Eskom	Standard	Technology

Title: **Cyber Security Standard for Operational Technology**

Document Identifier: **240-55410927**

Alternative Reference Number:

Area of Applicability: **Eskom Holdings SOC Ltd**

Functional Area: **Engineering**

Revision: **Draft 2.1**

Total Pages: **33**

Next Review Date: **March 2028**

Disclosure Classification: **Controlled Disclosure**

Compiled by	Supported by	Functional Responsibility (Gx)	Accepted by
Johan Botha **Senior Consultant** Date:	**Meenal Vala** **Cyber Security CG Chair** Date:	**Danie Odendaal** **Gx GM Engineering** Date:	**Sithembile Songo** **CISO** Date:

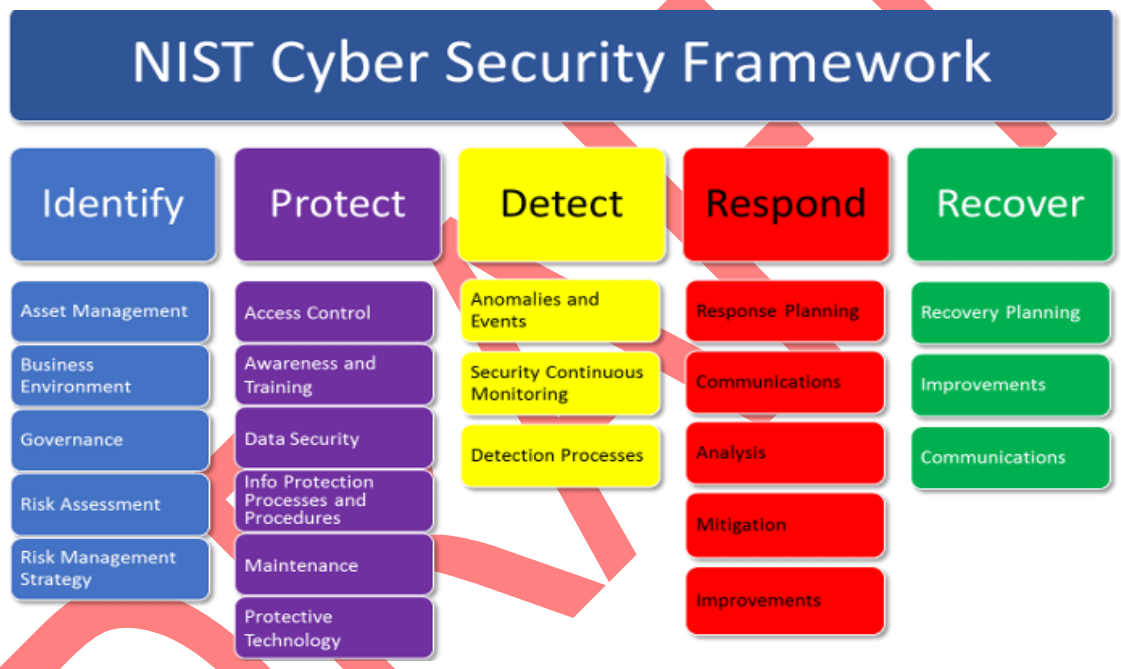
Functional Responsibility (Tx)	Functional Responsibility (Dx)	Supported by SCOT	Approved by
Naresh Hari **Tx GM Engineering** Date:	**Azwimbavhi Mamanyuha** **Dx GM Engineering** Date:	**Nelson Luthuli** **SCOT Chair** Date:	**Faith Burn** **CIO** Date:

Content

1 Introduction

Over the last few decades, Operational Technology (OT) systems are utilising more and more IT type computers and operating systems. In addition, the need for exchanging data with IT systems for management reporting, generation contracts, weather data etc., means that OT networks are more connected to IT networks than in the past.

This necessitates security policies and standards to protect OT systems. Eskom has decided to align its systems to the US National Institute of Standards and Technology (NIST) framework in order to protect its assets. The NIST framework was formulated to not only address cyber threats but also help in facilitating OT business objectives.



The NIST framework consists of the 5 main functions listed below that allows for a purpose-built business requirement approach to the risks, threats and vulnerabilities that an organisation would need to address.

Identify – Develop understanding of managing cybersecurity risk to systems, assets, data, and capabilities.
Protect – Develop and implement the appropriate safeguards to manage the impact of a potential cybersecurity event and ensure delivery of critical infrastructure services.
Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity threat and event within the environment.
Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity event within the environment.
Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event in the environment.

2 Supporting Clauses

2.1 Scope

The aim of this document is to define requirements for systems that would assist in achieving an acceptable level of protection and mitigation against cyber threats related to intrusions and malware, understanding the vulnerabilities of the OT cyber assets and ensure the risks to the OT environment are understood and mitigated.

Operational Technology (OT) Systems are defined as follows in the Definition of operational technology (OT) and OT / IT collaboration accountabilities document:

“In the Eskom context Operational Technology (OT) is defined as:

Operational systems which form part of Eskom’s plant / network assets, and which could by virtue of design, maintenance or operation directly result in the failure of these assets to meet their purpose and performance criteria, where:

1. Operational systems: are all systems (including electronic, telecommunications and computer systems and components) which process, store or communicate operational data or information.
2. Part of means contribute to the asset meeting its purpose and performance criteria.
3. Plant / network assets are any part of the “built environment” utilized by Eskom to run its production, delivery and logistics processes, including generation, transmission and distribution of electricity, etc.
4. Directly: means in real time or near real time. E.g. would include supervisory control systems but would exclude spares ordering applications (even though these could eventually result in the failure of the asset).
5. Purpose and performance criteria: The “design to”, “maintain to” and “operate to” criteria that are generally specified formally.

Systems, sensors, transducers, Intelligent Electronic devices (IEDs) and Programmable Logic Controller (PLC) equipment, which extract signals and measurements from the plant / network asset or its control environment or facilitate control over these assets generally meet the above criteria and qualify as OT, since their failure could directly result in the failure of the plant / network asset or its ability to meet its purpose and performance criteria.

In some cases, obvious failures of operational systems may not directly result in the failure of purpose or performance of the plant / network asset, but because of the way it is designed, normal operations or maintenance of the operational system could result in a risk to the plant / network asset. An example is:

• Voltage spike induced in a control circuit due to a lightning strike on the power supply of an IT server not fitted with the same spec of surge protection as used on the control circuit, and inadequate voltage supply decoupling (e.g. optical decoupling).

Such equipment generally meets the above criteria and qualifies as OT, since their design, operation or maintenance could directly result in the failure or impact of the plant / network asset or its ability to meet its purpose and performance criteria.”

2.1.1 Purpose

The purpose of this document is to ensure that all necessary measures are taken to ensure that Eskom business continuity is not affected due to any cyber related incident. It is recognised that there is a difference in the operation and risks associated with the technical operational assets of the business, as compared to the conventional Information Technology (IT) systems. Although there is increasing convergence of the IT technology utilised in both systems, there are unique differences in its application, responsibility, ownership, maintenance and the lifespan of the Operational Technology systems, which makes standard IT policies impractical or inadequate. OT equipment require a dedicated security approach as described in this standard.

2.1.2 Applicability

This document shall apply to Operational Technology environments throughout Eskom Holdings Limited.

