

	Standard	Generation Engineering
---	-----------------	-------------------------------

Title: **Generation Cyber Security Standard for Operational Technology** Unique Identifier: **559-577223024**

Alternative Reference Number: **N/A**

Area of Applicability: **Generation, Engineering**

Documentation Type: **Standard**

Revision: **1**

Total Pages: **36**

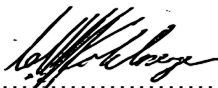
APPROVED FOR AUTHORISATION

☒ GENERATION ENGINEERING
DOCUMENT CENTRE ☎️ X4962

Next Review Date: **April 2029**

Disclosure Classification: **CONTROLLED DISCLOSURE**

Compiled by



Christoph Kohlmeyer
Chief Engineer: Generation Engineering, C&I

Date: 2024-03-28

Approved by



Jorge Nunes
Chief Engineer: Generation Engineering, C&I

Date: 2024-03-28

Authorised by



Thomas Conradie
General Manager: Generation Engineering

Date: 2024-03-28

Supported by SCOT SC



Dr Craig Boesack
Chairman: Power Plant C&I SC
Date: 2024-03-28

PCM Reference: 240-56355828

SCOT Study Committee Number/Name: **Power Plant C&I Study Committee**

CONTENTS

	Page
1. INTRODUCTION	4
2. SUPPORTING CLAUSES.....	5
2.1 SCOPE	5
2.1.1 Purpose	6
2.1.2 Applicability	6
2.2 NORMATIVE/INFORMATIVE REFERENCES.....	6
2.2.1 Normative	6
2.2.2 Informative	7
2.3 DEFINITIONS.....	7
2.3.1 Disclosure Classification	8
2.4 ABBREVIATIONS.....	8
2.5 ROLES AND RESPONSIBILITIES.....	9
2.6 PROCESS FOR MONITORING.....	9
2.7 RELATED/SUPPORTING DOCUMENTS.....	9
3. REQUIREMENTS FOR OT CYBER SECURITY MANAGEMENT	10
3.1 SYSTEM AND OT TECHNOLOGY CLASSIFICATION	10
3.1.1 Critical	10
3.1.2 Very High	10
3.1.3 High	10
3.1.4 Obsolete Technology (O)	11
3.1.5 Supported technology (S)	11
3.2 DATA CLASSIFICATION	11
3.3 IDENTIFICATION OF CRITICAL CYBER ASSETS.....	13
3.3.1 Identification of Critical Asset.....	13
3.3.2 Identification of Cyber Assets associated with Critical Assets.....	14
3.3.3 Identification of Critical Cyber Assets	15
3.3.3.1 Determine Cyber Assets which are Essential.....	15
3.3.3.2 Identifying Cyber Assets with Qualifying Connectivity	15
3.3.4 Audit requirements for this section - Identify:.....	19
3.4 PROTECT	19
3.4.1 Logical perimeter.....	20
3.4.2 Network	22
3.4.3 Authentication, Authorisation and Accounting (AAA).....	22
3.4.4 Endpoint and server protection	24
3.4.5 Physical	25
3.4.6 Audit requirements for this section - Protect:.....	26
3.5 DETECT	27
3.5.1 Logical	27
3.5.2 Physical	28
3.5.3 Audit requirements for this section:.....	28
3.6 RESPOND.....	29
3.6.1 Audit requirements for this section:.....	29
3.7 RECOVER.....	30
4. AUTHORISATION.....	32
5. REVISIONS	32
6. DEVELOPMENT TEAM	32
7. ACKNOWLEDGEMENTS	32
APPENDIX A : DIAGRAMS TO ILLUSTRATE ROUTABLE CYBER ASSETS	33

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

FIGURES

Figure 1: NIST Cyber Security Framework..... 4

Figure 2: Flow diagram to assist in identifying Critical Cyber Assets 16

Figure 3: Drawing 1 33

Figure 4: Drawing 2 33

Figure 5: Drawing 3 33

Figure 6: Drawing 4 34

Figure 7: Drawing 5 34

Figure 8: Drawing 6 34

Figure 9: Drawing 7 35

Figure 10: Drawing 8 35

Figure 11: Drawing 9 35

Figure 12: Drawing 10 36

Figure 13: Drawing 11 36

Figure 14: Drawing 13 36

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

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, plant 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) Cyber Security framework in order to protect its assets. The NIST Cyber Security framework was formulated to not only address cyber threats but also help in facilitating OT business objectives.

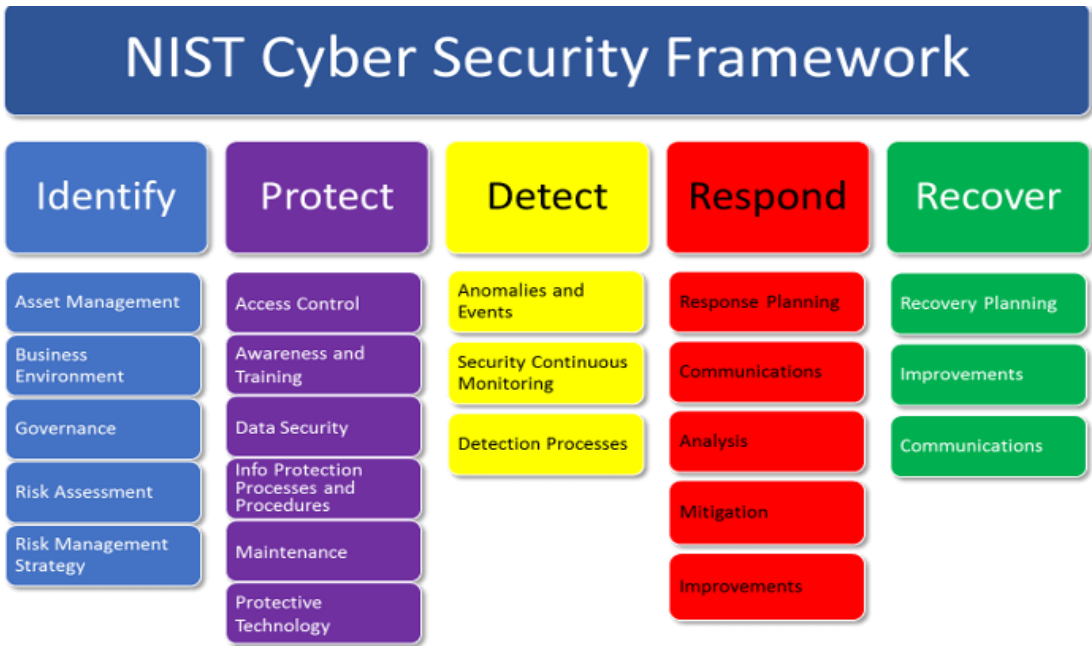


Figure 1: NIST Cyber Security Framework

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

The NIST framework consists of 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:

