| Eskom | Guideline | Technology |
|---|---|---|

Title: **CYBER SECURITY CONTROLS GUIDE FOR PHYSICAL SECURITY SYSTEMS**

| | |
|---|---|
| Unique Identifier: | **240-170000614** |
| Alternative Reference Number: | **<n/a>** |
| Area of Applicability: | **Engineering** |
| Documentation Type: | **Guideline** |
| Revision: | **1** |
| Total Pages: | **17** |
| Next Review Date: | **November 2026** |
| Disclosure Classification: | **Controlled Disclosure** |

| Compiled by | Approved by | Authorized by |
|---|---|---|
| **Raees Dalvie** | **Naresh Hari** | **Dr. Titus Mathe** |
| **Design Engineer** | **General Manager: Transmission Engineering** | **General Manager: RT&D** |
| Date: 2021/11/17 | Date: 2021-11-17 | Date: 2021-11-17 |

**Supported by SCOT/SC**

**Nelson Luthuli**

**PTM&C Technical Committee – Chairperson**

Date: 17 November 2021

PCM Reference: **Develop Functional Architecture**

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

# Content

Page

1. Introduction ....4
2. Supporting clauses ....4
   - 2.1 Scope ....4
     - 2.1.1 Purpose ....4
     - 2.1.2 Applicability ....4
   - 2.2 Normative/informative references ....4
     - 2.2.1 Normative ....4
     - 2.2.2 Informative ....4
   - 2.3 Definitions ....5
     - 2.3.1 General ....5
     - 2.3.2 Disclosure classification ....6
   - 2.4 Abbreviations ....6
   - 2.5 Roles and responsibilities ....6
   - 2.6 Process for monitoring ....6
   - 2.7 Related/supporting documents ....6
3. The Defense-in-Depth Model ....7
4. Cyber-Physical Security ....7
   - 4.1 General Requirements ....8
   - 4.2 The Physical Security Perimeter ....8
     - 4.2.1 Defining the Physical Security Perimeter ....8
     - 4.2.2 Zones ....8
     - 4.2.3 Critical Cyber Asset Components Communicating Beyond the PSP: ....9
   - 4.3 Physical Access Control Systems ....9
     - 4.3.1 Physical Access Control Risks ....10
     - 4.3.2 Physical Access Control Types ....11
     - 4.3.3 Physical Access Control Methods: ....12
     - 4.3.4 Securing the Physical Access Control System: ....13
     - 4.3.5 Enrolment guidelines ....13
   - 4.4 Physical Access Logging, Monitoring & Alarms ....14
     - 4.4.1 Securing the CCTV Feed ....14
     - 4.4.2 Logging & Monitoring the System ....15
   - 4.5 Employee Training & Education ....16
5. Authorization ....16
6. Revisions ....16
7. Development team ....17
8. Acknowledgements ....17

**Figures**

Figure 1: Defense in Depth Model ....7

Figure 2: Example Access Control Supporting Physical Access Management with RBAC ....10

Figure 3: Example Crossover Error Rate for an Access Control Mechanism ....11

**Tables**

Table 1: Physical Access Control Risks .....11

Table 2: Access Control Type Classifications .....11

Table 3: IAL Requirements Summary .....14

# 1. Introduction

According to the NIST defense-in-depth model, physical security and cyber security are mutually inclusive concepts. Due to the increasingly integrated nature of technologies, traditional access control systems meant to provide physical security controls are now intelligent and communicate over networked infrastructure. Inadequate physical security could lead to compromises and yield unauthorised access to critical cyber assets, bypassing any logical security controls that are in place. Conversely, inadequate cyber security controls can provide vectors to compromise or bypass physical security controls. This guide document discusses the cyber security controls for physical access control systems that secure critical cyber assets within the Eskom environment.

# 2. Supporting clauses

## 2.1 Scope

This document does not endeavour to define any physical security requirements, as there are already adequate standards in place for this purpose. The intent of this document is to discuss cyber security controls for physical security systems that protect critical cyber assets in the Operational Technology environment in Eskom.

