Eskom	**Standard**	**Technology**

Title: **CYBER SECURITY STANDARD FOR OPERATIONAL TECHNOLOGY**

Unique Identifier:	**240-55410927**
Alternative Reference Number:	**<n/a>**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**2**
Total Pages:	**38**
Next Review Date:	**February 2021**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	**Approved by**	**Authorized by**
Reshin Moodley	**Richard McCurrach**	**Danie Odendaal**
Chief Engineer	**Senior Manager – PTM&C**	**SGM Engineering (Acting)**
Date: 21/01/2016	Date: 21/1/2016	Date: 29/1/2016
Accepted by	**Accepted by SCOT**	**Supported by SCOT/SC**
Sean Maritz	**Rob Stephen**	**Philip Groenewald**
Acting CIO Information Technology	**SCOT Chairperson**	**Smart Grid Technology SC Chairperson**
Date: 26/01/2016	Date: 25/01/2016	Date: 21/01/2016

PCM Reference: **Develop Functional Architecture**

SCOT Study Committee Number/Name: **Smart Grid Technology**

Content

Page

Executive Summary 5
1. Introduction 6
2. Supporting clauses 6
2.1 Scope 6
2.1.1 Purpose 7
2.1.2 Applicability 7
2.2 Normative/informative references 7
2.2.1 Normative 7
2.2.2 Informative 7
2.3 Definitions 7
2.3.1 General 7
2.3.2 Disclosure classification 8
2.4 Abbreviations 9
2.5 Roles and responsibilities 10
2.6 Process for monitoring 10
2.7 Related/supporting documents 10
3. Requirements for OT Cyber Security Management 10
3.1 Sabotage Reporting 10
3.2 Critical Cyber Asset Identification 10
3.2.1 Critical Asset Identification Method 12
3.2.2 Identify Cyber Assets Associated with Critical Assets 13
3.2.3 Identify Critical Cyber Assets 14
3.3 Security Management Controls 18
3.3.1 Leadership 18
3.3.2 Exceptions 18
3.3.3 Information Protection (3) 18
3.3.4 Change Control and Configuration Management (3) 18
3.4 Personnel and Training 19
3.4.1 Awareness (3) 19
3.4.2 Training (3) 19
3.4.3 Personnel Risk Assessment (3) 20
3.4.4 Access to Evidence (3) 20
3.5 Cyber Security — Electronic Security Perimeter(s) 20
3.5.1 Electronic Security Perimeter 20
3.5.2 Electronic Access Controls 21
3.5.3 Monitoring Electronic Access 22
3.5.4 Cyber Vulnerability Assessment 23
3.5.5 Documentation Review and Maintenance 23
3.6 Cyber Security — Physical Security of Critical Cyber Assets (2) 23
3.6.1 Physical Security Plan 24
3.6.2 Protection of Physical Access Control Systems 24
3.6.3 Protection of Electronic Access Control Systems 24
3.6.4 Physical Access Controls (1) 24
3.6.5 Monitoring Physical Access (2) 25

3.6.6 Logging Physical Access (2) 25
3.6.7 Access Log Retention (2) 25
3.6.8 Maintenance and Testing (2) 25
3.7 Cyber Security — Systems Security Management 25
3.7.1 System Design and Configuration 25
3.7.2 System Maintenance and Operation 27
3.7.3 Malicious Software Prevention 27
3.7.4 Account Management 27
3.7.5 Security Patch Management 29
3.8 Cyber Security – Incident Reporting and Response Planning 29
3.8.1 Cyber Security Incident Response Plan (3) 29
3.8.2 Cyber Security Incident Documentation (2) 29
3.9 Recovery Plans for Critical Cyber Assets 30
3.9.1 Recovery Plans (2) 30
3.9.2 Exercises (3) 30
3.9.3 Recovery Plan Change Control (3) 30
3.9.4 Backup and Restore 30
3.9.5 Testing Backup Media (3) 30
4. Additional considerations 30
4.1 Outsourcing 30
4.2 NEW Project Implementation 31
5. Authorization 33
6. Revisions 33
7. Development team 34
8. Acknowledgements 34
Annex A – Interpretation of Connectivity Requirements 35

Figures

Figure 1: Critical Cyber Asset Identification 11
Figure 2: Definition of Risk 12
Figure 3: Process to identify Critical Cyber Assets 15
Figure A.1: Drawing 1 35
Figure A.2: Drawing 2 35
Figure A.3: Drawing 3 35
Figure A.4: Drawing 4 36
Figure A.5: Drawing 5 36
Figure A.6: Drawing 6 36
Figure A.7: Drawing 7 37
Figure A.8: Drawing 8 37
Figure A.9: Drawing 9 37
Figure A.10: Drawing 10 38
Figure A.11: Drawing 11 38
Figure A.12: Drawing 12 38

Tables

Table 1: Example of Cyber Asset Inventory List 16

Executive Summary

Exploitation of vulnerabilities in computer systems has been growing in frequency and impact for the last decade. Forms of cyber-terrorism have also occurred where industrial systems were deliberately targeted. Detailed security policies and standards need to be formulated and implemented to ensure that the Operational Technology networks and systems in Eskom are protected.

From a security perspective, the management of Eskom’s Operational Technology network resources are critical. Weaknesses in network infrastructure and the associated protocols used within these areas are prone to being exploited if employee and management vigilance is not active at all times. Global IT and interconnected systems, expose operational systems of utilities to attacks and Eskom is not exempt from such risks, hence the need to monitor and track vulnerabilities continuously. The success of any security standard implementation hinges on constant review, testing, updating and re-formulating the necessary strategies as issues and risks are encountered.

1. Introduction

This standard serves to guide the implementation of Cyber Security Principles in the Operational Technology (OT) environment. Although there is a convergence between Operation Technology and Information Technology, the standard practices of Information Technology (IT) are not directly applicable to OT, as OT generally requires stricter access control of external information, and the compromise of such information could have a greater impact. Furthermore, due to the lifespan of OT systems, they run for many years after support ends and for these reasons IT security policies can normally not be implemented in the OT environment without major modification.

This standard applies to the Operational Technology environment where there are Cyber Assets installed. This standard divides Cyber Assets according to criticality, and defines rules for protecting the different types. Critical Cyber Assets are cyber assets essential to the reliable operation of critical assets. OT System Owners should ensure the systems they are responsible for adheres to the requirements in the standard, and to justify deviations where adherence could not be achieved.

The statements in the document were assigned numbers to indicate criticality, where 1 is most critical, 2 is less critical and 3 is least critical. The purpose of this assignment is, during implementation, to put focus on the most critical areas first to ensure the highest risks are addressed quickly.

2. Supporting clauses

2.1 Scope

The primary aim of this document is to provide guidance on implementing an acceptable level of protection against cyber intrusions and malware in Operational Technology environments within Eskom.

Operational Technology (OT) Systems are defined as follows in the Definition of operational technology (OT) and OT / IT collaboration accountabilities document [2]:

“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 and Programmable Local Controller equipment, which extract signals and measurements from the plant / network asset or its control environment, or facilitate control over the 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 the Eskom business continuity is not affected due to any cyber type of incident. It is recognised that there is a difference in the operation and risks associated with the technical assets of the business, as compared to the conventional Information Technology systems. Although there is increasing convergence of the IT technology utilised in both systems, there are unique differences in its application in the Operational Technology systems, and they require a dedicated security approach as described in this Standard.

2.1.2 Applicability

This document shall apply to the 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.

2.2.1 Normative

[1] ISO 9001, Quality Management Systems.

[2] 240-55863502: Definition of Operational Technology (OT) and OT/IT collaboration accountabilities

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

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

2.2.2 Informative

[5] 240-91479924: Cyber Security Configuration Guideline of Networking Equipment for Operational Technology

[6] 32-85: Information security Policy

[7] 32-644: Eskom document management standard

[8] 204-53114002: Engineering Change Management Procedure

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

[10] National Key Point Act - – South African National document

2.3 Definitions

2.3.1 General

Definition	Description
Confidential	The classification given to information that may be used by malicious/opposing/hostile elements to harm the objectives and functions of Eskom Holdings SOC Limited.

