South African Intruder Detection Services Association

BY-LAW NO. 5

Standard Installation Specification for Intruder Alarm Systems for Residential, Commercial, Retail and Industrial Installations

AUGUST 2023 – Version 1.7

1. GENERAL

1.1 This specification lays down the minimum requirements for the construction, installation, operation and maintenance of intruder alarm systems. Specifications herein contain requirements to be applied in the aforesaid. Any deviation is to be indicated on the installation certificate and such deviation should not be seen as an acceptance of compliance.

1.2 SAIDSA does not accept any liability and/or responsibility for any defect there may be now or hereafter in the installation or any loss suffered by any party, due to its failure to operate at any time and no warranty or condition expressed or implied whether statutory or otherwise is given by SAIDSA in regard to the above installation either to the approved installer or to the customer.

1.3 This specification does not purport to cover all the necessary requirements for a particular installation and all efforts should be made to ensure correct risk assessment.

1.4 The customer must be clearly informed in the monitoring terms and conditions that the installed equipment does not prevent intrusion but is intended to detect or deter intrusion.

1.5 All equipment must be installed to manufacturer's specifications.

2. DEFINITIONS

2.1 For the purposes of this specification the following definitions apply:

2.1.1 **24-Hour Zone**: A zone that is permanently armed (Panic button, tamper switch).

2.1.2 **Alarm condition:** A condition whereby the alarm system, when armed, activates indicating a violation of any detection device.

2.1.3 **Alarm company:** A SAIDSA-approved installer prepared to enter into a contract for the provision of the installation and/or monitoring, reaction and maintenance of an intruder alarm system.

2.1.4 **APP (smartphone application):** A **mobile app** (application software) is a computer program designed to run on smartphones, tablet computers and other devices. Apps can be used for the view or control of remote systems, including intruder detection equipment. The APP should be sufficiently secure to prevent its misuse by third party. It is recommended that upon arming/disarming and bypass, the user ID is recorded in the control panel event log or server.

2.1.5 **Arming:** Putting an intruder detection system or part of it (switching on of the alarm) into such a condition that an alarm condition created by any of the associated detection devices in the alarmed area is signalled. This can be initiated via a keypad, keyfob, App or another suitable user interface.

2.1.6 **Back up battery:** Device responsible for ensuring a constant supply of backup power to the intruder alarm system in the event of a power failure.

2.1.7 **Bi-directional (2 way) Wireless transmission:** Allows the control panel and remote devices to both transmit and receive wireless signals. This allows the panel to monitor and control the device and the device to monitor the panel status and wireless connection.

2.1.8 **Bypass (Isolate):** A deliberate action whereby part (circuit) of the alarm system is disabled during a single full arming state and does not have the ability to signal an alarm condition.

2.1.9 **Central station/control room:** Continually manned premises, equipped to receive and display signals from intruder detection systems which complies with the requirements of By-Law 1 of SAIDSA and is prepared to enter into a contract for the provision of alarm monitoring.

2.1.10 **Cloaking:** The deliberate covering of an intruder using infrared blocking materials with the intent of hiding the infrared emission of the human body.
Anti-cloaking: A specific detector used to detect the deliberate covering of an intruder with infrared blocking materials.

2.1.11 **Closed circuit:** A circuit within an intruder alarm system which when opened creates an alarm condition.

2.1.12 **Closed circuit device:** A device arranged to create an alarm condition by opening a closed circuit.

2.1.13 **Code hopping:** A rolling code (Also called a **hopping code**) used in keyless entry systems to prevent the capture and recording of the code for duplication purposes. Such systems are typical in alarms, garage door openers and keyless car entry systems.

2.1.14 **Control equipment (Unit/Hub):** Equipment including switches, relays, indicators and other apparatus necessary for intruder alarm system arming, disarming, programming, fault and system indication and activation of signalling equipment.

2.1.15 **Control room Transmissions:** The transmission of intrusion detection events from the control equipment device to a control room. This can be done through a number of cable or wireless transmission methods including RF, GSM, IP, DSSS.

2.1.16 **Delay Zone:** A Detection Circuit which when the control equipment is armed will provide a time delay for the purposes of entry and exit arming or disarming.

2.1.17 **Deliberately operated device:** A device permitting the customer or his staff to deliberately create an alarm condition.