### 2.1.1 Purpose

The purpose of this document is to discuss security controls that could be implemented to ensure that critical cyber assets are adequately protected from risks that may emanate from individuals obtaining unauthorised physical access to them. According to international best practices and CIP-006-06 (Physical Security of BES Cyber Systems), one or more documented physical security plan(s) shall be put in place to adequately secure critical cyber assets. This document aims to discuss this requirement within the context of the Operational Technology environment in Eskom.

### 2.1.2 Applicability

This document shall apply throughout Eskom Holdings Limited Divisions.

## 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] 240-102220945, Specification for Integrated Access Control System (IACS) For Eskom Sites

[3] 240-55410927 Cyber Security Standard For Operational Technology

[4] CIP-006-06: Physical Security of Critical Cyber Assets

[5] NIST 1500-201 Framework for Cyber Physical Systems

[6] NIST 800-18 Developing Security Plans

[7] NIST 800-205 Access Control

[8] NIST 800-63a Digital Identity Guidelines

[9] 240-91190304 Specification for CCTV Surveillance with Intruder Detection

### 2.2.2 Informative

[10] SANS 2220- 2-1

## 2.3 Definitions

### 2.3.1 General

| Definition | Description |
|---|---|
| **Critical Cyber Asset** | Cyber assets essential to the reliable operation of critical assets |
| **Critical OT Systems** | OT Systems that, if compromised, destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the electricity supply network. |
| **Cyber Asset** | Programmable electronic devices and communication networks including hardware, software and data that are connected to a network with a routable protocol. |
| **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:<br>• Availability<br>• Integrity, which may include authenticity and non-repudiation<br>• Confidentiality |
| **Defense-in-depth** | Defense-in-depth is a security that provides multiple, redundant defensive measures in case a security control fails or a vulnerability is exploited. |
| **Demilitarised Zone** | A perimeter network segment that is logically inserted between internal and external networks. |
| **Firewall** | Firewalls are devices or programs that control the flow of network traffic between networks or hosts employing differing security postures. |
| **High Availability** | High availability (HA) is the ability of a system or system components to be continuously operational for a defined desirable amount of time. |
| **Internal Network** | In the context of industrial automation and control systems, the term internal network refers to the segment of the network that is the primary focus of protection. The internal network is viewed as trusted. |
| **Less Critical OT Systems** | Systems that rely on or connect to critical OT systems that has limited control and impact on the Eskom power system, or the information stored on the system is not classified as secret or top secret |
| **Logical Access** | Being able to interact with data through access control procedures such as identification, authentication and authorization. |
| **Nonprogrammable components** | Examples of nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels media converters, port savers, and couplers. |
| **Operational Technology** | All systems (including electronic, telecommunications, computer systems and components) that process, store or communicate operational data or information. |

| Definition | Description |
|---|---|
| **Trusted** | The internal network with the highest security posture. The trusted network contains systems (e.g. critical cyber assets) that require protection from the threats posed by external networks. |
| **Untrusted** | An external network with a different security posture than the trusted network. The untrusted network is viewed as unsecure and the potential source of cyberattacks on the trusted network. |

### 2.3.2 Disclosure classification

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

## 2.4 Abbreviations

| Abbreviation | Description |
|---|---|
| **CPS** | Cyber-physical Systems |
| **DMZ** | Demilitarised Zone |
| **ESP** | Electronic Security Perimeter |
| **HA** | High Availability |
| **ICMP** | Internet Control Messaging Protocol |
| **IDPS** | Intrusion Detection Prevention System |
| **IDS** | Intrusion Detection System |
| **IP** | Internet Protocol |
| **IPS** | Intrusion Prevention System |
| **IT** | Information Technology |
| **PSP** | Physical Security Perimeter |

## 2.5 Roles and responsibilities

This guide document serves to guide Eskom OT System owners. The Eskom OT System owners may delegate the responsibility of the implementation, management and support of the information defined in this guide.

## 2.6 Process for monitoring

This document will be revised from time to time as required, as the review of Eskom's corporate strategy and as functional IT, OT, Technology and Smart Grid strategies evolve, and will ultimately be superseded by revisions of the relevant policy and procedure documents.