Definition	Description
Critical Asset	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the electricity supply network.
Critical cyber assets	Cyber assets essential to the reliable operation of critical assets.
Cyber Asset	Programmable electronic devices and communication networks including hardware, software, and data.
Cyber Security	Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: • Availability • Integrity, which may include authenticity and non-repudiation • Confidentiality
Logical Access	Being able to interact with data through access control procedures such as identification, authentication and authorization.
Non-routable Protocol	A communications protocol that contains only a device address and not a network address. It does not incorporate an addressing scheme for sending data from one network to another.
Operational Technology (OT)	OT is the technology that is used to operate, monitor and control the power system. For a more specific definition refer to the OT Practice Note [2]
Physical access	Being able to physically touch and interact with the computers and network devices.
Public domain	Published in any public forum without constraints (either enforced by law, or discretionary).
Risk	Is a function of impact or consequences and the probability of occurrence
Routable Protocol	A communications protocol that contains a network address as well as a device address. It allows packets to be forwarded from one network to another.
Secret	The classification given to information that may be used by malicious/opposing/hostile elements to disrupt the objectives and functions of Eskom Holdings SOC Limited.
System Owner	The system owner, is the authorised Eskom representative that has overall accountability for the OT system in which the cyber asset resides
Top Secret	The classification given to information that may be used by malicious/opposing/hostile elements to neutralize the objectives and functions of Eskom Holdings SOC Limited.
Vulnerability	Is a weakness that can be accidentally triggered or intentionally exploited

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
AES	Advanced Encryption Standard
B2B	Back to Basics
CD	Compact Disc
CIP	Critical Infrastructure Protection
DDS	Detailed Design Specification
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS **DR**	Dynamic Name Server Disaster Recovery
DVD	Digital Versatile Disc
ESP	Electronic Security Perimeter
FAT	Factory Acceptance Test
FDS	Functional Design Specification
GPRS	General Packet Radio Service
GUI	Graphical User Interface
HMI	Human Machine Interface
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
MW	Megawatt
NAT	Network Address Translation
NERC	North American Reliability Council
OS	Operating System
OT	Operational Technology
SAT	Site Acceptance Test
SCSI	Small Computer System Interface
TCP	Transport Control Protocol
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 from time to time as required, as the review of Eskom's corporate strategy and as functional IT, OT, Technology and Smart Grid strategies evolve.

2.7 Related/supporting documents

This Standard is based on the requirements defined in the NERC Critical Infrastructure Protection (CIP) guidelines. Eskom specific requirements have been tailored to the Eskom environment, however the intent remains the same. As these CIP guidelines are updated from time to time, they will be periodically reviewed to assess if specific changes to the standard are required.

Standard CIP-001-1 — Sabotage Reporting

Standard CIP–002–3 — Cyber Security — Critical Cyber Asset Identification

Standard CIP–003–3 — Cyber Security — Security Management Controls

Standard CIP–004–3 — Cyber Security — Personnel and Training

Standard CIP–005–3 — Cyber Security — Electronic Security Perimeter(s)

Standard CIP-006-3c — Cyber Security — Physical Security

Standard CIP–007–3 — Cyber Security — Systems Security Management

Standard CIP–008–3 — Cyber Security — Incident Reporting and Response Planning

Standard CIP–009–3 — Cyber Security — Recovery Plans For Critical Cyber Assets

Security Guideline for the Electricity Sector: Identifying Critical Assets

Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets

3. Requirements for OT Cyber Security Management

3.1 Sabotage Reporting

Sabotage reporting is the responsibility of the Group Security Department in Eskom. All OT environments shall comply with the Corporate Security Department policies, processes, standards and procedures regarding sabotage / incident reporting.

a) Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate level of authority within Eskom.

b) *System Owners* shall provide its operating personnel with a sabotage / incident response guideline or procedure, including personnel to contact, for reporting disturbances due to sabotage events.

3.2 Critical Cyber Asset Identification

To enable an appropriate security framework for the monitoring and protection of Critical Assets needed to support reliable operation of the electricity supply network, it is required that a comprehensive identification process be followed to capture and record all critical cyber assets.

a) The system owner shall identify the list of critical cyber assets by using the Critical Cyber Asset Identification method prior to putting of the cyber asset in operation. This information shall be formally recorded for control purposes.

b) The *system owner* shall review the list of critical cyber assets annually and after changes in the operating environment or changes to the cyber asset.

c) The *system owner* shall retain an audit trail of the reviews.

The process below outlines the identification of Cyber Assets associated with its Critical Assets detailed in section 3.2.2 and to determine if these Cyber Assets are Critical Cyber Assets detailed in section 3.2.3. The process described consists of the following four steps:

1) Using the risk base assessment criteria, identify your critical Asset
2) Identify Cyber Assets associated with a critical asset
3) Determine Cyber Assets which are essential for operation of critical asset
4) Compile a list of critical cyber assets

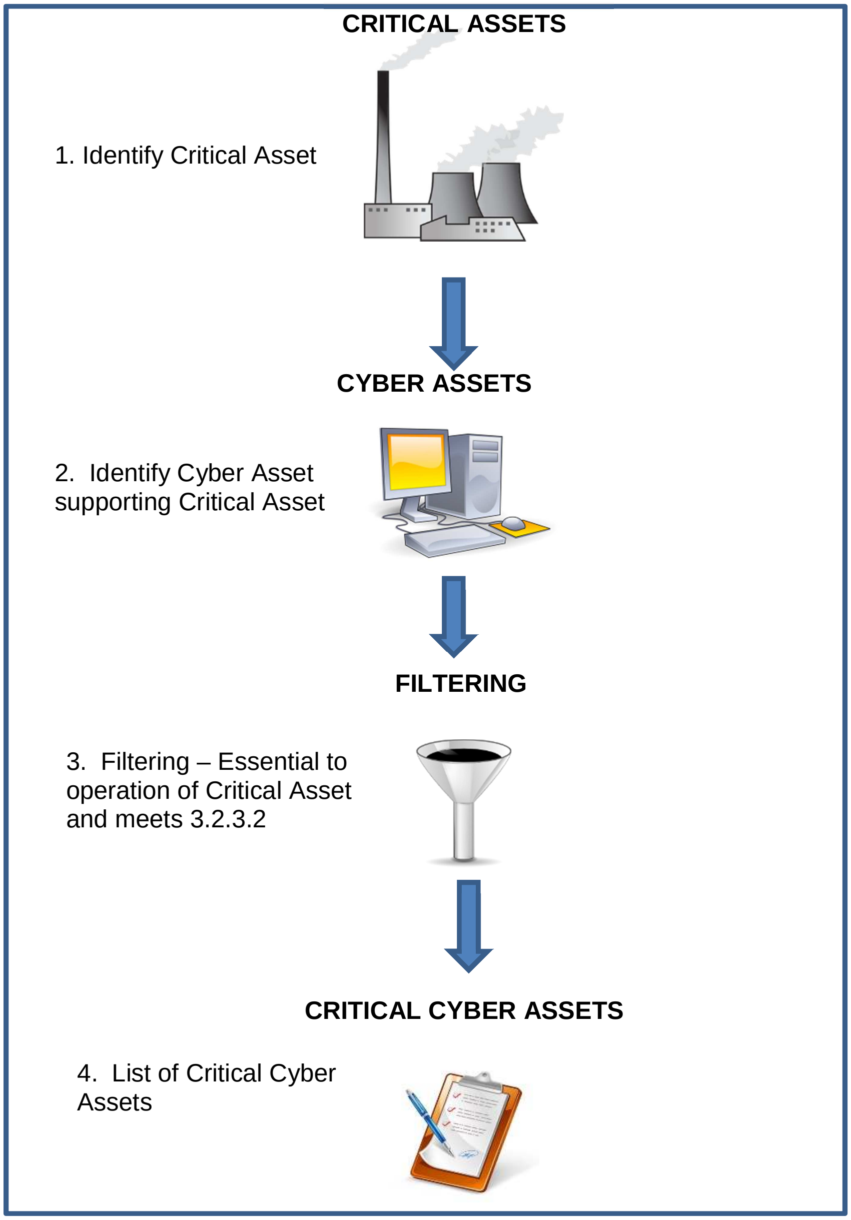

CRITICAL ASSETS
1. Identify Critical Asset
CYBER ASSETS
2. Identify Cyber Asset supporting Critical Asset
FILTERING
3. Filtering – Essential to operation of Critical Asset and meets 3.2.3.2
CRITICAL CYBER ASSETS
4. List of Critical Cyber Assets

Figure 1: Critical Cyber Asset Identification

3.2.1 Critical Asset Identification Method

3.2.1.1 Risk Base Assessment

The criticality of OT systems can be identified by evaluating its risk exposure (impact and probability) on the ability of Eskom to supply electricity.

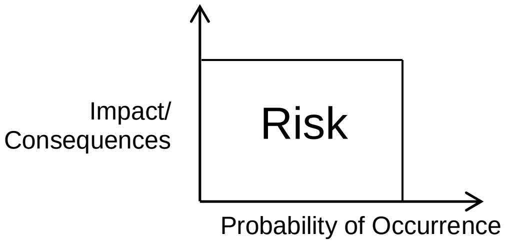


Figure 2: Definition of Risk

While traditional risk assessment normally considers both the probability of the loss of an asset and the impact or consequences if the asset is lost, this approach to critical Asset identification considers that the asset has been lost. This approach assumes that the potential for threats and vulnerabilities always exist (i.e, the probability of occurrence =1). The risk- based assessment essentially becomes an impact analysis.

Electricity supply assets to be evaluated against the risk-based criteria below may include facilities, systems, or equipment such as:

- Control centres and backup control centres
- Distribution and Transmission substations
- Generation resources
- Telecommunication control and backup centres.
- Supervising and control capability systems
- Systems and facilities critical to the power system restoration, such as blackstart
- Automatic load shedding schemes and special protection systems
- Situational awareness systems
- Any additional assets that support the reliable operating, control and protection of the power system.