- a. 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:
 - i. Operational systems: are all systems (including electronic, telecommunications and computer systems and components) which process, store or communicate operational data or information.
 - ii. Part of means contribute to the asset meeting its purpose and performance criteria.
 - iii. 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.
 - iv. 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).
 - v. Purpose and performance criteria: The "design to", "maintain to" and "operate to" criteria that are generally specified formally.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

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

The auxiliary systems that support the OT systems, are required to comply to the same stringent Cyber Security requirements of the systems its supporting. For example, the HVAC system that manages the OT system's environment, should have the same level of access control and user management than that the systems it's supporting.

2.1.1 Purpose

The purpose of this document is to ensure that all necessary measures are taken to ensure that Eskom's business continuity is not affected due to any cyber related incident. It is recognised that there are differences in the operation and risks associated with the Operational Technology (OT) 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 requires a dedicated security approach as described in this standard.

This standard also provides auditors and system owners guidance on what may typically be assessed as part of Cyber Security assessments, reviews and audits at the respective Gx Business Units.

2.1.2 Applicability

This document shall apply to Operational Technology environments throughout Eskom Generation. It replaces the previous standard 240-55410927 Cyber Security Standard for Operation Technology.

The requirements defined in this standard also apply to all 3rd party (including OEMs, contractors and auditors) service engineers or personnel that are accessing the Eskom Gx OT systems. It is Eskom's prerogative to subject any of the 3rd parties that perform work on a Gx OT system to an audit for compliance to this standard.

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.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

- [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
- [7] 240-55863502 Definition of Operational Technology (OT) and OT/IT Collaboration Accountabilities.
- [8] 240-56355910 Management of Plant Software Standard
- [9] 240-129014618 Generation Cyber Security Compliance Guideline
- [10] 240-82332463 Data and Information Security in Power Plant Operations Standard

2.2.2 Informative

- [11] 240-91479924: Cyber Security Configuration Guideline of Networking Equipment for Operational Technology
- [12] 32-85: Information security Policy
- [13] 32-644: Eskom document management standard
- [14] 204-53114002: Engineering Change Management Procedure
- [15] Minimum Information Security Standard (MISS) – South African National document
- [16] 240-157635971 Cybersecurity Strategy for Eskom
- [17] 240-131313815 Critical Cyber Assets List template

2.3 DEFINITIONS

Definition	Description
Approved by	The accountability of the Approver of the document is equivalent to the specified role of Functional Responsible/Owner as identified in 240-53114186 and 32-6 for Documents and Records Management.
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.
Cyber Assets	Cyber Assets are defined to be programmable electronic devices and communication networks including hardware, software, and data
Critical cyber assets	Cyber assets essential to the reliable operation of critical assets.
Cyber Security	Cyber Security is the process of safeguarding critical cyber assets from attack, through the implementation of policy, standards and procedures for cyber risk mitigation.
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.
Non-repudiation	Non-repudiation ensures that the sender of a message cannot deny that it is the origin of the message, or its authenticity.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

Definition	Description
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.
Risk	The probability a threat will be realised. Potential for loss or damage of assets caused by a threat.
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.
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.
Threat	Any condition that could cause harm, loss or damage the system.
Vulnerability	A weakness in the design or implementation of a system that would expose it to a threat or be exploited.

2.3.1 Disclosure Classification

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

2.4 ABBREVIATIONS

Abbreviation	Description
AAA	Authentication, Authorization, Accountability
AD	Active Directory
CD	Compact Disc
CIP	Critical Infrastructure Protection
CIS	Centre for Internet Security
DCS	Distributed Control System
ESP	Electronic Security Perimeter
FIPS	Federal Information Processing Standards
IED	Intelligent Electronic Device
ICS	Instrument and Control System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
LAN	Local Area Network
LAR	Limited Access Register
LDAP	Lightweight Directory Access Protocol
MFA	Multi Factor Authentication
NAT	Network Address Translation
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

Abbreviation	Description
OEM	Original Equipment Manufacturer
OS	Operating System
OT	Operational Technology
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TACACS	Terminal Access Controller Access Control System
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 Eskom's corporate IT, OT, Technology and Smart Grid strategies evolve.

2.7 RELATED/SUPPORTING DOCUMENTS

This document supersedes the Cyber Security Standard for Operation Technology 240-55410927 in the Generation Environment.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

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 AND OT TECHNOLOGY CLASSIFICATION

To balance the cyber security precautions taken with the consequence of a breach, the document has split the requirements into 3 categories for criticality: High (H), Very High (VH) and Critical (C) as well as the Technology status: Obsolete (O) / legacy and Supported (S) technologies.

The following criteria are used to determine in which category of criticality a system should fall:

3.1.1 Critical

- a) Result in immediate production losses involving multiple units at a power station (MUT) or sufficient capacity to initiate an under-frequency incident.
- b) Seriously injure or kill one or more persons.
- c) Violating National legislation, policy, licence or permit conditions.
- d) Compromise the integrity of, or alter in any way protection systems, devices, functions, settings or philosophy of level 1 plant.
- e) Result in loss of visibility and/or control of more than one unit of a power station.
- f) 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, HVAC etc.

