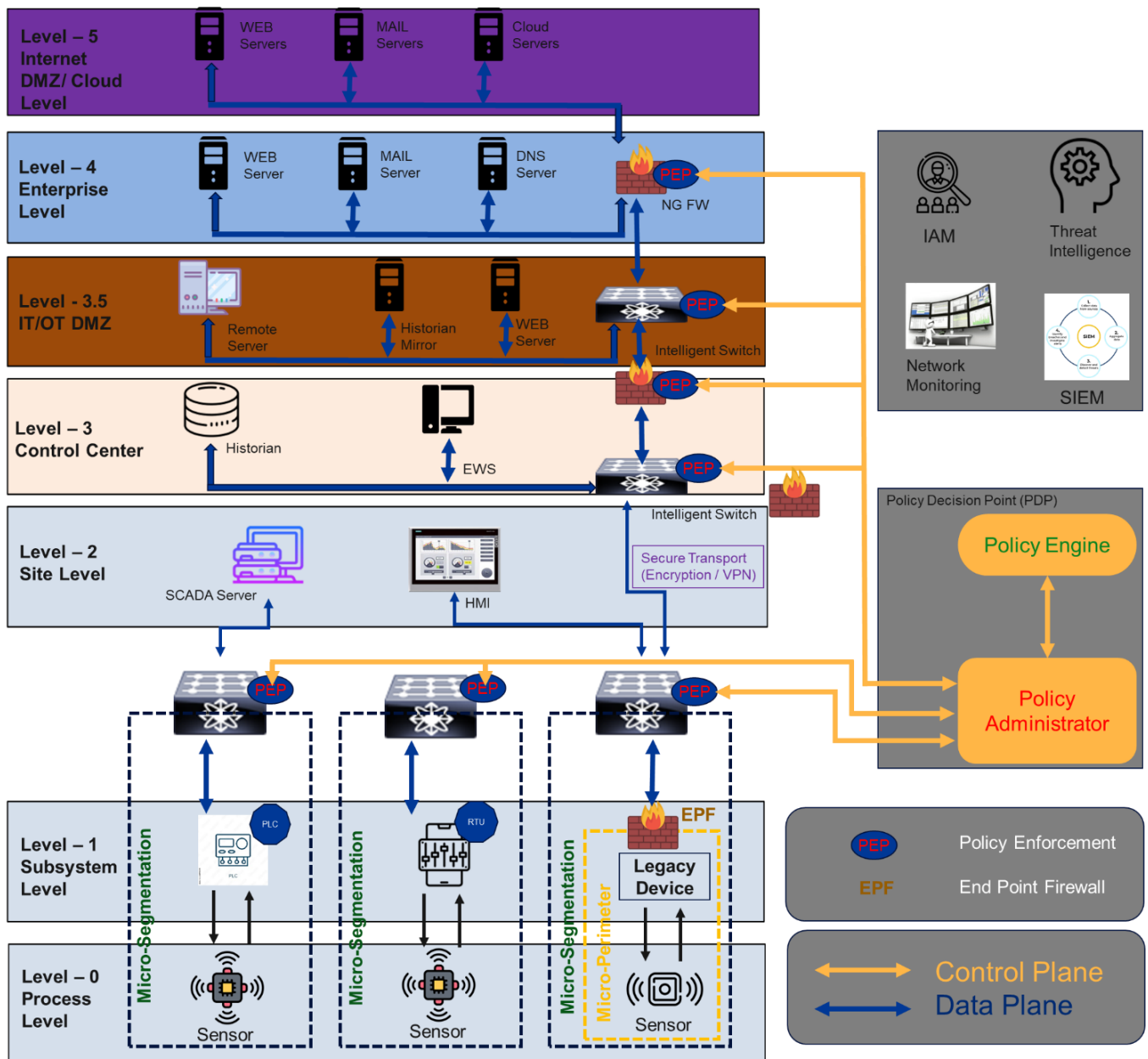


Figure 13: Zero Trust Architecture in Single OT site

CONTROLLED DISCLOSURE

3.4 Secure Areas, Security Zones and Electronic Security Perimeters

A secure area is a term used to secure a service both on-site and in transport. Secure areas are setup in a manner that prevents the propagation of a threat from one secure area to the next.

Segregation can be in the following:

- 1) **Physical insulation** – Systems can be isolated from each other physically. This can be done by having separate networks. A time delay in the transfer of data can also be seen as physical insulation. If data was transferred from one network to another through a medium such as a hard disk, this can be seen as physical insulation.
- 2) **Protocol insulation** – Insulation can be accomplished with the use of a different communication language between networks and systems. A converter is required to enable different networks or systems to exchange data.
- 3) **Data insulation** – Data can be isolated on a logical level. Data can be controlled, and only authorised connections will allow data to pass such as firewall segregation. Physical equipment can be virtualised to create isolation such as virtual local area networks (VLANs).

In IT, a common practice to segregate data or cyber assets based on their security requirement is with one or more demilitarized security zones (DMZ). A security zone is a grouping of logical or physical assets that share common security requirements. This is commonly done with firewalls to create different security zones. A similar concept is applied in NTCSA OT but is called an electronic security perimeter (ESP).

An ESP is defined as the logical perimeter of the system. For a generic OT site, the ESP usually correlates with the physical security perimeter (PSP) of the site. Because of this definition, there will be further ESPs or security zones inside the main ESP especially with the adoption of zero trust architecture as referenced above.

It is important to note that if deviations from the reference architecture are required, these deviations must be presented to the relevant DRT for review and acceptance.

CONTROLLED DISCLOSURE

3.4.1 ICT Network Security Framework Secure Areas in Reference to the Security Architecture for NTCSA.

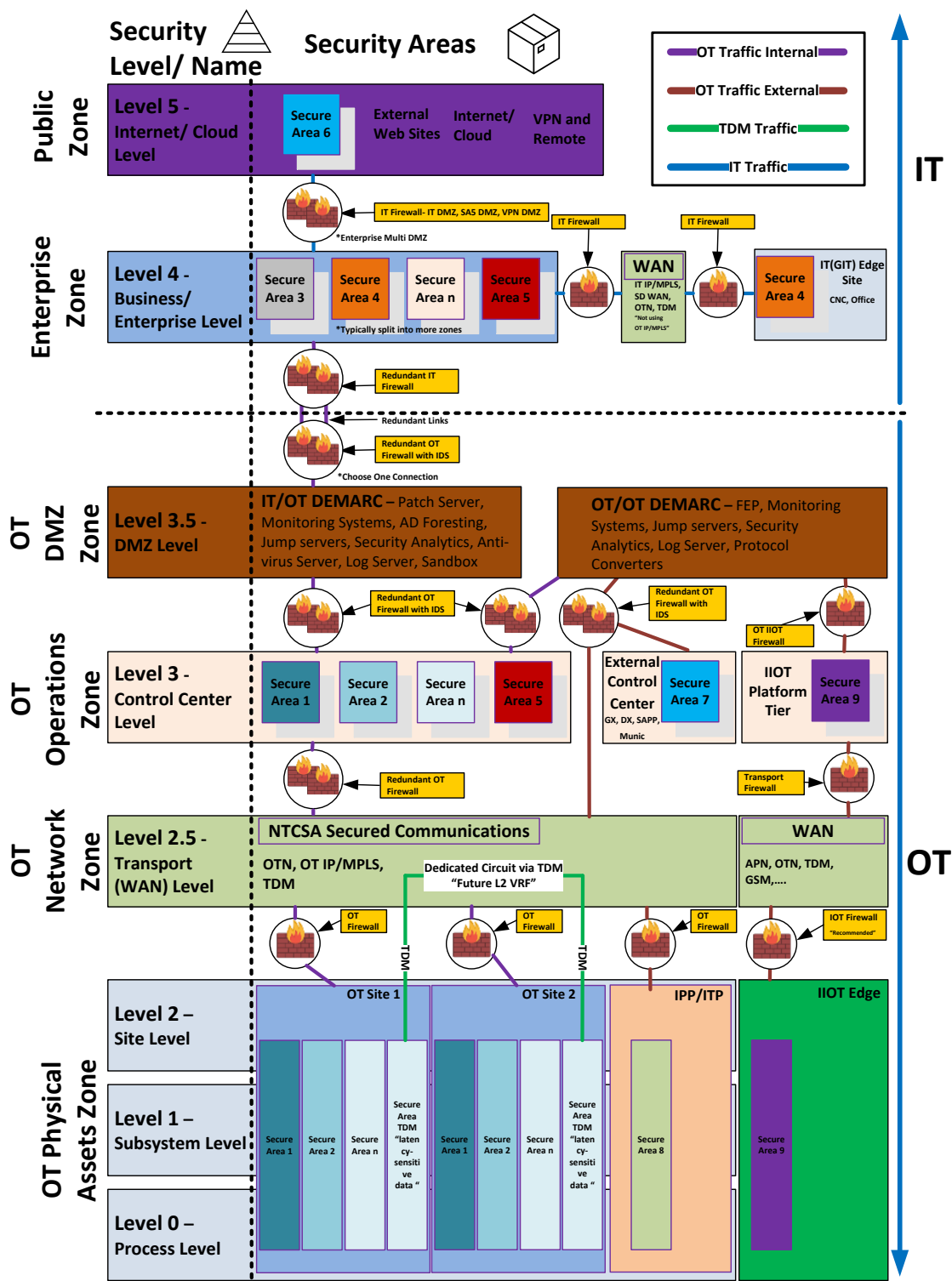


Figure 14: ICT Network Security Strategy Framework

CONTROLLED DISCLOSURE

Figure 14 above shows how the secure areas will be applied to secure the services of NTCSA. Merging the OT environment with the IT environment allows for interconnectivity and to sharing of resources across the business. This, however, also opens the systems to vulnerabilities that could propagate from one area to another hence the requirement for secure areas. The architecture is to apply a defence-in-depth approach and add the principles reverenced in this document to exchange data safely and securely. Figure 13 above shows PEP appliances, which represent the use of a security insulation technique such as, but not limited to, firewalls. Next-generation firewall enhancements like IDS/IPS, Application Control, AntiBot, Network Antivirus, ACL, URL Filtering etc. can increase network security insulation.

The PEP appliances should prevent the propagation of threats from one secure area to another. The other advantage of having secure areas is different governance can occur in each area. This allows multiple entities in the organisation to govern how data is respected in their domain.