If, the specific OT system, or group of systems sharing common technology, under consideration, it is identified that one or more of the following situations could occur due to the OT systems being compromised or have unplanned unavailability, it would be regarded as a Critical System.

- Result in immediate production losses on multipe Generating units involving a total capacity of ≥ 1 000 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.
- 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 500 MW production for > 1 week
- Interruption of the power delivery equivalent of 50MW on the network, resulting in customer loss of supply > 12hrs

- Compromise of a generation facility's ability to perform black starting
- Seriously injure or kill one or more persons
- Result in a significant environmental contravention situation
- Reduction of life of a significant plant Asset (value ≥ R250 million) by > 20%
- Significantly violating National legislation, policy, licence or permit conditions
- Increasing the longer term production costs of a plant by >20%
- 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 ≥ two weeks
- Compromise the integrity of, or alter in any way the protection devices, functions, settings or philosophy of significant plant
- Loss in the ability to perform emergency switching according to the definitions of the Plant Safety Regulations and the Operating Regulations for High Voltage Systems
- Initiate the activation of disaster recovery/management plans at an Eskom site
- Under certain situations, auxiliary systems that support Critical Assets should also be considered as critical – these include the access control systems, fire detection systems, power supply systems etc.

3.2.2 Identify 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.

a) The *system owner* shall Identify Cyber Assets associated with the operation of each identified Critical Asset.

b) This is not intended to be a complete inventory or 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.

Cyber Assets that should be considered include, at a minimum:

- Control systems comprising devices or sets of devices that act to manage, command, or regulate the behaviour of processes, devices, or other systems
- Data acquisition systems comprising collections of sensors and communication links that act to sample, collect, and provide data regarding the facility's systems to a centralised location for display, archiving, or further processing
- Networking equipment including devices such as routers, hubs, switches, firewalls, and modems
- Hardware platforms running virtual machines or virtual storage

When identifying Cyber Assets, the *system owner* should consider the different roles and functions that Cyber Assets play which could impact the reliable operation of a Critical Asset such as:

- Provides operation information in Real-time
- Controls manual or automated parameters
- Calculates parameters or limits
- Generates or displays prompts or alarms to an operator
- Provides connectivity between Cyber Assets
- Supports continuity of operations of the Critical Assets or local recovery plans

Consideration of Cyber 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 suggested. 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) and alarm systems

3.2.3 Identify Critical Cyber Assets

3.2.3.1 Determine 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.

3.2.3.2 Identifying Cyber Assets with Qualifying Connectivity is a Critical Cyber Asset

If this 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; 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 center; or,
- The Cyber Asset is accessible via dial-up or a Virtual Private Network (VPN).

If supporting systems are within the same Electronic Security Perimeter (ESP) as a Critical Cyber Asset, they must be afforded the same protection. Redundancy may increase the opportunity for a successful Cyber-attack, each Critical Cyber Assets and redundant Critical Cyber Asset should also be protected under this standard.

See Annexure A for diagrams illustrating which cyber assets are regarded as critical cyber assets in various scenarios:

The following Diagram as per figure 3 below, represents the process flow for Identifying Critical Cyber Assets.

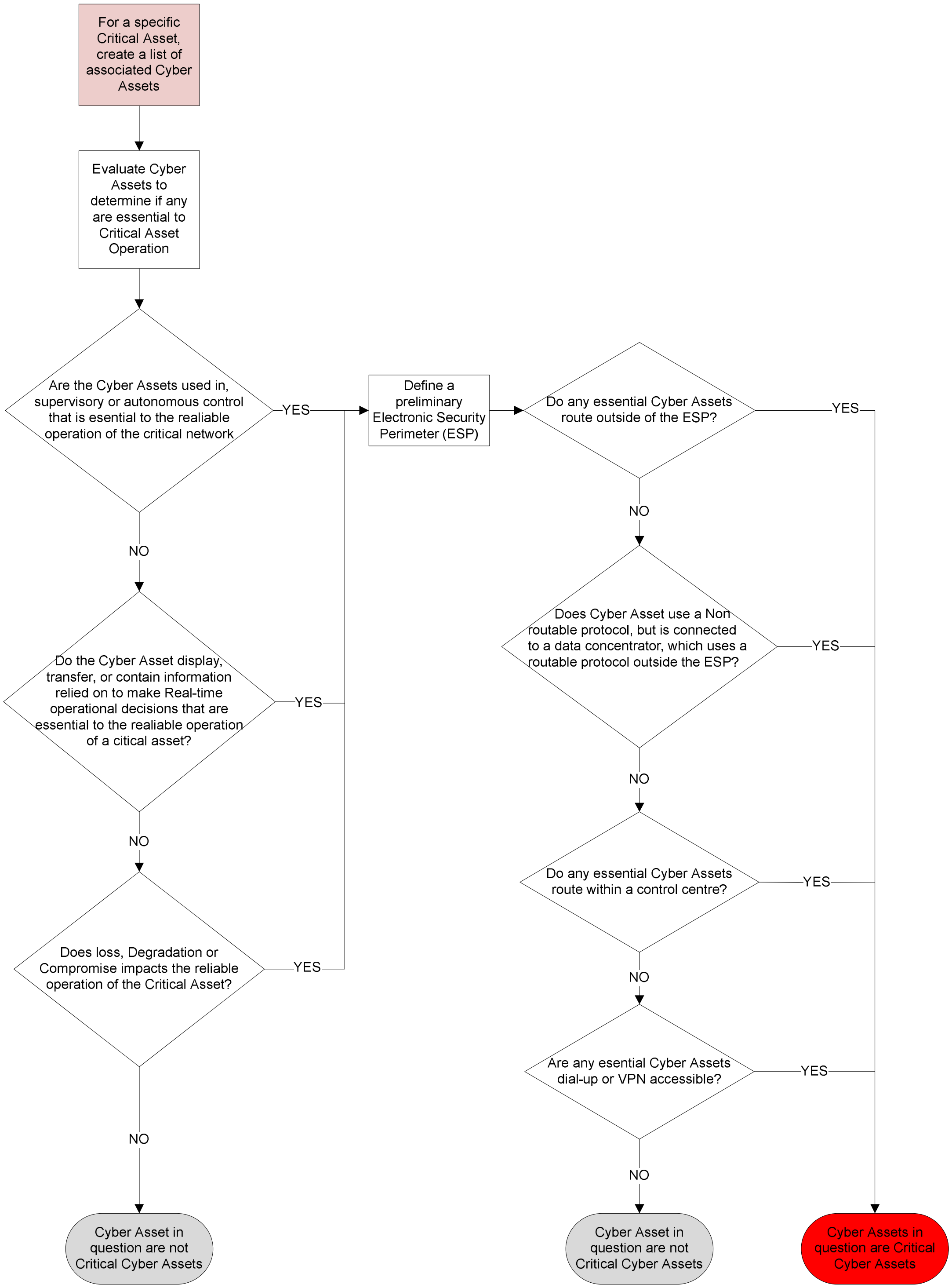

For a specific Critical Asset, create a list of associated Cyber Assets
Evaluate Cyber Assets to determine if any are essential to Critical Asset Operation
Are the Cyber Assets used in, supervisory or autonomous control that is esential to the realiable operation of the critical network
YES
NO
Do the Cyber Asset display, transfer, or contain information relied on to make Real-time operational decisions that are essential to the realiable operation of a citical asset?
YES
NO
Does loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?
YES
NO
Cyber Asset in question are not Critical Cyber Assets
Define a preliminary Electronic Security Perimeter (ESP)
Do any essential Cyber Assets route outside of the ESP?
YES
NO
Does Cyber Asset use a Non routable protocol, but is connected to a data concentrator, which uses a routable protocol outside the ESP?
YES
NO
Do any essential Cyber Assets route within a control centre?
YES
NO
Are any esential Cyber Assets dial-up or VPN accessible?
YES
NO
Cyber Asset in question are not Critical Cyber Assets
Cyber Assets in question are Critical Cyber Assets

Figure 3: Process to identify Critical Cyber Assets

EXAMPLE OF CYBER ASSET INVENTORY LIST

Table 1: Example of Cyber Asset Inventory List

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
Transmission Substation	Remote Terminal Unit	Provides input monitoring and control for SCADA	Yes	Yes	Yes	No	No	No	No	No
Transmission 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	No	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	Manages the BME connections	Yes	Yes	Yes	Yes	No	Yes	No	Yes

	Server									
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

3.3 Security Management Controls

3.3.1 Leadership

a) The System Owner shall be responsible for the implementation of the Cyber Security Standard for Operational Technologies.