2.1.18 **Detection circuit:** Circuit by means of which one or more detection devices or deliberately operated devices are connected to the control or signalling equipment of an intruder alarm system.

2.1.19 **Detection device – electronic** (e.g. passive infrared, microwave, glass break detector) : Apparatus or section of wiring intended to detect the attempted entry or tampering by an intruder.

2.1.20 **Disarming:** to disable the detection and recording of events in the disarmed section of the system.

2.1.21 **Dual Monitoring**: Dual communication/ Dual medium communication is a process where two different mediums or carriers are being used to transmit signal to control room or monitoring station.

2.1.22 **End of line resistance (EOL)**: A closed circuit so arranged that at severance or shorting-out of any part of the wiring will cause a detectable change in the resistance of the circuit.
Double End of Line Resistance (DEOL): A closed circuit so arranged and programmed that the control panel will register an alarm or tamper condition from a detection device when the system is armed or disarmed.

2.1.23 **Event Log:** History of stored events. Event log should contain: Information, Warning, Error, Success Audit (Security Log) and Failure Audit. The event log must not be erasable and/or via downloading. The event log could be stored in the cloud.

2.1.24 **External sounder:** an external device producing an alerting sound.

2.1.25 **Flooded Battery:** A battery with the ability to add distilled water.

2.1.26 **Follower zone:** A Detection Circuit which when the control equipment is armed and subsequently violated, prior to a Delay Zone being violated, results in an instant alarm. Should a delay zone be triggered first, this zone will be treated as a delay zone.

2.1.27 **GSM** (Global System for Mobile Communications): All cellular data technology generations including 2G, 3G, 4G and 5G, and all low power machine to machine data technologies including NB-IoT, Cat M1,2,3 & 4.

2.1.28 **Hybrid system:** Intruder alarm System comprising of wireless as well as hardwired components.

2.1.29 **Instant Zone:** A Detection Circuit which when the control equipment is armed and subsequently violated, results in an instant alarm.

2.1.30 **Internal sounder** Interior device producing an alerting sound.

2.1.31 **Intruder alarm system:** A means of detecting and signalling the attempted entry or tampering by an intruder into a protected premise.

2.1.32 **IoT Systems**
IoT devices are the non-standard computing devices that connect wirelessly to a network and have the ability to transmit data, such as the many devices on the internet of things (IoT). IoT involves extending internet connectivity beyond standard devices, embedded with technology, these devices can communicate and interact over the internet. They can also be remotely monitored and controlled.

2.1.33 **Jamming:** The transmission of radio signals with the purpose of interfering with the correct operation of wireless networks to disrupt information flow, including alarm, GSM, Radio and CCTV equipment in a security installation.

2.1.34 **Keypad**: A control device used for arming, disarming, programming and status reports

2.1.35 **Masking:** The deliberate or accidental covering or blocking of a detector where the detector is unable to detect infrared.
Anti-masking: A detector specifically designed to detect the covering or blocking of a detector.

2.1.36 **Multi-Shot:** A circuit capable of multiple Alarm Conditions during a single arming period.

2.1.37 **Open circuit:** A circuit within an intruder alarm system which when closed creates an alarm condition.

2.1.38 **Open Circuit device:** A device arranged to create an alarm condition by closing an open circuit.

2.1.39 **Partition:** A programmable feature within a control panel allowing a zone or group of zones to be operated independently from the rest of the system, each partition having its own keypad functions, access codes, account codes, and reporting functions and can be armed/disarmed independently.

2.1.40 **Power supply equipment:** Equipment providing power for the retaining of the battery in a good state of charge and for the operation of any component part of an intruder detection system, either independently or through the control equipment.

2.1.41 **Protected premises:** That part of the premises under the control of one or more users to which protection is afforded by an intruder alarm system.

2.1.42 **Remote:** (also known as a keyfob). A wireless handheld transmitting device used for the purpose of remotely arming and disarming a control panel and other auxiliary functions.

2.1.43 **Repeater:** A repeater is a device that amplifies or adds to incoming electrical signals and retransmits them, in order to compensate for transmission losses. A repeater receives a signal and retransmits it at a higher level or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances.

2.1.44 **Risk area: (Protected area)** Offices, rooms and other areas within the Protected Premises, which either contain or give, access to disposable movable property.

2.1.45 **Signalling Equipment & devices:** Equipment used to communicate information to a Central Station e.g. communicator, radio, etc.