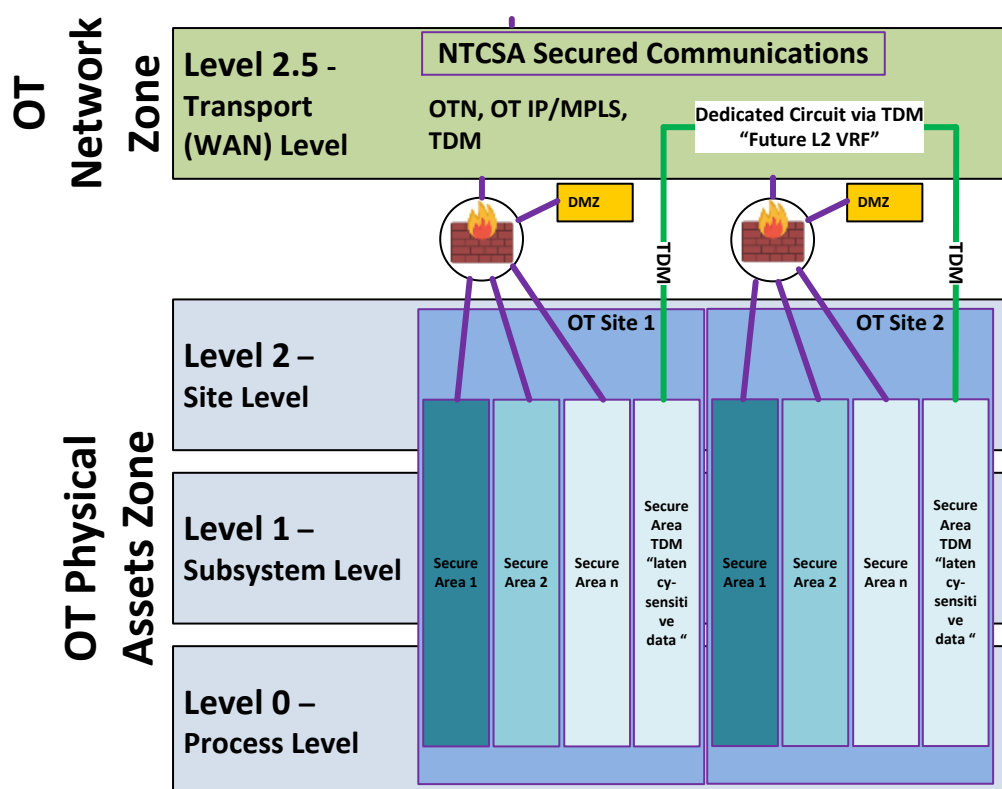


Figure 15: Security Zone / Electronic Security Perimeter and Secure Areas

Figure 15 shows how an ESP or security zone with DMZ integrates with a secure area. It is important to note that secure areas are not localised. Security zones can be seen as logical perimeters usually implemented with firewalls and other data segregation technologies like VRF's. Security zones can also be referenced to the different layers from the Purdue model and are a concept derived from the micro-segmentation and perimeter defense referenced in section 3.2.3.

Data between two sites or between two layers from the reference architecture will hit a PEP appliance and then go to the allocated secure area. A secure area, however, aims to secure the data flow as to reference to the zero trust principles. This means the source location its travel paths and destination all make up the secure area for the data. The secure area, therefore, allows segregated ESPs or security zones (DMZ's) to share information securely over an untrusted network. Encryption technologies (e.g. SSL/TLS/SFTP/VPN) can be used to further enhance the security of communications over WAN links and untrusted networks.

CONTROLLED DISCLOSURE

3.4.2 Operational Technology Areas (Area 1 and Area 2)

The OT environment can be broken down into two main groupings, this being a control data centre or a site. Sites will report to a national, and if required, a local data centre. OT secure areas allow data to flow securely between sites and control data centres.

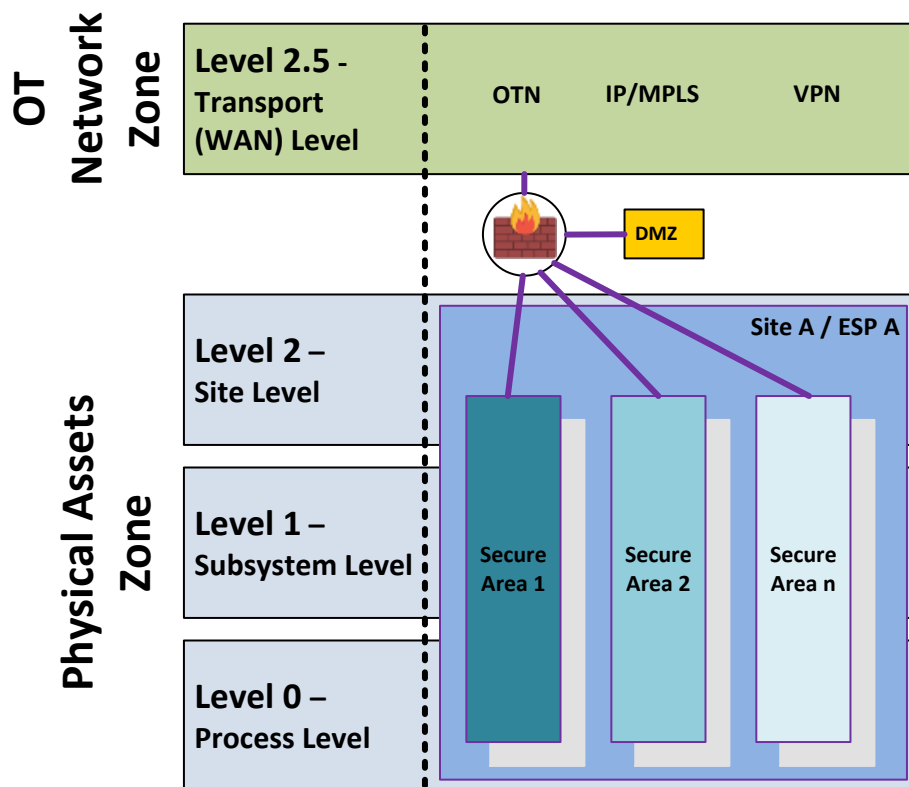


Figure 16: Logical Connection of Secure Area 1, Secure Area 2, OT/IT DMZ and WAN

Figure 16 above shows that data from the OT demilitarized zone (DMZ) will either go to Secure Area 1, Secure Area 2 or Secure Area N. It is to be noted that the adoption of the zero trust principles it will require that more Security areas be created. As a minimum 2 zones are required and only 2 areas are referenced. The number of firewalls will need to align with the OT DMZ Standard.

Secure Area 1

Secure Area 1 will be segregated over OSI Layer 3 between sites providing a similar setup to Time Division Multiplexing (TDM). For services that are not ready for IP, TDM will be used to facilitate these communications until the transition to a TCP/IP service. For latency-sensitive data that cannot pass through the firewall, a dedicated point-to-point Layer 2 (L2) service on the transport network will be required. GOOSE messages will also require a dedicated Layer 2 path to ensure reliable and low-latency communication. At this stage, only time-sensitive protection services will be allowed to connect to external sites without going through a firewall. It is required to apply an access list or a hub and spoke configured MP-BGP technology between sites for further enhancements and security by only allowing known addresses and services to be available at that site. Secure Area 1 is segregated from Secure Area 2 with an OT DMZ (Firewall or PEP enabled appliance). Service attempting to get to Secure Area 1 (e.g. remote access) will not go through Secure Area 2 first. Instead, it will go directly to Secure Area 1 and needs to make use of a jump server in the OT DMZ to access Secure Area 1.

Secure Area 2

CONTROLLED DISCLOSURE

Secure Area 2 will be segregated over layer 3 between sites. It is advised to apply an access list or a hub and spoke configured MP-BGP technology between sites for further enhancements and security by only allowing known addresses and services. Most services that require connection outside the ESP of the site will reside here. Introducing Secure Area 2 and Secure Area N will mitigate the risk of exposure to Critical Cyber Assets in the event of a cyber breach occurring within these secure areas.

3.4.3 Centralised IT / OT Demilitarised Zone

An OT DMZ shall be used for any communication convergence points between IT and OT. Having a centralised point ensures assurance that security is maintained in the flow of traffic between IT and OT. This allows greater use of financial and human resources to secure the OT DMZ. This DMZ zone (Level 3.5) is under the control of OT. A high-level example is shown in Figure 17.

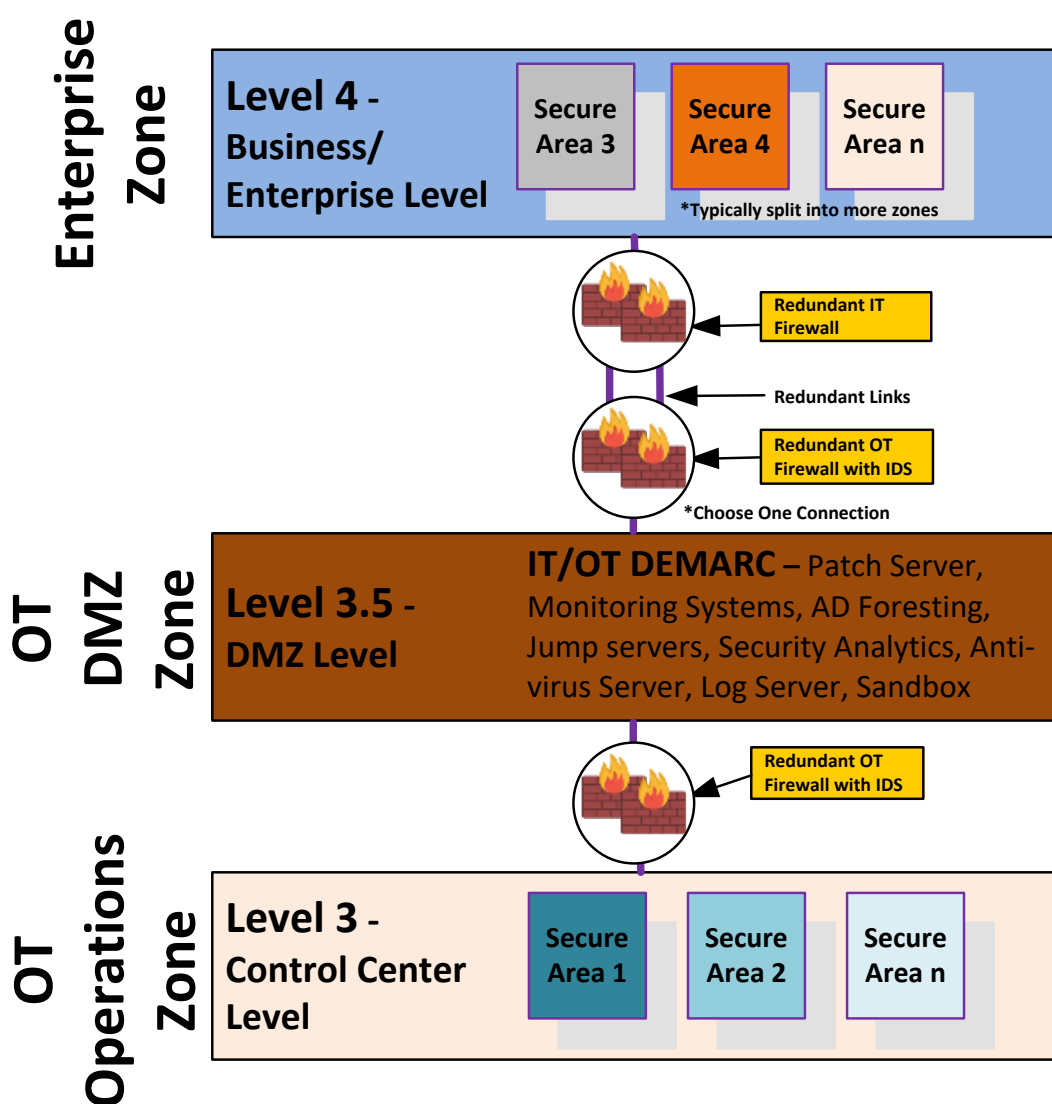


Figure 17: IT / OT exchanging data over a Central DMZ

CONTROLLED DISCLOSURE

3.4.4 Function and Purpose of Operational Technology Secure Areas

The OT area will be separated into two or more secure areas. One secure area will be designated for critical services and another secure area for Core to critical services and a third for physical security and so on. This will allow OT system owners to focus their efforts on securing critical cyber assets that are essential to their operations. It is advised to separate the cyber assets into more zones for further granularity with regards to data and resources access control and logging to comply to the micro-segmentation and ZTA principles.

Secure Area 1 – Critical Operational Technology Services

Secure Area 1 is dedicated to services that directly impact the control, monitoring and operations of the power system. A dedicated secure area for control is essential to the reliable operation of the power network. Systems that meet the definition of an essential service will reside in secure area 1. The creation of secure area 1 will allow OT system owners to focus their efforts on protecting essential systems.

Secure Area 2 – Non-Critical Operational Technology Services

Secure Area 2 is dedicated to services that support the critical operational environment (Secure Area 1). Services that are hosted by OT but do not meet the essential services definition will reside in secure area 2 or above.