3.3.2 Exceptions

a) Any deviation from the Cyber Security Standard for Operational Technology must be approved by the, Security Architecture Authority (SAA) in the context of the design and supported by the Generation or PTM&C **Design Review Team (DRT)**. The exception must be documented, by the *system owner* and include an explanation as to why the exception is necessary and any compensating measures that was put in place to mitigate possible risk.

b) Authorised exceptions to the OT cyber security standard shall be reviewed and approved annually by the Security Architecture authority (SAA) in the context of the design and supported by the Generation or PTM&C **Design review Team (DRT)** to ensure the exceptions are still required and valid. Such review and approval shall be documented.

3.3.3 Information Protection (3)

a) The *system owner* shall be responsible to identify, classify, and protect information associated with Critical Cyber Assets.

b) The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists of Critical Cyber Assets, network topology or similar diagrams, floor plans of computing centres that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

c) The *system owner* shall classify information to be protected based on the sensitivity of the Critical Cyber Asset information

d) The *system* owner shall be responsible to manage access to protected critical cyber asset information. This shall include:

- maintaining a list of designated personnel, by name and title, for authorising logical or physical access to protected information,
- the information the designated personnel can authorise access on.

e) The system owner shall review the list of designated personnel annually.

f) The designated personnel shall review the list of granted access privileges annually.

3.3.4 Change Control and Configuration Management (3)

Changes to critical cyber asset hardware or software shall be performed according to a formal change control procedure. The change control procedure shall ensure that supporting configuration management activities to identify control and document all Eskom or supplier related changes to hardware and software components of critical cyber assets are reviewed for relevancy and impact (business, technical and financial).

a) At a minimum, the change control procedure for planned changes shall include:

- a description of the proposed change,
- test procedure and roll-out plan and fall-back plan,
- test results of testing in a non-production environment,
- results from commissioning.

- time & duration to implement the change
- the risk the system is exposed to in implementing the change

b) Change control shall follow the Engineering Change Management Process [8]. The change control shall take into consideration breakdown versus planned maintenance.

c) Changes to a critical cyber-asset shall follow the accepted engineering practice for testing, and approval before implementation.

d) Any software change and/or update shall be controlled, where available, with version control and/or supporting documentation.

e) Fall-back procedures for aborting and recovering from unsuccessful changes shall be available and/or communicated.

f) Emergency changes shall be recorded.

g) The documentation for critical cyber assets shall be current, and shall be kept in the same secure environment or better than that of the cyber asset, and may be kept on the device if a backup device is in place.

h) The decommissioning of any cyber asset shall follow only after verifying that the cyber asset is no longer required or an upgrade/replacement is being installed. The decommissioning procedure shall include the removal of software and information available from the cyber asset. Sensitive software and information shall be securely removed.

i) The use of live data for testing new system or system changes may only be permitted where adequate controls for the security of the data are in place.

3.4 Personnel and Training

It is required that personnel having authorised cyber or authorised unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness prior to being granted access to the system.

3.4.1 Awareness (3)

The *System Owner* shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorised cyber or authorised unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.

a) Personnel security responsibilities shall support the Conditions of Service and ensure compliance during an individual’s employment.

b) Users’ cyber asset security roles and responsibilities shall be documented by the *System Owner*.

c) An OT cyber security awareness program shall be implemented to ensure personnel receive on-going reinforcement in sound security practices on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

3.4.2 Training (3)

An OT Cyber Security training program shall be documented, implemented, and maintained for personnel having authorised cyber or authorised unescorted physical access to Critical Cyber Assets.

a) The attendance records and date the training, at least annual, was completed shall be kept for at least one year by the *System Owners*.

b) Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets, and include, the following required items appropriate to personnel roles and responsibilities:

- The proper use of Critical Cyber Assets;
- Physical and electronic access controls to Critical Cyber Assets;
- The proper handling of Critical Cyber Asset information; and,
- Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

3.4.3 Personnel Risk Assessment (3)

a) New employees' references must be verified.

b) Employees, including contractors and service vendors, with authorised cyber or authorised unescorted physical access to Critical Cyber Assets must be vetted through the Eskom vetting process at least every five years after the initial vetting or for cause.

c) The line Manager shall be accountable to ensure the user's access is revoked on notification of resignation or change of job or responsibilities,

d) The System Owner can request the risk assessment / vetting of employees with access to the system to be reviewed.

3.4.4 Access to Evidence (3)

a) The *System Owner* shall have action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security/major incident. These action plans shall ensure that evidence / logs are kept in an unaltered state by cloning the data / machine onto a write-once DVD/ external hard drive, or similar procedure.

b) Where Eskom has reasonable grounds to suspect that its security has/is being compromised, Eskom reserves the right to:

- Intercept and peruse any data sent, received or stored by an employee (including any attachment thereto) and to monitor the use of its cyber asset including, but not limited to, hard drives, network drives and other computing systems.
- Conduct inspections of the cyber asset without advance notice to the employees,
- Examine the contents of any cyber asset that contains or is thought to contain Eskom information, including computers that have been purchased by the employees in their personal names and/or capacities.

3.5 Cyber Security — Electronic Security Perimeter(s)

3.5.1 Electronic Security Perimeter

System owners shall identify the Electronic Security Perimeter of their systems. Any access point to the system with a routable protocol crossing the perimeter will be an access point into the system.

a) Access points to the Electronic Security Perimeter can be dial-up modems or VPNs used to retrieve information or to perform maintenance and configuration on equipment. These remote access connections shall comply with the Information Security – IT/OT Remote Access Standard [3]. (1)

b) All of these access points shall be documented. Any 3G type connections shall also be through a VPN to a central point, where user authentication is done before access is granted to a remote 3G device. All 3G devices shall use an Eskom approved APN and traffic on the 3G network shall be encrypted. Any SIM card shall be locked to the device it is assigned to, to ensure a lost SIM cannot be used by a third party. (2)

c) Dial-up connections shall be from a central point. The remote modem shall only answer calls from authorised pre-programmed numbers. (2)

d) A user shall only have access to devices he is authorised to connect to. (1)

e) Logs should be sent to a log server, and usernames and passwords shall be managed through AAA and a TACACS or radius server. (2)

f) Serial communication links are not considered access points, as they use a non-routable serial protocol, as long as both sides of the link fall within an Electronic Security Perimeter.

g) For a Master Station or a Data Centre where data or information is accessed by individuals or systems outside the Electronic Security Perimeter, a Demilitarized Zone (DMZ) [4] shall be established. (1)

h) No Critical Cyber Asset shall reside in the DMZ. (1)

i) No Cyber Asset on the internal secure network shall be directly accessible from a system outside the Electronic Security Perimeter. (1)

j) 802.11 Wi-Fi and Bluetooth networks shall not be used on the Networks in the Electronic Security Perimeter, as it reduces security by eliminating the possibility of implementing physical security to the Cyber Security Perimeter. (1)

k) Where Wireless networks such as GPRS are used for telecommunications, the information shall be encrypted on the link layer with at least 128 bit AES. (2)

l) All cyber security logs, configuration, network layouts, procedures, Disaster Recovery (DR) Plans shall remain within a Secure Perimeter and shall be referenced in external documents with the same document classification. (1)

m) Where no DMZ is implemented, and ad-hoc connections out of or into the electronic security perimeter are required, perimeter firewalls should be opened and then immediately closed, after completion, instead of leaving them open. The firewall shall only allow access from / to the required source / destination on the required port. (1)

3.5.2 Electronic Access Controls

The *System Owner* shall implement and document the organisational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

a) These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified. (1)

b) At all access points to the Electronic Security Perimeter(s), the *System Owner* shall enable only ports and services required for operations and shall document, individually or by specified grouping, the configuration of those ports and services. (1)

c) Where external interactive access into the Electronic Security Perimeter has been enabled, the System Owner shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible. (2)

d) Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within the Electronic Security Perimeter. (1)

e) The required documentation shall, at least, identify and describe: (3)

- The processes for access request and authorization.
- The authentication methods.
- The review process for authorization rights.
- The controls used to secure VPN access connections.

f) Devices that are capable of configuring a banner shall contain a banner similar to the following: (3)

```
*********************************************************************************************************
         *                                                                               *
  *   WARNING  Access to this system is restricted to Authorized Personnel only        *
         *                                                                               *
  *   Terminate this session immediately if this system has been accessed in error    *
         *                                                                               *
       *   You are warned:                                                                 *
         *                                                                               *
  *    a) That unauthorised access to or modification of information held in this      *
         *     system,                                                                   *
         *     and/or;                                                                   *
  *    b) Unauthorised copying of software; shall render you liable to civil damages   *
    *     and/or criminal penalties in South Africa and other countries;               *
       *     and;                                                                        *
  *    c) That all sessions on this system are monitored, logged and recorded.          *
         *                                                                               *
    *   By continuing with this session you represent and warrant that you are        *
           *    authorised to access this system.                                    *
             *                                                                     *
*********************************************************************************************************
```

3.5.3 Monitoring Electronic Access

The System Owner shall implement and document a process for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

a) For dial-up accessible Critical Cyber Assets that use non-routable protocols, the System Owner shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible. (2)

b) Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the System Owner shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days. (2)

c) Firewall rules allowing access from outside the Electronic Security Perimeter should be set to at least log successful logins and failed attempts. (2)

d) All firewall rules shall have the identity of the person making the change, the date implemented, and the reason for the change in the description field. (1)