## 2.7 Related/supporting documents

[11] 240-102220945, Specification for Integrated Access Control System (IACS) For Eskom Sites

## 3. The Defense-in-Depth Model

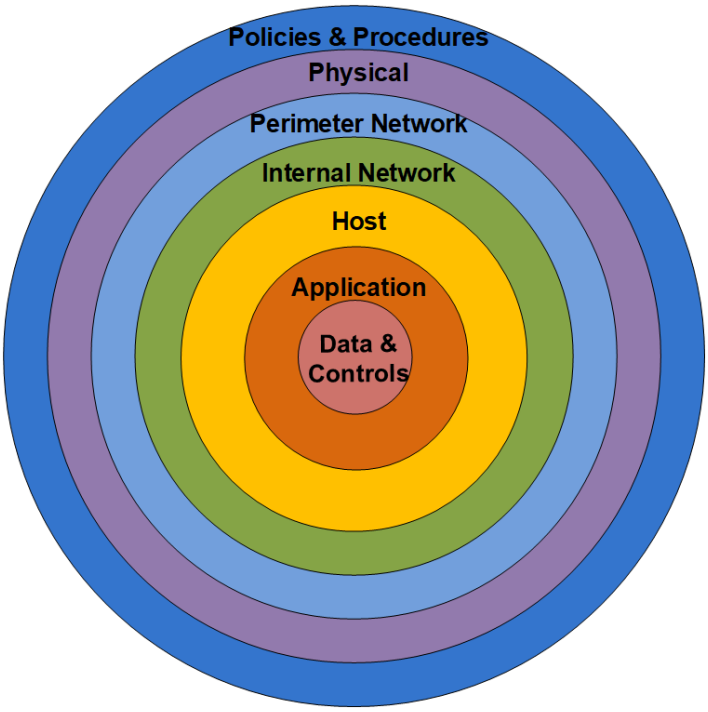



**Figure 1: Defense in Depth Model**

As can be seen in the generic defense-in-depth model in Figure 1, a thoroughly realised security posture is layered with various controls collaboratively protecting critical cyber assets. Physical security controls are paramount to the security of critical cyber assets, and a compromise in physical security controls could directly render many cyber security controls ineffective. Due to the integrated nature of technologies, physical security controls are now partly made up of cyber assets that contribute to the physical security of an environment.

## 4. Cyber-Physical Security

Examples of physical security controls that are also cyber assets, or otherwise stated, cyber assets that monitor and control access to physical environments include, but are not limited to the following:

- Access Control Systems
- Identity and Access Management Systems
- Card readers
- Biometric devices
- CCTV
- Pin pads
- Hardware tokens
- Thermal readers
- Logging and monitoring systems and databases
- Building Management Systems and subsystems

## 4.1 General Requirements

1) All access or attempts at access to critical cyber assets, authorised or unauthorised, should be monitored through a physical access point into the Physical Security Perimeter.

2) There should be logged through automated means (or by personnel who control entry) the entry and exit of each individual with or without authorised unescorted physical access into each Physical Security Perimeter, along with information to identify the individual and the date and time of entry. For individuals not authorised for unescorted physical access, the name of an individual point of contact responsible for the visitor shall also be logged. Such logs shall be stored in a secure, access controlled database.

3) Physical and digital access logs of entry of individuals with or without authorised unescorted physical access into each Physical Security Perimeter shall be kept for a predefined amount of time, depending on the criticality of the systems housed in the physical environment.

4) An alarm or alert shall be issued in response to detected unauthorised access through a physical access point into a Physical Security Perimeter. Such alarms shall be provided through a secure, access controlled channel. There shall be logs proving that the alarm was issued and communicated. Such logs shall be stored in a secure, access controlled database.

5) Physical access shall be restricted to cabling and other nonprogrammable communication components used for connection between applicable Critical Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. When physical access restrictions to such cabling and components cannot be implemented, one or more of the following should be implemented to mitigate risks:

   a) Encryption of data that transits such cabling or components

   b) Monitoring status of communication links composed of such cabling and components and issuing an alarm or alert in response to detected communication failures within 15 minutes of detection

## 4.2 The Physical Security Perimeter

### 4.2.1 Defining the Physical Security Perimeter

In addition to the Electronic Security Perimeter (ESP), the Physical Security Perimeter (PSP) is just as important for adequately securing critical cyber assets. Physical security is a key component of cyber security, and traditionally fills the outer layer of the Defense-in-Depth approach to securing cyber assets.