2.2 Normative/Informative References

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

Normative

[1] ISO 9001 Quality Management Systems

[2] 240-146054527 Information and Communications Technology Network Security Framework

[3] 32-373: Information Security - IT/OT Remote Access Standard

[4] 240-79669677: DMZ designs for Operational Technology

[5] Critical Infrastructure Protection Act 8 of 2019

[6] 32-143 Handling of classified items standard

Informative

[1] 240-91479924: Cyber Security Configuration Guideline of Networking Equipment for Operational Technology

[2] 32-85: Information security Policy

[3] 32-644: Eskom document management standard

[4] 204-53114002: Engineering Change Management Procedure

[5] Minimum Information Security Standard (MISS) – South African National document

[5] NIST Cybersecurity Framework V1.1

2.3 Definitions

Definition	Description
Cyber Assets	Cyber Assets are defined to be programmable electronic devices and communication networks including hardware, software, and data
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	Electronic Security Perimeter (ESP) is defined as the logical boundary between the system and external networks.
Stateful firewall	A stateful firewall is a firewall that monitors the full state of active network connections and will keep track of established sessions labelling them as LISTEN, ESTABLISHED, or CLOSING for example.

2.4 Abbreviations

Abbreviation	Explanation
AD	Active Directory
CD	Compact Disc
CIP	Critical Infrastructure Protection
CIS	Centre for Internet Security
ESP	Electronic Security Perimeter
FIPS	Federal Information Processing Standards
IDS	Intrusion Detection System
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MFA	Multi Factor Authentication
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OS	Operating System
OT	Operational Technology
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TACACS	Terminal Access Controller Access Control System

Abbreviation	Explanation
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network

2.5 Roles and Responsibilities

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

2.6 Process for Monitoring

This document will be revised as required and as Eskom's corporate IT, OT, Technology and Smart Grid strategies evolve.

3 Requirements for OT Cyber Security Management

Part of a defence-in-depth strategy is to acquire a thorough understanding of possible attack vectors on a system. Poorly configured or vulnerable firewalls, no segmentation, the use of insecure protocols and privileged access from the outside and other design or configuration mistakes will reduce security. Defence in depth is needed to prevent a mistake or vulnerability on one level resulting in the full system being compromised. These systems would include air-gapped systems with USB port access and OT systems connected to IT networks where web, database and file exchange servers may be found with possible application or protocol vulnerabilities. As part of the defence in depth strategy, network topologies will need to be clear and concise and ensure all integrations points between OT and IT are documented and clearly discussed and understood.

The focus should be on systems rather than just devices. Where there are other systems that are duplicates of the evaluated system, the impact of all these systems together should be considered to determine the appropriate level of protection that should be implemented, especially if these systems are reachable from remote locations.

3.1 System Classification

To balance the cyber security precautions taken with the impact of a breach, the document has split the requirements into 3 categories: High (H), Very High (VH) and Critical (C). The following criteria are used to determine in which category a system should fall:

Critical

- Result in immediate production losses involving a total capacity of ≥ 4 000 MW or sufficient capacity to initiate an under-frequency incident.
- Seriously injure or kill one or more persons.
- Violating National legislation, policy, licence or permit conditions.

- Compromise the integrity of, or alter in any way protection systems, devices, functions, settings or philosophy of significant plant.
- Result in immediate power delivery loss on the network affecting 10 000 customers <50 MW for 12 hours.
- Result in loss of visibility / control of more than 50% of managed equipment for any control centre managing critical assets.
- Under certain situations, auxiliary systems that support these Critical Systems should also be considered as critical – these include the physical access control, fire detection, power supply systems, etc.

Very High

- Result in immediate production losses involving a total capacity of ≥ 800 MW or sufficient capacity to initiate an under-frequency incident.
- Result in immediate power delivery loss on the network, resulting in >10,000 general customer disconnection ≥4 hrs or large load centre for < 2 hrs (0.1 to 1 system minutes).
- Compromise of a generation facility's ability to perform black starting.

High

- Result in immediate power delivery loss on the network, resulting in disconnection of a key customer in contravention of contractual conditions.
- Interruption of the equivalent of 400 MW production for > 1 week.
- Interruption of the power delivery equivalent of 50MW on the network, resulting in customer loss of supply > 12hrs.
- Result in a significant environmental contravention situation.
- Reduction of life of a significant plant asset (value ≥ R250 million) by > 10%.
- Increasing the longer-term production costs of a plant by >10%.
- Negatively expose any part of Eskom to national media for ≥ 2 weeks.
- Reducing the level of back-up redundancy provided to a significant plant for ≥ a week.
- Loss in the ability to perform emergency switching
- Initiate the activation of disaster recovery/management plans at an Eskom site.

The system would be classified into the highest applicable category and must comply to the requirements applicable to that category.

3.2 Data Classification

Data from or information about systems must be classified in different categories based on the value to the organization, the sensitivity of the information and the increased risk to Eskom if it were to be disclosed. OT and IT data are differentiated and the definitions below are to be read in conjunction with the 32-143 Handling of classified items standard.

The primary difference between IT and OT is how data is used. IT is more focused on broad business needs. This means it deals with enterprise application transactions, business voice communication, data storage – often in unstructured databases – and other meta-level data needs.

By contrast, OT deals with machine-driven data meant to be consumed in real-time at the user or manager level. This data comes from the control of physical devices through digital technologies such as software with advanced analytics engines dedicated to optimizing processes. The NIST 800-53 recommends the utilisation of 3 categories for the potential adverse impact level of unauthorised disclosure of Data, namely, Low impact (limited adverse effects), moderate impact (serious adverse effects) and high impact (severe or catastrophic adverse effects).

Unclassified data can be released to the public and general availability within the business. No impact from data disclosure.

Controlled/Internal disclosure information is company-wide and should be protected with limited controls. Controlled disclosure documents and data may include various standards, policies and Eskom wide memos. It can also be classified as general business communication, non-operational data that can be shared within the business without higher levels of clearance and can be made available to External parties when requested and approval is given to allow access to the Data. Low impact to the disclosure of data.

Confidential Data (OT communications, non-operational data that could affect operations if disclosed, field data for historian and analytics for Tx and Dx)

Classification allocated to all information that may be used by malicious, opposing, hostile elements to harm the objectives and function of an individual and/or an institution.

Compromise thereof can lead to the disruption of cyber assets essential to the reliable operation of critical plant assets which are those facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the electricity supply network affecting a specific area, region or customer base and/or compromise the stability and availability of the grid. This would also relate to the damage/loss to critical plant assets >400MW if the breach would cause the deliberate destruction or failure of said plant. This would extend to any deliberate or unintended danger to persons. Moderate impact to disclosure of data.

Secret Data (All power network OT data: SCADA/CNI and Automation data that allows control)

Classification allocated to all information that may be used by malicious, opposing, hostile elements to disrupt the objectives and function of an institution and/or state.

Compromise thereof can lead to the disruption of Cyber assets essential to the reliable operation of critical plant assets which are those facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the electricity supply network affecting a large area, region or distribution customer base and/or compromise the stability and availability of the grid for an extended period. This would also relate to the damage/loss to critical plant assets of >800MW if the breach would cause the deliberate destruction or failure of said plant.

Compromise thereof can also disrupt the effective execution of operational plans; can damage operational relations between the Transmission and Distribution operators; can endanger the public. Moderate to high impact to disclosure of data.

Top Secret Data (SCADA, Automation and Plant data at Gx)

Classification allocated to all information that may be used by malicious, opposing, hostile elements to neutralise the objectives and function of an individual and or an institution.