3.4.5 Information Technology Secure Areas (Area 3 and Area 4)

The IT Network security environment should also cater for a minimum of two areas, one to host OT Services and another for IT Services.

Secure Area 3 – Production Services

Secure Area 3 is dedicated to OT services hosted by IT. The reliance of OT on IT makes a requirement that OT hosted applications on IT systems be segregated from the rest of the IT enterprise network. Systems that need to be hosted in Secure Area 3 include Core/Critical and Line of Business systems. These systems, which are hosted by IT and impact OT, will adhere to an agreed-upon governance framework established between IT and OT. Secure Area 3 may also be used to host IT Services pertaining to the site requirements, these services should not be mixed with OT services.

Secure Area 4 – Line of Business

Secure Area 4 is dedicated to Line of business services maintained by IT that have no impact to OT operations. Enterprise services follow IT governance. OT governance has no influence on these systems. Secure Area 4 may comprise different service offerings, for e.g. Internet Access, VPN, etc.

CONTROLLED DISCLOSURE

3.4.6 Function of Information Technology Secure Areas

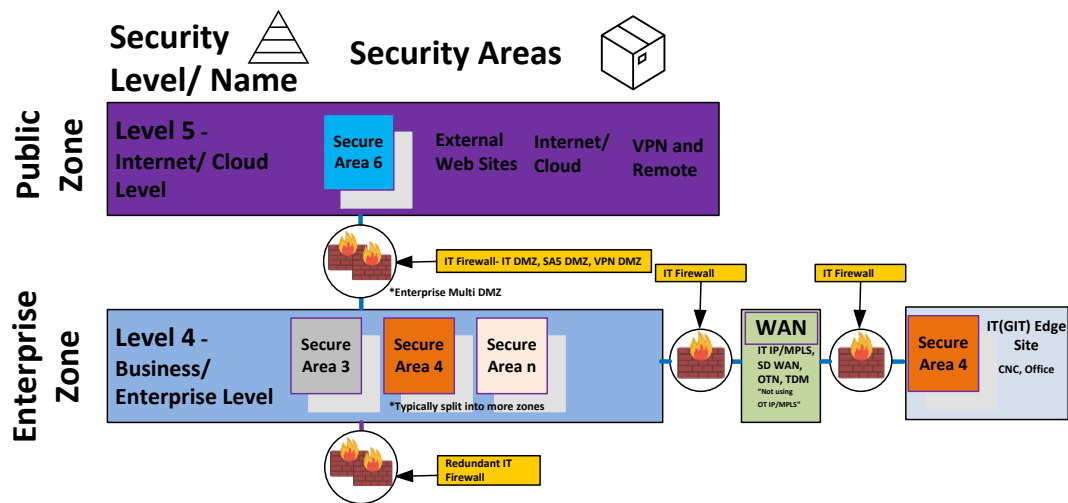


Figure 18: Logical Connection of the IT Secure Areas

Figure 18 shows that when data enters the business from the internet or level 5, the data will go to the relevant secure area requesting that data. In cases such as a remote connection, once authenticated, will only be configured to go to the relative IT / OT DMZ.

Secure Area 3

Secure Area 3 will be segregated over layer 3 between sites. Important to note that all services must pass through Secure Area 4 to get to Secure Area 3. This access is statically configured on all firewalls that the connection traverses.

Secure Area 4

Secure Area 4 will be segregated over layer 3 between sites. Group Technology services will remain in the area unless it serves an operational purpose and then will move to a higher (lower number) secure area.

3.4.7 IT Segregation and Site VPN

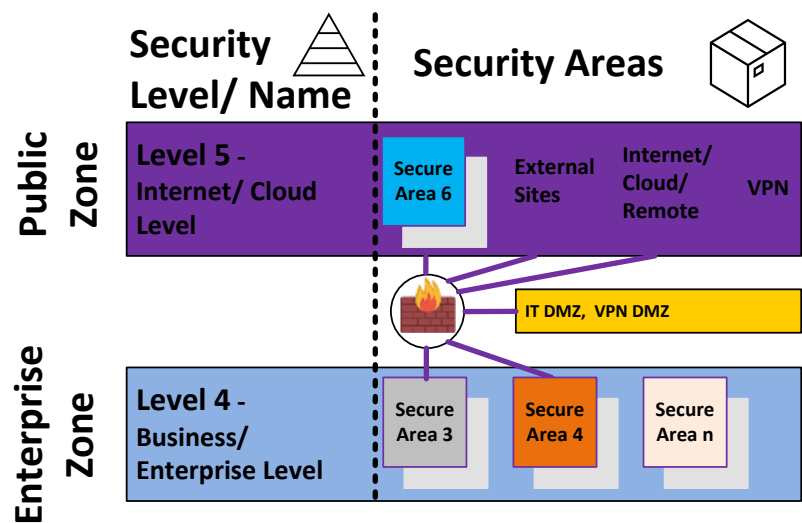


Figure 19: Information Technology Site-to-site Virtual Private Network

Group Technology also segregates Secure Area 3 services from Secure Area 4 services. Group Technology may also setup site-to-site VPNs where required. This is shown in Figure 19. If these sites require internet access, they will break out at the Group Technology data centre, which is the central logical entrance of the Eskom business and NTCSA.

3.4.8 Information Technology Centralised Demilitarised Zone

The IT centralised DMZ will be the breaking in and out point for all communications to the internet. For OT services requiring internet and remote access, it is important that all communications go through this central point. This will allow other areas of the business to benefit from Group Technology security control measures for remote access.

Secure Area 5 – Security Operations Centre (SOC)

Secure Area 5 is dedicated to services controlled by a Threat Centric Security Operations Centre (TC - SOC) Unit.

Function of Secure Area 5 – TC - SOC

Secure Area 5 will reside in both IT (Level 4) and OT (Level 3) environments. Security incidents will be fed from Secure Area 1-6 to Secure Area 5 directly via data diodes or level 7 firewalls. This information can have a confidentiality rating or higher. Declassified information from Secure Area 5 can be shared back to the secure areas via their respective DMZ connections.

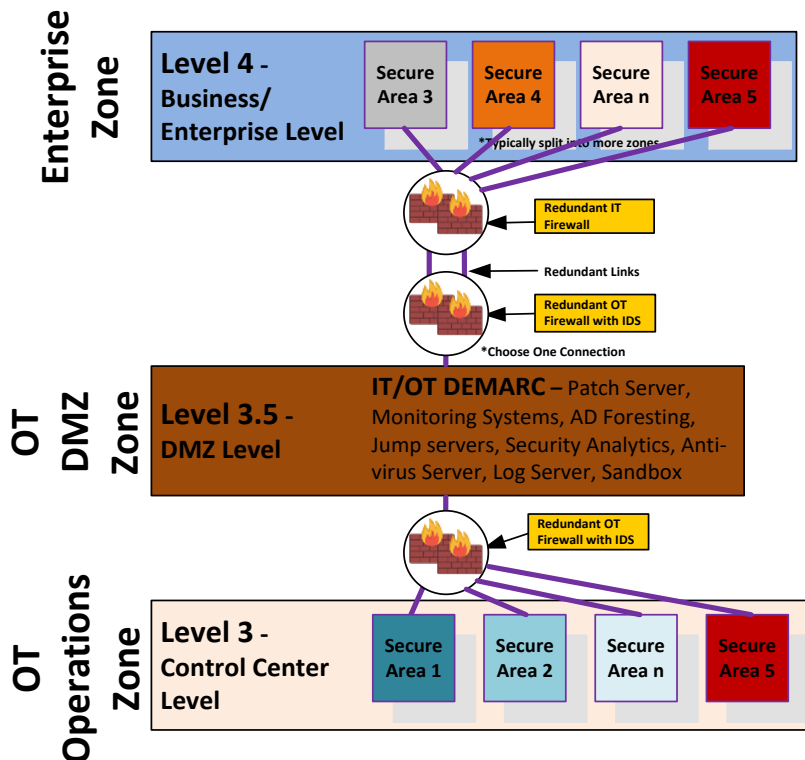


Figure 20: Secure Area 5

Secure Area 5 is reserved for the TC – SOC / OT SOC units and shown in Figure 20. The units will look at cyber and physical threats across the business by taking data sent by the different areas of the business and processing this to identify the threats and enhance NTCSA security posture by actively searching for and responding to malicious threats in the network.

Unlike traditional SOC, which may also focus on compliance and general security operations, a Threat-Centric SOC is specifically geared towards identifying and countering security threats. It actively seeks out new and emerging threats, helping NTCSA prioritize incidents and detect higher-risk threats more effectively.

In the realm of cybersecurity, a Threat-Centric SOC plays a critical role in safeguarding data and infrastructure by staying ahead of evolving threats and vulnerabilities. It is the main source of evidence for policy enforcement point decision-making

The data sent from Secure Area 1 - 6 is of a highly sensitive nature. Declassified information is returned to the relevant secure area and system owners can review the results.

Secure Area 5 also has communications to external sites referred to as trusted collaboration partners. These external sites are used in the collaboration of combating cyber threats which include but are not limited to:

- 1) Agreed upon commitments with Cyber Response Committees.
- 2) Government organisations such as the South African Police Service.

This unit will deploy its own technology in the different domains to collect information securely and will have its own data centre.

A Threat-Centric SOC is a specialized security unit that make it an asset in modern cybersecurity operations and verifying all the principals described in this document are applied.

CONTROLLED DISCLOSURE

Figure 21 and Figure 22 shows the role of the TC-SOC unit as an integrated security operations centre.

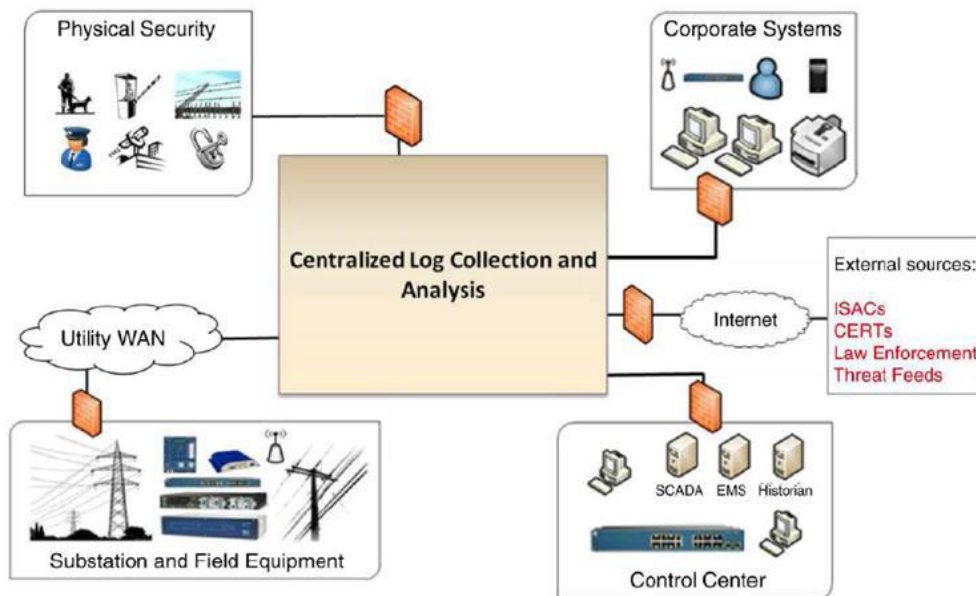


Figure 21: Guidelines for Planning an TC Security Operations Center, by G. Rasche, December 2013, EPRI