It is important to understand the PSP (the “six-wall” border (walls, floor, and roof)) thoroughly in order to understand risks associated with the cyber assets that operate within the context of physical security, and controlling physical access to such cyber assets.

### 4.2.2 Zones

As defined in the *Specification for Integrated Access Control System (IACS) For Eskom Sites* [2] standard, critical cyber assets are secured by Access Control System Classes 4 and 5. As such, the following zones are applicable:

Class 4 – Unique Access Card

In a class 4 access control system, it shall be possible to decentralise the intelligence. Each card shall have a code chosen from at least ten million possibilities and any attempt to change or modify the code shall destroy the card. It shall be possible to add cards to or delete cards from the system.

The cards shall not be accepted by any system other than the one in which they are intended to operate.

This class of access control systems shall incorporate a central control and monitoring system whereby the central processor software can be used to generate reports on the status of any card.

Class 5 – Unique Access Card and Personal Identification Number (PIN)

A class 5 access control system shall have at least the same features as a class 4 system, but shall also use a PIN of at least four digits or use biometrics.

In both Class 4 and Class 5, other access control data carrier technologies such as Biometrics may be used instead of a card.

### 4.2.3 Critical Cyber Asset Components Communicating Beyond the PSP:

All cabling and nonprogrammable communication components that are within an ESP, but extend outside of the PSP housing Critical Cyber Assets should be protected. Protection can be achieved by either physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or though data encryption, circuit monitoring, or equally effective logical protections. It is intended that such physical protection reduces the possibility of tampering or obtaining direct access to the nonprogrammable devices. Examples of these types of protections include:

- Conduit
- Secured cable trays
- Secured communication closets
- Armoured cabling
- Stainless steel or aluminium tubes

Such protection should cover the entire length of the cabling and any termination points that may be outside of a defined PSP. Exposed communication pathways outside of the PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of the Critical Cyber Assets residing within the PSP.

These physical security measures should be implemented in such a way that they provide a mechanism to detect or recognise that someone could have tampered with the cabling and nonprogrammable components. This could be as simple as a padlock on a communications closet where it can clearly be recognised that the padlock has been cut off.

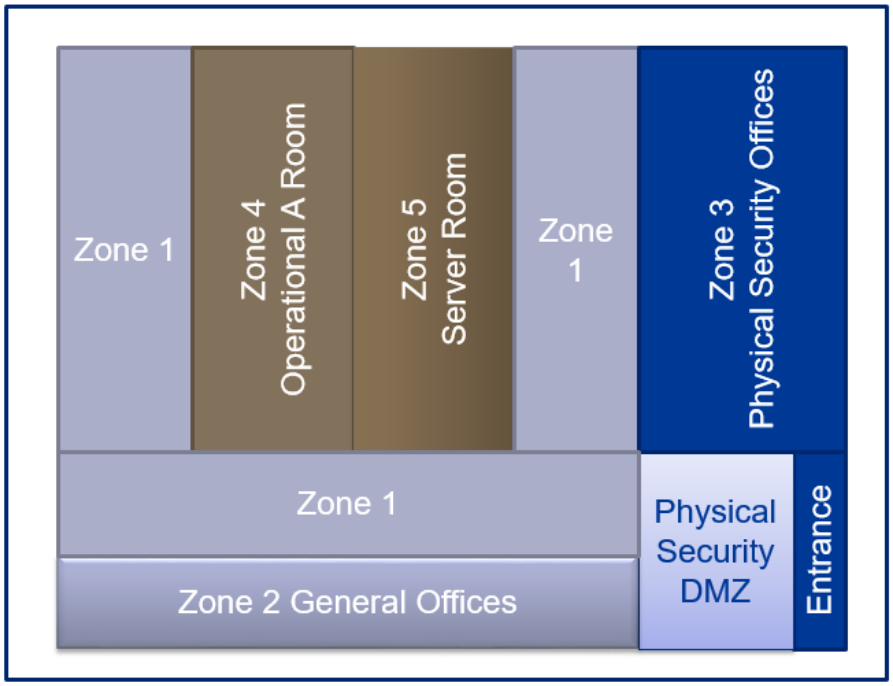
These controls cover only those portions of cabling and nonprogrammable communications components that are located outside of the PSP. Where cabling and nonprogrammable communications components exist within the PSP, this need for this protection no longer applies.