Compromise thereof can disrupt the effective execution of operational plans; Can seriously damage operational plans between institutions; Can lead to the discontinuation of diplomatic relations between states; can result in declaration of war.

Compromise thereof can lead to the disruption of Cyber assets essential to the reliable operation of critical plant assets which are those facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the electricity supply network affecting the country and/or compromise the stability and availability of the grid for an extended period resulting in complete black out. This would also relate to the damage/loss to critical plant assets >4000MW if the breach would cause the deliberate irreparable destruction or failure of said plant and would require extensive time for repair and return of operations.

Compromise thereof can disrupt the effective execution or operational plans of the business; can disrupt the effective functioning of the grid; can damage the governing of the country; can endanger the public. High impact to the disclosure of data.

3.3 Identification of Critical Cyber Assets

The purpose of this section is to identify and classify the critical cyber assets that needs to be protected.

3.3.1 Identification of Critical Asset

The South African Critical Infrastructure Protection Act of 2019 classifies Critical Infrastructure as follows:

1. Infrastructure qualifies for declaration as critical infrastructure, if—
    a. the functioning of such infrastructure is essential for the economy, national security, public safety and the continuous provision of basic public services; and
    b. the loss, damage, disruption or immobilisation of such infrastructure may severely prejudice—
        i.the functioning or stability of the Republic;

ii. the public interest with regard to safety and the maintenance of law and

iii. order; and

iv. national security.

2. In determining whether the qualifying requirements contemplated in subsection (1) are met, one or more of the following criteria must be applied:

   a. the infrastructure must be of significant economic, public, social or strategic importance;

   b. the Republic's ability to function, deliver basic public services or maintain law and order may be affected if a service rendered by the infrastructure is interrupted, or if the infrastructure is destroyed, disrupted, degraded or caused to fail;

   c. interruption of a service rendered by the infrastructure, or the destruction, disruption, degradation, or failure of such infrastructure will have a significant effect on the environment, the health or safety of the public or any segment of the public, or any other infrastructure that may negatively affect the functions and functioning of the infrastructure in question;

   d. there are reasonable grounds to believe that the declaration as critical infrastructure will not have a significantly negative effect on the interests of the public;

   e. the declaration as critical infrastructure is in pursuance of an obligation under any binding international law or international instrument; and

   f. any other criteria which may, from time to time, be determined by the Minister by notice in the Gazette, after consultation with the Critical Infrastructure Council.

In this regards, bulk generation, transmission and distribution of electricity would be classified as critical infrastructure. Each systems' role in the electricity chain must be evaluated to determine if an attack on the system, or a synchronised attack on all other duplicates of the system, will have a combined effect, resulting in the system being viewed as a critical system according to extract from the CIP act listed above.

The following must be kept in mind:

- Amount of generation loss
- Number of customers without services
- Duration of disconnection to a customer
- Disconnection of key customers contravening contractual obligations
- Financial impact to Eskom due to energy sales lost
- Compromise of facility's ability to perform black starting
- Possible death of severe injury of one or more persons
- Negatively expose any part of Eskom to national media
- Significant reduction in plant life or asset value
- Significant environmental contravention
- Significantly violating National legislation, policy or permit conditions

- Significantly increasing long term production costs of a plant
- Reducing the redundancy of a plant for a non-trivial duration
- Compromise protection on equipment including fire detection
- Loss of the ability to perform emergency switching

3.3.2 Identification of Cyber Assets associated with Critical Assets

Cyber Assets are defined to be programmable electronic devices and communication networks including hardware, software, and data. Software, data and cabling are considered to exist within the framework of the Cyber Asset and therefore are not separate Cyber Assets themselves.

The system owner shall Identify Cyber Assets associated with the operation of each identified Critical Asset. This is not intended to be a complete inventory of all Cyber Assets at the facility, but rather an evaluation and then identification of all Cyber Assets that could impact the reliable operation of the Critical Asset.

It is necessary to identify and list the different types of cyber assets in the system, and to classify them according to criticality, to determine what level of protection each type should have and to place them in different network security zones if appropriate. This should be done at system installation and if any changes are made that would impact the list. The criticality of OT systems can be identified by evaluating its risk exposure (impact and probability) on the ability of Eskom to supply electricity.

Consideration of Critical Assets in secondary or supporting systems whose loss, degradation, or compromise impacts both operation of Critical Cyber Asset(s) and their associated Critical Asset(s) is recommended. These secondary or supporting systems may include:

- Cyber Assets deployed in installed standby mode or installed spare Cyber Assets which may be used during recovery and restoration.
- Environmental systems such as heating, ventilation, and air conditioning (HVAC).
- Support systems such as uninterruptable power supplies (UPS), alarm systems and fire suppression systems.
- Physical security access and monitoring systems.

3.3.3 Identification of Critical Cyber Assets

3.3.3.1Determine Cyber Assets which are Essential

Any Cyber Asset which is essential in the operation of a Critical Asset can be a Critical Cyber Asset. To determine whether Cyber Assets are essential, their impact on the reliable operation of a Critical Asset should be evaluated. If a Cyber Asset is associated with or is connected to a Critical Asset but has no impact on the reliable operation of the Critical Asset, then it can be removed from further consideration as a Critical Cyber Asset.

A Cyber Asset could be considered essential to the reliable operation of a Critical Asset, if one or more of the following criteria are met:

- The Cyber Asset participates in, or is capable of, supervisory or autonomous control that is essential to the reliable operation of a Critical Asset.
- The Cyber Asset displays, transfers, or contains information relied on to make Real-time operational decisions that are essential to the reliable operation of a Critical Asset.
- The Cyber Asset fulfils another function essential to the reliable operation of the associated Critical Asset and its Loss, Degradation, or Compromise would affect the reliability or operability of the Power System.

Cyber assets should be grouped into zones according to how essential they in the operation of the critical asset, and cyber assets in a supporting role for essential cyber assets may also be placed in the same zone as the essential cyber asset if required.