3.1.2 Very High

- a) Result in immediate production losses of a single power station unit or sufficient capacity to initiate an under-frequency incident.
- b) Compromise of a generation facility's ability to perform black starting.

3.1.3 High

- a) Result in a significant environmental contravention situation.
- b) Reduction of life of a significant plant asset (value \geq R250 million) by $> 10\%$.
- c) Increasing the longer-term production costs of a plant by $>10\%$.
- d) Negatively expose any part of Eskom to national media for ≥ 2 weeks.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

- e) Reducing the level of back-up redundancy provided to a significant plant for ≥ 1 week.
- f) 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 with the requirements applicable to that category.

The following criteria are used to determine in which category of Technology a system should fall:

3.1.4 Obsolete Technology (O)

Obsolete Technology is technology that is no longer supported by the OEM. It has usually been replaced by something newer, better, more cost effective or profitable. An obsolete OT product has reached the end of production and active support by the OEM in terms of development, spares, training and OEM expert support.

OT Systems falling in this category have solutions that were not developed with Cyber Security in mind and have different vulnerabilities at much less functionality or capability from a Cyber perspective than more modern solutions.

3.1.5 Supported technology (S)

Supported Technology is technology that is fully supported by the OEM in terms of:

- a) Product development related to hardware (e.g. firmware updates)
- b) Product development related software (version updates and patches)
- c) Spares availability
- d) Training on the installed technology

Modern or new technology has a different risk profile to that of Obsolete Technology. While more capable Cyber Security related tools are available to mitigate against Cyber threats, new and additional risks are introduced due to a much more interconnected network and convergence with IT and business systems.

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, in accordance with the standard, 240-82332463 Data and Information Security in Power Plant Operations. 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).

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No	Data Classification	Description
1	Unclassified data	Can be released to the public and general availability within the business. No impact from data disclosure.
2	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.
3	Confidential Data	Includes OT communications, non-operational data that could affect operations if disclosed, field data for historian and analytics. 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.
4	Secret Data	OT data related to SCADA/C&I and Automation data that could potentially allow 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
5	Top Secret Data	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.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

		<p>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.</p> <p>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.</p> <p>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</p>
--	--	---

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;

CONTROLLED DISCLOSURE

- 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 regard, 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:

- a) Amount of generation loss
- b) Number of customers without services
- c) Duration of disconnection to a customer
- d) Disconnection of key customers contravening contractual obligations
- e) Financial impact to Eskom due to energy sales lost
- f) Compromise of facility's ability to perform black starting
- g) Possible death of severe injury of one or more persons
- h) Negatively expose any part of Eskom to national media
- i) Significant reduction in plant life or asset value
- j) Significant environmental contravention
- k) Significantly violating National legislation, policy or permit conditions
- l) Significantly increasing long term production costs of a plant
- m) Reducing the redundancy of a plant for a non-trivial duration
- n) Compromise protection on equipment including fire detection
- o) 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.

CONTROLLED DISCLOSURE

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:

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

3.3.3 Identification of Critical Cyber Assets

3.3.3.1 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:

- a) The Cyber Asset participates in, or is capable of, supervisory or autonomous control that is essential to the reliable operation of a Critical Asset.
- b) 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.
- c) 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 are 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.

3.3.3.2 Identifying 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:

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

Diagrams to illustrate these are shown in Appendix 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.

