

Electrical Security Installations

Part 2:

Access Control

PUBLIC REVIEW DRAFT

KS 2112-2: 2009

TECHNICAL COMMITTEE REPRESENTATION

The following organizations were represented on the Technical Committee:

Eveready Batteries Kenya Ltd.
Associated Battery Manufacturers
Kenya Railways Corporation
Securicor Alarms (K) Ltd.
Kenya Power & Lighting Company Ltd.
Automotive Industrial Battery Manufacturers (A.I.B.M) (K) Ltd.
Ministry of Energy
Jomo Kenyatta University of Agriculture and Technology — Electrical Engineering Department.
General Electric
Kenya Pipeline Company
Standard Chartered Bank
Kenya Police
Ministry of Information and Communication
Chloride Exide
KK Security Group
BM Security Services

Kenya Bureau of Standards — Secretariat

REVISION OF KENYA STANDARDS

In order to keep abreast of progress in industry, Kenya Standards shall be regularly reviewed. Suggestions for improvements to published standards, addressed to the Managing Director, Kenya Bureau of Standards, are welcome.

© Kenya Bureau of Standards, 2009

Copyright. Users are reminded that by virtue of Section 25 of the Copyright Act, Cap. 12 of 2001 of the Laws of Kenya, copyright subsists in all Kenya Standards and except as provided under Section 26 of this Act, no Kenya Standard produced by Kenya Bureau of Standards may be reproduced, stored in a retrieval system in any form or transmitted by any means without prior permission in writing from the Managing Director.

Electrical Security Installations

Part 2:

Access Control

KENYA BUREAU OF STANDARDS (KEBS)

Head Office: P.O. Box 54974, Nairobi-00200, Tel.: (+254 020) 605490, 602350, Fax: (+254 020) 604031
E-Mail: info@kebs.org, Web: <http://www.kebs.org>

Coast Region

P.O. Box 99376, Mombasa-80100
Tel.: (+254 041) 229563, 230939/40
Fax: (+254 041) 229448

Lake Region

P.O. Box 2949, Kisumu-40100
Tel.: (+254 057) 23549, 22396
Fax: (+254 057) 21814

Rift Valley Region

P.O. Box 2138, Nakuru-20100
Tel.: (+254 051) 210553, 210555

Foreword

© KEBS 2009 — All rights reserved

KS 2112-2: 2009

This Kenya Standard was prepared by the Extra Low Voltage Equipment Technical Committee under the guidance of the Standards Projects Committee, and it is in accordance with the procedures of the Kenya Bureau of Standards.

Access control to premises is a key element of security in buildings. Access control is a means of controlling access by unauthorised persons and also of restricting movement to designated areas by any authorized persons. Such restrictions will be found in banks, other financial institutions and libraries (however, the usage is not restricted to these premises)

It is the demand for such systems due to their role in enhancing security and the continued expansion on their usage which necessitated the need for standards which will give guidance in their installation, maintenance, monitoring, e.t.c.

During the preparation of this standard, reference was made to the following documents:

SANS 10222-2:2007; Electrical Security Installations. Part 2; Access Control.

Acknowledgement is hereby made for the assistance derived from these sources.

PUBLIC REVIEW DRAFT

Electrical Security Installations

Part 2: Access Control

1 Scope

1.1 This part of KS 2112 establishes general principles for the planning, design, installation, operation and maintenance of access control systems.

1.2 Requirements for the components of access control systems are given in KS 2112-2-1 to KS 2112-2-7.

2 Normative references

The following standards contain provisions that, through reference in this text, constitute provisions of this part of KS 2112. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of KS 2112 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Information on currently valid national and international standards may be obtained from Kenya Bureau of Standards.

KS 2112-1, *Electrical security installations – Part 1: General.*

KS 2112-2-1, *Electrical security systems – Part 2-1: Access control systems: General characteristics.*

KS 2112-2-2, *Electrical security systems – Part 2-2: Access control systems: Central processor.*

KS 2112-2-3, *Electrical security systems – Part 2-3: Access control systems: Card readers.*

KS 2112-2-4, *Electrical security systems – Part 2-4: Access control systems: Reader controllers.*

KS 2112-2-5, *Electrical security systems – Part 2-5: Access control systems: Biometric readers.*

KS 2112-2-6, *Electrical security systems – Part 2-6: Access control systems: Access cards.*

KS 2112-2-7, *Electrical security systems – Part 2-7: Access control systems: Barriers.*

3 Definitions

3.1

acceptable

acceptable to the authority administering this standard, or to the parties concluding the purchase contract, as relevant cubicle that has two or more doors, which are unlocked in a sequence controlled by an access control system

3.3

access card

card or token capable of storing a unique code that is intended to be read by a card reader

3.4

access card facility code

unique code stored on an access card and that refers to the facility at which the card is to operate

3.5

access card presentation

way in which an access card is presented to the sensor of a card reader, e.g.:

- a) swallow: the card is drawn into the reader for later retrieval;
- b) swipe: the card is swiped through a slot in one direction past the reader sensor;
- c) push: the card is pushed into a slot and then pulled out;

KS 2112-2: 2009

d) proximity: the card is brought within a specified angle and specified distance of the reader sensor.