3.3.3.2Identifying Cyber Assets with Qualifying Connectivity

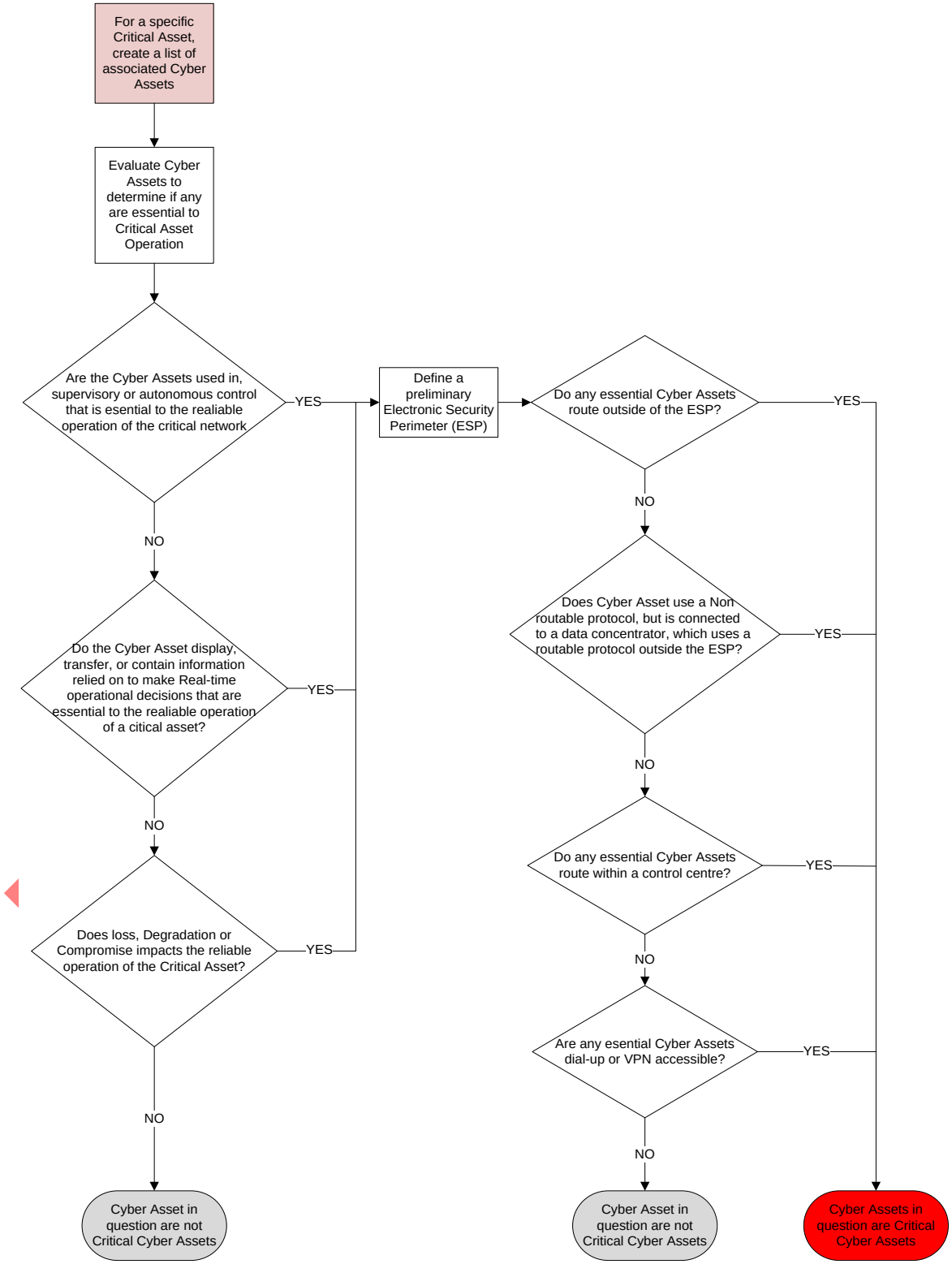
If this essential Cyber Asset has one of the following characteristics it shall be deemed as a Critical Cyber Asset:

- It uses a routable protocol to communicate outside the Electronic Security Perimeter of the system; or,
- a non-routable protocol is used, but it is connected to a data concentrator, which uses a routable protocol outside the Electronic Security Perimeter.
- The Cyber Asset uses a routable protocol within a control centre; or,
- The Cyber Asset is accessible via dial-up or a Virtual Private Network (VPN).

Diagrams to illustrate these are shown in Annex A.

Any supporting system or redundant cyber asset within the same Electronic Security Perimeter (ESP) as a Critical Cyber Asset, must be protected to the same level of the Critical Cyber Asset.

Flow diagram to assist in identifying Critical Cyber Assets:



The following table provides examples for identifying Cyber Assets

Critical Asset	Associated Cyber Asset	Application of Function	Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?	Displays, transfers, or contains information relied on to make Real- time decisions impacting reliable operation of the Critical Asset?	Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?	Communicate with systems outside the ESP using a routable protocol?	A non-routable protocol is used, but it is connected to a data concentrator, which uses a routable protocol outside the ESP	Routable Protocol within a Control Center?	Dial-up or VPN Accessible?	Critical Cyber Asset
Control Centre	SCADA equipment (grouped)	Servers used to collect and process SCADA data	Yes	Yes	Yes	No	No	Yes	No	Yes
Control Centre	Operator Information	Servers providing additional information to controllers to improve decisions	No	No	No	No	No	Yes	No	No
Control Centre	Market	Servers required to run the market system	No	No	No	No	No	Yes	No	No
Control Centre	Remote SCADA	Equipment providing access to real time SCADA from remote control rooms	Yes	Yes	Yes	No	No	Yes	No	Yes
Control Centre	State Estimator – App Server	Provides info to control centre operators, used to make operational decisions.	No	Yes	Yes	No	No	Yes	No	Yes
Control Centre	Print Server	Printing	No	No	No	No	No	Yes	No	No
Substation	Remote Terminal Unit	Provides input monitoring and control for SCADA	Yes	Yes	Yes	No	No	No	No	No

Substation	Remote Terminal Unit	Provides input monitoring and control for SCADA	Yes	Yes	Yes	Yes	Yes	No	No	Yes
Transmission Substation	Protection Relay	Provides real time protection function	Yes	Yes	Yes	Yes	Yes	No	No	Yes
Transmission Substation	Disturbance recorder	Fault recording	No	No	No	Yes	No	No	Yes	No
Generating Plant	Integrated Plant control system	Controls turbine, steam generator, water treatment	Yes	Yes	Yes	No	No	Yes	No	Yes
Generating Plant	Main feed Water control system	Controls the main feed water	Yes	No	Yes	No	No	Yes	No	Yes
Generating Plant	Revenue Meter	Metering	No	No	No	No	No	No	Yes	No
BME	Element Active Manager Server	Manages the BME connections	Yes	Yes	Yes	Yes	No	Yes	No	Yes
NMC Voice	Call Manager Server	Server hosting the call management software	Yes	Yes	No	Yes	No	Yes	No	Yes
DCN	Ericson Management server	Manages the connections on the Ericson SDH	Yes	Yes	Yes	Yes	No	Yes	No	Yes
EAS	EAS Server	Server for the Environmental Alarm System	No	Yes	No	Yes	No	Yes	No	Yes

Audit requirements for this section:

- Asset Management
  - Inventory of physical devices
  - Inventory of Software platforms and applications
  - Communication and data flows map
  - External information systems catalogue
  - List of resources prioritised based on classification, criticality and business value
  - Established roles and responsibilities for workforce and stakeholders
- Governance
  - Information security policy established
  - Information security roles & responsibility coordinated and aligned with internal roles and external partners
  - Legal and regulatory requirements communicated
  - Cybersecurity risks addressed in governance and management processes
  - Budgeting includes cyber security related expenses
  - Cyber security strategy with long- and short-term perspectives
  - Industry recognised cyber security standards used
- Risk Assessment
  - Identify and document asset vulnerabilities
  - Identify and document internal and external threats
  - Identify potential business impacts and likelihoods
  - Identify and prioritise risk responses
- Risk Management Strategy
  - Risk management processes should be established, managed and agreed to by stakeholders
  - Risk tolerance should be determined and expressed
  - Independent audits and reviews / assessments are used to identify gaps in security capabilities and expertise
  - Processes are in place to identify skills improvement requirements in cyber security
  - Program for talent recruitment, retention and succession planning in cyber security planning

3.4 Protect

Requirements for this section are split in High (H), Very High (VH), and Critical (C). The system owner has to decide to which level it should be protected based on the risk to the power system in case of a compromise. This is just a guideline, and where feasible, stricter controls can be implemented. Adequate training needs to be made available for system owners and administrators to allow for the best deployment of solutions. This can be in the form of vendor specific training by the OEM or by industry standard courses.