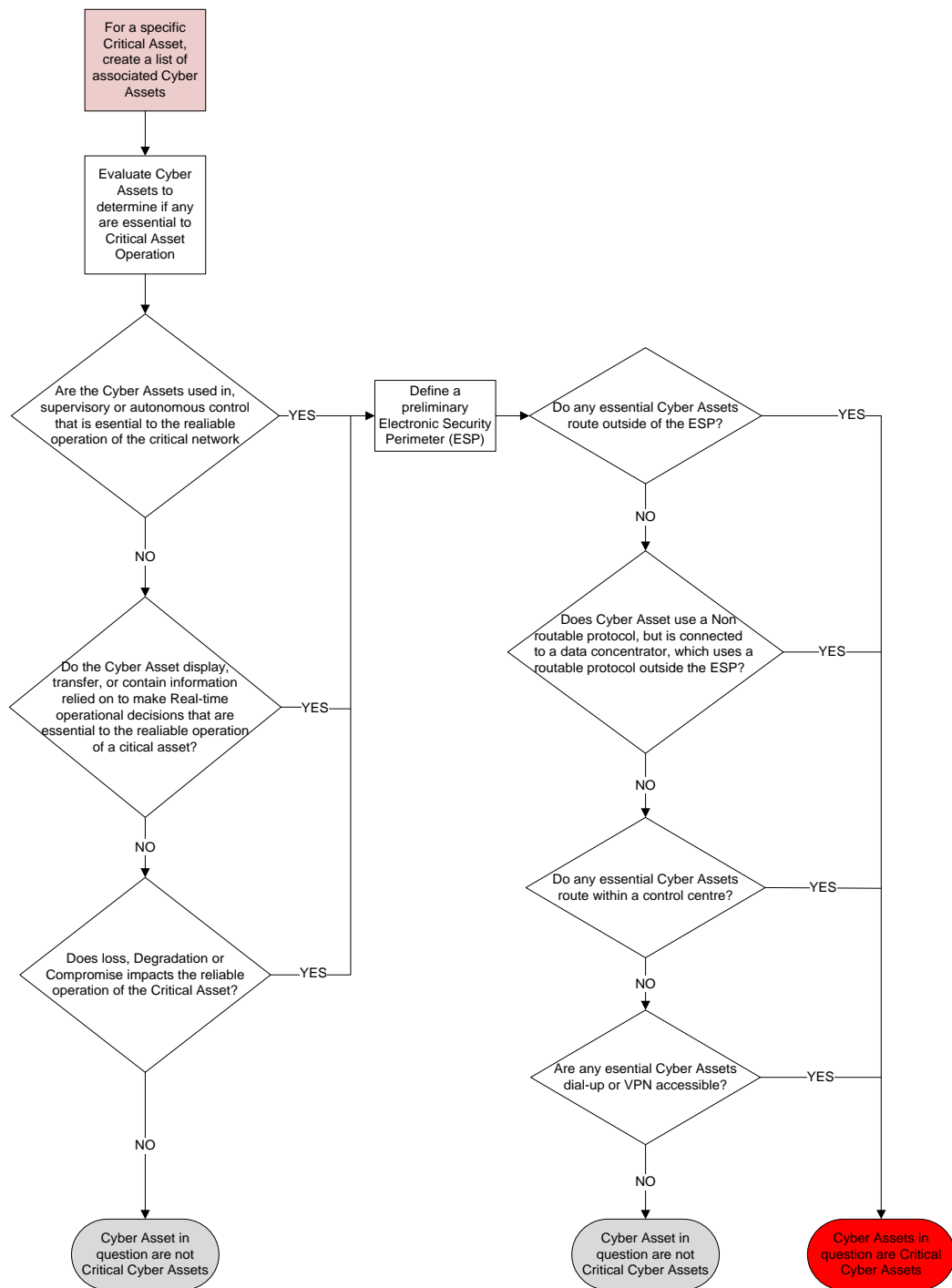


Figure 2: Flow diagram to assist in identifying Critical Cyber Assets

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

The following table provides examples for identifying Cyber Assets, the 240-131313815 Critical Cyber Assets List template should be used for this purpose.

Critical Asset	Associated Cyber Asset	Application of Function	IP Address	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	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
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

Generation Cyber Security Standard for Operational Technology

Unique Identifier: **559-577223024**

Revision: **1**

Page: **18 of 36**

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
Generation Control & Equipment Rooms	DCS, SCADA, PLC's (Grouped)	Various servers, controllers, PLC's used to collect information from the field devices to the operators and other users through HMIs and Historians		Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Generation Control & Equipment Rooms	Plant Historians	Collection of data from industrial control systems such as DCS's, SCADA & PLC's for real time or offline usage on the enterprise network		No	No	No	Yes	No	Yes	Yes	No

3.3.4 Audit requirements for this section - Identify:

- a) Asset Management
 - i. Inventory of physical devices
 - ii. Inventory of Software platforms and applications
 - iii. Communication and data flows map
 - iv. External information systems catalogued
 - v. Established roles and responsibilities for workforce and stakeholders
- b) Governance
 - i. Information security policy established
 - ii. Information security roles & responsibilities coordinated and aligned with the internal roles of personnel and those of the external partners
 - iii. Legal and regulatory requirements communicated
 - iv. Cybersecurity risks addressed in the governance and management processes
 - v. Budgeting includes for the cyber security related expenses
 - vi. Cyber security strategy with long- and short-term perspectives in place
 - vii. Industry recognised cyber security standards used
- c) Risk Assessment
 - i. Identify and document assets and processes vulnerabilities.
 - ii. Identify and document internal and external threats
 - iii. Identify potential business impacts and likelihoods
 - iv. Identify and prioritise risk responses
- d) Risk Management Strategy
 - i. Risk management processes should be established, managed and agreed to by stakeholders
 - ii. Risk tolerance should be determined and expressed
 - iii. Independent audits and reviews / assessments are used to identify gaps in security capabilities and expertise
 - iv. Processes are in place to identify skills improvement requirements in cyber security
 - v. 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 and select to which level it should be protected based on the risk to the power system in case of a compromise and criteria of Section 3.1. These are minimum requirements, 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.

No	Requirement	H	VH	C	O	S
1	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	X	X
2	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	X	X
3	Use firewalls from different OEM's for the inner and outer firewalls. Preferably from different countries.		X	X	X	X
4	Where possible, implement one way flow between different zones. (e.g. use of data diodes or one-way gateways).			X	X	X
5	Block all communication through the firewall that are not required.	X	X	X	X	X
6	All connections between the secure control network and the corporate network shall be through a firewall.	X	X	X	X	X
7	Implement filtering rules in both in-bound and out-bound directions that are equally stringent.	X	X	X	X	X
8	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	X	X
9	No systems other than firewalls should be configured with multiple network adapters that span the secure - DMZ or DMZ - corporate networks.	X	X	X	X	X
10	Where possible, connections should be initiated from the more secure zone to the less secure zone.	X	X	X	X	X
11	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	X	X
12	DMZ servers with different userbases should be grouped in different DMZ zones.		X	X		X
13	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	X	X
14	The base rule should be to deny all connections from outside the perimeter.	X	X	X	X	X
15	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.	X	X	X	X	X

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

	<ul style="list-style-type: none"> 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. 					
16	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	X	X
17	It is recommended to use static address translation instead of dynamic on firewalls.			X	X	X
18	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	X	X
19	Intrusion Detection Systems or Intrusion Prevention Systems should be implemented on the network to monitor traffic from outside the system.			X	X	X
20	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 OEM procedures to facilitate change of users, etc.) while more critical information should only be made available to auditors for viewing on site.	X	X	X	X	X
21	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	X	X
22	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	X	X
23	If unencrypted data passes through the perimeter firewall, deep packet inspection firewalls should be used. NAT should be used on all OT IP addresses visible from the IT network.			X	X	X
24	Equipment that is decommissioned shall be sanitised before disposal. A procedure that describes the process shall be available and followed.	X	X	X	X	X

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

3.4.2 Network

Network segmentation involves partitioning the network into smaller networks, logically grouping networked assets 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 physical separate switches and ports on a firewall, or VLANs where additional hardware is not available, by logically grouping related VLAN's on a physical port. Different ports on the connected switch are then assigned to specific VLAN's.