3.5.4 Cyber Vulnerability Assessment

Where technically feasible the System Owner shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least every 3 years. The vulnerability assessment shall include, as a minimum, the following:

a) A document identifying the vulnerability assessment process; (3)

b) A review to verify that only ports and services required for operations at these access points are enabled; (1)

c) The discovery of all access points to the Electronic Security Perimeter; (1)

d) A review of controls for default accounts, passwords, and network management community strings; (1)

e) Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan. (1)

3.5.5 Documentation Review and Maintenance

The System Owner shall review, update, and maintain all documentation to support compliance with the requirements of this OT Cyber security standard.

a) The System Owner shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change. (1)

b) The System Owner shall retain electronic access logs for at least ninety calendar days. (2)

3.6 Cyber Security — Physical Security of Critical Cyber Assets (2)

The facilities chosen to locate information resources and to store data must be suitably protected from physical intrusion, theft, fire, flood and other hazards.

a) Information resources premises must be safeguarded against unlawful and un-authorised physical intrusion.

b) When locating information resources and other hardware, suitable precautions are to be taken to guard against the environmental threats of fire, flood, hazardous material and excessive ambient temperature / humidity.

c) All computer premises must be protected from un-authorised access using an appropriate balance between simple ID cards to more complex technologies to identify, authenticate and monitor all access attempts.

d) All employees are to be aware of the need to challenge strangers on Eskom premises.

e) Criteria shall exist for the categorisation of all information resource areas, and the appropriate control requirements developed for each category.

f) Photographic, video, audio or other recording equipment shall not be used in an area housing critical information resources as categorised, without the relevant authorisation.

g) Procedures shall be developed to address secure disposal of information resources.

h) Agreements shall be in place to ensure the security, and confidentiality of information stored on information resources that are subject to third party repair and maintenance.

i) The System owner will be responsible to grant physical access to cyber assets

3.6.1 Physical Security Plan

A physical security plan, approved by the senior manager or delegate(s) shall be documented, implemented and maintained. The plan shall address, at a minimum, the following:

a) All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets. (1)

b) The identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points. (1)

c) Processes, tools, and procedures to monitor physical access to the perimeter(s). (2)

d) Appropriate use of physical access controls, including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls. (2)

e) Review of access authorization requests and revocation of access authorization (2)

f) A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing as a minimum the following:

- Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters. (2)
- Continuous escorted access of visitors within the Physical Security Perimeter. (1)

g) Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

h) Annual review of the physical security plan. (2)

3.6.2 Protection of Physical Access Control Systems

Protection of physical Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

a) Be protected from unauthorised physical access. (1)

b) Be protected from unauthorised logical access to the same level as other Critical Cyber Assets. (1)

3.6.3 Protection of Electronic Access Control Systems

a) Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter in Eskom. (1)

b) Management of the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside in an Electronic Security Perimeter and protected from external access to the same level as the Critical Cyber Asset. (1)

c) The access control to a Critical Cyber Asset shall not be managed from a third party's premises. (2)

3.6.4 Physical Access Controls (1)

Operational and procedural controls shall be documented and implemented to manage physical access at all access points to the Physical Security Perimeter. One or more of the following physical access methods shall be implemented:

a) Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

b) Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.

c) Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

d) Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

3.6.5 Monitoring Physical Access (2)

The technical and procedural controls for monitoring physical access at all access points shall be documented and implemented. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified. One or more of the following monitoring methods shall be used:

a) Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

b) Human Observation of Access Points: Monitoring of physical access points by authorized personnel.

3.6.6 Logging Physical Access (2)

Sufficient information to uniquely identify individuals and the time of access shall be logged. The technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter shall be documented and implemented using one or more of the following logging methods or their equivalent:

a) Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method.

b) Video Recording: Electronic capture of video images of sufficient quality to determine identity.

c) Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

3.6.7 Access Log Retention (2)

Physical Access Logs shall be retained for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Section 3.8.

3.6.8 Maintenance and Testing (2)

The System Owner shall implement a maintenance and testing program to ensure that all physical security systems are tested on a cycle no longer than three years.

All testing and maintenance records shall be kept for a period as determined by Section 3.8. Outage records regarding access controls, logging, and monitoring shall be retained for a minimum of one calendar year.

3.7 Cyber Security — Systems Security Management

This section describes methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (less critical) Cyber Assets within the Electronic Security Perimeter(s).

3.7.1 System Design and Configuration

a) A process to ensure that only those ports and services required for normal and emergency operations are enabled on all Critical Cyber Assets / Cyber Assets within the Electronic Security Perimeter, shall be established, documented and implemented.

b) No protocols using clear text to transmit usernames and passwords shall be used on the network, and no password shall be stored in clear text on any system. (2)

c) No internet / intranet access or corporate email retrieval access shall be possible from any Cyber Asset within the Electronic Security Perimeter. (1)

d) DNS shall not be used for access to Critical Cyber Assets. Nodes can be listed in the hosts file, to eliminate the risk of a DNS malfunction preventing logical access to critical Assets. (3)

e) ICMP (ping) traffic shall not be allowed to leave the Electronic Security Perimeter. (2)

f) DHCP shall not be used for Cyber Assets permanently connected to the network, and the use of DHCP shall be avoided where possible. This is to prevent an asset used on the OT network, being connected to the business LAN, and reconnected to the OT LAN or visa-versa. (1)

g) Where possible, a host firewall shall be configured on all Critical Cyber Assets that only allows access from authorised clients on authorised ports, and denies all other access to the system. (1)

h) Where possible, an application firewall such as AppArmor shall be implemented on Critical Cyber Assets. (3)

i) The factory default passwords on all equipment shall be changed. (1)

j) Where possible, unused ports on networking equipment shall be administratively shut down. (2)

k) Where HMI Cyber Assets in the security perimeter are not manned 24/7, 802.1x authentication shall be used on switch ports to ensure only authorised users have access to the network. (3)

l) If, during implementation, the system or a subsystem is available with similar features on multiple platforms, preference shall be given to the operating system / software solution with the lowest cyber risk. As an alternative, where feasible, the system should be installed on a secure host in a virtual machine (guest), using Network Address Translation (NAT) to access the system, with only required ports being forwarded to the guest system. Where a network connection for the update of Anti-virus signatures is not available, the use of Microsoft Windows should be avoided. (2)

m) Avoid using environments such as Java, Adobe Flash, Acrobat and Silverlight where possible. (2)

n) Reduce the amount of applications installed on Critical Cyber Assets by only installing required applications. Application white-listing can also be implemented where possible. (2)

o) Reduce the amount of services running on Critical Cyber Assets by removing all services not required for the operation and maintenance of the system. (1)

p) Most vulnerabilities on the operating system exist on the Graphical User Interface (GUI). Where possible to reduce the risk, the GUI on a server shall not be started. (1)

q) Where mail servers or shared storage devices are installed or used on Cyber Assets, these services and equipment shall not be used for the import of data/information into the Cyber Asset. These services should be provided by another Cyber Asset in the specific OT environment. The architectural and cyber-security requirements shall be explicitly defined in the detail design documentation of the Cyber Assets.” (3)

r) LANs shall be segregated as much as possible. For example, if a group of Critical Cyber Assets only communicates with another group, a VLAN can be used to remove the group from the default LAN. (2)

s) Where possible, a high security zone shall be established for critical cyber assets. (2)

t) Different systems should also be placed in separate firewalled zones where possible. (2)

u) If Management ports on Critical Cyber Assets are used, it shall not be connected to the default LAN, but to its own dedicated LAN or VLAN, with separate dedicated management and configuration workstations. (1)

v) Network routing and management protocols shall be placed in their own VLAN where possible. (2)

w) Session time-outs shall be implemented on all critical cyber assets. (1)

x) Limits shall be set on the amount of MAC addresses allowed per port on switches to prevent ARP poisoning attacks. (1)

y) The perimeter network security stack shall implement rules on both incoming and outgoing traffic, and an implicit deny rule shall be configured in both directions. Rules shall also be specific with regard to host and host groups as well as ports and port groups. Where possible, the default gateway of the firewall shall not be set, or shall be set to an internal monitoring node, to prevent malware establishing connections to their master stations. The use dynamic NAT shall also be avoided where possible. (1)

z) No device shall under any circumstances bypass any firewalls by being connected to two different networks simultaneously. (1)

aa) Switches shall be configured to limit the amount of MAC addresses allowed on a port to prevent an ARP poisoning attack. (1)

bb) SSH shall be used to configure routers and switches. (1)