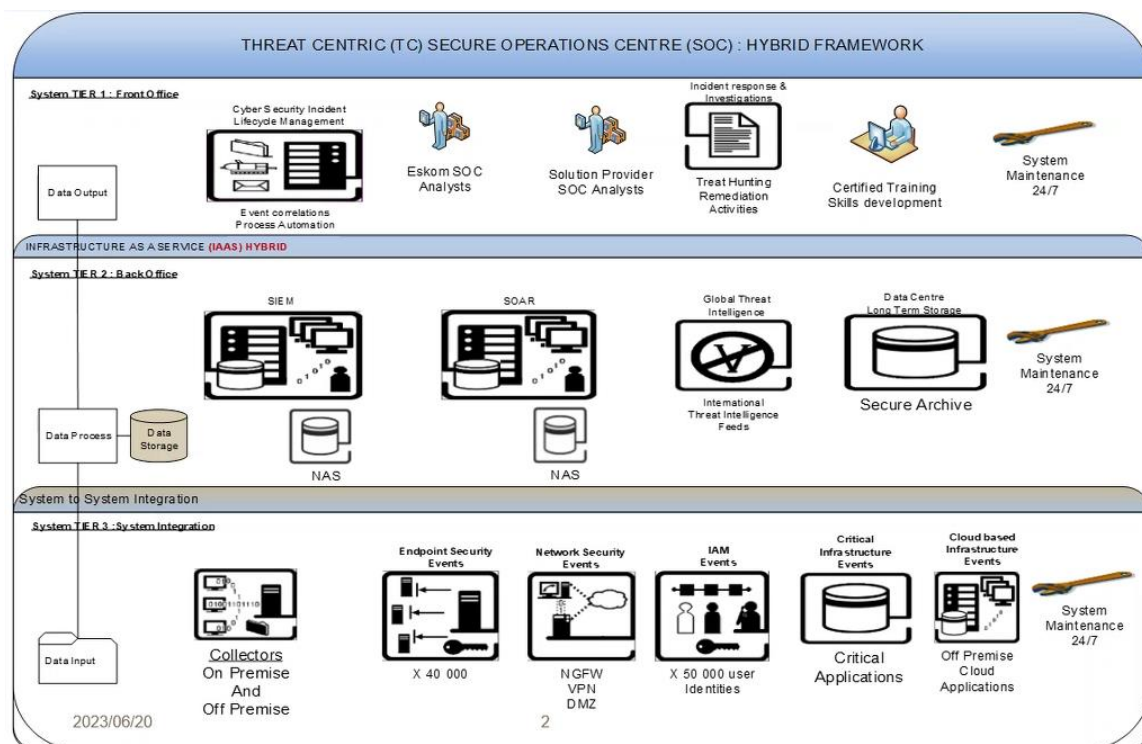


Figure 22: Threat Centric Secure Operations Centre: Hybrid Framework

3.4.9 External Service (Secure Area 6)

Secure Area 6 is reserved for external IT services on the NTCSA network.

CONTROLLED DISCLOSURE

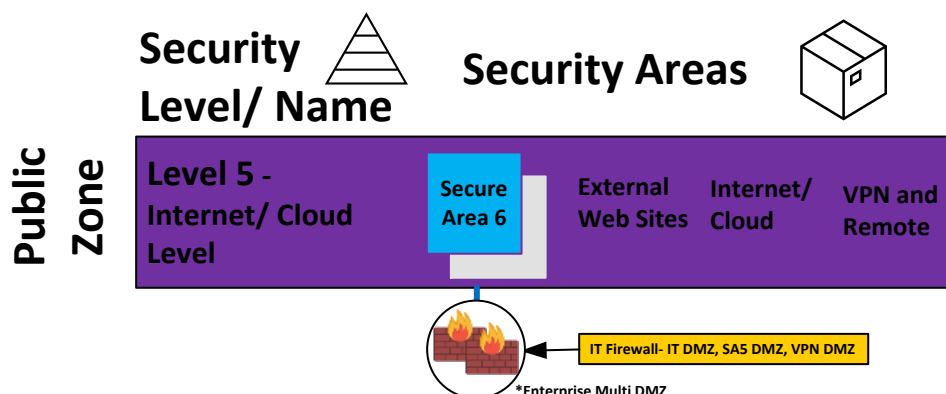


Figure 23: Secure Area 6

Function of External Service – Area 6

If NTCSA would like to lease excess bandwidth, a secure area is established to accommodate the service. This secure area will only exist on the shared transport infrastructure and will not interact with the rest of the secure areas and thus, NTCSA data.

3.4.10 External Control Canters (Secure Area 7)

Secure Area 7 is specifically designed to manage connections to external control centres, such as the GX and DX networks, the Southern African Power Pool, and various municipalities. This area serves as the primary gateway for NTCSA to interface with these external control entities. The data flow within Secure Area 7 will connect to a dedicated demarcation point (DEMARC) specifically for Operational Technology (OT) to OT communication, ensuring that critical data exchanged between NTCSA, and external control centres is secured. Secure Area 7 employs a combination of firewall protection and demarcation techniques to safeguard the integrity of these communications, maintaining a secure boundary between NTCSA's internal systems and external partners.

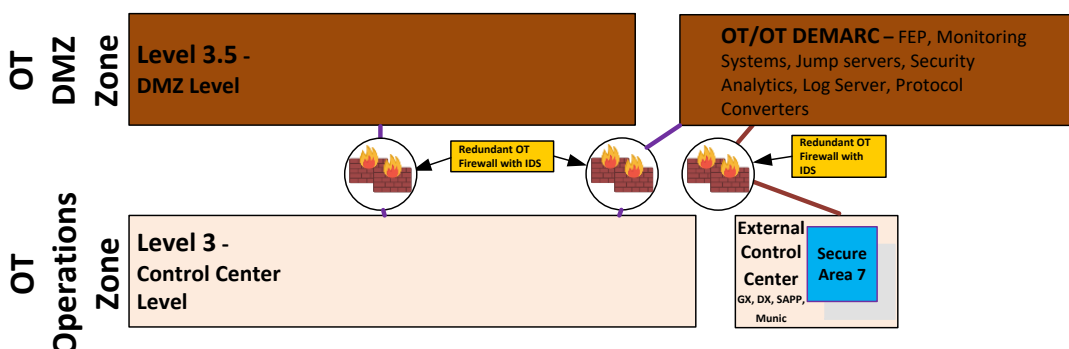


Figure 24: External Control Canters (Secure Area 7)

CONTROLLED DISCLOSURE

3.4.11 Independent Power Producers (IPP) and Independent Transmission providers (ITP) (Secure Area 8)

Secure Area 8 is dedicated to handling communications with Independent Power Producers (IPPs) and Independent Transmission providers (ITPs). A firewall must be implemented at each IPP or ITP site, which then connects to the OT to OT DMZ and controlled/ operated by NTCSA. Secure data transmission from IPPs to OT DMZ firewall can occur via NTCSA's secure communication channels or through third-party providers. When utilizing NTCSA's secure communication infrastructure, it is crucial that IPP data remains isolated from the rest of the OT data to avoid any risk of data compromise. If third-party service providers are used, encryption technologies must be employed to ensure data security during transmission. Secure Area 8 enforces strict control measures to protect the data integrity of power generation entities and to prevent unauthorized access to NTCSA's internal systems.

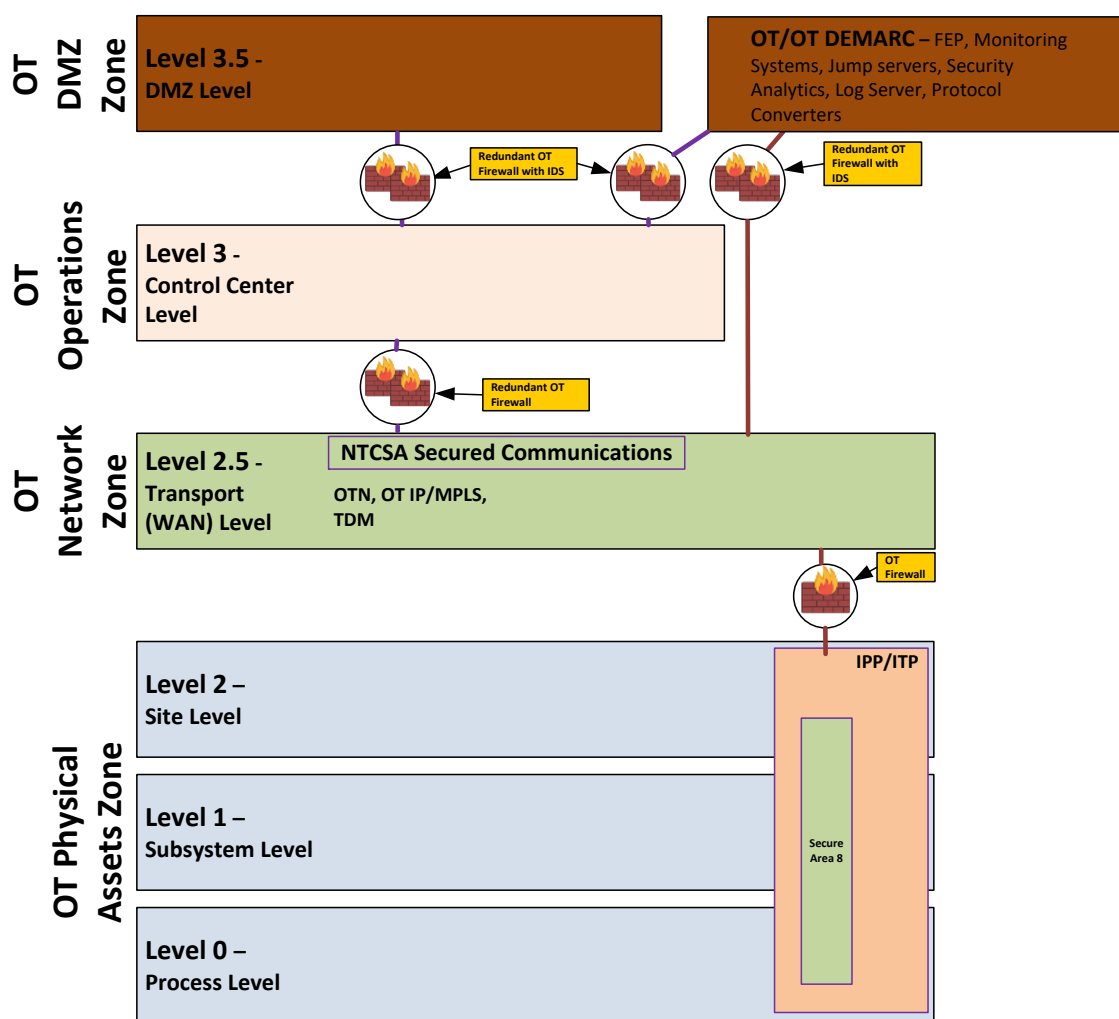


Figure 25: IPPs and ITPs (Secure Area 8)

CONTROLLED DISCLOSURE

3.4.12 Industrial Internet of Things (IIoT) (Secure Area 9)

Secure Area 9 is to support the integration of Industrial Internet of Things (IIoT) field devices into NTCSA's network. The data from these IIoT devices will be routed through the OT-to-OT firewall using a dedicated Policy enforce Point (PEP) appliance, which acts as a security buffer between the field devices and the core OT systems. While a firewall at the site level is recommended to enhance security, it is not mandatory. The security controls in this area include encryption technologies and the use of PEP appliances where applicable, to create a layered defence mechanism that restricts unauthorized data flows. Secure Area 9 is crucial for establishing secure communication channels to IIoT devices, enabling real-time data exchange while maintaining a high level of security. The use of isolated or dedicated services for IIoT device connections is encouraged to prevent unauthorized access and ensure the secure flow of data across the network. Secure Area 9 represents the first line of defence in NTCSA's cybersecurity strategy for IIoT, ensuring that all devices are continuously monitored and protected in line with zero trust principles.