No	Requirement	H	VH	C	O	S
1	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	X	X
2	Traffic between zones should be denied by default and allowed by exception.	X	X	X	X	X
3	Implement one-way data flow (using data diodes or unidirectional gateways depending on the requirements), especially between different security domains where possible.			X		X
4	SNMP v1 and v2 should not be used as they are insecure.	X	X	X	X	X
5	Accurate time should be kept across all network devices using secure NTP or a similar mechanism. This is to ensure logging and other timestamps from different sources can be used to investigate an incident.	X	X	X	X	X
6	All available security measures should be configured, for example Access Control Lists on routers to limit traffic as far as possible.	X	X	X	X	X
7	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		X
8	Troubleshooting services and protocols using broadcast messaging should be disabled where possible, as they can be used to facilitate intruders in network exploration.			X	X	X

3.4.3 Authentication, Authorisation and Accounting (AAA)

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.

Authorisation relates to when an entity such as a user, hosts, services, and resource etc. is given access to certain data or areas of a system/s. Authorisation follows after authentication and can be determined in several ways, including permissions, access control lists, time-of-day restrictions, and other login and physical restrictions or aspects. Accounting is the tracking of the activities pertaining to the access granted to certain data or areas of a system/s. Accounting is achieved through logging, auditing, and monitoring of the data and resources.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No	Requirement	H	VH	C	O	S
1	A system must be configured and setup correctly 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	X	X
2	Shared credentials must be avoided when possible. When credentials are shared, accountability for actions taken are lost and the purpose of AAA and non-repudiation is defeated.	X	X	X	X	X
3	Enforce secure authentication (validation of user's identity) of all users seeking to gain access to the system network.	X	X	X		X
4	Authentication should be separate from the corporate IT 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	X	X
5	Display a legal warning banner (software or physical) on the access point (logical or / and physical) to the OT system to improve successful prosecution of unauthorised access.	X	X	X	X	X
6	Implement automatic logout of all inactive terminal sessions after an appropriate time.	X	X	X		X
7	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		X
8	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		X
9	Passwords 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		X
10	Multi-factor authentication (MFA) should be used for all interactive sessions from outside the system.	X	X	X	X	X
11	Based on a least privilege model, and if technically possible, users should be restricted and allowed to only get access to the nodes on the control network necessary for their job function.		X	X	X	X
12	User accounts should be suspended immediately for employees that have left the organisation or were suspended and removed after 5 years. The same requirements hold for employees that have left the department (but remain employed within Eskom in another capacity) that had privileged user accounts on the respective OT systems. All privileged users are required to inform the respective system administrators when they leave the organisation or department.	X	X	X	X	X
13	If user accounts cannot be removed, the administrator should change the password of the account holder.	X	X	X	X	X
14	The number of incorrect logins to the OS and OT software, made by someone, should be reported and logged by the user management system. A suitable	X	X	X		X

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

	time delay between tries should be implemented and account lockout after a set number of failed attempts.					
15	Default accounts and passwords on all equipment must be changed before the system goes into commercial operation.	X	X	X		X
16	Remote access to the system should comply with the 32-373 Eskom IT/OT Remote Access Standard.		X	X	X	X

3.4.4 Endpoint and server protection

Endpoint and Server protection relates to the protection of such devices through the implementation of hardening techniques, device access controls, host-based firewalls, and compensating controls such as antimalware / application whitelisting, endpoint detection and response (EDR), redundancy etc.

No	Requirement	H	VH	C	O	S
1	All endpoints and servers should be hardened according to an appropriate standard such as the CIS Benchmark or OEM recommended best practice.	X	X	X	X	X
2	Servers should be installed in an appropriate access-controlled server room. (Refer to section 3.4.5)		X	X	X	X
3	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		X
4	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		X
5	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	X	X
6	Removable devices or media 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	X	X
7	The OS' AutoPlay functionality for removable media should be disabled on all endpoints.		X	X	X	X
8	The host firewall on all Cyber assets should be configured with strict rules where technically possible.	X	X	X		X
9	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. The timeout is implemented on both levels: The applicable OT application (s) and the OS if technically possible, but as a minimum via the OS	X	X	X	X	X
10	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	X	X
11	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	X	X

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

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.

No	Requirement	H	VH	C	O	S
1	Controls for monitoring physical access, maintaining logs, and handling visitors must be in place. Logs should be kept for at least 180 days. CCTV and digital access control is required for OT equipment, computer and server rooms that house the critical cyber assets. The Limited Access Register (LAR) procedure needs to be followed for these locations, but it complements the security technologies, it does not replace it.	X	X	X	X	X
2	Servers should be placed in locked areas and authentication mechanisms (such as keys, cards and/or biometric) should be in place.	X	X	X	X	X
3	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	X	X
4	The secured area should also be compatible with the environmental requirements of the devices.	X	X	X	X	X
5	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	X	X
6	The suitably sized UPS supplies (powered by the redundant UPS supplies in the Equipment Room per Unit and similarly for the BOP) should be provided to ensure power for the OT systems, considering the criticality of the OT systems.		X	X	X	X
7	The UPS power distribution should be such that <u>common OT Cyber monitoring systems</u> (e.g. SIEM, IDS, NIDS, Cyber Security station etc.) are always powered, even during Unit outages.		X	X	X	X
8	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	X	X
9	Fire systems (both fire detection systems and fire protection systems typically gas suppression, etc) 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 fire gas release/suppression systems to avoid damaging electronics and spinning disks due to the shock wave (Solid State Disks can be considered as an alternative).		X	X	X	X
10	The management systems of i. HVAC ii. Fire suppression, iii. Access control iv. Access monitoring (CCTV) should be protected to the same level as the OT systems housed inside the server/engineering rooms.		X	X	X	X