3.7.2 System Maintenance and Operation

a) Regular network scans shall be done on the network to detect unauthorised nodes. (2)

b) If a backup server is implemented on the network, communication with this server shall be encrypted, and the server shall be protected to at least the same level as the most critical backup stored on the server. (1)

c) Log analysis of the log server should be automated as much as possible. (2)

d) Where a critical cyber asset is configured outside of the secure perimeter for any purpose, and the aim is to reintroduce this critical cyber asset into the secure perimeter, measures shall be taken to protect this critical cyber asset from all threats similar to critical cyber assets inside the secure perimeter. Where adequate protection was not possible, the critical cyber asset shall be re-installed before reintroduction into the secure perimeter. (2)

3.7.3 Malicious Software Prevention

a) Anti-virus software and other malicious software (“malware”) prevention tools shall be implemented, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter. (1)

b) In the case where anti-virus software and malware prevention tools are not installed, compensating measure(s) applied to mitigate risk exposure shall be documented. (1)

c) A process for the updating of anti-virus and malware prevention “signatures” shall be documented. The process must address testing and installing the signatures. (3)

d) Unauthorised software shall not be installed and/or used on Critical Cyber Assets. (1)

e) Removable media (including memory sticks and flash memory devices) that are purchased for business purposes must be safeguarded and protected at all times. (2)

f) Where technically feasible, USB, serial ports, CD/DVD, SCSI, and any other medium that can be used for access, to Cyber Assets within the Security Perimeter shall be disabled. (1)

3.7.4 Account Management

a) Users shall not share or divulge their user identification and passwords. (2)

b) A standard to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts shall be documented and implemented. (3)

c) The standard shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service. Accounts of users that are no longer required shall first be disabled for a period before being removed, to be able to associate log entries with the relevant user for investigation purposes. (3)

d) Where possible, remote access using the default administrator account shall be disabled. (2)

e) Individual and shared system accounts and authorized access permissions shall be consistent with the concept of “need to know” with respect to work functions performed. (3)

f) All accounts shall have a responsible/accountable person associated with it. (3)

g) User accounts shall be implemented with access rights as approved by designated personnel. (1)

h) Logs of sufficient detail to create historical audit trails of individual user account access activity shall be generated and kept for a minimum of ninety days. (2)

i) User accounts shall be reviewed at least annually to verify access privileges, and no user shall be allowed to work as root / administrator on a continuous basis. (1)

j) Individuals with access to shared accounts shall be identified. Where such accounts must be shared, a standard for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination) shall be documented and implemented. (3)

k) As a minimum, as technically feasible, passwords for Critical cyber assets should adhere to the following:

- Each password shall consist of a minimum of eight characters. (1)
- Each password shall consist of a combination of alpha, numeric, and “special” characters. (2)
- Each password shall be changed at least every 15 months, or more frequently based on risk. (2)

l) All Critical Cyber Assets within the Electronic Security Perimeter, as technically feasible, shall implement automated tools or organizational process controls to monitor system events that are related to cyber security. (2)

m) The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents. (2)

n) Organizational processes and technical and procedural mechanisms for monitoring of security events on all Critical Cyber Assets within the Electronic Security Perimeter shall be documented and implemented. (3)

o) Logs of system events related to cyber security shall be kept, where technically feasible, to support incident management as determined in Section 3.8. (2)

p) These logs shall be reviewed for events related to cyber security and retained for ninety calendar days.(2) Formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter shall be established and implemented. (3)

q) All data shall be securely destroyed prior to the disposal or redeployment of such assets to prevent unauthorized retrieval of sensitive cyber security or reliability data. (1)

r) Records shall be kept of such assets that were disposed of or redeployed in accordance with documented procedures (3). The documentation shall be reviewed and updated at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed. (3)

3.7.5 Security Patch Management

a) A security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Critical Cyber Assets within the Electronic Security Perimeter shall be established, documented and implemented. (3)

b) Upgrades and patches for Hardware Firmware, Operating Systems or Applications should first be tested on a duplicate of the environment, or on a similar system if a duplicate is not available. This system should be tested to ensure no functionality is lost, and should be run a period to ensure stability of the system is not affected by the released patches. (2)

c) If a separate system is not available, but multiple cyber assets are available that perform the same function, the cyber assets can be divided into groups. Updates can then be applied to one group, and only applied to the other group after confirmation that the updates did not cause a reduction in functionality on the first group. (2)

d) The assessment of security patches and security upgrades for applicability shall be documented within thirty calendar days of availability of the patches or upgrades. Implementation of security patches shall be documented, and in any case where the patch is not installed, compensating measure(s) applied or already in place to mitigate risk exposure shall be documented (3)

e) Where no DMZ is implemented, perimeter firewalls should be opened and then immediately closed, after obtaining the updates, instead of leaving them open. The firewall shall only allow access for a repository server to access the update servers, on the required port. (1)

3.8 Cyber Security – Incident Reporting and Response Planning

The *System Owner* shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents.

3.8.1 Cyber Security Incident Response Plan (3)

a) The Cyber Security Incident response plan shall classify events and document the appropriate response actions, including roles and responsibilities of the response teams, incident handling procedures, and communication plans.

b) Employees shall be made aware of what constitutes an incident, and how to react to incidents.

c) The Cyber Security Incident response plan shall be updated within thirty calendar days of any changes.

d) The Cyber Security Incident response plan shall be reviewed at least annually after a test. 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.

e) Cyber Security incidents must be properly investigated by suitably trained and qualified personnel.

f) 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.

g) 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.

3.8.2 Cyber Security Incident Documentation (2)

a) The System Owner must ensure that all reportable Cyber Security Incidents are reported within 60 days to outside authorities through the authorised channels whenever this is required to comply with legal requirements or regulations.

b) The *System Owner* shall keep relevant documentation related to reportable incidents for three calendar years.

3.9 Recovery Plans for Critical Cyber Assets

3.9.1 Recovery Plans (2)

The System Owner shall create and annually review recovery plan(s) for Critical Cyber Assets.

a) The recovery plan(s) shall specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

b) The roles and responsibilities of responders shall be documented.

c) The recovery plans shall be reviewed regularly using business impact and risk assessments methodologies.

d) Recovery plans shall be updated with relevant changes, managed through the change control process.

3.9.2 Exercises (3)

a) The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

3.9.3 Recovery Plan Change Control (3)

a) Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident.

b) Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s).

c) Recovery plan(s) shall be updated with relevant changes, managed through the change control process.

3.9.4 Backup and Restore

a) A formal retention procedure to ensure the operational state of the Critical cyber asset shall be developed and maintained by the *System Owner. (3)*

b) The information created and/or stored by a Critical cyber asset must be retained for a minimum period that meets both legal and business requirements where applicable. (3)

c) A backup strategy may include spare electronic components or equipment, written documentation of configuration settings, redundant configurations to be replicated during restoration, tape backup, etc. (2)

3.9.5 Testing Backup Media (3)

a) Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available.

b) Testing can be completed off site.

4. Additional considerations

4.1 Outsourcing

a) Obtaining of an outsourced service has to follow the standard Eskom commercial process. The requirement should include:

- Where possible, outsourcing shall be limited to on-site hardware or software maintenance, installation and configuration, and the accountability shall remain with the System Owner. (2)

- Usernames and passwords that are used by external contractors shall be managed and controlled by Eskom employees. (1)
- Outsourced services shall be from reputable vendors that operate in accordance with Eskom quality standards which should include a suitable Service Level Agreement that meets Eskom security requirements, and a non-disclosure agreement. (1)
- A formal risk assessment shall be performed prior to considering the utilisation of outsourced services (financial & third party assessment). Acceptance of tenders should be subject to both the contracting firm and its personnel being appropriately screened. With vetting criteria being adjusted continuously, even if a particular contractor has obtained clearance previously it will not automatically be renewed. An appropriate and systematic process of security investigation will be exercised on each occasion. (2)
- All security requirements shall be addressed in a contract agreement between the parties.(1)

b) Eskom shall ensure that outsourced service providers comply with all applicable Eskom security policies and procedures, and non-disclosure agreements. (1)

c) Eskom shall ensure that service providers return all Eskom information assets at the external site at the end of the contract, and that all service provider access rights to Eskom information resources, are revoked, (1)

d) No management of the logical and/or physical access control shall be possible from outside the Electronic Security Perimeter of a Critical Cyber Asset. (1)

4.2 NEW Project Implementation

All new projects shall follow the appropriate engineering and/or IT governance processes as per the referenced Practice Note [1]

When a new project is planned that would include Critical Cyber Assets, the following criteria shall be met:

- The 5 phase Engineering Methodology, or similar methodology, as described shall be followed. Cyber security measures shall be included in all phases of the methodology. Phase 1 - Functional Design Specification (FDS)

This phase consists of the production of a Functional Design Specification comprising of a Functional Specification document and a System Design Report. It is the intention of this phase to finalise all requirements and subsequently document the proposed design to form the baseline for the following phases. All Cyber security requirements shall be included in the FDS

- Phase 2 - Detailed Design Specification (DDS)

This phase consists of the production of a Detailed Design Specification for both hardware and software components of the system and specifies the procedures for testing. All Cyber security requirements shall be included in the DDS and testing procedures.