3.4.1 Logical perimeter

The first and most critical area to protect the OT system from remote attacks, is at the Electronic Security Perimeter. The DMZ Designs for Operational Technology standard provides a guide on firewall placement to create DMZ zones. A DMZ is a separate network segment that connects directly to the firewall. Servers containing the data from the OT system that needs to be accessed from the corporate network are put on this OT DMZ network segment and vice versa.

Requirement	H	VH	C
No traffic should by-pass the OT DMZ zone by traversing from outside to inside or visa-versa. All traffic should terminate on an OT DMZ. Traffic from any internal zone to any external zone and visa-versa should be explicitly denied as the first rule for that interface.	X	X	X
OT DMZ servers should be physically separate from those in a higher security zone and should not be virtualised on the same hardware.		X	X
Use firewalls from different OEM's for the inner and outer firewalls. Preferably from different countries.		X	X
Where possible, implement one way flow between different zones.			X
Block all communication through the firewall that are not required.	X	X	X
All connections between the secure control network and the corporate network shall be though a firewall.	X	X	X
Implement filtering rules in both in-bound and out-bound directions that are equally stringent.	X	X	X
Reduce the number of connections to the outside world where possible – preferably only one redundant pair of firewalls. This allows the system to be easily severed from the corporate network in times of serious cyber incidents.	X	X	X
No systems other than firewalls should be configured with multiple network adapters that span the secure - DMZ or DMZ - corporate networks.	X	X	X
Where possible, connections should be initiated from the more secure zone to the less secure zone.	X	X	X
All rules should be stateful rules that are both IP address and port specific. Stateful rules monitor the handshaking for connection establishment.	X	X	X

DMZ servers with different userbases should be grouped in different zones.		X	X
Where possible, the address portion of the rules should restrict incoming traffic to a very small set of shared devices on the secure network from a controlled set of addresses on the corporate network.	X	X	X
The base rule should be to deny all	X	X	X
Rules between the corporate network and the OT system should be evaluated and permitted on a case-by-case bases before implementation, with documented justification for each permitted incoming and outgoing data flow, responsible person, duration requirement and date implemented. This information should be kept in a secure zone. • All "permit" rules should be both IP address and TCP/UDP port specific, and stateful if appropriate. • All rules should restrict traffic to a specific IP address or range of addresses. • All outbound traffic from the control network to the corporate network should be source and destination-restricted by service and port. • Outbound packets from the control network or DMZ should be allowed only if those packets have a correct source IP address that is assigned to the control network or DMZ devices. • Control network devices should not be allowed to access the Internet or receive email. • Control networks should not be directly connected to the Internet, even if protected via a firewall.	X	X	X
All firewall management traffic should preferably be carried on a separate, secured management network (out of band). Only on-site modification to rules should be allowed. Management traffic should also be restricted by IP address to specific management stations which are in secure zones.		X	X
It is recommended to use static address translation instead of dynamic on firewalls.			X
Protection devices should be configured to fail in a predetermined state. Preferred failure states for systems involve balancing multiple factors including safety and security. Control of the system shall not be compromised if a protection device or a pair of protection devices fail.	X	X	X
Intrusion Detection Systems or Intrusion Prevention Systems should be implemented on the network to monitor traffic from outside the system.			X
All sensitive information (e.g., user account details, network drawings etc.) of the system shall be kept inside the secure perimeter. Documents and information with a suitable classification (non-sensitive) may be given to an auditor for off-premises assessment (for example certain Eskom standards and	X	X	X

OEM procedures to facilitate change of users, etc.) while more critical information should only be made to auditors for viewing on site.			
No third-party software or scripts are to be installed on the control and protection systems without the control system OEM approval and support and would need to follow the Eskom Engineering Change Management processes (only, when the OEM is in support of the change).	X	X	X
SMTP is the primary email transfer protocol on the Internet. Email messages often contain malware, so inbound email should not be allowed to any control network device. Outbound SMTP mail messages from the control network to the corporate network are acceptable for sending alert messages.	X	X	X
If unencrypted data passes through a firewall, deep packet inspection firewalls should be used. NAT should be used on all OT IP addresses visible from the IT network.			X
Equipment that are decommissioned shall be sanitised before disposal. A procedure shall that describes the process shall be available and followed.	X	X	X

3.4.2 Network

Network segmentation involves partitioning the network into smaller networks. For example, one large OT network is partitioned into multiple OT networks, where the partitioning is based on factors such as level of trust, vulnerability, functionality, etc. This can be implemented with VLAN's where firewalls do not have sufficient ports, by logically grouping related VLAN's on a physical port. Different ports on the connected switch are then assigned to specific VLAN's.

Requirement	H	VH	C
Between different segments, the principle of least privilege and need-to-know should be followed. If a system doesn't need to communicate with another system, it should not be allowed to. If a system needs to talk only to another system on a specific port or protocol and nothing else, it should be restricted as such.		X	X
Traffic between zones should be denied by default and allowed by exception.	X	X	X
Implement one-way data flow (data diodes), especially between different security domains where possible.			X
SNMP v1 and v2 should not be used as they are insecure.	X	X	X
Sticky MAC addresses should be configured on network points that are not in physically secure areas or areas manned 24/7 if possible.		X	X
Troubleshooting services and protocols using broadcast messaging should be disabled where possible, as they can be used to facilitate intruders in network exploration.			X

3.4.3 Authentication, Authorisation and Access control

Authentication describes the process of positively identifying potential network users, hosts, applications, services, and resources using a combination of identification factors or credentials. There is flexibility to employ varying protection levels of authentication methods including simple passwords, complex passwords, multi-factor authentication technologies, tokens, biometrics and smart cards. The result of this authentication process then becomes the basis for permitting or denying further actions.

Requirement	H	VH	C
A system must be able to verify that persons being granted access are who they say they are (usually using something the person has, such as an access card or key; something they know, such as a personal identification number (PIN) / password; or something they are, using a biometric device).	X	X	X
Enforce secure authentication of all users seeking to gain access to the system network.	X	X	X
Authentication should be separate from the corporate system and users should have different passwords where applicable and possible, to prevent a compromised corporate username and password to weaken security on the OT system.	X	X	X
Display a legal warning banner on the access point to the system to improve successful prosecution of unauthorised access.	X	X	X
Implement automatic logout of all inactive terminal sessions after an appropriate time	X	X	X
Centralised account management on larger systems with LDAP, Kerberos or AD where credentials for users on servers and workstations are stored. Account management server should preferable be dual redundant, and must be very well protected, preferably in its own zone.		X	X
A user management system such as LDAP or similar should be installed where possible for systems with a large amount of networking equipment that are not managed out of band on an air-gapped network.		X	X
~~P~~asswords should not be sent across any network unless protected by some form of FIPS-approved encryption or salted cryptographic hash designed to prevent replay attacks.	X	X	X
Multi-factor authentication (MFA) should be used for all interactive sessions from outside the system.	X	X	X
Based on a least privilege model, users should be restricted and allowed to only get access to the nodes on the control network necessary for their job function.		X	X
Accounts should be suspended immediately for employees that left the organisation or were suspended and removed after 365 days.	X	X	X

The number of incorrect logins made by someone should be reported, with a suitable time delay between tries should be implemented and account lockout after a set number of failed attempts	X	X	X
Default accounts and passwords on all equipment must be changed before the system goes into commercial operation.	X	X	X
Remote access to the system should comply to the Eskom IT/OT Remote Access Standard and should be VPN-over-VPN or have an additional MFA at the OT system access point.		X	X