3.6

access control

means of providing automated passage for authorized personnel

3.7

access control system

system consisting of a combination of components selected from the following:

- a) a central processor;
- b) reader controller(s);
- c) card reader(s);
- d) biometric reader(s);
- e) barrier(s);
- f) access cards;
- g) a power unit;
- h) system software; and
- i) signalling interface(s) (modem) for a remote station

3.8

access level

programmable level of access that allows or denies persons access to controlled areas, depending upon their degree of authorization

3.9

access point

point at which entry or exit or both is controlled by a barrier such as a door or a turnstile

3.10

anti-passback

logic facility that denies multiple access or egress without a corresponding reversal of access or egress status

3.11

availability

indication of reliability in accordance with the formula, $A = (MTBF - MTTR) / MTBF \times 100$, where A is availability, MTBF is the mean time between failures and MTTR is the mean time to repair

3.12

barrier

means intended to deny unauthorized persons access to a controlled area

3.13

biometric system

system that incorporates a device (reader) that is capable of comparing a physical characteristic of a person with previously stored records of that person's characteristics, such as fingerprints, retina patterns, hand dimensions, signatures, voice patterns or pictures

3.14

card issue level

access level assigned to a specified person or party and recorded on the access control software program

3.15

card reader

device that has a sensor capable of reading unique codes stored on an access card

3.16

card reader technology

technique used to store on or in an access card codes that can be read by a card reader

3.17

central display

VDU screen that serves as a logged message output device, as an operator's screen and as an alarm displaying terminal

3.18

central processor

device that is either a separate unit or an integral part of the access control system, and that modifies, stores or isolates information about the access control system by means of dedicated software and hardware

3.19

central processor software

access control application program transportable between several computers that have similar architecture

3.20

combined system

access control system that incorporates additional functions such as alarms or staff attendance registers

3.21

common code

code number unique to the access control system, and allocated to every user

3.22

controlled area

area to which access is controlled by an access control system

3.23

data memory

data base that contains valid code identities

3.24

detection loop

sensor that is buried in a road at a barrier, to detect vehicle movement

3.25

fail safe

mode of operation that deactivates a locking mechanism in the event of a power failure

3.26

fail secure

mode of operation that activates a locking mechanism in the event of a power failure

3.27

fingerprint reader

biometric device that, with the aid of its microprocessor, is capable of recognizing a person's fingerprint pattern by comparing it with stored records

3.28

hand-geometry reader

biometric device that, with the aid of its microprocessor, is capable of recognizing a person's hand by comparing it with stored records

3.29

inductive card reader

device that is capable of recognizing a unique punched conductive foil within a card

KS 2112-2: 2009

3.30

infra-red bar code card

card that can so process (or allow low-level infra-red light to pass through) a special or unique invisible bar code imprinted in the card that the code can be read (typically on the opposite side of the card) by light-sensitive devices

3.31

intelligent card

smart card that contains a complete microprocessor with a memory, which can contain factory-encoded data to allow for information to be taken to different facilities

3.32

interface capability

means of coupling by which parts of the access control system (e.g. a card reader or a reader controller) are connected to the central processor

3.33

key override

manual means of overriding the control function of a barrier in case of malfunction or in an emergency situation

3.34

keypad

digital data entry point, to permit users to enter a code number into a system

3.35

lift time

lower time time taken by a boom to move from a completely closed (or completely opened) position to a completely opened (or completely closed) position

3.36

magnetic reader

device that is capable of reading a code on a card by using magnetic field density to measure the permeability of the card, the permeability being controlled by holes punched in the card

3.37

magnetic stripe access card

card that has a thin surface-mounted strip of magnetic recording tape with various tracks on which information is encoded

3.38

manual controls

manually operated switches, push buttons or keys that influence the operation of a barrier

3.39

mechanical crank

device that is operated manually in the case of a power failure in order to change the status of an access control barrier, e.g. lift, lower, open, close