- Phase 3 - Development, System Integration and Factory Acceptance Test (FAT)

Phase 3 shall commence on completion of Phase 2. This phase consists of the procurement of hardware required for testing, any required development and supply of software, training of the Eskom personnel, database population and system integration if required, which is to be followed by formal testing of the system at the Supplier's premises, in the presence of Eskom personnel. Cyber security measures shall be tested during the FAT

- Phase 4 - Delivery, Installation, Testing and Commissioning

Phase 4 shall commence on completion of Phase 3. This phase comprises of delivery of hardware, software, documentation and manuals to site, installation in conjunction with Eskom personnel and training. Thereafter, the system shall be commissioned in accordance with operating constraints of the power system.

- Phase 5 - Site Acceptance Test (SAT)

Phase 5 shall commence on completion of Phase 4. This phase consists of conducting tests according to the SAT Procedure document and shall be inclusive of Cyber Security Testing.

a) All Software developments shall follow an approved system development methodology.

b) The integrity of Eskom operational software code shall be safeguarded using a combination of technical access controls and restricted privilege allocation and robust procedures.

c) If any component of the system was connected to an insecure network during any phase of the system development or testing, all nodes shall be re-installed before performing the SAT. This includes cases where the firewall, that connected the system to any less secure network, was not properly configured while parts of the system was being developed or tested.

d) The development of software is only to be considered, if warranted by a strong Business Case and supported both by management and adequate resources over the projected lifetime of the resultant software.

e) If the system or a subsystem is available with similar features on multiple platforms, preference shall be the operating system / software solution with the lowest cyber security risk. As an alternative, where feasible, the system should be installed on a secure host in a virtual machine, using Network Address Translation (NAT) to access the system, with only required ports being forwarded to the guest host.

f) Documentation pertaining to Systems Acquisition, Development and Maintenance and security controls shall be retained, and kept up to date.

g) The production, test and development environment shall be segregated.

h) The acquisition and development procedure of application systems shall take into account the security requirements and controls, which must be tested as part of the system development-testing phase.

i) Post-implementation reviews shall be conducted for new or significantly changed application systems.

j) Formal change control procedures must be utilised for all amendments to systems.

k) All username and passwords shall be changed when the system is put into operation.

l) Any changes to routine systems operations are to be fully tested and approved before being implemented.

m) Necessary upgrades and patches to the systems shall have the associated risks identified and be carefully planned, incorporating tested fall-back procedures.

n) System faults are to be formally recorded and reported to those responsible for software support / maintenance.

o) Data used for testing purposes shall be protected and controlled in accordance with item –3.3.3 Information Classification.

p) Newly acquired systems shall be approved by the relevant governing structures.

q) Procedures to have the ability to reload all OS and software from scratch. This is a vital step after an attack, and should be tested at FAT and SAT.

5. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Prudence Madiba	Senior Manager – Control and Instrumentation
Alison Maseko	Senior Manager – Eskom Telecommunications
Marius van Rensburg	Transmission Grid Representative
Cornelius Naidoo	Middle Manager – Telecommunications Technology and Support
Steven Papadopoulos	Middle Manager – Control and Automation Technology and Support
Amelia Mtshali	Middle Manager – Metering, DC and Security Technology and Support (Acting)
Rosalette Botha	Corporate Specialist – System Operator
Reshin Moodley	Chief Engineer – OT Cyber Security Care Group Convenor
Craig Boesack	Chief Engineer – Control and Instrumentation
Jorge Nunes	Chief Engineer – Control and Instrumentation
Zameka Qabaka	Senior Technologist – Koeberg Power Station
Rishi Hariram	Chief Engineer – Control and Automation
Ian Naicker	Chief Engineer – Control and Automation
Marcus Veeraragaloo	Chief Advisor – Information Risk and Compliance
Veemal Naik	Chief Advisor – Information Risk and Compliance
Tertius Hyman	Engineer – Western Cape Operating Unit
Johan Botha	Senior Consultant- System Operator
Jason Hector	Senior Engineer -Control and Automation
Lloyd Chego	Engineering Design Manager - NWOU, Asset Creation
Matthew Taljaard Oswald	Engineer – Telecommunications Technology and Support

6. Revisions

Date	Rev	Compiler	Remarks
Feb 2016	2	Reshin Moodley	Revised document as per Deloitte recommendations
July 2013	1	Johan Botha	Updated cover page and acceptance table
March 2013	0	Johan Botha	New document

7. Development team

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

- OT Cyber Security Care Group

8. Acknowledgements

Not applicable.

Annex A – Interpretation of Connectivity Requirements

(Drawings as per NERC Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets)

■	Cyber Asset essential to Critical Asset functions(s)	■★	Critical Cyber Asset essential to Critical Asset function (s) and meets qualifying 3.2.3.2 connectivity requirements	□	Cyber Asset not essential to Critical Asset functions(s)

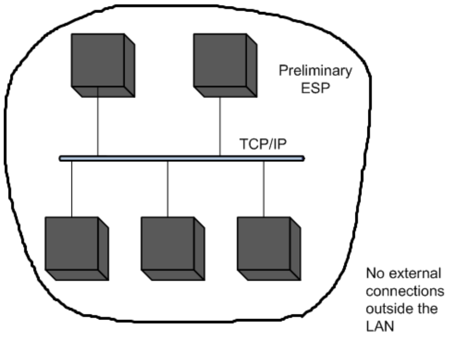


Figure A.1: Drawing 1

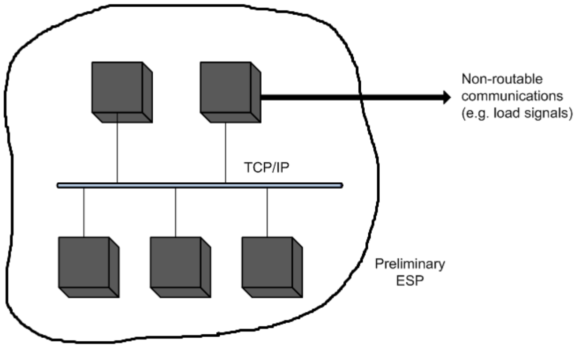


Figure A.2: Drawing 2

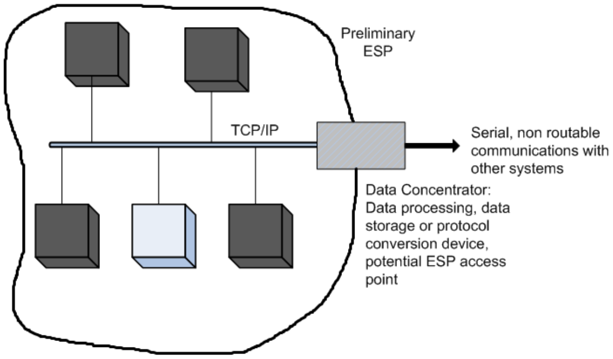
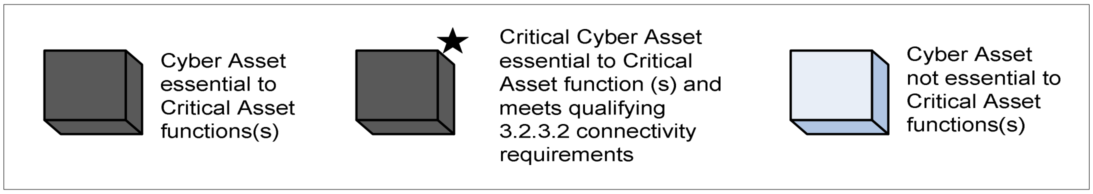

Preliminary ESP
TCP/IP
Serial, non routable communications with other systems
Data Concentrator: Data processing, data storage or protocol conversion device, potential ESP access point

Figure A.3: Drawing 3


Cyber Asset essential to Critical Asset functions(s)
Critical Cyber Asset essential to Critical Asset function (s) and meets qualifying 3.2.3.2 connectivity requirements
Cyber Asset not essential to Critical Asset functions(s)

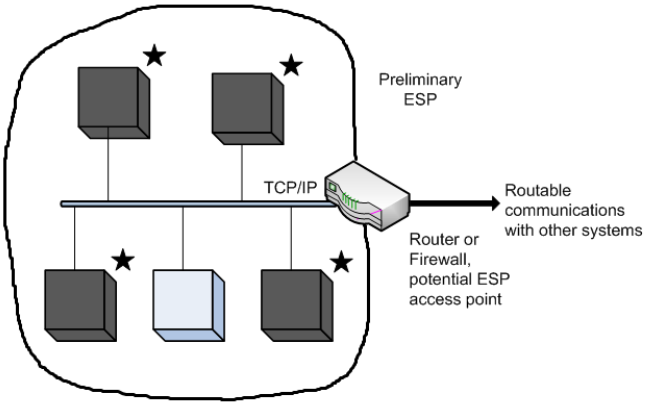

Preliminary ESP
TCP/IP
Routable communications with other systems
Router or Firewall, potential ESP access point