3.4.4 Endpoint and server protection

Requirement	H	VH	C
Endpoints and servers should be hardened according to an appropriate standard such as the CIS Benchmark.	X	X	X
Servers should be installed in an appropriate access-controlled server room.		X	X
The user should not use the administrator / root account on endpoints, and only support personnel should have access to these privileged accounts	X	X	X
802.1x security should be implemented on all network points that are not manned 24/7 or in a physical secure server room.		X	X
Application Whitelisting should be implemented to prevent unauthorised applications from executing where possible. As an alternative, a patch management system should be defined and implemented that follows a defined change control process.		X	X
Removable devices i.e., USB and CD-ROM should be disabled in the BIOS and password protected on all endpoints. Where this is not possible, exemptions should be documented with reasons.	X	X	X
The host firewall on all Cyber assets should be configured with strict rules where technically possible.	X	X	X
Sessions should be automatically locked after an appropriate time-out not exceeding 10 minutes, with a password protected screen saver, except in the case of 24/7 staffed desks.	X	X	X
Static IP addresses should be used on the OT network, which can only be changed by an administrator, to prevent equipment being connected to any less secure network and moved back to the secure network.	X	X	X
Applications on servers should be configured to limit the range of ports opened for connection to reduce the range of ports required to be opened on firewalls. The host firewalls should match these required ports.	X	X	X

3.4.5 Physical

Enforcing physical access control to limit authorized access to OT system components is necessary, as many logical controls can be bypassed if physical access is obtained. A system can also be physically disabled if access is obtained. To prevent this, physical access must be controlled and monitored at all times. Access control should be reliable, yet not hinder routine or emergency duties of plant personnel.

Requirement	H	VH	C
Controls for monitoring physical access, maintaining logs, and handling visitors must be in place.	X	X	X
Servers should be placed in locked areas and authentication mechanisms (such as keys, cards and/or biometric) should be in place.	X	X	X
Network devices for the system, including switches, routers, network jacks, servers, workstations, and controllers, should be located in a secured area that can only be accessed by authorized personnel.	X	X	X
The secured area should also be compatible with the environmental requirements of the devices.	X	X	X
Within an area, access to network and computer cabinets should be limited to only those who have a need, such as network technicians and engineers, or computer maintenance staff. Wiring should be neat and within cabinets.	X	X	X
A suitably sized UPS should be provided to ensure power for the system, considering the criticality of the system.		X	X
Backup generators should be provided to provide power to the system during extended power interruptions.		X	X
Heating, ventilation, and air conditioning (HVAC) systems for server and control rooms must support operations during normal conditions as well as during an emergency situation such as a loss of power.		X	X
Fire systems must be carefully designed to avoid causing more harm than good for example to avoid mixing water with incompatible products such as electricity and for gas release systems to avoid damaging spinning disks due to the shock wave. Solid State Disks can be considered as an alternative.		X	X
The management systems of HVAC, fire suppression, access control and access monitoring should be protected to the same level as the systems housed inside the server room.		X	X

Audit requirements for this section:

- Identity Management
  - *Identities, credentials, access permissions and authorisations should be managed and revoked on resignations or role changes*
  - *Physical access should be managed*

- *Remote access should be managed*

- *Awareness and training*
  - *All users should be informed and trained on cyber security and how to identify and escalate potential security issues*
  - *Physical security personnel, privileged users, senior executives and stakeholders should understand roles and responsibilities*
  - *Cybersecurity risks should be actively discussed at Business meetings*
- *Data security*
  - *Data is protected at rest, in transit and against leaks*
  - *Asset management should be managed through removal and transfer*
  - *Integrity checking of software, firmware, hardware and informational*
  - *Development and testing environment should be separate from production environment*
- *Information protection*
  - *System development life cycle should be implemented*
  - *Configuration chance control processes should be in place*
  - *Backups should be done and tested periodically as required*
  - *Incident response and Business continuity plans should be in place (tested?)*
  - *Cyber security should be included in HR practices (deprovisioning and personnel screening)*
  - *Vulnerability management plan / process should be in place (aligned with OEM?)*
  - *Defence in depth protective strategies should be followed*
- *Protective Tech*
  - *Removable media should be protected and use restricted*
  - *Systems should be configured based on least functionality required*
  - *Communication and control networks should be protected*
  - *Protection should be incorporated during design phase of systems*

3.5 Detect

3.5.1 Logical

The security architecture of the system must also incorporate mechanisms to monitor, log, and audit activities occurring on various systems and networks. Additionally, strong system monitoring, logging, and auditing is necessary to troubleshoot and perform any necessary forensic analysis of the system.

Requirement	H	VH	C
Roles and responsibilities for detection and monitoring shall be defined.		X	X
A Security Information and Event Management (SIEM) system should be installed and monitored.			X
A host intrusion detection, a network intrusion system or an anti-malware system should be installed if possible.			X
Detection processes shall be tested by simulating an event that should trigger an alert.			X
Communication channels for communicating a breach should be established and listed in the incident response plan.		X	X
Auditing on servers should be enabled where available.		X	X

3.5.2 Physical

Requirement	H	VH	C
Roles and responsibilities for detection and monitoring shall be defined		X	X
Access monitoring systems include still / video cameras, sensors, and other types of identification systems. These devices do not specifically prevent access to a particular location; rather, they store and record either the physical presence or the lack of physical presence of individuals, vehicles, animals, or other physical entities. They would also deter unwanted access into security zones by use of warning signs and notifications of security monitoring. Adequate lighting should be provided based on the type of access monitoring device deployed.			X
Biometric and card access systems logs shall be logged on a central server and kept for a period of 365 days.			X
Communication channels for communicating a breach should be established		X	X

Audit requirements for this section:

- Anomalies and Events
  - *Network operations and expected data flows should be established*
  - *Any detected events should be analysed to understand attack targets and methods*
  - *Event data should be collected and correlated from multiple sources*
  - *Incident alert threshold should be established*
- *Continuous monitoring*
  - *The network, personnel activity? and physical environment should be monitored to detect potential Cybersecurity events*
  - *There should be detection for malicious code*
  - *External service provider activity should be monitored to detect potential security events*
  - *Monitoring for unauthorised personnel, connections, devices and software should be performed*
  - *Vulnerability scans should be performed*
- *Detection process*
  - *Roles and responsibilities for detection are well defined to ensure accountability*
  - *Detection processes should be tested*
  - *Event detection information's should be communicated to the appropriate parties*
  - *Detection processes should be continuously improved*

3.6 Respond

Requirement	H	VH	C
Employees shall be made aware of what constitutes an incident, and how to react to incidents.	X	X	X
Evidence shall be preserved in the case of a system breach for post event analysis.	X	X	X
The Cyber Security Incident response plan shall be updated within thirty calendar days of any changes.	X	X	X
The test of the response plan shall be at least annually. A test can range from a paper drill, to a full/training operational exercise, to the response to an actual incident.	X	X	X
Cyber Security incidents must be properly investigated by suitably trained and qualified personnel.	X	X	X

Where feasible appropriate actions plans shall be developed to permanently mitigate the risk associated with the Cyber Security Incident or control measures shall be documented and communicated to reduce the risk.	X	X	X
Where feasible, actions to isolate the affected areas shall be taken after Cyber Security Incidents deemed to be critical to the continuous safe operation of the power system.	X	X	X
Cyber Security Incidents shall be reported within 60 days to outside authorities through the authorised channels		X	X
Documentation related to reportable incidents shall be kept for three calendar years.	X	X	X

A written plan (playbooks) documenting the types of incidents and the response to each type should be prepared. This will provide guidance during times when there might be confusion or stress due to the incident.