3.40

motorized boom

barrier that, on instruction from an access control system, is lifted and lowered by means of an electric motor

3.41

off-line reader

reader that is not connected to a central processor

3.42

on-line reader

reader that is connected to a central processor

3.43

personal identification number

PIN random sequence of digits allocated to each individual user of a system or keypad

3.44

power supply

part of an access control system that provides power for the operation of the whole or part of the system

3.45

proximity-type card reader

device that is capable of reading a card that is brought within a specified distance of and within a specified angle to the reader sensor

3.46

push-type card reader

device that is capable of reading a card that is inserted into a slot and then pulled out

3.47

reader

device that is capable of extracting data from an encoded card or from a person

3.48

reader controller

device that is capable of interpreting codes read by a card reader or biometric reader and allowing or denying access by operating a barrier

3.49

retina scanner

biometric device that, with the aid of its microprocessor, is capable of recognizing a person's retina pattern by comparing it with stored records

3.50

signature recognition reader

biometric device that, with the aid of its microprocessor, is capable of recognizing a person's signature by comparing it with stored records

3.51

stand-alone card reader (see 3.41 **off-line reader**)

3.52

swallow-type card reader

device that is capable of reading a card that has been drawn into the reader for later retrieval

3.53

swipe-type card reader

device that is capable of reading a card that is swiped through a slot in one direction past the reader sensor

3.54

system-sensing proximity system

system that senses the presence of a coded device that contains no power source and where the device communicates with the system by re-radiating an interrogating RF signal back to the system at a specified frequency

3.55

tail-gating

two people or two vehicles obtaining access or egress in a single recognition process

3.56

tamper protection

application of electrical or mechanical means to prevent deliberate interference with any part of an

KS 2112-2: 2009

access control system

3.57

time zone

programmable period of time during which system parameters are automatically evaluated, e.g. denial of access outside of normal working hours, and pin override

3.58

transaction

logical series of events that occurs within a system, such as the acceptance of a door alarm report or the release of a barrier following a valid recognition procedure

3.59

transaction memory

part of the reader controller that stores transactions

3.60

transaction time

time between the start of the recognition procedure and the appropriate response

3.61

user-activated proximity system

system in which the user initiates the code to the controller

NOTE Such a device, carried by the user, normally incorporates a power source.

3.62

validation

process whereby access or egress, through software manipulation, is made valid or invalid

3.63

vehicle boom

barrier, controlled by an access control system, in the form of a pole that is lifted and lowered by means of an electric motor or hydraulics to allow or deny access to vehicles

3.64

vehicle stopper

barrier, controlled by an access control system, that is lifted and lowered by means of an electric motor or hydraulics or both, to allow or deny access to vehicles and to prevent an attempted forced entry

3.65

voice recognition system

biometric system or device that, with the aid of its microprocessor, is capable of recognizing a person's voice or speech pattern by comparing it with stored records

3.66

wiegand access card

card that has pieces of magnetic material (tungsten nickel alloy) embedded in it during its manufacture, and that is read by an array of magnetic sensing heads that determine whether there is a slug at each of the possible positions. (A slug comprises a small piece of wire that is heat treated under tension, resulting in a magnetic snap-action that creates a consistent reading signal over a wide range of reading speeds)

4 Planning

4.1 General

The type of environment in which an access control system is to be utilized and the requirements of the facility (software) shall be investigated before a decision is made regarding the type and class of access control system required.

The requirements of the access control system shall be decided upon by consultation between the parties concerned (such as the client, the consultant, the supplier of the system, the telecommunications

authority, and, if relevant, the local police or fire authority, the insurer and any public authority involved).

4.2 Choice of system

The choice of system to be installed depends upon the predetermined level of security required. The required level of security influences the type and number of access points and how they are to be controlled.

Plans or specifications or both, classified at an appropriate security level, shall be prepared and shall show:

- a) schematic drawings of the proposed access control system installation;
- b) the siting of the equipment;
- c) any provisions, such as ducts, conduits and channels that are required for wiring, including the need for segregation of wiring where necessary; and
- d) the mains power connections required.

4.3 Extensions

To remain efficient, an access control system installed in a building may eventually require extensions or modifications or both. The size and layout of ducts, chases, etc., shall be sufficiently flexible that (as far as can be foreseen) such extensions and modifications can be undertaken.

Ease of maintenance and adequate protection against both mechanical damage and deliberate interference are also important. During the allocation of the space required for control, communication and power supply equipment, it is necessary to ensure that the access control equipment is easily accessible for maintenance purposes, but at the same time, is adequately protected against deliberate interference. The system software shall also provide for extensions.