## 4.3 Physical Access Control Systems

The most deployed authorisation scheme in use today is role-based access control (RBAC), where roles (e.g., manager, accounts receivable clerk, loan officer) provide a means of expressing a subject's authority, responsibilities, or job functions. The process of assigning a role attribute value to a subject indirectly grants the subject permissions that are associated with the role.

Confidence in access control decisions is dependent on the accuracy, integrity, and timely availability of role attributes. If a subject is inappropriately assigned an attribute value, whether through complacency, error, delay, or malice, the result is the same—an inappropriate access state occurs.

For physical access, a matrix can be created with the job function and the security floor plan to show access. This is shown in the figure below.




Role Based Access Control model allows easy management of physical access.

| Job | Zone |
|---|---|
| Support Staff | 1, 2 |
| Server Admin | 1, 4, 5 |
| Operator | 1, 4 |
| Manager | 1, 2 |
| Security | 1, 3 |

**Figure 2: Example Access Control Supporting Physical Access Management with RBAC**

According to [2], access to a Class 4 zone requires the use of a unique access card for authorisation. A Class 5 zone requires two-factor authentication through means of a unique access card and personal identification number (PIN). Technologies such as biometrics may be used instead of a card.

RBAC along with access controls assist with the identifying and implementing of the following:

1) Separation of Duties is widely known control set in place to prevent fraud and other mishandling of information. Separation of duties means that different people control different procedures so that no one person controls multiple procedures.

2) Job rotation is the concept of not having one person in one position for a long period of time. The purpose is to prevent a single individual from having too much control. Allowing someone to have total control over certain assets can result in the misuse of information, the possible modification of data, and fraud. Job rotation should be used to reduce the risk of fraud or corruption by an individual.

3) Mandatory vacation policies have a fraud deterrent purpose similar to job rotation. Many companies will have a policy of requiring employees in sensitive positions to take mandatory vacations. As with job rotation, the knowledge that another person will be performing their duties and examining their work is often enough to deter the fraudster.

4) Dual control means that two or more people are required in order to control a single process. This is recommended for critical operations and reduces the risk of a rogue employee performing unauthorised operations.

### 4.3.1 Physical Access Control Risks

When physical access control systems make use of biometrics in order to authenticate individuals, there is always a risk of false rejection and false acceptance. This is due to the inaccurate nature of biometrics, and the likelihood that, for example, a fingerprint could be incorrectly interpreted by the access control system.

**Table 1: Physical Access Control Risks**

| Risk | Description | Result | Mitigation |
|---|---|---|---|
| False Rejection Rate (FRR) | Type 1 Error – Denies access to an authorised individual | Authorised employees unable to obtain legitimate access. Can result in security controls being disabled in order to provide employees needed access. | As the sensitivity of a biometric system increases, FRRs will rise and FARs will drop. Fine-tune the FRR to an acceptable rate. |
| False Acceptance Rate (FAR) | Type 2 Error – Allows access to an unauthorised individual | Unauthorised entry into the premises. | As the sensitivity is lowered, FRRs will drop and FARs will rise. Fine-tune FAR to an acceptable rate. |
| Access Control Bypassed | Access control either is manually bypassed, defeated or not working | Unauthorised entry into the premises. | Use multiple types of access controls. |

The Crossover Error Rate (CER) is when the False Rejection Rate (FRR) and False Acceptance Rate (FAR) cross as shown in the figure below. The lower the value of the CER, the more reliable the access control. If an access control is not working as intended, a lower CER access control is required.