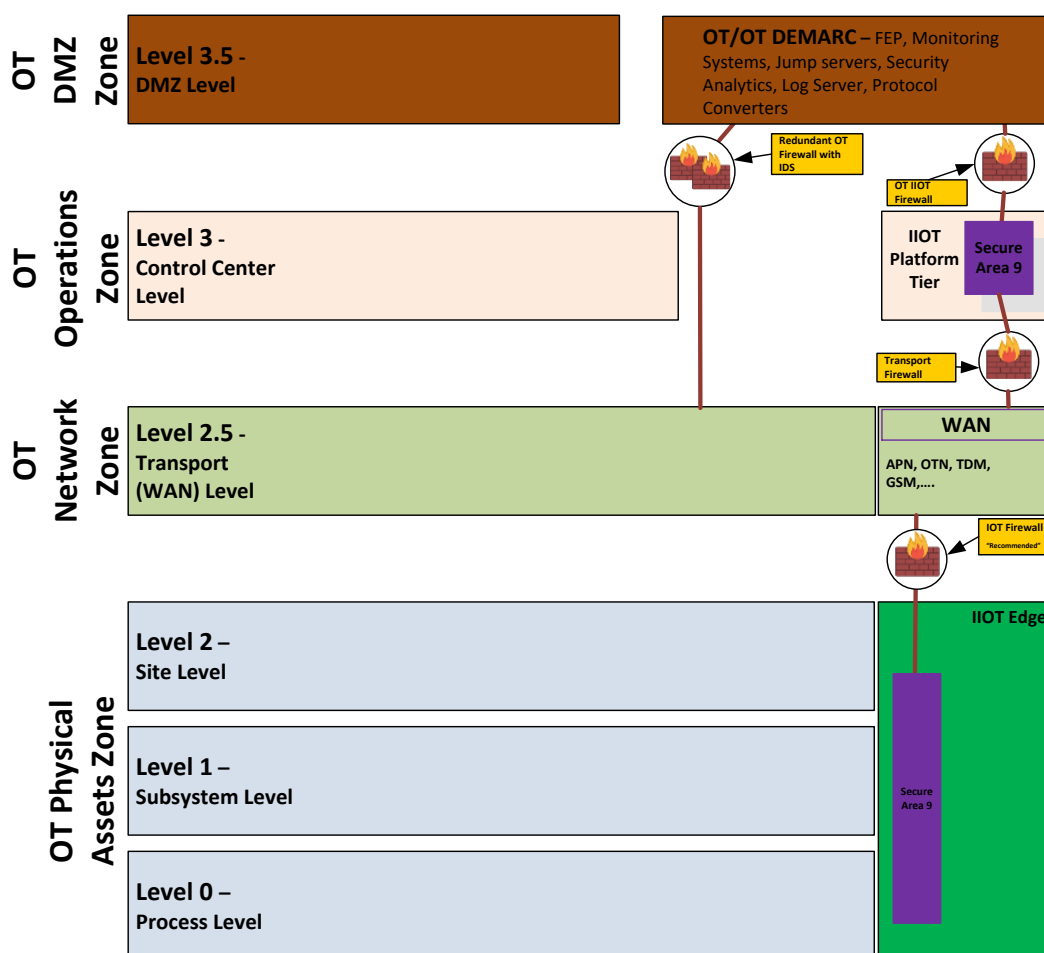


Figure 26: Industrial Internet of Things (Secure Area 9)

These secure areas (1 to 10) enhance NTCSA's cybersecurity architecture by implementing robust measures to protect communication channels, both within the internal network and with external partners. By following a defence-in-depth approach, NTCSA ensures the secure exchange of data while minimizing risks and vulnerabilities across its interconnected systems.

CONTROLLED DISCLOSURE

4. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Alvin Francis	Senior Advisor - IM Strategy and Architecture
Andre De La Geurre	Middle Manager – PTM&C Protection Technology
Beresford Jelliman	Chief Advisor - Information Management Security
Bongani Shezi	Chief Engineer – PTM&C Telecommunications Technology
Cornelius Naidoo	Middle Manager – PTM&C Telecommunications Technology
Ernest Mpshe	Middle Manager – National Control Systems Support
Ian Naicker	Chief Engineer – Control and Automation
Johan Botha	Snr Consultant Energy Mng – System Operator
Johan Pieterse Chief Engineer	TX Secondary Plant, Works Planning and Centralised Services
Kgomotso Manyapetsa	Chief Engineer – PTM&C Cyber Security Technology
Kholofelo Halefose	Snr Advisor IM Security
Lenah Mothata	Senior Manager - Grids
Meenal Vala	Chief Advisor IM – Cyber Security
Moagaesi Motlhodi	Middle Manager – IM Operations
Mondli Dlamini	Chief Engineer – Group IT Security
Mpumelelo Mathe	Middle Manager – PTM&C Cyber Security Technology
Oscar Ngwenya	Chief Engineer – Grid Modernisation
Rakesh Ragoonanthun	Middle Manager Information Management Architecture
Sithembile Songo	Senior Manager - Information Security
Tsepo Thamae	Senior Advisor Cyber Security
Unathi Dyantyi	Middle Manager – Operations NMC
Zwelandile Mbebe	Corporate Specialist – Telecommunication

5. Revisions

Date	Rev.	Compiler	Remarks
Feb 2025	1	Pieter Mocke	Document superseding 240-146054527

6. Development team

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

Bongani Shezi

Johan Botha

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

Kgomotso Manyapetsa

Meenal Vala

Zwelandile Mbebe

7. Acknowledgements

This document is supported by the following committees:

- Cybersecurity Committee (Group Technology / Corporate)
- Cybersecurity Study Committee (Cross divisional representation)
- Enterprise Architecture Advisory Board (EAAB) (Cross divisional representation)
- NTCSA Architecture and Data Committee
- NTCSA Cybersecurity & Risk Committee
- PTM&C Design Review Team Committee
- Voice and Data Care Group

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

Annex A – Zero Trust Architecture in OT

A.1 – Zero Trust Example

This section illustrates how NTCSA Zero Trust architecture governs access requests.

Scenario: A user (subject) with a valid network authentication token attempts to access a NTCSA resource.

Zero Trust principles dictate that all subjects are initially considered untrusted. Consequently, the Policy Enforcement Point (PEP) intercepts the access request and forwards it to the Policy Decision Point (PDP) for evaluation.

The PDP analyses various factors to determine the appropriate level of access (if any) for the subject:

- **Subject identity:** This includes user identity, the application used, and the device attempting access.
- **Security posture:** The health of the subject's device is assessed using data from the Continuous Diagnostics and Mitigation (CDM) system.
- **Subject behaviour:** The PDP considers historical user and device behavior patterns to identify anomalies.
- **Authorization:** The subject's role within NTCSA is evaluated to determine permitted resource access levels.

Access Granting:

- If the PDP's risk assessment deems access acceptable, it conveys its recommendation and access level to the Policy Administrator (PA).
- Based on the PDP's analysis, the PA configures the session with appropriate privileges. On the NTCSA network using a NTCSA-owned device, a user might be granted full access based on their role. However, on a public network, stricter limitations might be applied.

Micro-Segmentation and Continuous Assessment:

NTCSA need to utilize micro-segmentation to establish security zones around individual resources (Figure 9). These zones can be implemented using next-generation firewalls, layer 3 switches, or multihomed PEP appliances. The PDP grants access to specific security zones.

7.1.1.1 Example: Accessing Engineering Server (Figure 27)

1. Alex, a NTCSA employee on the internal network, tries to access the Engineering server.
2. The request is intercepted by the PEP and forwarded to the PDP for evaluation.
3. The PDP analyses relevant data and grants permission based on Alex's role, device health, and behaviour.
4. The PA configures the session, and the PEP grants Alex access to the Engineering server.

CONTROLLED DISCLOSURE

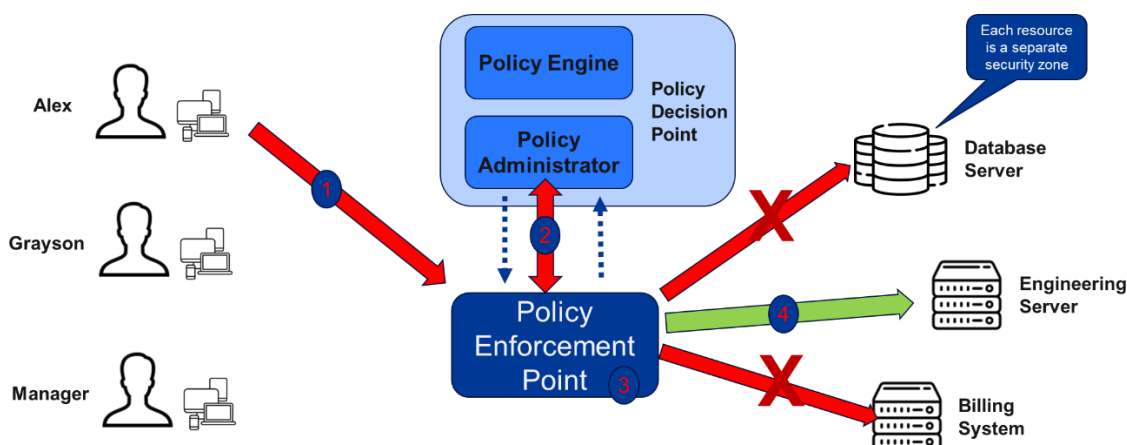


Figure 27 - Example of PEP and PDP Access System 1

Key Points:

- Each server/service needs to reside within its own security zone.
- Every access attempt by a subject trigger a fresh PDP assessment. Sessions are terminated upon completion of authorized workflows.

7.1.1.2 Additional Scenarios:

Subsequent Resource Access (Figure 28): Once Alex finishes with the Engineering server and attempts to access the Billing system, her previous Engineering server access is terminated. A new PDP evaluation is initiated for the Billing system access request.

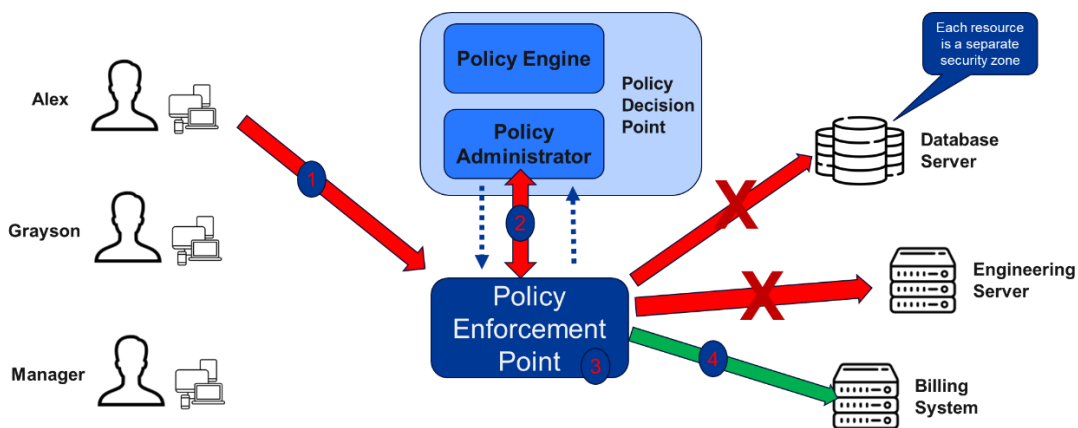


Figure 28 - Example of PEP and PDP Access System 2

Remote Access (Figure 29): Grayson, assigned to the same role as Alex, attempts to access the Engineering server from a remote location. The PDP detects his remote network location and grants access with a reduced privilege level compared to Alex's on-network access.