2.1.46 **Customer:** A person or organisation utilising the services of a SAIDSA-approved alarm company for the installation and maintenance of an intruder alarm system.

2.1.47 **Spread Spectrum:** Long range wireless communication network technologies including Spread Spectrum, Ultra Narrow Band and LPWAN e.g. FHSS, DSSS, THSS, CSS, LoRaWAN and Sigfox.

2.1.48 **Swinger shutdown:** whereby a zone or zones are automatically bypassed/shutdown by the system after a pre-programmed number of alarm conditions within a single arming event. (see Multi-Shot)

2.1.49 **Tamper:** Any unauthorised entry into component parts of the alarm system and detection devices.

2.1.50 **Trouble condition:** An abnormal condition in any part of an intruder alarm system, which must be eliminated to restore correct operation.

2.1.51 **Visual Verification:** Visual Verification is the management by exception of an Intruder Alarm Activation at any site being monitored, providing a means of visually verifying the intruder alarm activation.
The purpose of Visual Verification is to quickly discriminate a positive alarm that requires urgent attention from any other event that should not be considered as a positive alarm by providing a minimum level of visual information to verify an intruder alarm activation and respond to it accordingly.

2.1.52 **Volumetric Detector:** A detector capable of sensing human movement in a volume such as a room.

2.1.53 **Web Interface:** A user interface which allow users to control and interact with their security installation through a web browser. This can be used for a remote control, system management, visual feedback, and many other functions.

2.1.54 **Wireless Transmissions:** The transmissions of alarm information from a transmitting device (i.e. detector, magnetic contact or transceiver to a receiving device or console within an approved ICASA RF band.

2.1.55 **Zone (Circuit):** See closed and open circuit.

3. Risk Assessment and Planning

A full risk assessment must be conducted based on a site survey of the premises to be protected, taking into account the following:

3.1.1 Size of property including number of areas to be protected;
3.1.2 High volume areas;
3.1.3 Accessibility and human traffic within and surrounding the area;
3.1.4 Proximity in relation to the following high risk locations must be taken into account:
- 3.1.4.1 Open field
- 3.1.4.2 Construction site
- 3.1.4.3 Train Station
- 3.1.4.4 Shopping mall
- 3.1.4.5 Hospital
- 3.1.4.6 Taxi Rank

3.1.5 Number of entry / egress points;
3.1.6 Perceived vulnerability of the premises to be protected;
3.1.7 Nature and value of the assets to be protected;
3.1.8 How prone are the assets to criminal attack?
3.1.9 Weak points existing at the premises to be protected;
3.1.10 Consultants observations and recommendations.

3.2 Residential

In the case of residential premises, the following should be taken into account during the site survey:

Internal:

3.2.1 How many people are residing on the property?
3.2.2 Do different people use different entrances?
3.2.3 Are there pets inside the premises?
3.2.4 Is the ceiling area accessible?
3.2.5 Are there people with special needs or disabilities?
3.2.6 Are there high value goods kept on site?
3.2.7 Has there been a prior break-in and if so, where?

External:

3.2.8 Is there heavy shrubbery in the garden?
3.2.9 Are partitions required? E.g. Cottage, storeroom, granny flat.
3.2.10 Is there sufficient lighting in the garden?
3.2.11 Is there a history of stray or natural wildlife accessing the property?
3.2.12 Are there any high frequency devices such as cell towers in close proximity?
3.2.13 Has there been a prior break-in and if so, where?

Perimeter:

3.2.14 Is there sufficient lighting surrounding the property?
3.2.15 Are there walls or fences surrounding the property?
3.2.16 Where are the vulnerable points of entry into the property?
3.2.17 Are there points of easy access to roof or 2nd floor?

3.3 Retail, Commercial and Industrial

In the case of retail, commercial and industrial premises, the following should be taken into account during the site survey:

Internal:

3.3.1 Are there multiple buildings or areas to be protected?
3.3.2 Are partitions required?
3.3.3 Do different employees use different entrances?
3.3.4 Are there air-conditioners, vibrating machinery, fans, heaters or motors present?
3.3.5 Are there high risk areas containing computers, safes, firearms, etc.?
3.3.6 What is the nature of business being conducted on site?
3.3.7 Are there people with special needs or disabilities?
3.3.8 Are there high value goods kept on site?
3.3.9 Has there been a prior break-in and if so, where?
3.3.10 Where is the main entry/exit point?
3.3.11 Will there be multiple people using the alarm system?