The response plan should contain the following:

- Roles and responsibilities of the response teams
- Incident handling procedures
- Communication plans
- Reporting structure
- Contingency plans

Audit requirements for this section:

- Response planning
  - *A response plan should exist which could be activated during or after an incident*
- Communications
  - Personnel should know their roles and order of operations when a response is needed
  - Incidents should be reported (to who?)
  - Information should be shared.
  - Coordination with stakeholders should occur during response according to the plan or pre-established criteria
- Analysis
  - Notification from detection systems should be investigated
  - The impact of an incident should be performed
  - Forensics should be performed
  - Incidents should be categorised according to response planning

- Processes should be established to analyse and respond to vulnerabilities disclosed from internal and external sources

- Improvements
  - Response plans should incorporate lessons learned and strategies should be updated
- Response Training
  - Incident response training should be done and tested
- Contingency planning
  - A contingency plan for in case of incidents should be drawn up
  - Alternate site / location for backups should be determined

3.7 Recover

Business continuity planning addresses the overall issue of maintaining or re-establishing production in the case of an interruption. Long-term outages (disaster recovery) and short-term outages (operational recovery) should both be considered.

Recovery actions should be documented so that the system can be returned to normal operations as quickly and safely as possible. Recovery actions for an intrusion that affects operation of the ICS will closely align with the system's Disaster Recovery Plan and should consider the planning and coordination already established.

Requirement	H	VH	C
A comprehensive backup solution should be implemented, including image backups of servers, backups of configuration of equipment and offline backups of critical servers.	X	X	X
Complete and up-to-date logical network diagram should be available	X	X	X

The recovery plan should include the following:

Requirement	H	VH	C
Required response to events or conditions of varying duration and severity that would activate the recovery plan.		X	X
Procedures for operating the system in manual / island mode with all external electronic connections severed until secure conditions can be restored.		X	X
Roles and responsibilities of responders.		X	X
Processes and procedures for the backup, restoration and secure storage of information.	X	X	X
Personnel list for authorized physical and cyber access to the system	X	X	X

Communication procedure and list of personnel to contact in the case of an emergency including vendors, network administrators, support personnel, etc.	X	X	X
Current configuration information for all components.	X	X	X
Information on the safe storage of backups including off-line backups	X	X	X
Information on the safe storage of installation media, license keys, and configuration information where applicable.	X	X	X

4 Acceptance

This document has been seen and accepted by:

Name	Designation
Richard McCurrach	Senior Manager IM Tx
Malcolm Van Harte	Senior Manager Smart Grid Dx
Alison Maseko	Senior Manager – Eskom Telecommunications
Christoph Kohlmeyer	Chief Engineer – Cyber Security Gx
Mervin Mottian	Middle Manager IM
Cornelius Naidoo	Middle Manager – Telecommunications Technology and Support
Nosipho Bodlingwe	Middle Manager Network Operations Dx
Jorge Nunes	Chief Engineer – Control and Instrumentation Gx
Ian Naicker	Chief Engineer – Control and Automation
Bongani Shezi	Chief Engineer
Craig Boesack	Chief Engineer – Control and Instrumentation
Comfort Masike	Senior Manager Technical Operations
Mziwakhe Macina	Senior Advisor Cyber Security Dx
Tsepo Thamae	Senior Advisor Cyber Security Tx
Zanele Fikizolo	Cyber Security CoE Dx
Kgomotso Manyapetsa	Senior Engineer Tx
Quincy Ntuli	CRO IM Operations Tx
Rosalette Botha	Corporate Specialist – System Operator

5 Revisions

Date	Rev.	Compiler	Remarks
January 2016	2	Reshin Moodley	First update
February 2013	1	Johan Botha	Initial version