5 Design

5.1 General

An access control system consists of a component that causes a signal to be generated when access is requested by means of a card reader or a biometric reader; a component that transmits the signal; and a component that receives, evaluates and processes the signal. The components used in the design shall be compatible and shall be such that the system can be extended or modified.

During the design of an access control system, the following shall be considered:

- a) whether sufficient access points are available to cope with peak traffic flow;
- b) whether to include more than one barrier for use by physically handicapped people; and
- c) whether the system is to be fail safe or fail secure in the event of a power failure.

5.2 Environmental

Components of access control systems are installed under various environmental conditions. During the design of a system, the following shall be considered for each component:

- a) temperature;
- b) humidity;
- c) dust and other air contaminants;
- d) vibration;
- e) the need for adequate ventilation;

KS 2112-2: 2009

f) the noise generated by printers; and

g) the actual positioning, to avoid vandalism (especially in the case of barriers that are outside) and to avoid unauthorized use.

5.3 Safety

It is necessary to consider how an access control system should operate in an emergency situation. The system shall allow emergency evacuation to take place safely and, where appropriate, panic buttons shall be provided.

6 Installation

6.1 General

Access control systems shall be installed in accordance with the relevant provisions of clause 5 of KS 2112-1:2007. All wired connections and the power supply shall be within the controlled area and protected against tampering. Any wiring that passes out of the controlled area shall be suitably protected, e.g. in metal conduit, and if the access control system is of class 4 or class 5 (see KS 2112-2-1), junction boxes shall be provided with tamper protection. The power supply to the central processor shall be protected against electrical spikes.

6.2 Siting of components

All components shall be securely mounted at a suitable height in such a position as to allow access for maintenance but to discourage tampering. Central processors shall be installed in a position that is physically secure but allows supervision by authorized persons.

7 Operation

7.1 General

Before an access control system is handed over, tests shall show that the system operates satisfactorily and complies with all relevant requirements. The commissioning procedure shall include the following:

- checking of all wiring;
- checking and recording the power supply to appropriate parts of the system;
- checking the operation of each barrier, including all interlocking mechanisms;
- programming and verifying the access levels;
- disconnecting the mains supply and ensuring that the system continues to work for the required period of time; and
- checking the operation of all tamper protection.

7.2 Operating instructions and procedures

7.2.1 All operators of an access control system shall receive adequate training, and the necessary operating instructions shall be available.

7.2.2 The operating instructions shall be clearly set out and handed over to the client in typewritten, printed or other agreed form. The instructions shall include the procedure for summoning assistance in the case of a system malfunction. The instructions shall be updated after extensions or modifications (or both) or as and when practical experience makes it necessary.

7.2.3 A log book shall be provided in which problems can be recorded. The operators shall be instructed in how to record and report problems.

8 Maintenance

8.1 Attention by client

Liaison shall be established with those responsible for maintenance of the building to ensure that their work does not cause faults on or otherwise interfere with the operation of the access control system. If structural or occupancy changes occur, the client/new client shall ensure that any necessary changes to the access control system are considered at an early stage. It is the client's responsibility both to ensure that members of staff are familiar with the agreed procedures and to ensure that the operating procedures are observed. Routine tests shall be carried out to detect faults not disclosed by the normal monitoring procedures.

8.2 Service arrangements

To ensure reliability of the access control system, the supplier of the system shall offer the client an agreement for regular servicing of the system. The agreement should include requirements that service personnel be on call at all times, both inside and outside normal working hours, and that authenticated verbal requests over the telephone for emergency service be executed promptly.

If no service contract has been arranged because of special circumstances, or where it is not possible to obtain service personnel on call at all times, at least one employee (with suitable experience of electronic equipment of the client shall have had special training with the manufacturer, supplier or installer, to deal with the more simple servicing (first level maintenance), but the employee(s) shall be given instructions not to attempt to exceed the scope of that training. The agreement shall specify the methods of liaison required to provide access to the premises. Servicing arrangements shall be made immediately on completion of the installation, whether the premises are occupied or not. An up-to-date log book of maintenance history shall be kept.

8.3 Routine maintenance

Routine maintenance visits to the access-controlled premises shall be made at suitable intervals by a representative of the supplier of the access control system. Should this company, the client or his insurer require a specified interval between maintenance visits that is shorter than that laid down in any relevant specification, this shall be clearly stated in the log book and in the contract documents.

9 Certification

The client or his representative shall certify that the required maintenance has been carried out as agreed. On commissioning the system, the client or his agent representative shall certify compliance with the relevant standards.