External:

3.3.12 Is there sufficient lighting outside the premises
3.3.13 Are there loading bays?
3.3.14 Is there a history of stray or natural wildlife accessing the property?
3.3.15 Are there any high frequency devices such as cell towers in close proximity?
3.3.16 Are high value goods kept on the property?
3.3.17 Has there been a prior break-in and if so, where?

Perimeter:

3.3.18 Are the premises visible from the main road?
3.3.19 Are there walls or fences surrounding the property?
3.3.20 Are there current security layers in place? e.g. Electric fencing, Armed guards, patrols, Video Surveillance.
3.3.21 Where are the vulnerable points of entry into the property?
3.3.22 Are there points of easy access to the roof or 2nd floor?

4. GENERAL REQUIREMENT:

The intruder detection system may consist of various detection devices, control equipment, signalling equipment and the necessary power backup equipment for detecting and/or verifying unwanted intrusion.

4.1.1 The housing tamper must be connected in all installations. Electronic detection devices e.g. PIR, glassbreak, etc, must be tamper protected on a 24-hour zone in retail, commercial, industrial and high-risk residential installations.
4.1.2 Where ceiling access is possible, the control equipment, signalling equipment and antenna shall be installed a minimum of 1,5m below the ceiling, or in an area that is not vulnerable to tampering from within the ceiling void. These devices must be protected by a volumetric detector on an instant zone when the area is not occupied. This will not apply in the stay mode.
4.1.3 The control equipment must not be visible from the outside of the premises.
4.1.4 All LED's within detectors are to be disabled after installation set-up. (Voluntary for residential, compulsory for Commercial installations.)
4.1.5 All external doors must be protected by a magnetic, electromagnetic, electromechanical or wireless door contact.
4.1.6 The use of flooded car batteries, mechanical keyswitches, mechanical vibration switches and shuntlocks (cut out switches) is not permitted.
4.1.7 All detectors must be fixed using wall plugs and screws in mortar bricks, concrete, wood or dry walling. In the case of glass, aluminium, or treated surfaces, a secure attachment method must be used. Eg. Epoxy glue. The use of double-sided tape, cable glue or glue guns are not permitted.
4.1.8 Where signalling equipment / devices are used, the power cables must be terminated at the battery via a radio battery connection pc board.
4.1.9 Detector lenses must be suitably fixed in such a way as to prohibit their easy removal from the outside of the housing.
4.1.10 All zones must be multi-shot. It is recommended that the swinger shutdown is disabled or set to maximum in respect of each zone. Where the client requests a lower number of alarm conditions to be set in the swinger shutdown, this must be marked as an exception on the Certificate of Compliance.
4.1.11 It is recommended that anti-masking and/or anti-cloaking detectors be used in retail, commercial and industrial installations.

4.1.12 It is not recommended that electric fences be connected to alarm system zones, but if done it should be optically isolated from the system or by means of a relay. Standard automation transmitters and receivers are not permitted.

4.1.13 It is recommended that an electric fence has its own signalling device.

5. EQUIPMENT REQUIREMENT

5.1 Hardwired

5.1.1 It is recommended that reference is taken from SANS2220-1-7:2006 & SANS 10142-1-2021

5.1.2 Wiring of electronic detectors should be done with solid copper/stranded copper wiring. No CCA (Copper Clad Aluminium) cable may be used.

5.1.3 Wiring of electronic detectors may not use a common negative.

5.1.4 The detection devices and other parts of the alarm system shall be so mounted and located to reduce the possibility of interference by mechanical, magnetic or electrical means.

5.1.5 Every detection circuit forming part of the intruder detection system shall be monitored for fault, trouble, status conditions and display a fault condition during arming.

5.1.6 A detection circuit/zone must consist of only one of the following combinations:

- Five (5) Magnetic contacts
- One (1) infrared beam or one pair of beams in parallel (dual beam units).
- One (1) Outdoor electronic detection device eg. Passive infrared detectors, PIR/MW
- Two (2) Indoor electronic detection devices. (eg. Passive infrared detectors, PIR/MW detectors)
- Two (2) audio detection devices. (eg. Glassbreak detectors)
- Five (5) electronic shock sensors.
- Ten (10) anti-tamper detection devices.
- Five (5) sealed magnetic pull switches with an end-of-line resistor.