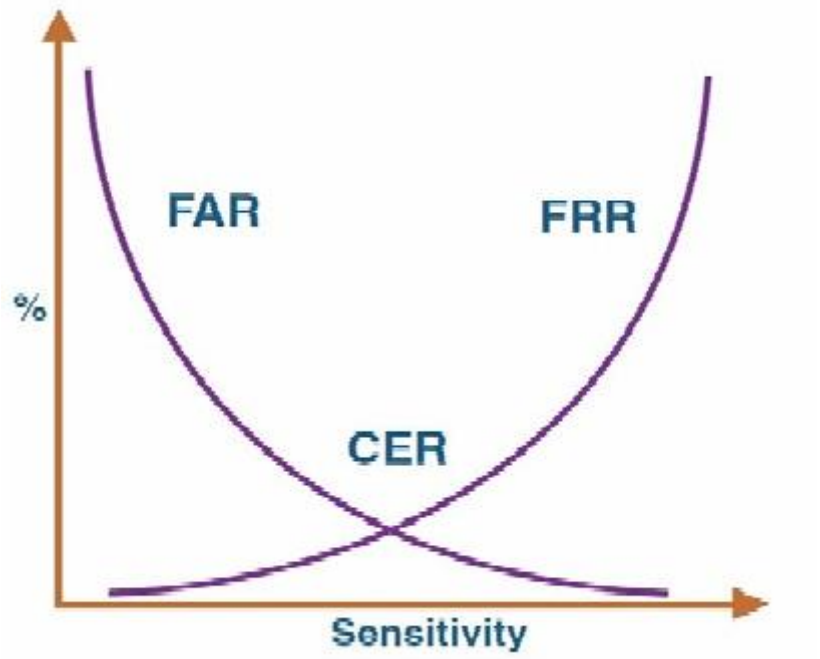



**Figure 3: Example Crossover Error Rate for an Access Control Mechanism**

### 4.3.2 Physical Access Control Types

**Table 2: Access Control Type Classifications**

| Type | Description | Examples |
|---|---|---|
| **Type 1** | Something you know | Password, Pin Code |
| **Type 2** | Something you have | Key, Smart Card, Token, One Time Pin. |
| **Type 3** | Something you are | Biometrics |

Access controls can be broken into three types as shown in the table above. Generally, the most secure access control is type three, and least secure is type one. It is expensive to implement type two and type three controls compared to type one controls. Therefore, it is important to decide whether the security risk associated with the environment being protected justifies the investment in type two or type three security. Generally, in order to protect areas housing critical cyber assets, a combination of types 1, 2, and/or 3 is used. This is known as multi-factor authentication.

### 4.3.3 Physical Access Control Methods:

For access into Physical Security Perimeters housing Critical Cyber Assets, at least two of the following access control methods should ideally be in place:

- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. Security personal are important to have when discretion is needed in a security control. Security personnel who operate or use access control systems should receive the appropriate cyber security and awareness training, as they often interface directly with access control systems.
- Pin Code Lock (Type 1): A lock where an input must be given to gain access. Employees should keep their codes confidential.
- Card Key (Type 2): 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. Employees should keep their card keys safe and not allow anyone else access to it.
- Tokens (Type 2): A key that is uniquely generated and communicated to the authorized individual. The individual then inputs this key to authenticate. Tokens come in two forms:
    - Hash-based One Time Pins (HOTP) – HOTPs are generated and given to the individual. They do not expire and can be used only once. Multiple HOTPs can be generated at once. HOTP is favoured when a communication channel for a token is not available and the token must be generated in advanced.
    - Time-base One Time Pins (TOTP) – TOTP (also known as One Time Pins) are generated when a user requires access and must be used in a short time span (e.g. 30 seconds). TOTP is favoured when a communication channel is available. It is also considered more secure than HOTP as the OTP can expiry and cannot be used in the future. TOTPs can also be has-based, and therefore generated offline and expire within a short time-span.
- Special Locks (Type 2): These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- Biometrics (Type 3): Access control mechanism where an individual is uniquely identified and authenticate based on their unique biology. Biometrics come in various types:
    - Eye Scanners – Uses your eye to authenticate.
        - Retina Scanner captures the complex arrangement of blood vessels to the eye. Highly accurate, but the eye can change over time due to illness like diabetes, glaucoma, or retinal degenerative disorders.
        - Iris Recognition captures the complex pattern of your Iris and is unlikely to change for the lifetime of a person.
        - While both are contactless, retinal scanning is considered to be invasive because it beams visible light into the eye, whereas iris recognition uses a digital photograph for identification and is non-invasive, and also typically less expensive.
    - Thermography Recognition – A thermogram is a representation of infrared energy in the form of a temperature distribution image. Because blood vessels are highly unique, corresponding thermograms are also unique – even among identical twins.
    - Facial Recognition – Facial recognition software measures the geometry of the face.