Figure A.4: Drawing 4

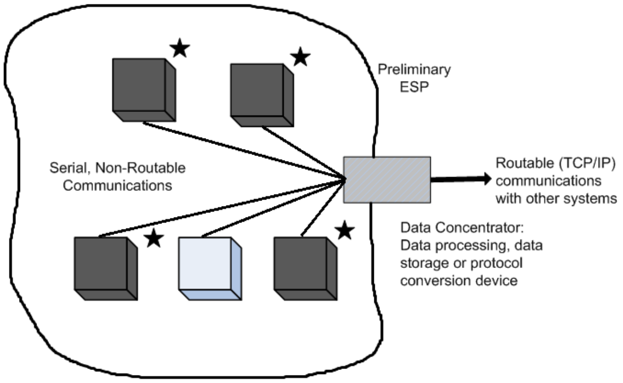

Preliminary ESP
Serial, Non-Routable Communications
Routable (TCP/IP) communications with other systems
Data Concentrator: Data processing, data storage or protocol conversion device

Figure A.5: Drawing 5

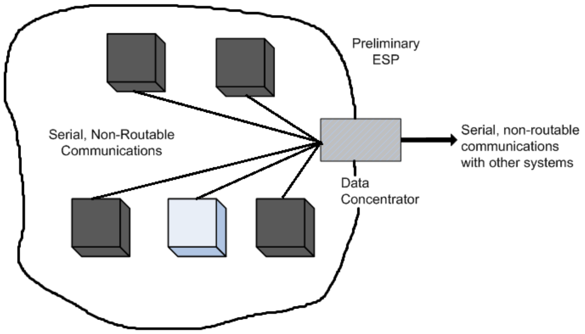
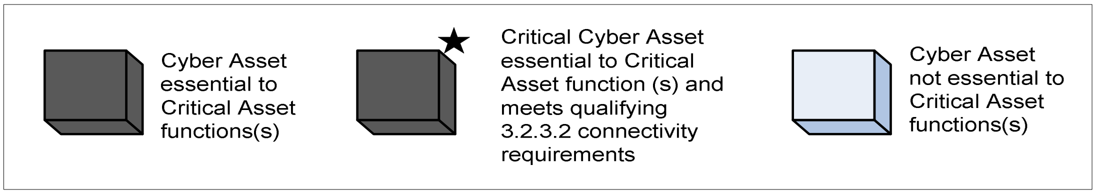

Preliminary ESP
Serial, Non-Routable Communications
Serial, non-routable communications with other systems
Data Concentrator

Figure A.6: Drawing 6


Cyber Asset essential to Critical Asset functions(s)
★
Critical Cyber Asset essential to Critical Asset function (s) and meets qualifying 3.2.3.2 connectivity requirements
Cyber Asset not essential to Critical Asset functions(s)

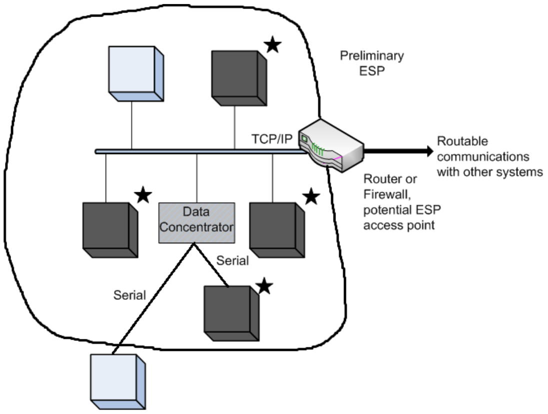

Preliminary ESP
TCP/IP
Routable communications with other systems
Router or Firewall, potential ESP access point
Data Concentrator
Serial
Serial

Figure A.7: Drawing 7

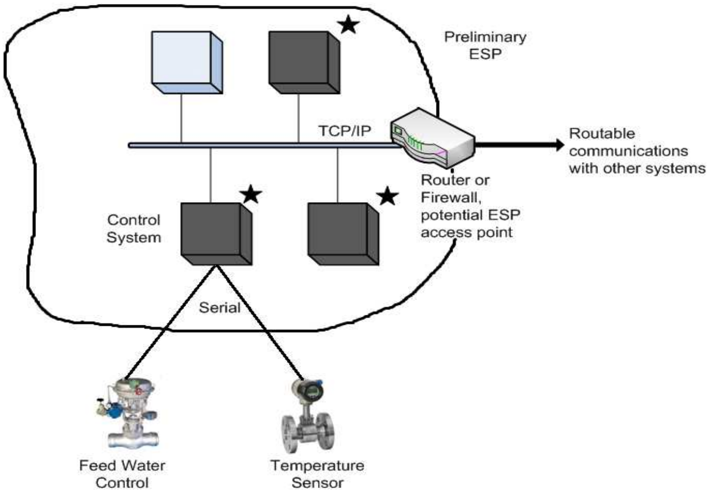

Preliminary ESP
TCP/IP
Routable communications with other systems
Router or Firewall, potential ESP access point
Control System
Serial
Feed Water Control
Temperature Sensor

Figure A.8: Drawing 8

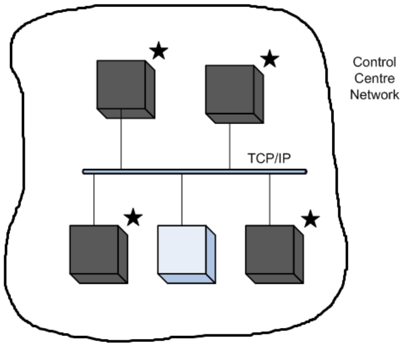
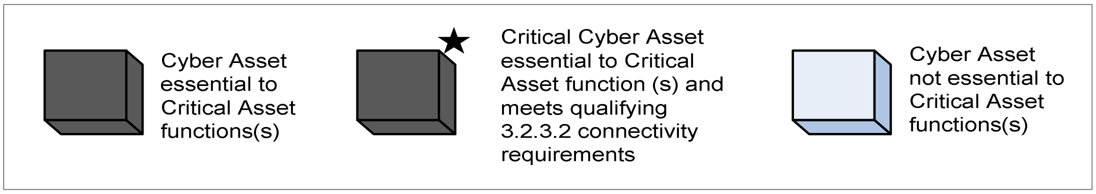


Figure A.9: Drawing 9


Cyber Asset essential to Critical Asset functions(s)
★
Critical Cyber Asset essential to Critical Asset function (s) and meets qualifying 3.2.3.2 connectivity requirements
Cyber Asset not essential to Critical Asset functions(s)

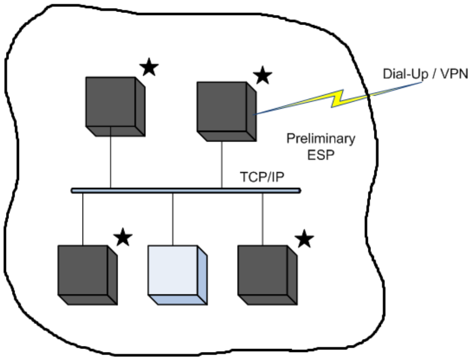


Figure A.10: Drawing 10

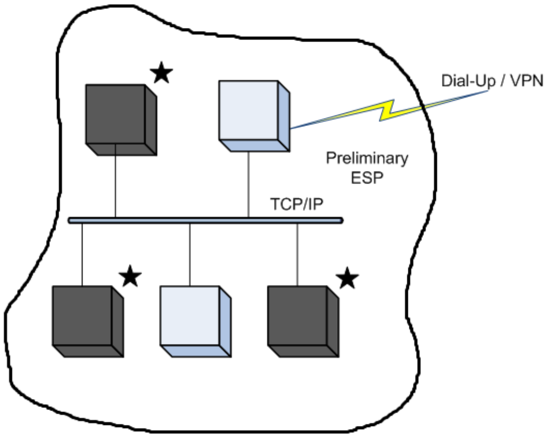


Figure A.11: Drawing 11

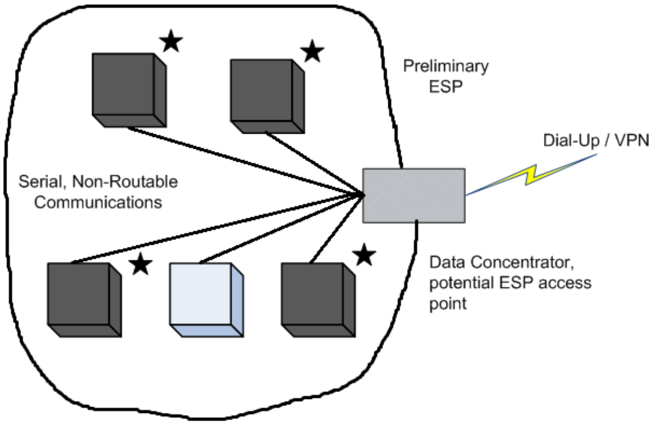

★
★
Preliminary ESP
Dial-Up / VPN
Serial, Non-Routable Communications
★
★
Data Concentrator, potential ESP access point

Figure A.12: Drawing 12