5.1.7 All joints must be soldered and insulated or in a junction box containing screw terminal blocks.

5.1.8 The use of a cigarette lighter or any other flame-producing device for the purpose of soldering, is not permitted.

5.1.9 Cables within the control equipment (Unit/Hub) must be marked and/or terminated in an enclosure, using solder, crimping ferrules or strip connectors (chocolate blocks). Cables must be identified either by marking, labelling or colour coding.

5.1.10 All detector zones must be supervised. Where single end-of-line or double end-of-line monitoring are used, the resistors must to be installed at the detector end of the line, i.e. within the detector.

5.1.11 Cables must run neatly in such a manner so as to avoid physical damage. All cables that are vulnerable to corrosion and damage as well as external wiring must be suitably protected or placed in conduit

5.2 Power Supply Equipment

5.2.1 The mains transformer must be in accordance with the electrical and manufacturers specifications and as per the design of the system and charging capacity.

5.2.2 It is recommended that all transformers are fused and surge protected.

5.2.3 The control panel must provide a low battery cut-off of a minimum of 10.2v. (Exclusive of wireless systems).

5.2.4 All batteries should be used in accordance with manufacturers specifications in terms of Series/Parallel connections, size and type of charging circuit as well as housing and ventilation requirements.

5.2.5 The use of liquid electrolyte lead acid type or flooded car batteries is not permitted.

5.2.6 Where lead acid or gel batteries are added, batteries of the same type and condition must be used and be switched over using a relay.

5.2.7 Where a security system is connected via solar or inverter, it must be installed in accordance with SANS 10142/1/2 where applicable.

5.2.8 Where Lithium Ion batteries are used, the following cable diameters are recommended:

- Up to 3 metres – 1mm core diameter.
- Further than 10 metres – 1.5mm core diameter.

5.2.9 It is recommended that a mains failure or low battery signal is transmitted to the central station.

5.2.10 The cable from the transformer to the control panel must have a minimum core diameter of 0.5mm (Cabtyre)

5.2.11 The transformer shall be correctly earthed according to the manufacturer's instructions using an electrical earth.

5.3 Audible sounders

5.3.1 The audible sounders shall be capable of sounding for a minimum period of three (3) minutes and must comply with the relevant Municipal Regulation.

5.3.2 All sounders must be audible unless agreed to in writing between the customer and the installation company.
5.3.3 External sounders shall have their cables monitored for tamper by the control equipment.

5.4 Wireless (Should only be done with two-way technology)
5.4.1 The wireless system shall operate on a South African ICASA approved frequency.
5.4.2 Wireless detectors must include a battery saving feature.
5.4.3 When wireless connections are selected, careful consideration should be given to the influence of intentional or unintentional transmissions using the same frequency and/or means of signal modulation as those of the transmitting device. Such transmissions may result in receiver units generating tamper or fault conditions or prevent the interconnections from functioning correctly.
5.4.4 Consideration should be taken of electrical and or mechanical devices within close proximity to wireless devices.
5.4.5 All wireless receivers/repeaters shall be installed within a protected area and protected by a two-way supervised wireless detector.
5.4.6 Supervision: All wireless alarm systems installed must have the ability to report specific activations such as supervision, low battery, and tamper.

5.5 Hybrid
5.5.1 The same general principles should apply as with Hardwired & Wireless.
5.5.2 It is recommended that at least 30% in Residential and at least 50% in commercial and Industrial to be hardwired, except where bi-directional systems are installed.
5.5.3 All wireless receivers/repeaters shall be installed within a protected area and protected by a hard-wired volumetric PIR detector.

5.6 IoT Systems
5.6.1 The same general principles should apply as with Hardwired & Wireless.
5.6.2 All wireless receivers/repeaters shall be installed within a protected area and protected by a two-way supervised wireless detector.
5.6.3 The wireless system shall operate on a South African ICASA approved frequency.
5.6.4 Wireless detectors must include a battery saving feature.
5.6.5 When wireless connections are selected, careful consideration should be given to the influence of intentional or unintentional transmissions using the same frequency and/or means of signal modulation as those of the transmitting device. Such transmissions may result in receiver units generating tamper or fault conditions or prevent the interconnections from functioning correctly.
5.6.6 Consideration should be taken of electrical and or mechanical devices within close proximity to wireless devices.
5.6.7 A secondary means of communication other than the internet should be used as a medium to the central station. This could be a self-contained RF transmitter such as VHF or UHF.
5.6.8 A secondary means of controlling the Hub/Iot device other than a cellular phone on the cellular or internet network should be provided to control the system such as a keypad, key fob or Bluetooth device to the hub.