6 Development Team

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

- Meenal Vala

Annex A

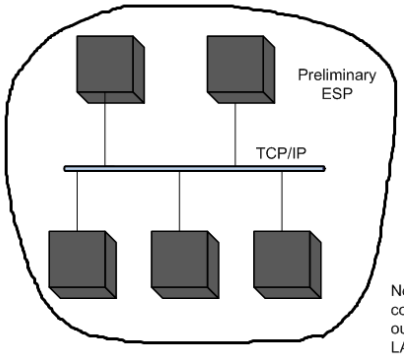


Figure.1: Drawing 1

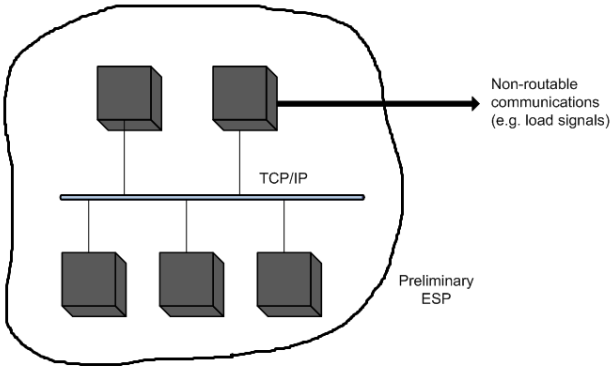


Figure.2: Drawing 2

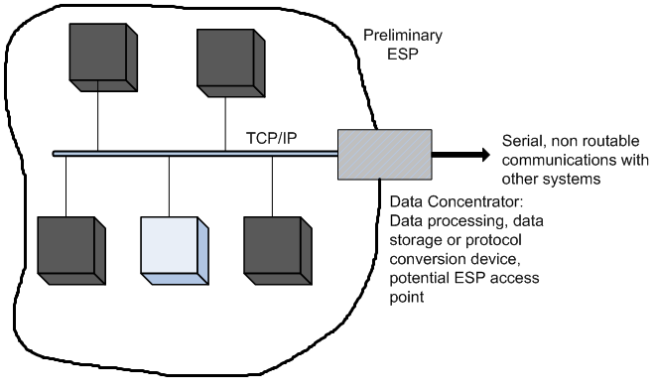


Figure 3: Drawing 3

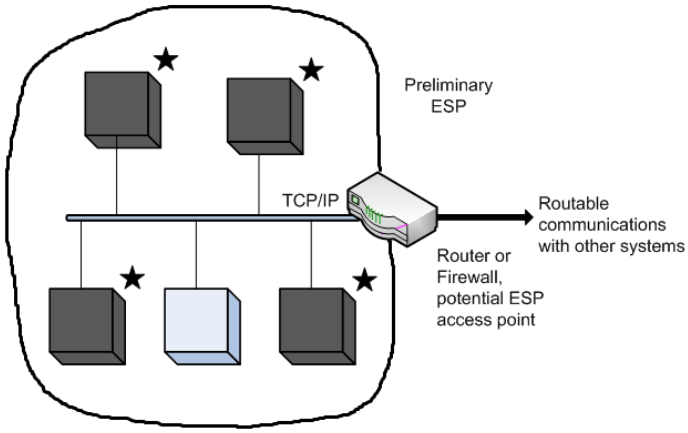


Figure.4: Drawing 4

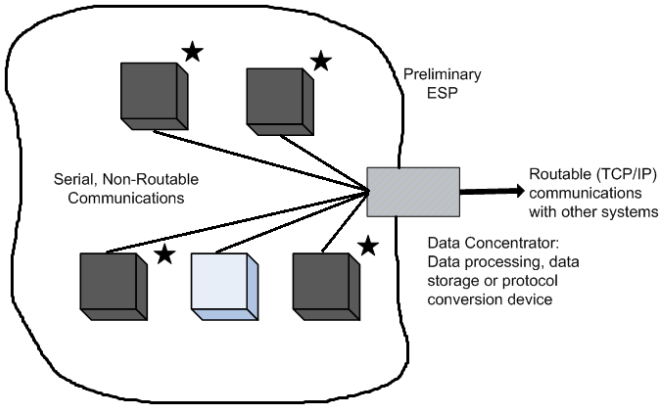


Figure.5: Drawing 5

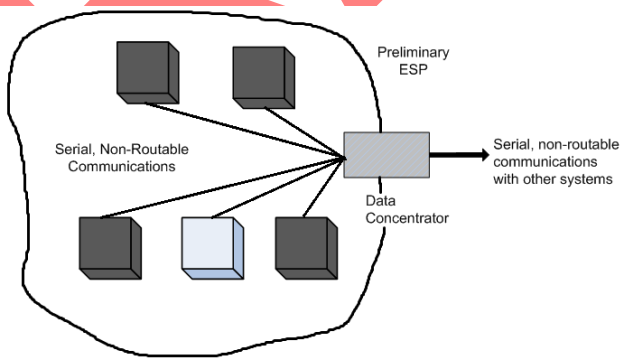


Figure.6: Drawing 6

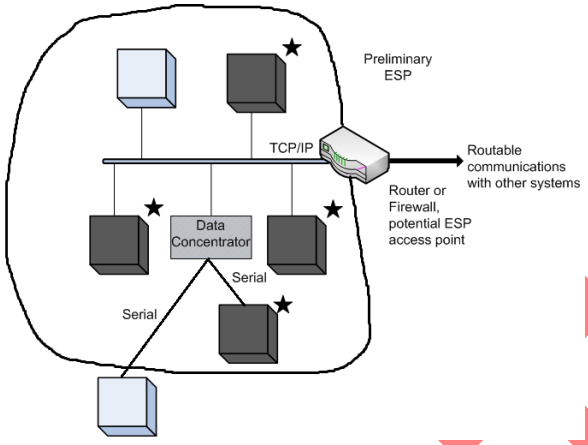


Figure.7: Drawing 7

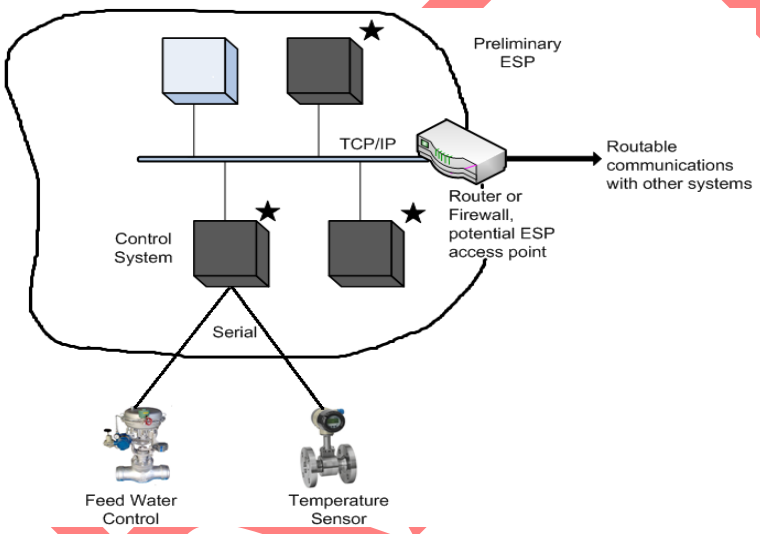


Figure.8: Drawing 8

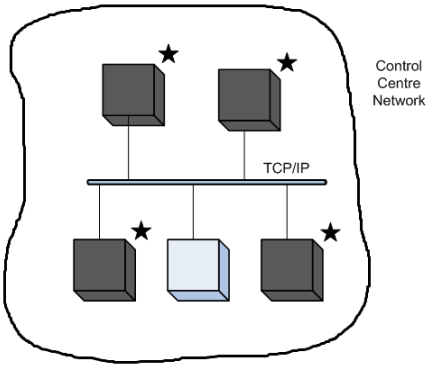


Figure.9: Drawing 9

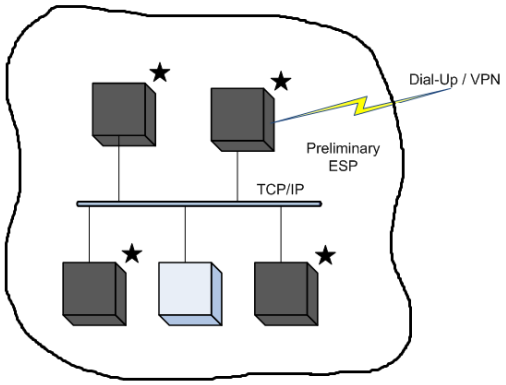


Figure.10: Drawing 10

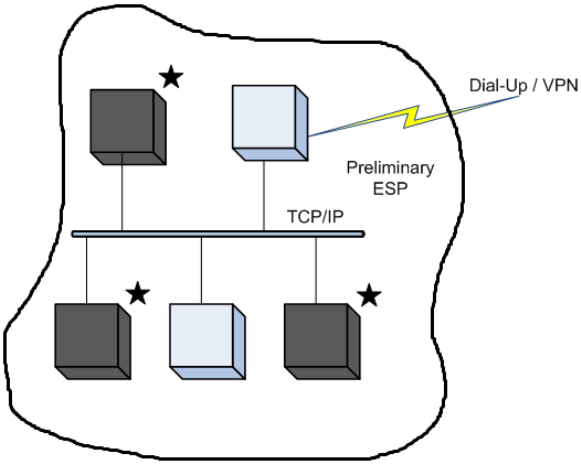


Figure.11: Drawing 11

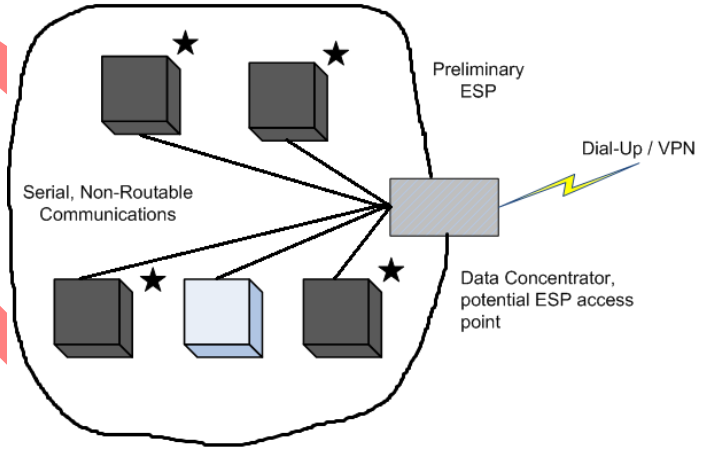


Figure.12: Drawing 12