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

3.4.6 Audit requirements for this section - Protect:

- a) Identity Management
 - i. Identities, credentials, access permissions and authorisations should be managed and revoked on resignations or role changes
 - ii. Physical access should be managed (access monitoring and control using a combination of CCTV, Access control, LAR Access register or in person security).
- b) User access should be managed
 - i. Staff with privileged user accounts are vetted in accordance with MISS.
- c) Awareness and training
 - i. All users should be informed and trained on cyber security and how to identify and escalate potential security issues
 - ii. Physical security personnel, contractors, privileged users, management, senior executives and stakeholders should understand roles and responsibilities
 - iii. Cybersecurity risks should be actively discussed at Business meetings
- d) Data security
 - i. Data is protected at rest, in transit and against leaks
 - ii. Asset management should be managed through removal and transfer processes
 - iii. Integrity checking of software, firmware, hardware and informational
 - iv. Development and testing environment should be separate from production environment
- e) Information protection
 - i. System development life cycle should be implemented
 - ii. Configuration change control processes should be in place
 - iii. Backups should be done and tested periodically as required
 - iv. Incident response and Business continuity plans should be in place
 - v. Cyber security should be included in HR practices (personnel screening)
 - vi. Vulnerability management plan / process should be in place
 - vii. Defence in depth protective strategies should be followed
- f) Protective Tech
 - i. Removable media should be protected and use restricted
 - ii. Systems should be configured based on least functionality required
 - iii. Communication and control networks should be protected
 - iv. 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.

No	Requirement	H	VH	C	O	S
1	Roles, responsibilities and boundaries for detection and monitoring tools shall be defined, i.e. what tools monitor which systems and with what configuration of reporting.		X	X	X	X
2	A Security Information and Event Management (SIEM) system should be installed and monitored for real-time security visibility across the OT systems.			X		X
3	A host intrusion detection system (HIDS) shall be installed on all end-points of the OT network.			X		X
4	A Network Intrusion Detection System (NIDS) shall be installed to monitor the OT networks for anomalies and intrusions.		X	X		X
5	An anti-malware solution shall be installed on all OT end-points (workstations, servers etc.).	X	X	X		X
6	Anti-malware definition or signature files should be updated on a regular basis, at least monthly.	X	X	X		X
7	Anti-malware definition or signature files should be tested and obtained from the respective OT system's OEM, to ensure compatibility.		X	X		X
8	Detection processes shall be tested where possible by simulating an event that should trigger an alert.			X	X	X
9	Communication channels and responsibilities for communicating a breach should be established and documented in the incident response plan.		X	X	X	X
10	Auditing on servers should be enabled where available.		X	X	X	X

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

3.5.2 Physical

No	Requirement	H	VH	C	O	S
1	Roles, responsibilities and boundaries for physical detection and monitoring solutions shall be defined and documented.		X	X	X	X
2	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	X	X
3	Biometric and card access systems logs shall be logged on a central server and kept for a period of 365 days.			X	X	X
4	Communication channels for communicating a breach should be established and documented in the incident response plan.		X	X	X	X

3.5.3 Audit requirements for this section:

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

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

3.6 RESPOND

No	Requirement	H	VH	C	O	S
1	Employees shall be made aware of what constitutes a Cyber incident, and how to react to incidents.	X	X	X	X	X
2	Evidence shall be preserved in the case of a system breach for post event analysis.	X	X	X	X	X
3	The Cyber Security Incident response plan shall be updated within thirty calendar days of any changes that need to be made to keep it current. (for example a change in telephone numbers or individual stakeholders).	X	X	X	X	X
4	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	X	X
5	Cyber Security incidents must be properly investigated by suitably trained and qualified personnel.	X	X	X	X	X
6	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	X	X
7	Where feasible, actions to isolate the affected areas shall be taken after a Cyber Security Incident, if deemed critical for the continuous safe operation of the power system.	X	X	X	X	X
8	Cyber Security Incidents shall be reported within 60 days to outside authorities through the authorised channels, in alignment with the Cyber Incident response plan or procedure.		X	X	X	X
9	Documentation related to reportable incidents shall be kept for three calendar years.	X	X	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 Cyber Incident response plan should contain the following:

- a) Roles and responsibilities of the response teams
- b) Incident handling procedures
- c) Communication plans
- d) Reporting structure
- e) Contingency plans

3.6.1 Audit requirements for this section:

- a) Response planning
 - i. A response plan should exist which could be activated during or after an incident
- b) Communications
 - i. Personnel should know their roles and order of operations when a response is needed

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

- ii. Incidents should be reported in alignment to the respective BU's incident response plan.
- iii. Information should be shared.
- iv. Coordination with stakeholders should occur during response according to the plan or pre-established criteria

c) Analysis

- i. Notification from detection systems should be investigated
- ii. The impact of an incident should be performed
- iii. Forensics should be performed
- iv. Incidents should be categorised according to response planning
- v. Processes should be established to analyse and respond to vulnerabilities disclosed from internal and external sources

d) Improvements

- i. Response plans should incorporate lessons learned and strategies should be updated

e) Response Training

- i. Incident response training should be done and tested annually

f) Contingency planning

- i. A contingency plan for in case of incidents should be drawn up
- ii. Alternate site / location for backups should be determined. Alternative location to be within the boundaries of the respective BU, but in a physically different building.

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.

No	Requirement	H	VH	C	O	S
1	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	X	X
2	Backups and Restoration should be in alignment with the 240-56355910 Management of Plant Software Standard.	X	X	X	X	X
3	Complete and up-to-date logical network diagrams should be available.	X	X	X	X	X

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

The recovery plan should include the following:

No	Requirement	H	VH	C	O	S
1	Required response to events or conditions of varying duration and severity that would activate the recovery plan.		X	X	X	X
2	Procedures for operating the system in manual / island mode with all external electronic connections severed until secure conditions can be restored.		X	X	X	X
3	Roles and responsibilities of responders.		X	X	X	X
4	Processes and procedures for the backup, restoration and secure storage of information.	X	X	X	X	X
5	Personnel list for authorized physical and cyber access to the system	X	X	X	X	X
6	Communication procedure and list of personnel to contact in the case of an emergency including vendors, network administrators, support personnel, etc.	X	X	X	X	X
7	Current configuration information for all components (hardware, software and firmware).	X	X	X	X	X
8	Information on the safe storage of backups including off-line backups	X	X	X	X	X
9	Information on the safe storage of installation media, license keys, and configuration information where applicable.	X	X	X	X	X

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

4. AUTHORISATION

This document has been seen and accepted by:

Name & Surname	Designation
Jorge Nunes	Chief Engineer – Gx Eng C&I
Christoph Kohlmeyer	Chief Engineer – Gx Eng C&I
Tertius Rossouw	Engineer – Gx Koeberg Cyber Security
Orrin Veerasamy	Senior Engineer – Gx Koeberg Security
Dr Craig Boesack	Chief Engineer – Gx Peaking C&I
Lemuel Zwart	Duvha Gx C&I Engineer
Elsabe Pretorius	Senior Advisor – Lethabo C&I
Thokozani Msibi	Chief Engineer – Gx Eng C&I
Mondli Dlamini	Chief Engineer – Group IT
Mdu Shoji	Medupi Gx C&I Engineer
Nimesh Soodhoo	Koeberg Gx C&I Engineer
Felix Bosch	Generation Engineering Documentation Manager

5. REVISIONS

Date	Rev.	Compiler	Remarks
March 2023	0.1	Johan Botha	First Draft for Comments Review Process
Feb 2024	0.2	C. Kohlmeyer	Final Draft after Comments Review Process
March 2024	1	C. Kohlmeyer	Final Document for Authorisation and Publication

6. DEVELOPMENT TEAM

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

- Johan Botha
- Meenal Vala
- PTM&C C&I Cyber Security Care group

7. ACKNOWLEDGEMENTS

- Johan Botha as compiler of first draft of this standard.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