6. OPERATIONAL REQUIREMENT
6.1.1 Dual communication is compulsory on all systems. If not accepted by the customer, this must be noted on the certificate as non-compliant.
6.1.2 On low risk installations the dual communication may be in a single device – ie: sim card and fibre, provided that the router back up battery is the same as the alarm system.
5.1.3 On high risk and commercial installations two separate communication devices must be used.

7. SYSTEM COMPONENTS

7.1 Control equipment
7.1.1 The control equipment (Unit,Hub) shall be microprocessor controlled, keypad or App operated.
7.1.2 Where permissible the system may be controlled via remote control as defined in 7.2.1.5 and 7.2.1.6.
7.1.3 The control equipment (Unit/Hub) must have the capability of storing the last 500 events.
7.1.4 All equipment must be installed to manufacturer's specifications.

7.2 Control interface

7.2.1 Keypad

7.2.1.1 The keypad shall have an internal sounder.
7.2.1.2 Digital keypads are to be of the data transfer technology type.
7.2.1.3 In the case of an intruder alarm system having a keypad as an integral part of the enclosure, this keypad may not be used as the primary control point. The keypad must be in a protected area and must not be vulnerable to tampering.
7.2.1.4 In the case of an intruder alarm system having a keypad as an integral part of the enclosure, it may not be part of the entry/exit area. In the armed state, a person must not be able to gain

access to the control panel within the entry delay period. The control panel and battery must not be in an entry/exit delay zone. It is recommended that remote arming or a second keypad be used.

7.2.1.5 All remote arming devices and/or software applications must be encrypted.

7.2.1.6 In commercial installations, remote arming is only permissible if the code verification takes place within the control panel using a unique user identification.

7.2.1.7 The customer must be clearly informed of any possible risks associated with the use of remote arming.

7.2.1.8 **Disarming**
When using a time delay on a zone protecting the keypad, such entry delay shall not exceed 30 seconds.

7.2.1.9 **Arming**
During the arming period procedure, the status of all isolated circuits or faulted circuits shall be easily accessible.

7.2.1.10 **Circuit Identification**
Where more than one detection circuit is used, the control equipment shall be capable of indicating immediately the individual circuit in which the alarm condition occurred, on disarming the control panel.

7.2.1.11 **Bypass/Isolation**
Once armed, no bypassed zones shall be indicated on the keypad.

7.2.2 When using an App in place of a keypad, the following must be taken into account

7.2.2.1 The app must be linked to a specific user and the open & closing per user must be stored in the event log.

7.2.2.2 The app must authenticate the cell phone (ie: via imei number) each time it connects to the cloud.

7.2.2.3 Bypassing of zones via the app must show in the event log.

7.2.2.4 The Event log must be stored for minimum of 12 months and must be date and time stamped and tamper proof.

7.2.2.5 Apps must be set up for push notification and must always run in the background.

7.2.2.6 The App must show zones in an alarm state when opening the app before disarming the system.

7.2.2.7 Consideration should be given for end user apps as well as installer apps and hand over of Administration/installer rights.

8. SIGNALLING EQUIPMENT SYSTEMS

8.1.1 The use of 2G/3G technology is not recommended, but if used client should be informed of imminent sunset of this technology with risk/cost involved.

8.1.2 **To Central Stations/Control rooms.**

8.1.2.1 Dual communication path is compulsory on all systems. If not accepted by the customer, this must be noted on the certificate as non-compliant.

8.1.2.2 On low risk installations the dual communication may be in a single device – ie: sim card and fibre, provided that the router back up battery is the same as the alarm system.