- Voice Recognition - Voice recognition technology falls under both the physiological and behavioural biometric umbrellas. Physically speaking, the shape of a person's vocal tract, including the nose, mouth, and larynx determines the sound produced. Mismatches due to illness or other factors can occur.
- Fingerprint recognition, which measures a finger's unique ridges, is one of the oldest forms of biometric identification, and widely used due to its non-invasive nature and affordability.
- Finger/Hand Veins - Veins are considerably harder to hack than other biometric scans because they occur deep within the skin. Infrared lights pass through the skin surface where they absorb into deoxygenated blood.
- Hand geometry biometrics refer to the measurement of hand characteristics like the length and width of fingers, their curvature, and their relative position to other features of the hand. Legacy authentication method and replaced with fingerprint biometrics.

**Note**: Based on CER, the Iris scanner is considered the best and the voice Recognition is considered the worst as it is prone to many issues to prevent authorized user access.

The use of two-factor authentication is acceptable at the same entry points if a non-layered, single perimeter is used (e.g. the use of both a card key and biometrics to enter one access point into the Physical Security Perimeter is acceptable). For physical layered protection, two single authentication factors may be used (e.g. a locked gate in combination with a locked control-building), provided no single authenticator (e.g. a card or a key) can provide access through both. All Physical Access Control Systems into the Physical Security Perimeter shall be housed within the Perimeter it is protecting.

### 4.3.4 Securing the Physical Access Control System:

The physical access control system should be classified as a critical cyber asset, and therefore all applicable controls for critical cyber assets should apply to it.

- The physical access control system should be located inside the PSP in its entirety. Where it communicates outside of the PSP, the applicable security controls apply, as discussed in the previous sections.
- Additional security requirements are detailed in the Cyber Security Standard for Operational Technology [3].

### 4.3.5 Enrolment guidelines

It is important that authorised users are correctly vetted for the access required. NIST 800-63a recommends the following identity assurance levels (IALs):

1) IAL 1: There is no requirement to link the applicant to a specific real-life identity

2) IAL2: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing.

3) IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained Credential Service Provider (CSP) representative.

**Table 3: IAL Requirements Summary**

| Requirement | IAL1 | IAL2 | IAL3 |
|---|---|---|---|
| Presence | Not required | In-person and unsupervised remote. | In-person and supervised remote. |
| Resolution | Not required | The minimum attributes necessary to accomplish identity resolution. | The minimum attributes necessary to accomplish identity resolution. |
| Evidence | No identity evidence is collected | One piece of SUPERIOR or STRONG evidence as defined by NIST, or<br>Two pieces of STRONG evidence, or<br>One piece of STRONG evidence plus two (2) pieces of FAIR evidence. | Two pieces of SUPERIOR evidence, or<br>One piece of SUPERIOR evidence and one piece of STRONG evidence as defined by NIST, or<br>Two pieces of STRONG evidence plus one piece of FAIR evidence. |
| Validation | No validation | Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented. | Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented. |
| Verification | No verification | Verified by a process that is able to achieve a strength of STRONG. | Verified by a process that is able to achieve a strength of SUPERIOR. |
| Address Confirmation | No requirements for address confirmation | Required. Enrolment code sent to any address of record. Notification sent by means different from enrolment code | Required. Notification of proofing to postal address. |
| Biometric Collection | No | Optional | Mandatory |
| Security Controls | N/A | SP 800-53 Moderate Baseline (or equivalent federal or industry standard). | SP 800-53 High Baseline (or equivalent federal or industry standard). |

Access should be periodically reviewed to ensure that access is still relevant and if not, then removed.

## 4.4 Physical Access Logging, Monitoring & Alarms

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorisation. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerised Logging: Electronic logs produced by an access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorised to control and monitor physical access.

### 4.4.1 Securing the CCTV Feed

Considerations for the protection of CCTV data include integrity, privacy and disruption. IP devices and servers incorporating encryption solutions such as 256-bit Advanced Encryption Standard help prevent intruders from reconfiguring devices, gaining unauthorised access to stored data or interfering with live data streams from cameras. All CCTV solutions should therefore make use of end-to-end encryption for recording and streaming.

The recording media should be removable, hot swappable and lockable. The stored footage should be encrypted to prevent unauthorised access. There should be a minimum of 2 access levels to stored footage:

- Level 1 should provide viewing of footage only, with no ability to delete footage or view or change settings.
- Level 2 should provide full administrative rights.