APPENDIX A: DIAGRAMS TO ILLUSTRATE ROUTABLE CYBER ASSETS

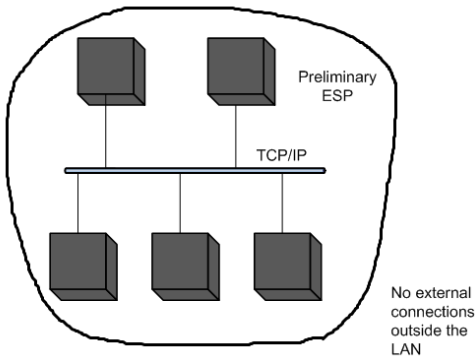


Figure 3: Drawing 1

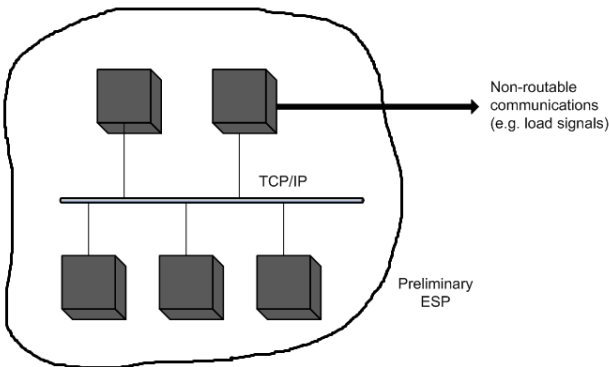


Figure 4: Drawing 2

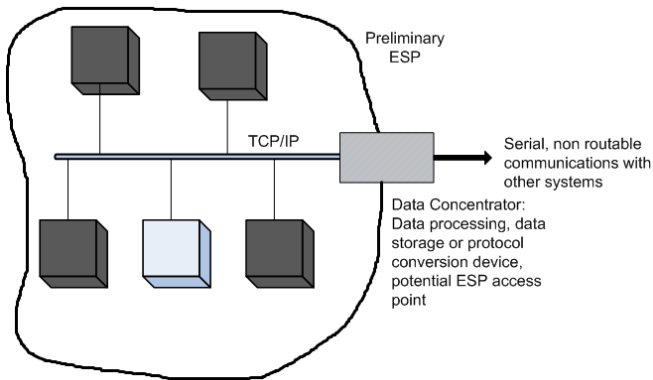


Figure 5: Drawing 3

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

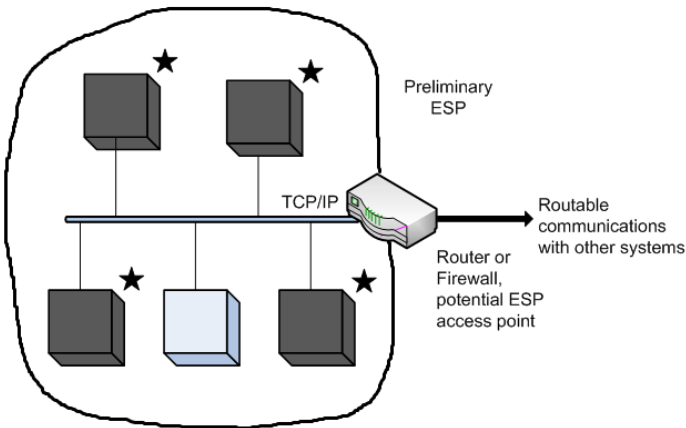


Figure 6: Drawing 4

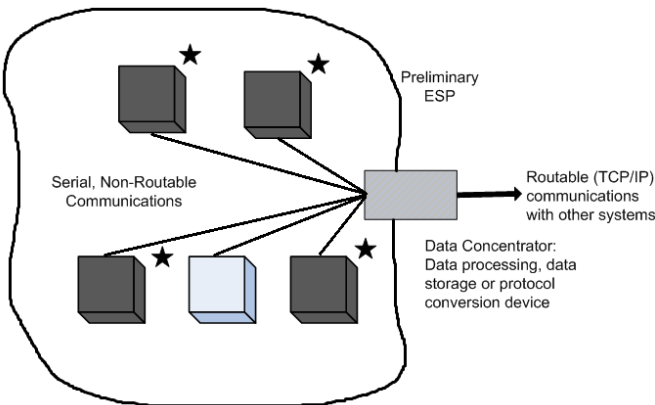


Figure 7: Drawing 5

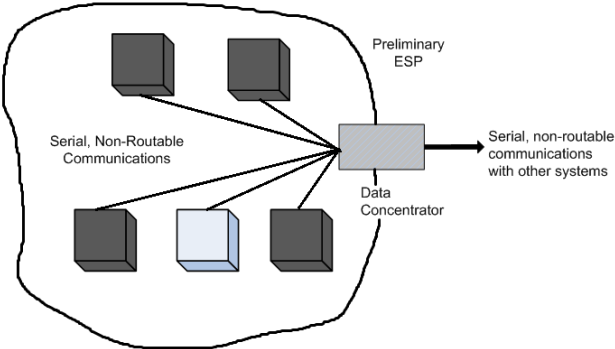


Figure 8: Drawing 6

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

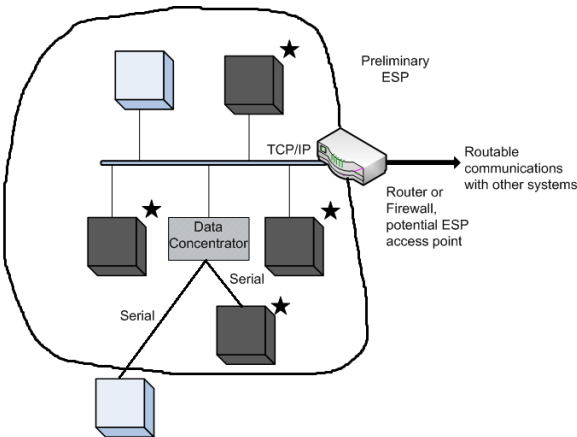


Figure 9: Drawing 7

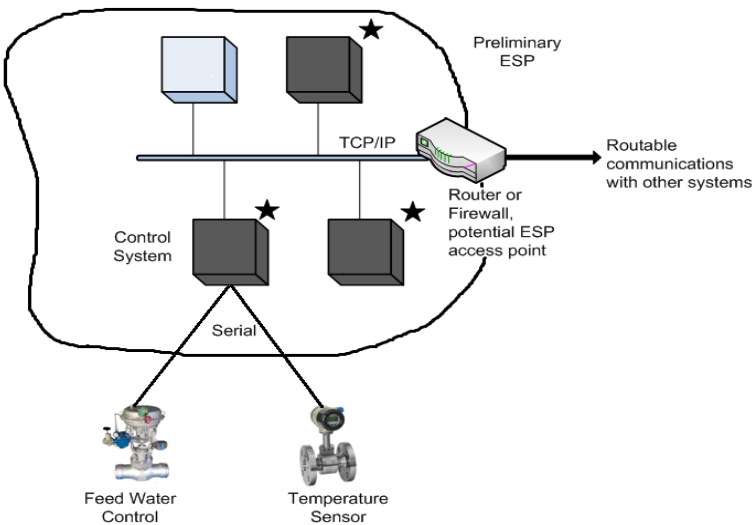


Figure 10: Drawing 8

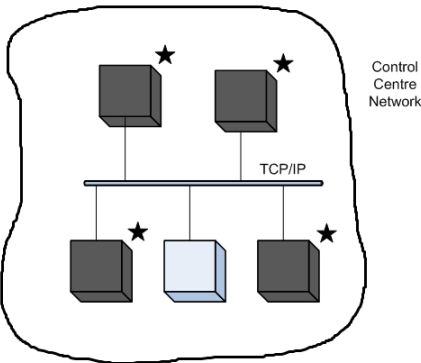


Figure 11: Drawing 9

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

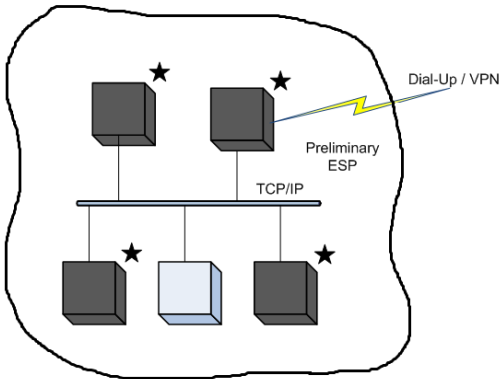


Figure 12: Drawing 10

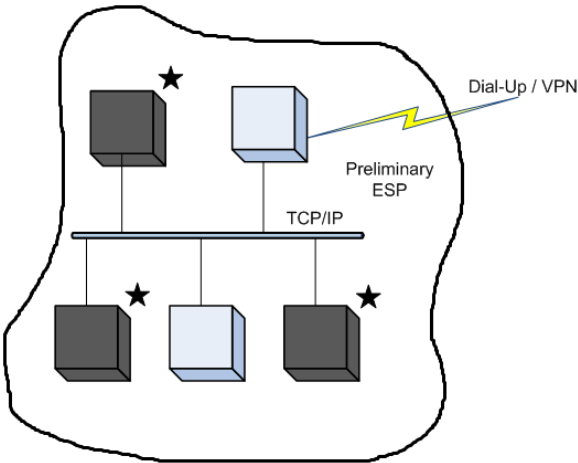


Figure 13: Drawing 11

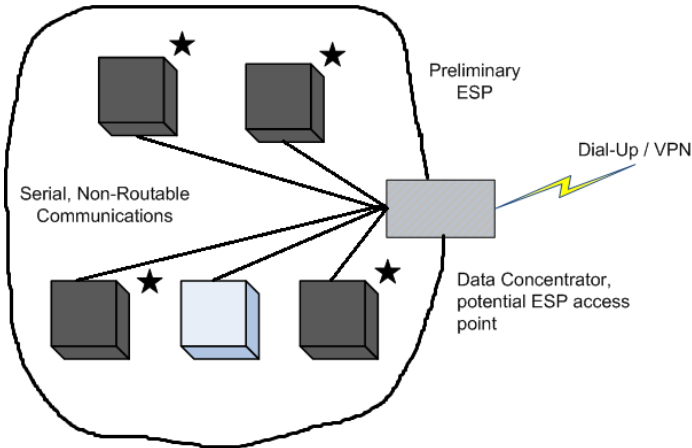


Figure 14: Drawing 13

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.