CONTROLLED DISCLOSURE

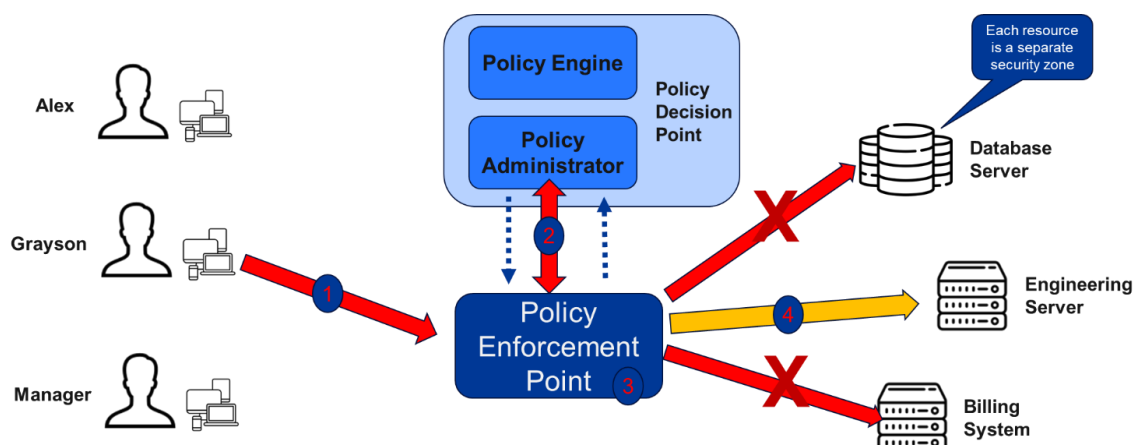


Figure 29 - Example of PEP and PDP Access System 3

Anomalous Device Behavior (Figure 30): Alex and Grayson's manager tries to access the Engineering server. The PDP evaluation process detects anomalous device behavior through SIEM or XDR data and denies access, potentially before a security team receives an alert.