8.2.2.3 On high risk and commercial installations two separate communication devices must be used.

8.2.2.4 Dual monitoring using different technologies or carrier mediums is recommended.
All communication devices, if not powered by the control panel / hub, must have equal or better power than the control panel / hub.
The following methods are considered acceptable:

- VHF/ UHF Radio
- GSM Communication
- TCP/IP
- Spread Spectrum

8.1.3 In the event that a Radio transmitter and antenna is used, they must be correctly installed according to manufacturers specifications. The DC power cable from the Radio transmitter to the control panel must have a minimum core diameter of 0.5mm (Cabtyre or Ripcord)

8.1.4 Minimum signals i.e. burglary and panic must be monitored separately.

8.1.5 Where required, all communication equipment shall be ICASA approved.

8.1.6 It is recommended that where possible, GSM/IP communication is not used as a single communication medium or as a primary means of communication.

8.1.7 No pre-paid SIM cards will be permitted.

8.1.8 In the event that a GSM transmitter is used, the customer must be clearly informed that they are being monitored by GSM technology as well as any risks associated with the connection of this equipment to the cellular network.

8.1.9 Communication cable shall not form part of main wiring harness and shall be run in such a manner as to protect them from tampering or physical damage. Cables to the communications devices must be wired below the ceiling.

9. WIRELESS SYSTEMS

9.1 Wireless Installation Considerations

9.1.1 When wireless connections are selected, careful consideration should be given to the influence of intentional or unintentional transmissions using the same frequency and/or means of signal modulation as those of the transmitting device. Such transmissions may result in receiver units generating tamper or fault conditions or prevent the interconnections from functioning correctly.

9.1.2 Consideration should be taken of electrical and or mechanical devices within close proximity to wireless devices.

9.2 Low Battery

When the transmitting device or detector has a low battery condition indicating battery close to end of life cycle and due for replacement, it is recommended that the devices lost from the system due to battery failure, low or dead should be visible, by zone, either at keypad and/or e ach device.

9.3 Environmental considerations

9.3.1 Wireless device tampers must raise immediate tamper events at the keypad and/or offsite monitoring. It is recommended that the device ID should be available with all reporting.

9.3.2 It is recommended that the signal strength should be tested at the point of installation.

9.3.3 it is the responsibility of the installer to assess these environmental factors and plan the installation appropriately. Where environments are not suitable for a reliable wireless installation, wired detectors should be used.

9.3.4 The customer must be clearly informed that natural or manmade environmental changes could affect the operation of the system.

9.3.5 It is recommended that the installer tests the environment for interference by means of a frequency analyser.

9.4 Supervision

9.4.1 All wireless alarm systems installed must have the ability to report specific activations such as supervision, low battery, and tamper.

9.4.2 The system must have the ability to monitor and communicate RF jamming.

9.4.3 Outdoor detectors must have front and mounting tampers for monitored supervision. **(Commercial and High Risk Residential installations)**

9.4.4 All devices must be bi-directional. **(Commercial and High Risk Residential installations)**

9.4.5 Detector & transceiver must have a common battery for reporting purposes.

9.5 Management of RF jamming

9.5.1 The receiving device used should continually monitor the area for any signals that could cause signals from enrolled detectors to be compromised.

9.5.2 It is recommended that the system sends RF jamming or any other signal such as low battery on detectors, more than once to the control room.

9.5.3 It is recommended that the system uses a second form of communication to send RF Jamming signals or any other signals such as low battery on detectors.

10. OPERATIONAL PROCEDURES

When the system is installed, the customer shall receive a practical demonstration of the systems full functionality and shall be required to enter alarm user code. An operating instruction manual for the control panel must be available on request.

11. RECORDS

The Alarm Company shall maintain accurate records relating to each intruder alarm system installed.

12. ALARM COMPANY REPRESENTATIVE IDENTIFICATION

All representatives of the alarm company shall carry an identification card bearing the company name, PSIRA number, photograph and identity number.

13. CERTIFICATE OF COMPLIANCE

13.1 A SAIDSA certificate of compliance must be issued to the customer when the intruder alarm system has been installed. The Installation Company must keep duplicate certificates for the duration of the contract.

13.2 All certificates and/or guarantees provided by the installer will be null and void if any third party, including the customer, tampers, adds, removes or replaces any equipment in the installation. SAIDSA must be informed by the installer of any such occurrence.

13.3 Any non-compliance exceptions are to be clearly noted on the certificate.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage or retrieval system, without permission in writing from the publishers. Every effort has been made to ensure accuracy of information at the time of going to print. However, the authors and publishers cannot be held responsible for errors or omissions for any reason whatsoever.
Copyright - South African Intruder Detection Services Association (SAIDSA) – All rights reserved 1994-2023