All footage should be kept for a minimum of 30 days and for as long as storage allows. It should be possible to 'flag' or export important footage, such as that deemed so by authorised personnel or events triggered by video analytics, so that it will not be overwritten. When the video storage is full, recording should continue by overwriting the oldest recordings first. Flagged or exported footage shall not be overwritten.

The Network Video Recorder shall keep a time stamped electronic log of the following:

- User who has logged in to make changes
- Changes made
- System Errors
- Interruption of Camera streams

### 4.4.2 Logging & Monitoring the System

A physical security system can only be expected to effectively protect an organization if security personnel are always paying attention to the status of the system.

System monitoring should be able to record all relevant events, including:

- Successful entry: Every employee entry to an area must be logged.
- Unsuccessful entry: Every "Access Denied" must be logged and investigated, this is to determine whether an employee was attempting access to a restricted zone or if someone with an illegal card is trying to gain access.
- Impossible activity: This includes employees being at two places at the same time, this could be the result of employee card being cloned. Multiple entry must be logged.
- Reader tampering: Card tampering reader detection should be installed, this will log when someone is trying to tamper with the system or remove it.
- Equipment faults: Malfunctions of any device must be logged, this will keep track of equipment that are not working properly as well as possible signs of tampering.
- Door ajar: These events should be logged and flagged by the access control system.
- Power failures: Back-up power must be installed and power failures must be logged.
- Employee access card change: All changes to an employee's access must be logged.
- Zone and general system configuration change: All changes to the system configuration must be logged as well as the name of the person making the changes.

The purpose of system monitoring is to be aware of critical events in physical security, critical events include:

- Tampered Reader: This notifies the department or the person monitoring the system in the form of an alarm. This indicates an intruder is attempting to gain access to a facility that they are not permitted to enter.
- Forced doors: Any event where the combination of request-to-exit device, door status, and key card system indicates that a door was opened from the outside without a key card may represent a forced entry or an equipment malfunction.
- System abnormalities: Problems including "Reader offline" as well as system malfunctions and lockups require immediate investigation. They could indicate tampering or an intrusion attempt.

- Network intrusion: Firewalls and network intrusion detection systems that protect the physical security system may detect an attempted or even a successful network break-in. This may be an emergency situation requiring a temporary shutdown of the physical security system.

Alarms:

- False intrusion alarms: Some doorways are more prone to false alarms, especially when request-to-exit devices don't scan a wide enough area. Multiple request-to-exit motion detectors with a wide "Visual" range, a request-to-exit button switch, or a crash bar or door latch with an integrated request-to-exit can be used.

### 4.5 Employee Training & Education

Employee education is critical. By helping employees understand why security is important, and by providing them proper training on the systems that they need to interface with, they are far more likely to contribute to an increased security posture and mitigate many risks associated with physical and cyber security.

Additional points employees need to be aware of include:

a) Doors should not be propped: If there is construction, remodeling, or a lot of equipment being moved through the building, the facilities management team should make appropriate arrangements to provide supervision of open doors or prevent their propping altogether.

b) Do not tailgate: One card, one entry policy should be implemented, this is to prevent tailgating.

c) Avoid door holds: Employees should be encouraged not to hold doors for each other as each employee should use their own access cards to gain access.

d) Do not loan or borrow access cards.

e) Report lost or stolen cards immediately.

f) Do not leave access control systems unattended.

## 5. Authorization

This document has been seen and accepted by:

| Name and surname | Designation |
|---|---|
| Dr Titus Mathe | General Manager – RT&D |
| Naresh Hari | General Manager – Transmission Engineering |
| Nelson Luthuli | Chairperson – PTM&C Technical Committee |
| Abraham Parbhunath | Chairperson – OT Cyber Security Care Group |
| Prathaban Moodley | Chairperson – Smart Grid Technologies Study Committee |

## 6. Revisions

| Date | Rev | Compiler | Remarks |
|---|---|---|---|
| Nov 2021 | 1 | R Dalvie | First issue of guide document. |

## 7. Development team

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

- Billy Petzer
- Matthew Taljaard
- Raees Dalvie

## 8. Acknowledgements

Not applicable.