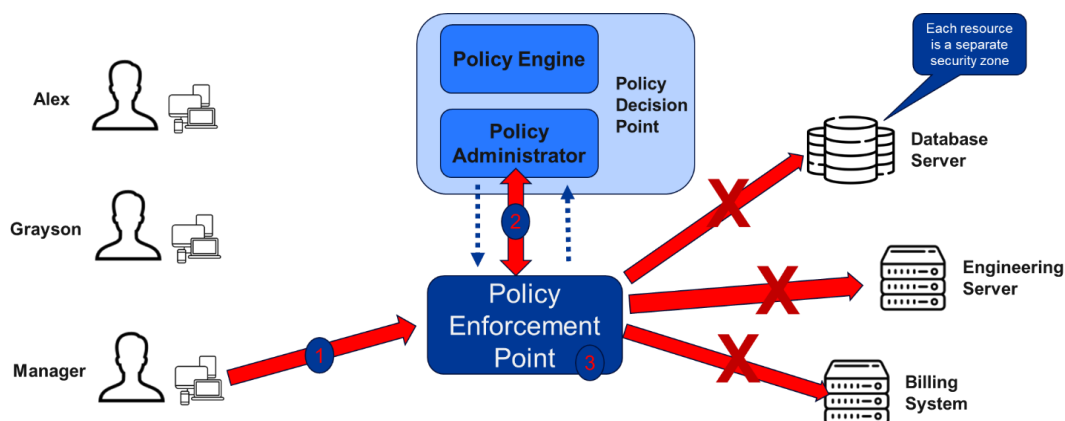


Figure 30 - Example of PEP and PDP Access System 4

CONTROLLED DISCLOSURE

A.2 – Zero Trust Architecture in OT with multiple sites

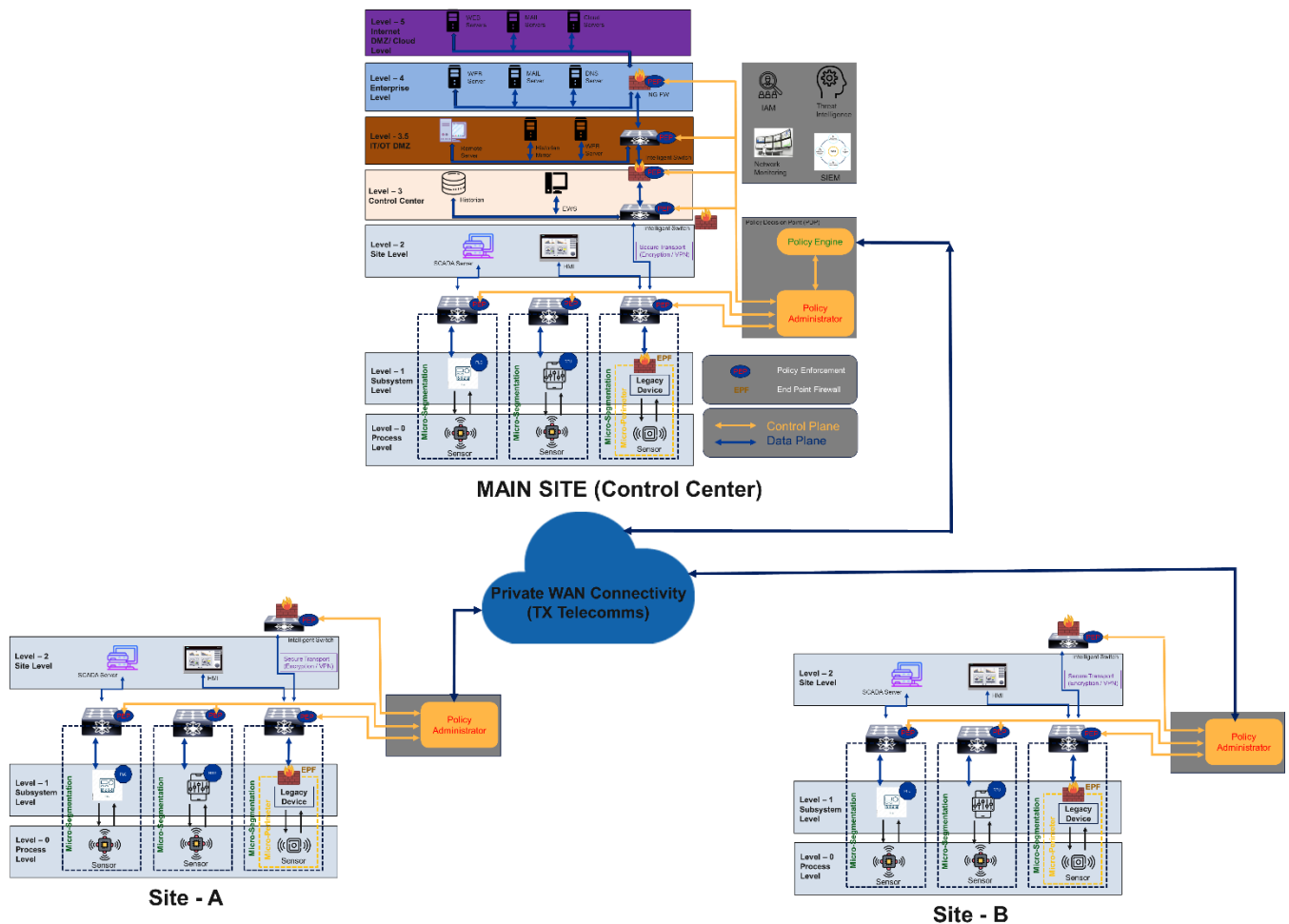


Figure 31 - Zero Trust Architecture in OT with Multiple Sites

CONTROLLED DISCLOSURE

A.3 – Zero Trust Architecture in OT Scenario 1: Data Flow

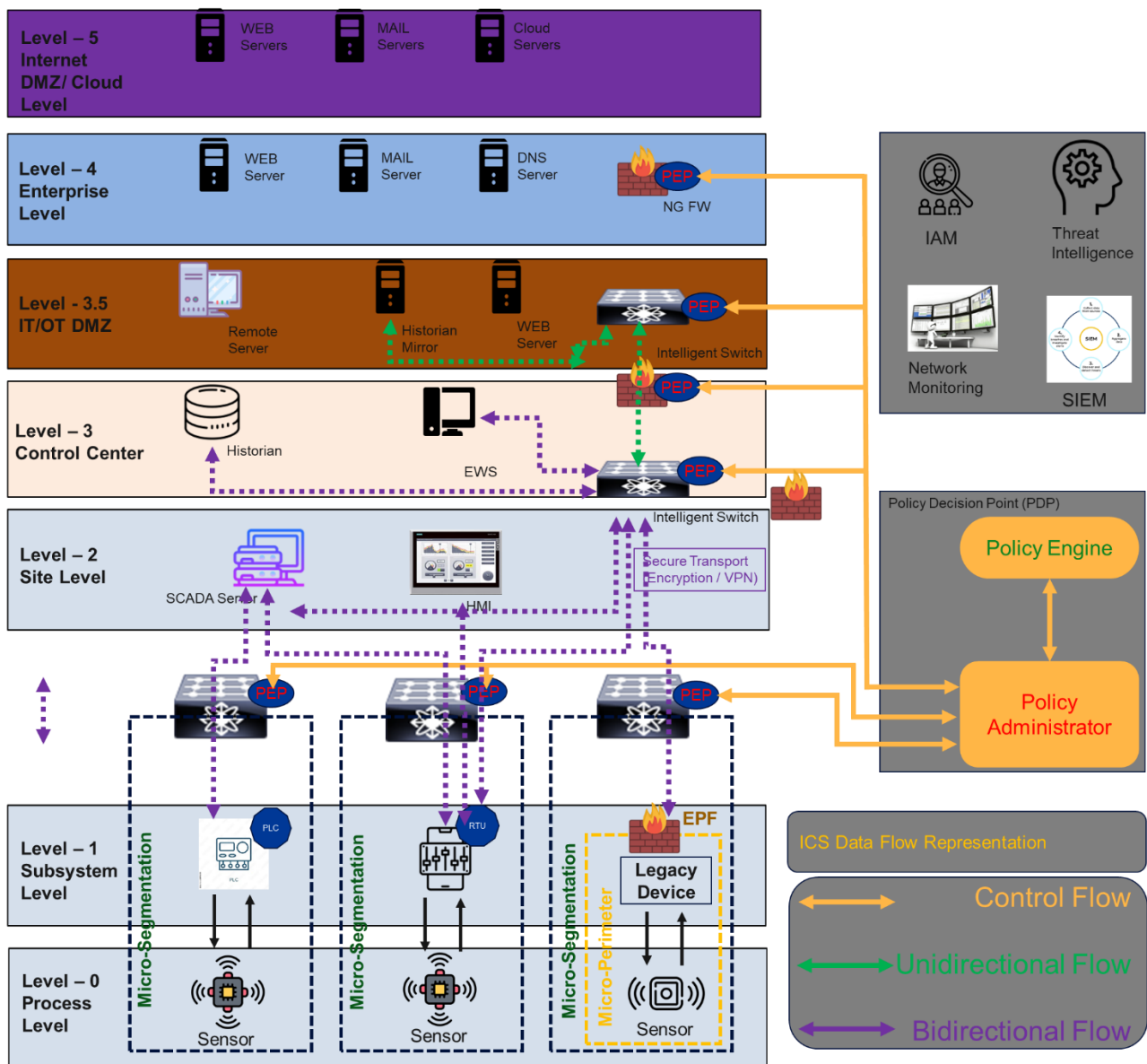


Figure 32 - Zero Trust Architecture in OT Scenario 1: Data Flow

CONTROLLED DISCLOSURE

A.4 – Zero Trust Architecture in OT Scenario 2: Remote Access and IAM

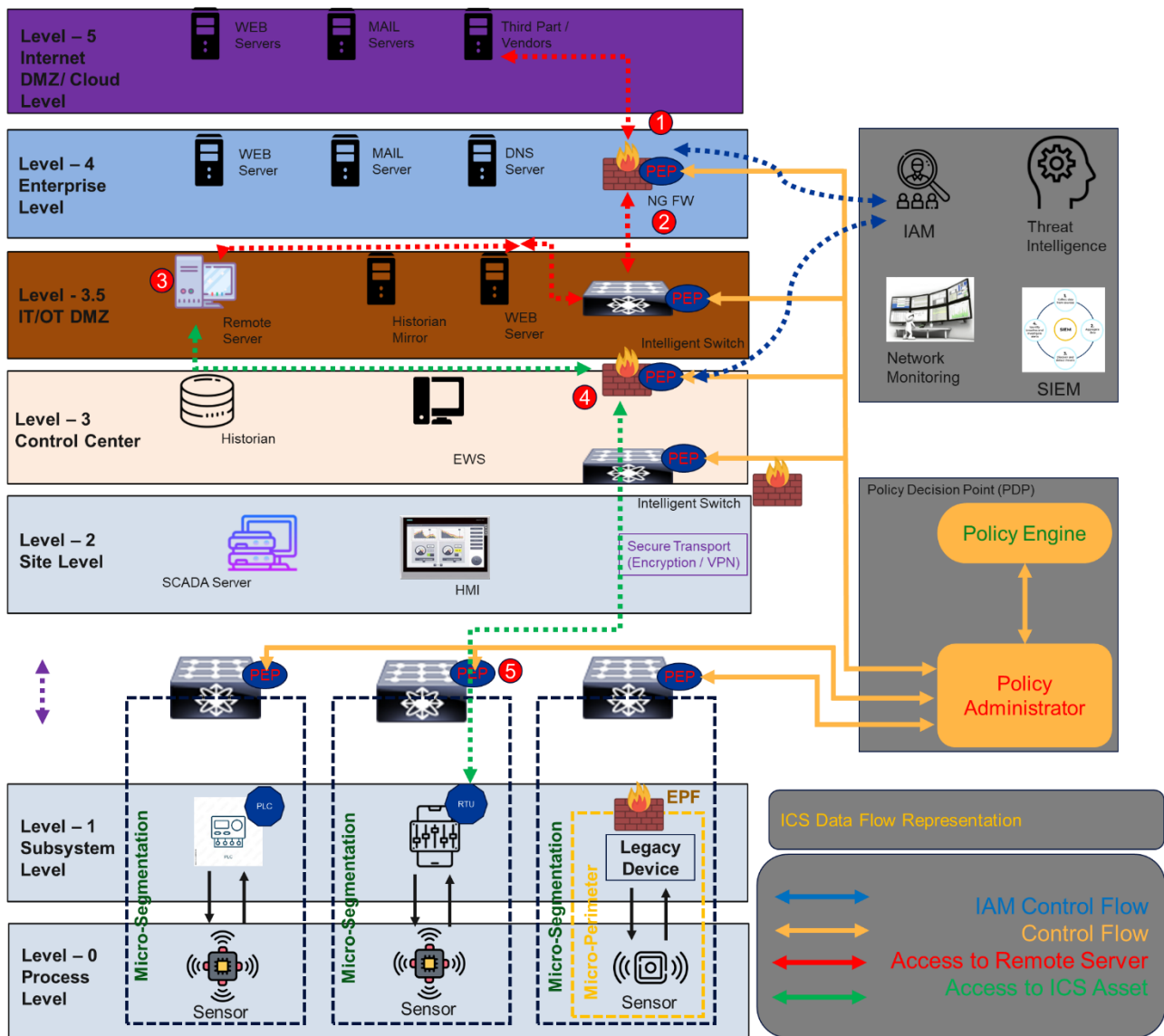


Figure 33 - Zero Trust Architecture in OT Scenario 2: Remote Access and IAM

CONTROLLED DISCLOSURE

A.5 – ZTA within Legacy infrastructures

With NTCSA having several legacy devices in the network the following model for deployment of ZTA for the legacy environment can be used:

1. Device Agent / Gateway (Recommended)
2. Enclave – Based (Recommended)
3. Resource Portal-Based
4. Device Application Sandboxing

Different technologies can be utilized to achieve trust for legacy device/subsystems by enabling.

- Micro-perimeter and
- Micro-segmentation

Some Products that can help to achieve ZTA with systems are:

1. SDN-based switch/ Gateways.
2. PEP enabled switch.
3. PEP enabled firewall.
4. Endpoint firewall

Figure 32 illustrates how the above can be applied to legacy devices.

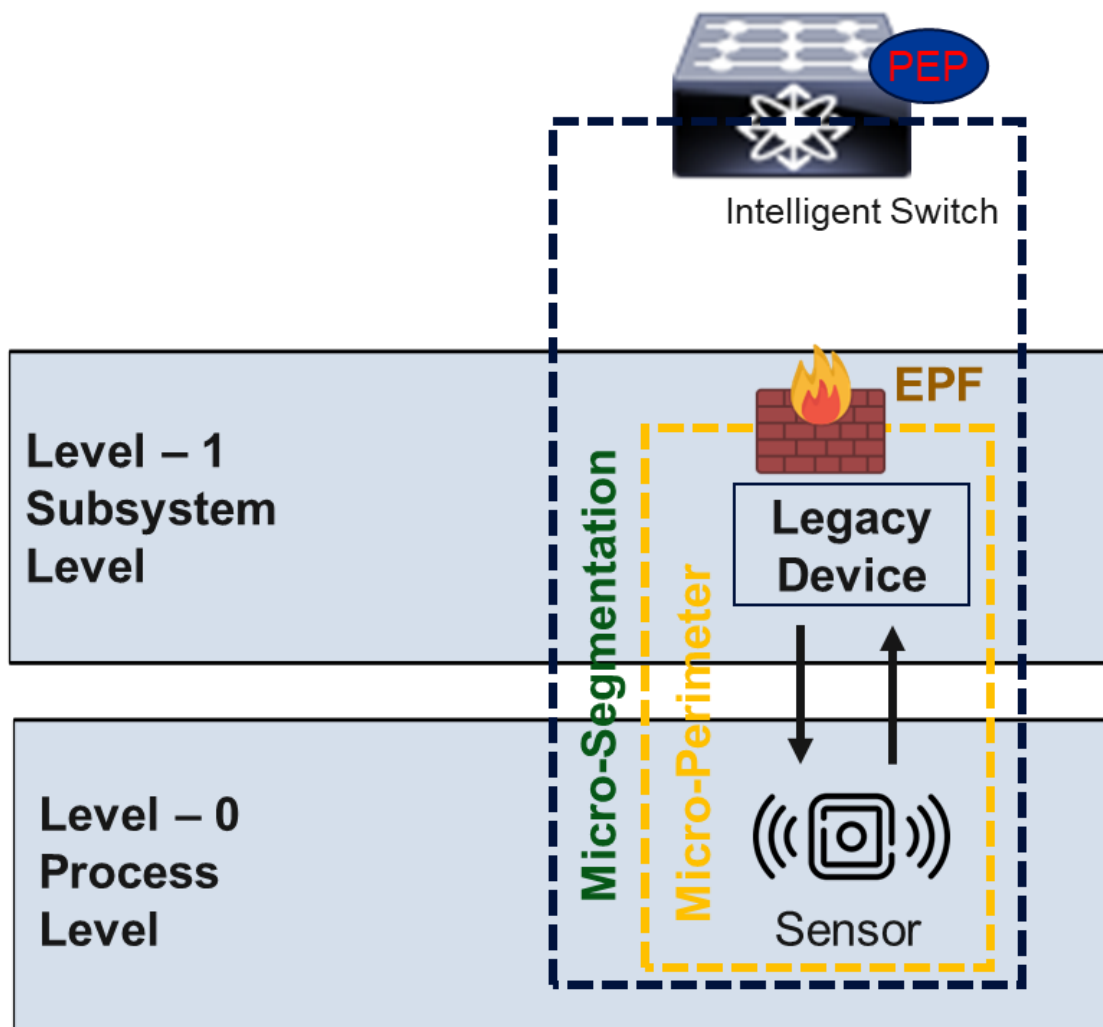


Figure 34 - ZTA within Legacy infrastructures

A.6 – Zero Trust Adoption

Figure 35 provides a hi-level process or 4 steps of achieving the Zero Trust adoption. This can be achieved by consistent application of security controls to critical areas regardless of location or hosting model.

1. Strong Authentication
2. Adaptive Policy Engine
3. Grant and limit access
4. Monitor and alert

CONTROLLED DISCLOSURE

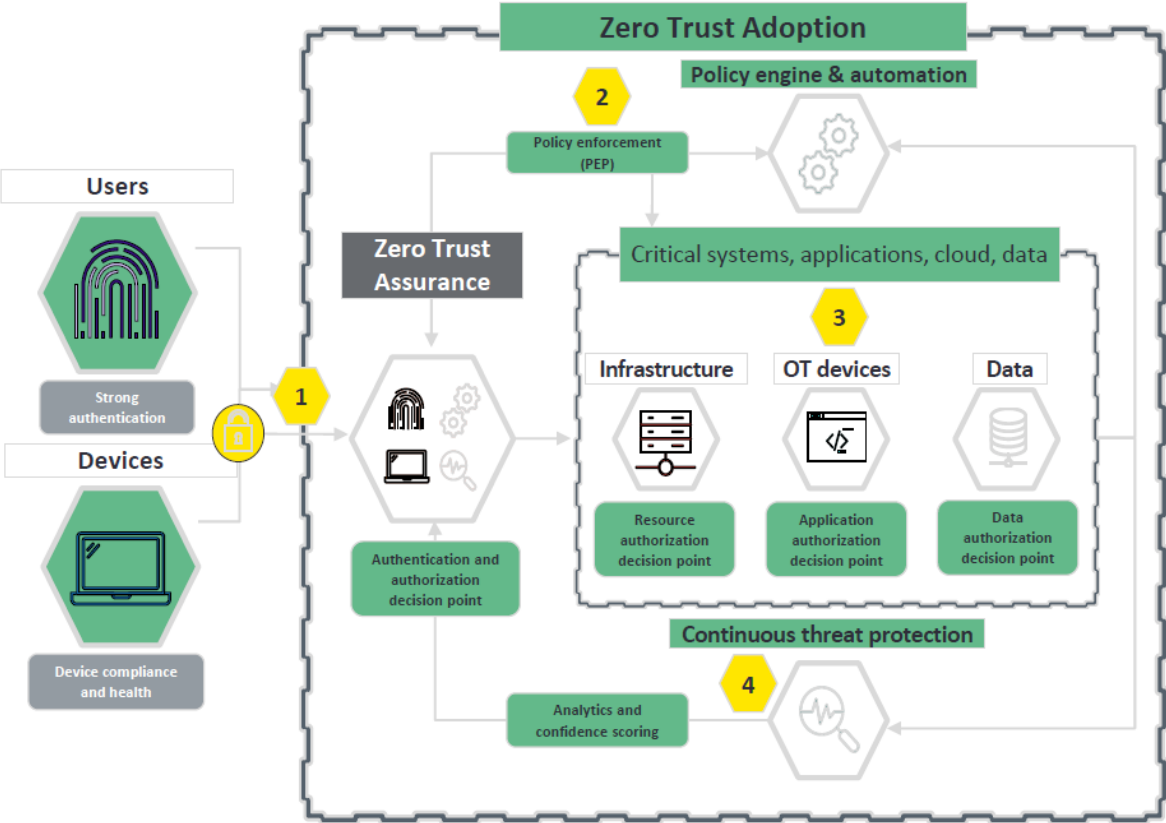


Figure 35 - Transforming to Achieve Zero Trust Adoption

CONTROLLED DISCLOSURE

A.7 – Current technology landscape: From ZTA Perspective

The current technology landscape is characterized by several key trends and challenges at the different levels. From a ZTA perspective, it involves a shift towards a more proactive and granular approach to cybersecurity. Figure 34 provides a technology landscape from a ZTA perspective and reverence the state of ZT implementation at the different layers.

Current technology landscape: From ZTA Perspective					ZT Implemented		Technology is fully rolled out and aligned to ZT			
					ZT Partially implemented		Technology is rolled out but not from ZT perspective			
					ZT Not implemented		Technology is not yet rolled out			
Gateway Layer	Secure Web Gateway	Email Security Gateway	Sandbox		Web Application Firewall	Threat Intelligence Platform	Next Generation Firewall	IPS/IDS		
Authentication and Authorization Layer	MFA	Identity Access Management	ZTNA/ Adaptive Policy Engine		Privileged Access Management					
Network Access Layer	CASB	SSE/SASE	NAC		Micro-segmentation	PKI (Digital Certificates)	SDN	SD-WAN		
Applications/ Business Logic Layer	Container Scanning (Sys Dig)	Secure Code Review			Vulnerability scanner	Micro Services Gateway	Open-Source Software Scanning	SAST,DAST	Comprehensive Secure Connectivity for Composite Applications (CASCE)	
Data Access Management Layer	Classification Tool	Attack Surface Management	DLP	DRM	File integrity Monitoring					
Security Monitoring layer	Insider Risk Management (Veriato)	Advanced EDR			SIEM	Log Management	Database Activity Monitoring	Cloud Security Posture Management (CSPM)		
Governance Layer	Operationalize / Monitoring Proces	Integration with Cyber Operations			Secure API Process					

Figure 36 - Current technology landscape: From ZTA Perspective

CONTROLLED DISCLOSURE

Annex B – Secure Area Attributes

Table 1 - Secure Area Attributes

Attribute	Secure Area 1	Secure Area 2	Secure Area 3	Secure Area 4	Secure Area 5	Secure Area 6	Secure Area 7	Secure Area 8
Purpose	Critical network infrastructure (e.g. SCADA), monitoring and Protection. Critical work force enablement. Synchronisation Distribution.	Non-real time OT monitoring. Physical Security. Work force enablement.	OT systems hosted by IT.	Enterprise business systems.	Threat-Centric Security Operations Centre (TC-SOC)	External Services	External Control Center GX, DX, SAPP, Munic	OT Systems to IPP/ITP
Confidentiality	Confidential (default)	Confidential (default)	Confidential (default)	Confidential (default)	Secret (default)	Confidential (default)	Confidential (default)	Confidential (default)
Data flow control between secure areas	All connections entering or leaving the secure area shall be through a DMZ. Data leaving the secure area	All connections entering or leaving the secure area shall be through a DMZ. Data entering the secure area	All connections entering or leaving the secure area shall be through a DMZ. Data entering the secure area	All connections entering or leaving the secure area shall be through a DMZ. Data entering the secure area	All connections entering or leaving the secure area shall be through a DMZ. Data leaving the secure area	Data in this secure area shall not have connectivity with other secure areas.	All connections entering or leaving the secure area shall be through an OT/OT DMZ. Data entering the secure area	All connections entering or leaving the secure area shall be through a DMZ. Data entering the secure

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

	must be pushed to a DMZ (unidirectional data flow). Data entering the secure area must come through a hardened jump server from the DMZ. Connections must be verified (e.g. multi-factor authentication) and monitored.	must come through a jump server from the DMZ.	must come through a jump server from the DMZ.	must come through a jump server from the DMZ.	must be pushed to a DMZ (unidirectional data flow). Data entering the secure area must come through a hardened jump server from the DMZ. Connections must be verified (e.g. multi-factor authentication) monitored.		must come through a jump server from the DMZ. Connections must be verified (e.g. multi-factor authentication) and monitored.	area must come through a jump server from the DMZ.
Governance	OT	OT	IT and OT	IT	ISOC and supplemented with IT and OT.	IT and OT	OT	OT
Connections between a secure area	Data in transport between this secure area shall be segregated from other data	Data in transport between this secure area shall be segregated from other data in a	Data in transport between this secure area shall be segregated from other data in a	Data in transport between this secure area shall be segregated from other data in a	Data in transport between this secure area shall be segregated from other data in a	Data in transport between this secure area shall be segregated from other data in a different secure	Data in transport between this secure area shall be segregated from other data in a different secure	Data in transport between this secure area shall be segregated from other data

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

	in a different secure area. Encryption and authentication should be applied where possible.	different secure area.	different secure area.	different secure area.	different secure area.	area. Encryption and authentication should be applied where possible.	area. Encryption and authentication should be applied where possible.	in a different secure area.
Data storage	Data stored shall be segregated from other data in a different secure area.	Data stored shall be segregated from other data in a different secure area.	Data stored shall be segregated from other data in a different secure area.	Data stored shall be segregated from other data in a different secure area.	Data stored shall be segregated from other data in a different secure area.	Data stored shall be segregated from other data in a different secure area.	Data stored shall be segregated from other data in a different secure area.	Data stored shall be segregated from other data in a different secure area.
System Owner	OT system owner.	OT system owner	IT system owner	IT system owner	ISOC system owner	IT and OT system owners	OT system owner	OT system owner
Centralisation	Centralised OT service hosted by OT. Only centralise for OT. Cannot provide services for IT or ESD. Possible for centralised server of secure area 2 service to reside in secure area 1.	Possible to centralise non-essential services.	Centralised OT service hosted by IT. Service is provided for OT only.	Centralised IT service hosted by IT. Can provide service for entire business.	Centralised service hosted by Monitoring and Reporting Unit. Can provide service for entire business.	Possible to centralise non-essential services. Can provide service for entire business.	Possible to centralise non-essential services.	Possible to centralise non-essential services.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

Third party networks	Third party networks should be avoided where possible.	Third party networks are acceptable.	Third party networks are acceptable.	Third party networks are acceptable.	Third party networks should be avoided where possible.	Third party networks should be avoided where possible, but may be acceptable depending on service requirements	Third party networks should be avoided where possible.	Third party networks should be avoided where possible.
----------------------	--	--------------------------------------	--------------------------------------	--------------------------------------	--	--	--	--

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

Annex C – NTCSA Security Design checklist.

D1. Establish the context before designing a system.

Before you can create a secure system design, you need to have a good understanding of the fundamentals and take action to address any identified shortcomings.

D2. Make compromise difficult.

Designing with security in mind means applying concepts and using techniques that make it harder for attackers to compromise your data or systems.

D3. Make disruption difficult.

When high-value or critical services rely on technology for delivery, it becomes essential that the technology is always available. In these cases, the acceptable percentage of 'downtime' can be effectively zero.

D3. Make compromise detection easier.

Even if you take all available precautions, there's still a chance your system will be compromised by a new or unknown attack. To give yourself the best chance of spotting these attacks, you should be well positioned to detect compromise.

D5. Reduce the impact of compromise.

Design to naturally minimise the severity of any compromise.

Table 1- Design Principles Related to Cyber Resiliency

Generally Accepted Design Principle	Corresponding Cyber Design Principle(s)	How this can be achieved
Design to reduce exposure to attack	Reduce attack surfaces.	Limit the number of entry points an attacker could exploit. Implement measures like network segmentation, minimal privilege, and secure configurations.
Design to reduce persistence of access by the adversary	Maximize transience; minimize persistence.	Regularly update and rotate credentials, use ephemeral services, and implement session timeouts to prevent long-term unauthorized access.
Design to reduce adversary's ability to act	Control visibility and use. Contain and exclude behaviours.	Implement strict access controls and monitoring to limit what attackers can see and interact with. Use network segmentation and application sandboxing to prevent attackers from moving laterally within your system.
Design to limit the consequences of attack	Contain and exclude behaviours. Manage resources (risk-) adaptively.	Use containment strategies such as isolating affected systems and deploying intrusion detection systems. Continuously assess and adapt resource management based on evolving threats and impacts.
Design to minimize common cause failure	Focus on common critical assets. Maintain redundancy.	Identify and protect key assets to prevent systemic failures. Implement backup systems and failover mechanisms to ensure continued operation in case of a failure.

CONTROLLED DISCLOSURE

Design to tolerate compromise	Assume compromised resources. Limit the need for trust.	Design systems with the assumption that components may be compromised. Use techniques like encryption and access controls to limit damage. Implement zero-trust principles where every access request is authenticated and authorized.
Design to degrade gracefully	Manage resources (risk-) adaptively.	Ensure that the system can continue operating in a reduced capacity without a complete shutdown.
Design to crash early and recover quickly	Manage resources (risk-) adaptively.	Implement mechanisms to detect failures early and automate recovery processes to minimize downtime.
Additional Design Principle	Corresponding Cyber Design Principle(s)	
Design for integrity and availability	Determine ongoing trustworthiness.	Implement continuous monitoring and validation processes to ensure that systems maintain their integrity and availability over time.
Design to be threat independent	Expect adversaries to evolve.	Design systems that can adapt to new and evolving threats. This involves creating flexible security frameworks and updating threat models regularly.
Design to be vulnerability independent	Expect adversaries to evolve.	Develop systems that are resilient to changes in attack strategies. Utilize robust and adaptive security measures that do not rely on fixed vulnerabilities.
Design such that users will not seek to circumvent security and resilience features	Make unpredictability and deception user transparent.	Integrate security measures that are seamless and invisible to users, ensuring they do not interfere with usability or encourage attempts to bypass them.
Design with distributed and localized decision support	Make resources location versatile.	Implement decision-making systems that can operate effectively in diverse and distributed environments, allowing for flexible and localized responses.
Integrate horizontally for resilience of the whole system / mission	Control visibility and use. Layer and partition defences.	Use horizontal integration techniques to maintain comprehensive visibility and control across all system components. Apply layered security measures and partition defenses to manage risks and prevent systemic failures.
Design components with computational plasticity (alternative functional paths to achieve the computing results)	Support agility and architect for adaptability.	Design components that can adapt and switch functional paths as needed, supporting agility and flexibility in response to changes and failures.

CONTROLLED DISCLOSURE

Design for simplicity and modularity to change easily / frequently	Support agility and architect for adaptability.	Build systems with simple, modular components that can be easily updated or replaced, enhancing adaptability and ease of maintenance.
--	---	---

Table 2- Operational Principles Related to Cyber Resiliency

Operational Principle	Corresponding Cyber Resiliency Design Principle(s) from Table 2
Actively look for bad guys in the system	Assume compromised resources. Expect adversaries to evolve.
Leverage cyber intelligence to inform operations	Assume compromised resources. Expect adversaries to evolve.
Operate to reduce adversary's ability to act	Control visibility and use. Contain and exclude behaviours. Layer and partition defences.
Operate to contain vulnerabilities	Control visibility and use. Contain and exclude behaviours. Layer and partition defences.
Operate to reconstitute and recover quickly to an acceptable level of trust	Determine ongoing trustworthiness.
Prioritize operational TTPs based on mission assurance needs	Maintain situational awareness.
Balance / coordinate local defence with global defence	Control visibility and use. Contain and exclude behaviours. Layer and partition defences.
Operate to control / limit the damage / consequences of attack	Manage resources (risk-) adaptively.
Operate with agility and alternative operational contingencies	Manage resources (risk-) adaptively.
Operate to confuse, deceive, and impede the adversary (but not the mission operators)	Make unpredictability and deception user transparent.
Monitor integrity and availability, and respond accordingly	Maintain situational awareness.
Train operators to understand cyber impact to mission operations to operate in ways that ensure mission execution success	Manage resources (risk-) adaptively.

CONTROLLED DISCLOSURE